Review article

The future of secure communications: Device independence in quantum key distribution

Seyed Arash Ghoreishi [a,b], Giovanni Scala [c,d,e], Renato Renner [f],
Letícia Lira Tacca [g,h], Jan Bouda [b], Stephen Patrick Walborn [g,h,*],
Marcin Pawłowski [e]

[a] RCQI, Institute of Physics, Slovak Academy of Sciences, Dúbravská cesta 9, 84511 Bratislava, Slovakia
[b] Faculty of Informatics, Masaryk University, Botanická 68a, 602 00 Brno, Czech Republic
[c] Dipartimento Interateneo di Fisica, Politecnico di Bari, 70126 Bari, Italy
[d] INFN, Sezione di Bari, 70126 Bari, Italy
[e] International Centre for Theory of Quantum Technologies, University of Gdańsk, Jana Bażyńskiego 1A, Gdańsk, 80-309, Poland
[f] Institute for Theoretical Physics, ETH Zürich, 8093 Zürich, Switzerland
[g] Departamento de Fisica, Universidad de Concepción, Concepción, Bío-Bío, Chile
[h] Millennium Institute for Research in Optics, Universidad de Concepción, Concepción, Bío-Bío, Chile

A R T I C L E   I N F O

A B S T R A C T

In the ever-evolving landscape of quantum cryptography, Device-independent Quantum Key Distribution (DI-QKD) stands out for its unique approach to ensuring security based not on the trustworthiness of the devices but on nonlocal correlations. Beginning with a contextual understanding of modern cryptographic security and the limitations of standard quantum key distribution methods, this review explores the pivotal role of nonclassicality and the challenges posed by various experimental loopholes for DI-QKD. Various protocols, security against individual, collective and coherent attacks, and the concept of self-testing are also examined, as well as the entropy accumulation theorem, and additional mathematical methods in formulating advanced security proofs. In addition, the burgeoning field of semi-device-independent models (measurement DI-QKD, Receiver DI-QKD, and One-sided DI-QKD) is also analyzed. The practical aspects are discussed through a detailed overview of experimental progress and the open challenges towards the commercial deployment in the future of secure communications.

Contents

* Corresponding author at: Departamento de Fisica, Universidad de Concepción, Concepción, Bío-Bío, Chile.
  E-mail addresses: arash.ghoreishi@savba.sk (S.A. Ghoreishi), giovanni.scala@poliba.it (G. Scala), renner@ethz.ch (R. Renner), letacca@udec.cl
(L.L. Tacca), bouda@fi.muni.cz (J. Bouda), swalborn@udec.cl (S.P. Walborn), marcin.pawlowski@ug.edu.pl (M. Pawłowski).

1. Introduction

1.1. Overview of modern cryptography

Facta lex inventa fraus — the principle that every established law is followed by the invention of a way to circumvent it — does not hold, *in theory*, for modern cryptography. With the advent of Quantum Cryptography [1–3], the security of communication protocols has shifted from complex, yet vulnerable algorithms, to fundamental quantum principles (uncertainty, entanglement, complementarity, no-cloning, non-locality, etc.), providing a mechanism for inherently secure communication channels. The pioneering application of these revolutionary techniques has led to Quantum Key Distribution (QKD), (and beyond [4]), representing a significant leap forward in security compared to traditional public-key standards such as Diffie–Hellman [5] and RSA (Rivest–Shamir–Adleman) [6]. *Facta lex inventa fraus* — the principle that every established law is followed by the invention of a way to circumvent it — does not hold, *in theory*, for modern cryptography. While traditional public-key cryptography employs the concept of one-way functions to encrypt/decrypt information, QKD detects the potential intrusion of an eavesdropper, Eve, due to the principle of no-cloning or, equivalently, through the uncertainty principle. Fig. 1 visually compares RSA[1] with the *prepare-and-measure* scenario of BB84 [7] (emblematic of QKD). The players' preparation (in Alice's lab $\mathcal{A}$) and measurements (in Bob's lab $\mathcal{B}$) can be the red or blue buttons. While in the classical case, Eve has no button (she can make perfect copies of the encoded messages sent and manipulate the copies however she chooses), in QKD Eve must choose and perform a measurement to obtain information. If Alice selects red and Eve selects blue, then the effect of Eve's disturbance appears in Bob's measurements as a purple ball (a mix of red and blue).

Not only has the security of many public-key ciphers never been formally proven, but it is also well known that many of those currently in use are vulnerable to quantum computers [8]. QKD, on the other hand, creates robust encryption methods based on Kerckhoffs's principle [9], which posits that a cryptosystem's security should be maintained even if everything about it is public knowledge, except the secret key. However, theoretical security and practical security are different issues. Experiments have demonstrated vulnerabilities in QKD systems [10–15], raising questions about whether the theory or the experiments of QKD need refinement. Claiming that the principles of quantum theory are fundamentally flawed would be an exaggeration. The real issues predominantly reside in the practical implementation of QKD. While the theoretical basis of QKD is robust, its real-world application involves new technology, such as single-photon detectors, and can be compromised by unavoidable imperfections in the devices.

> "Theory and experiment are the same, in theory, but experimentally different".
>
> *(The Yale Literary Magazine, Feb, 1882, B. Brewster)*

Therefore, to truly ensure security at the paranoid level under QKD necessitates addressing an additional layer of scrutiny: the independence from underlying devices [16]. This prerequisite gave rise to the concept of Device-Independent Quantum Key Distribution (DI-QKD). DI-QKD, and its slightly more lenient version, Semi-Device-Independent (SDI) QKD, ensure security based solely on the principles of quantum mechanics, without dependence on the specifics of the hardware used. Thus, potential vulnerabilities or backdoors due to device malfunctions or imperfections are eliminated, providing a robust mechanism for secure communication.

---

[1] In Fig. 1(a), one might think spectroscopy could reveal each purple's components, but the process resembles a one-way cryptographic function: easy to mix, hard to reverse. Like password hashing, the color mixture conceals the original inputs, preventing unauthorized decryption.
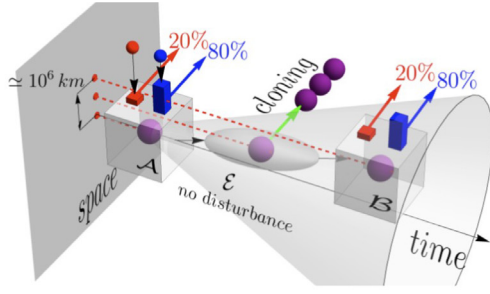
(a) *One−way function in classical public-key encryption*   (b) *Quantum key distribution (BB84).*
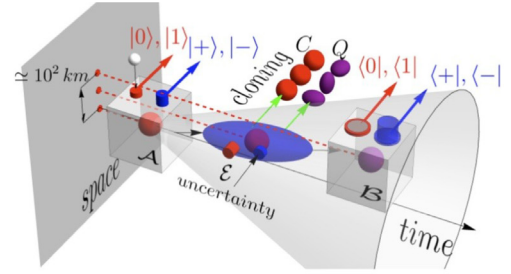
Fig. 1. *Illustration on the fundamental physical principles behind the need of quantum cryptography* – In Fig. 1(a) a color-mixing analogy represents the encoding in public-key cryptography as a purple sphere, symbolizing an encrypted message open to all. Yet, only holders of the private key can accurately decrypt it. Alice creates the purple sphere with a specific combination of colors (20% red, 80% blue) mimicking a one way function (Eve cannot perfectly decompose the purple shade into component colors). Bob, having some information about the precise mix (the private key), can decrypt it. In Fig. 1(b) quantum cryptography. Colors represent the basis (red $\{|0\rangle, |1\rangle\}$, blue $\{|+\rangle, |-\rangle\}$). Due to no-cloning, Eve's interference changes the color and shape of the ball. If Alice uses the red button and Eve guesses the blue button, the result in Bob's box is purple. Contrary to classical cryptography, in the quantum case, Eve's intrusion affects the outcome at Bob's station. Bob detecting purple with a red button, signals Eve's presence. Traditional cryptography and QKD protocols are realized in the same causal cone at today's distances, which are on the order of $\sim 10^6$ km for classical techniques, while QKD can reach $\sim 10^2$ km for fiber-based schemes without quantum repeaters. For satellite QKD, much longer distances on the order of $\sim 10^3 - 10^4$ km have been achieved [17,18].

1.2. From classical to quantum cryptography

Classical cryptography is broadly categorized into two main types: secret (or symmetric) key cryptography and public-key (asymmetric) cryptography. In secret key cryptography, a single key is employed for both encrypting and decrypting messages, exemplified by the one-time pad (OTP) [19,20] or the Advanced Encryption Standard (AES) [21]. The OTP can achieve perfect information-theoretic security against adversaries with unlimited computational power, as discussed in Ref. [1]. Moreover, the threat of quantum attacks on AES requires only doubling the size of the key to achieve equivalent levels of security [22].[2] The primary challenge with symmetric cryptography lies in the secure distribution of the secret key prior to communication.

Public-key cryptography, such as the Diffie–Hellman [5] and RSA [6] protocols, circumvents this issue by employing a pair of keys for each participant: a public key, which can be shared openly, and a private key, which remains confidential. This enables Alice to encrypt a message using Bob's public key, ensuring that only Bob can decrypt it with his private key. This eliminates the need to exchange secret keys in advance. Importantly, public-key cryptography also provides a mean for authentication: Bob can sign a message with his private key, and Alice (or anyone) can use the public key to confirm that it was indeed signed by Bob. From a practical standpoint, public-key systems are slower in that they require larger keys and more communication between users, compared to symmetric encryption. Thus, in current communication protocols such as Transport Layer Security (TLS), for example, a public-key method is used for authentication and key exchange in an initial handshaking session, while subsequent data encryption employs symmetric encryption [24,25].

Nowadays, the security of many public key ciphers is built on the computational difficulty of mathematical problems like *integer factorization* or the *discrete logarithm problem*, making it potentially vulnerable to advances in quantum computing. Notably, algorithms capable of solving these problems in polynomial time on a quantum computer have already been proposed [26,27]. It is thus through quantum mechanics that *Facta lex inventa fraus* is realized, through the emergence of quantum computing as a significant threat, (the *fraus*) to the security of current public key cryptography. Still, quantum physics itself offers a new and robust set of laws (*lex*) through QKD, capable of providing unconditionally secure key distribution in theory.

1.3. Standard quantum key distribution

1.3.1. Theoretical security of QKD

To introduce standard prepare and measure QKD, we specifically elaborate the BB84 protocol [20] or conjugate coding [28], sketched in Fig. 1(b). A general protocol for prepare-and-measure (PM) QKD can be found in Box 1.

Step 1 –(Data generation) Alice prepares eigenstates of σ_z or σ_x bases (red or blue of Fig. 1) and attached them with a classical register. Then the classical–quantum preparation is

$$\psi_{C_{A_i} Q_i} = \frac{1}{4} \sum_{a_i, x_i \in \{0,1\}} |x_i a_i\rangle\langle x_i a_i| \otimes H^{x_i} |a_i\rangle\langle a_i| H^{x_i}, \tag{1}$$

---

[2] Known quantum attacks on AES use Grover's search algorithm, which provides quadratic speedup [23]. Thus, to achieve "quantum-safe" security equivalent to AES256 (256 key bits) under classical attacks requires upgrading to AES512.

where the first system corresponds to her classical register, storing values of classical bits x_i, a_i (x_i, $a_i \in \{0, 1\}$). The second system is the quantum state ψ_{Q_i}, which she sends to Bob. Here H is the Hadamard matrix, such that $H^0 = \mathbf{1}$ is identity.

Bob is unaware of Alice's input x_i, so he randomly selects a measurement basis y_i and obtains result b_i (Here y_i, $b_i \in \{0, 1\}$). To each result he attaches a random classical bit T_i, so that with probability $p(T_i = 1) = \gamma$, b_i will be used for security check ($T_i = 1$), else it will be used to generate final key ($T_i = 0$). The classical–quantum state describing his measurement result is

$$N^{T_i}_{b_i|y_i} = |T_i\rangle\langle T_i| \otimes \frac{1}{2}H^{y_i}|b_i\rangle\langle b_i|H^{y_i}. \tag{2}$$

Step 2 − (Public discussion and raw key) Alice and Bob must partially compare preparation and measurement results stored in classical registers $C_{A_i} = (x_i, a_i) \in \mathcal{C}_{A_i}$ and $C_{B_i} = (y_i, b_i, t_i) \in \mathcal{C}_{B_i}$, respectively. To do so, Bob publicly announces (y_i, t_i) (but not b_i) so that Alice can inform Bob in which rounds $x_i = y_i$, so that Alice can define a raw key bit $\kappa_{A_i} = a_i$ and Bob $\kappa_{B_i} = b_i$. When $x_i \neq y_i$, both parties discard their results, defining null bits $\kappa_{A_i} = \kappa_{B_i} = $ Null. Provided no errors occurred or no one manipulated the qubits sent, Bob has a string of bits identical to Alice's: $\kappa_B = \kappa_A = \{\kappa_{A_i} \neq \text{Null}\}_i$.

Step 3 − (Error correction and Security Check) Both noise and/or intrusion by Eve will produce errors in Bob's bit string κ_B. To correct them, Alice and Bob publicly communicate k^{EC} for error correction (cascade, LDPC, parity check) on their key bits ($T_i = 0$). Let us say that is Bob to perform a security check on results with $T_i = 1$. For each result, he defines errors using (see Box 1)

$$c_i = \begin{cases} \text{Null} & \text{if } x_i \neq y_i \vee T_i = 0, \text{ no useful check,} \\ 1 & \text{if } x_i = y_i \wedge T_i = 1, \text{ check passed,} \\ 0 & \text{else, check failed.} \end{cases} \tag{3}$$

Then, Alice and Bob can estimate Q_i's, ($i \in \{Z, X\}$), the Quantum Bit Error Rate (QBER) for each basis,

$$Q_Z = \frac{\big|\{i \mid x_i = y_i = 0, \ c_i = 0\}\big|}{\big|\{i \mid x_i = y_i = 0, \ c_i \neq \text{Null}\}\big|}, \quad Q_X = \frac{\big|\{i \mid x_i = y_i = 1, \ c_i = 0\}\big|}{\big|\{i \mid x_i = y_i = 1, \ c_i \neq \text{Null}\}\big|}. \tag{4}$$

Whenever a protocol involves only a single key-generation basis, we denote its QBER by Q, omitting the subscripts Z and X. A QBER below a threshold indicates minimal interference or eavesdropping, so Alice and Bob can agree under a certain level of confidence that they final keys $\{k_{A_i} = k_{B_i}\}_{i|T_i=0}$ are correctly distributed and the technique for the step 3.4 discussed in the tutorial can be applied [20]. This refined key, now highly secure, is suitable for encrypting messages (see Section 5 to bound Eve's knowledge about the key).

Box 1: General QKD prepare-and-measure protocol

The most general QKD prepare-and-measure protocol can be defined as [29]:

– *Data generation:* for $i = 1, \ldots, n$, where n is the number of rounds Alice prepares $\psi_{C_A^n Q^n} = \psi_{C_A Q}^{\otimes n}$ and stores in a classical register $(x_i, a_i) \in \mathcal{C}_{A_i}$ her i−th preparation label by a_i and setting x_i. She sequentially sends ψ_{Q_i} via a public channel to Bob; Bob chooses y_i and measures $N_{y_i} = \{N_{b_i|y_i}\}_{b_i=1}^{d_B}$ storing $(y_i, b_i) \in \mathcal{C}_{B_i}$ at each round, where b_i labels one of the d_B possible outcomes.

– *Public discussion for the raw key generation:* Alice and Bob publicly exchange information, i.e. PD : $\mathcal{C}_{A_i} \times \mathcal{C}_{B_i} \mapsto T_i$ with $\iota_i = \text{PD}((x_i, a_i), (y_i, b_i))$ such that Alice can compute the raw key $\kappa_A = \{\kappa_{A_i}\}_i$, with $\kappa_{A_i} = \text{RK}((x_i, a_i), \iota_i) \in \mathcal{S}_i$ via RK : $\mathcal{C}_{A_i} \times T_i \mapsto \mathcal{S}_i$.

– *Post-processing:* The players exchange a string $\kappa^{EC} \in \{0, 1\}^{\lambda_{EC}}$ to define the final key $k_A = k_B$ via

1. *Error correction:* the players exchange κ^{EC} from $\mathcal{C}_{A_i}$, $\mathcal{C}_{B_i}$ and T_i so that Bob compute $\kappa_B = \{\kappa_{B_i}\}_i \in \mathcal{S}$ where $\kappa_{B_i}(\kappa_i^{EC}, (y_i, b_i), \iota_i) \in \mathcal{S}_i$.

2. *Raw key validation:* for $\varepsilon_{KV} > 0$ Alice chooses an universal hash function HASH : $\mathcal{S} \mapsto \{0, 1\}^{\lceil -\log \varepsilon_{KV}\rceil}$ and publishes a description of it and the value HASH(κ_A). Bob computes HASH(κ_B) and if HASH(κ_B) $\neq$ HASH(κ_A) the protocol aborts.

3. *Statistical security check:* Bob sets EV : $\mathcal{C}_{B_i} \times T_i \times \mathcal{S}_i \mapsto \mathcal{C} \ni q_{B_i}$. Bob then computes $q_B = \text{CA}(\text{freq}(q_B))$, where CA is an affine function corresponding to collective attack bound q_{CA}. If the required amount of single-round entropy generation is $q_B < q_{CA}$, he aborts the protocol.

4. *Privacy amplification:* Alice and Bob respectively have κ_A, $\kappa_B \in \{0, 1\}^m$. Alice chooses a seed $\mu \in \{0, 1\}^m$ uniformly at random and publishes her choice. Alice and Bob independently compute ℓ−bit string $k_A = \text{EXT}(\kappa_A, \mu)$ and $k_B = \text{EXT}(\kappa_B, \mu)$ where EXT : $\{0, 1\}^m \times \{0, 1\}^m \mapsto \{0, 1\}^\ell$ is a quantum-proof strong extractor.

Notably, in BB84 the no-cloning theorem [30] prohibits the duplication of quantum states (we represent no-cloning in Fig. 1 as a not perfect copy process giving deformated spheres), ensuring that any attempt by Eve to intercept and

replicate the qubits would introduce detectable errors. Additionally, if Eve measures a qubit without knowing the correct basis, (only Alice knows x), the original information encoded in the other basis is irreversibly lost due to the uncertainty principle. Consequently, any eavesdropping attempt increases the QBER, which can be measured by Alice and Bob. Specifically, after comparing $m = |\{c_i|c_i = 1 \vee c_i = 0\}_i|$ bits, the probability that Eve can eavesdrop without being detected drops to $(3/4)^m$. Here the 3/4 probability of a single correct guess follows from the 1/4 error probability in an intercept/resend attack (see below): there is a 50% chance that Eve guesses the correct basis (same Alice's color in Fig. 1), and thus a 50% chance that Eve guesses wrong, and within those wrong cases, there is another 50% chance that Bob's measurement will yield an incorrect result (Alice's color differs from Eve and Bob's color in Fig. 1). The theoretical security proofs depend on Eve's ability to perform *(i) individual attacks*, measuring states separately; *(ii) collective attacks*, measuring individually with joint classical post-processing; *(iii) coherent attacks*, using joint quantum measurements on all states stored in a memory.

1.3.2. Implementation issues and quantum hacking

As is traditionally advertised in regards to QKD, any attempt by Eve to uncover information of the key results in an increase in the QBER. A simple and straightforward example are Intercept-and-Resend Attacks, where Eve intercepts ψ_{Q_i} sent by Alice, measures it in a chosen basis, prepares a new photon state based on her measurement result and sends it to Bob [31–33]. Since she chooses the wrong basis some of the time, her disturbance increases the QBER and is thus detectable. Evaluation of the QBER can give an upper bound for the amount of information Eve has about the key. Thus, QKD can be *theoretically* secure. However, even in a noise-free scenario, the difference between theory and practice can result in vulnerabilities. Indeed, if $\psi_{Q_i} \in \mathcal{H}$ with uncontrolled dim $\mathcal{H}$ and no Bell Inequality (BI) violation is measured, QKD is insecure, because the same BB84 correlations ($p(a_i = b_i|x_i = y_i) = 1$ and $p(a_i \neq b_i|x_i \neq y_i) = 1/2$) produced by $|\psi\rangle = (|00\rangle + |11\rangle)/\sqrt{2} \in \mathbb{C}^2 \otimes \mathbb{C}^2$ are also reproduced by a four-qubit separable state [34], ([35] in app. A),

$$\rho = \frac{1}{4} \left(|00\rangle\langle00| + |11\rangle\langle11| \right) \otimes \left(|++\rangle\langle++| + |--\rangle\langle--| \right),$$

when Alice measures the first (third) qubit in the σ_z (σ_x) basis, and Bob measures the second (fourth) qubit in the σ_z (σ_x) basis. As there is no quantum correlation, a secure key cannot be established.

While this type of quantum state manipulation might seem to give too much power to Eve, it is indeed true that operational imperfections present considerable opportunities for hacking [36,37]. For example, Eve can exploit the fact that weak coherent pulses (WPCs), used in some QKD systems, can contain more than one photon to implement the Photon Number Splitting (PNS) attack. By separating and storing one of the photons from a WCP, Eve can measure it later, once the measurement basis has been publicly announced. In this way, she can obtain full information without disturbing the state of the photons sent to Bob [38–40]. Other examples include side-channel [41–44], trojan horse [45,46], and device calibration [12,47–51] attacks (for a full list see Ref. [20]). To effectively counter these vulnerabilities, the best approach is to use security proofs based on minimal principles and strategies that reduce or eliminate reliance on trusted components. Among these, DI-QKD stands out as the ultimate solution.

1.4. Overview of device-independent QKD

The internal workings and security of the quantum devices involved in QKD protocols, as we analyzed, are often faulty and vulnerable to quantum hacking. DI-QKD represents a significant advance in that it aims to ensure the utmost security of QKD, irrespective of the reliability or trustworthiness of the devices used. This security is achieved through nonlocal correlations verified by BI violation, as depicted in Fig. 2. In general, the correlations, or *behaviors* are indicated as points $\boldsymbol{p} = \{p(ab|xy)\}_{a,b,x,y}$ in the convex correlation space characterized by the regions $\mathcal{L} \subset \mathcal{Q} \subset \mathcal{NS}$ respectively for local and realistic, quantum, and no-signaling behaviors, respectively. A BI violation ($\boldsymbol{p} \notin \mathcal{L}$), classified as "strongly nonclassical" [52], implies one of two possibilities, or both: (1) a and b are determined only when observed; (2) a nonlocal influence ensures that the key is established solely through interactions between the trusted parties. In either case, Eve cannot access the information without being detected because any interference would deviate from the expected nonlocal correlations. Fig. 3 shows the evolution of DI-QKD, from BB84 and E91 protocol [53] up to the formalization of theoretical techniques and the first implementations in 2022 [54–56] (details in Fig. 4). Remarkably, the first successful implementation of DI-QKD was reached after overcoming all the Bell test loopholes, highlighting the challenges in realizing DI-QKD and its connecting with BI experiments. Fig. 4 compares the current experimental reach of DI-QKD - specifically, the distances of 2 m, approximately 200 m, and 400 m — with those achieved using Measurement Device Independent-QKD (MDI-QKD), a related but distinct approach that is easier to implement. Despite the challenges that lie ahead in terms of practical implementation and scalability, as the technology readiness level [57] currently stands at 2–3 (concept formulated/experimental proof of concept), with expectations to advance to level 4–5 in the coming years (technology validated in lab/relevant environment), the pursuit of DI-QKD continues to push the boundaries of what is possible for secure communications negating the possibility of *inventa fraus*.

(a) *Non-local Bell-test*

(b) *Werner state ρ_W and specific behaviors $\boldsymbol{p} = \{p(ab|xy)\}$*

(c) *Eve's strategy in CHSH protocol of Eq.(56)*

(d) *general Bell-test against Eve's strategy*
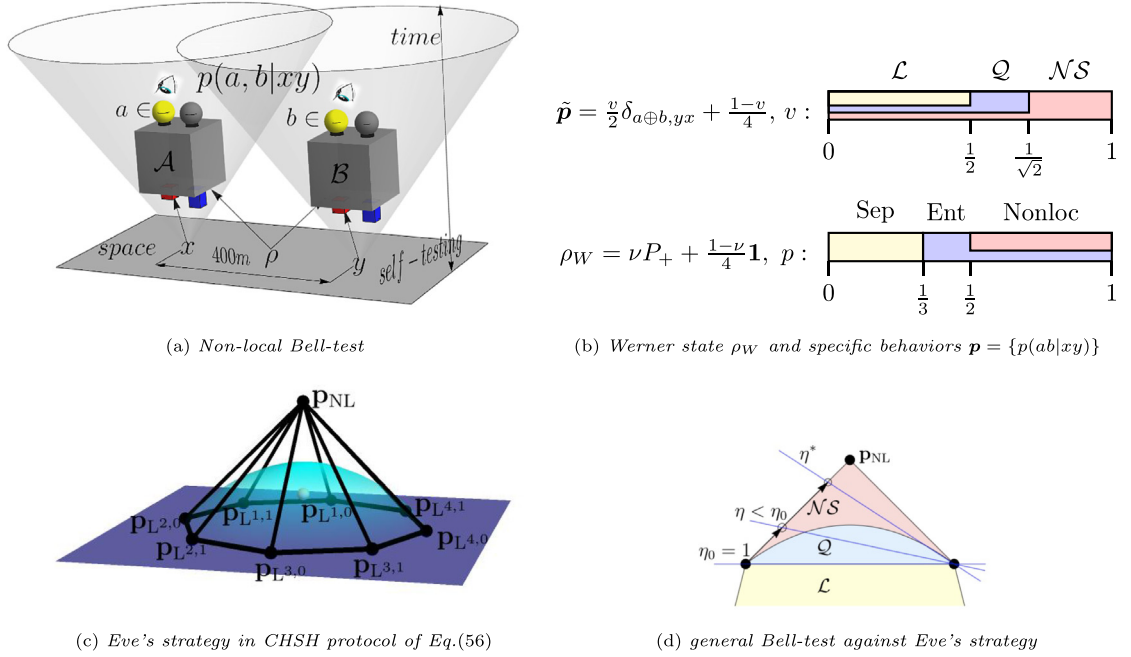
Fig. 2. DI-QKD and Bell's Theorem — only by the observed correlations $\boldsymbol{p}$ from two causal cones in Fig. 2(a), the security of DI-QKD is tested by BI determining if $\boldsymbol{p} \notin \mathcal{L}$ (see Section 2). Self-testing may also be possible, a time retrodictive process that infers the inputs x, y, ρ from $\boldsymbol{p}$ [58]. Fig. 2(b) shows the tolerance level v in a Werner state ρ_W required to witness nonlocality, along with the visibility in a specific $\tilde{\boldsymbol{p}}$ across the different regions $\mathcal{L}$, $\mathcal{Q}$, and $\mathcal{NS}$ in the space of correlations of Figs. 2(c)–2(d) (see 3.4.2). η^* in Fig. 2(d) is the critical detection efficiency, if $\eta < \eta^*$ then $\nexists$ BI to assert $\boldsymbol{p} \in \mathcal{Q} \setminus \mathcal{L}$. In Section 2 we will introduce the behavior $\boldsymbol{p}_{\text{NL}}$, a.k.a. PR box.
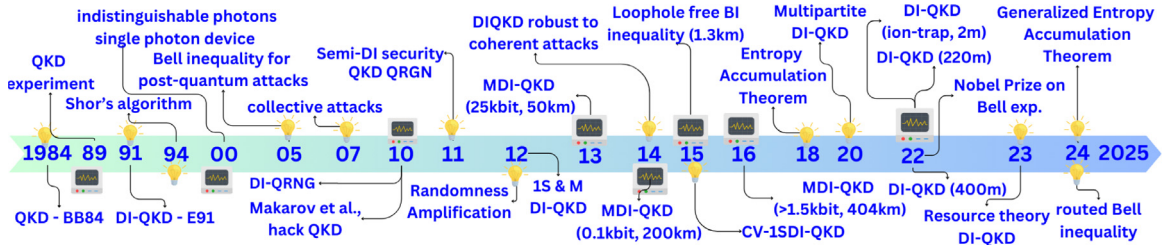
Fig. 3. Timeline highlighting key events using a lamp and oscilloscope, distinguishes theoretical and experimental contributions (MDI — measurement device independent; 1S — One-sided; QRGN — Quantum random generator number; CV — continuous variable).
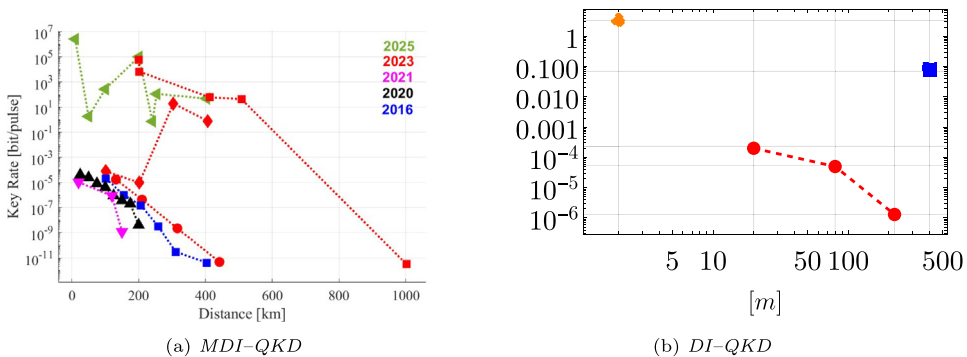
(a) *MDI−QKD*

(b) *DI−QKD*

Fig. 4. Comparative analysis of DI-QKD and MDI-QKD Experiments — Fig. 4(a) encapsulates the progress in quantum communication distances achieved through MDI-QKD implementations [59–68] (see. 3). In contrast fully-DI-QKD in Fig. 4(b) at distances: 2 m (yellow) [54], 20 m, 100 m, and 200 m (red) [55], and 400 m (blue) [56].
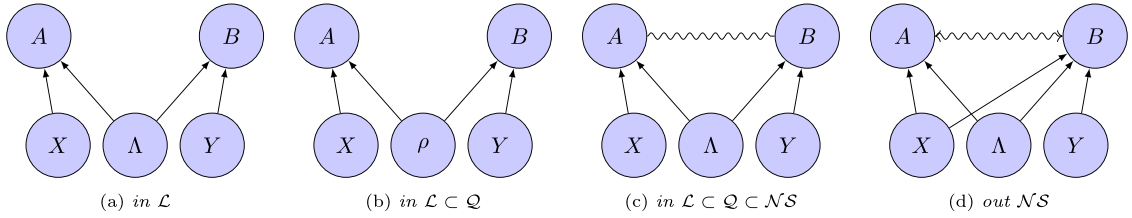
Fig. 5. Bell-test causal structure − directed acyclic graphs (DAGs) with nodes for random variables and arrows for direct causal influence [138,140] . From Fig. 2(b) the correlations with $0 \leq v \leq 1/2$ are compatible with 5(a); for $v \leq 1/\sqrt{2}$ with 5(b) where nonlocal correlations arise from the entangled state; for $v \leq 1$ the nonlocal correlations in 5(c) come from a post-quantum common cause (correlations stronger than quantum are represented as a wavy connection between A and B, but satisfying no-signaling); for $v > 1$ faster-than-light signals are allowed, e.g. X directly influences B or between A and B (the wavy connection can signalize).

1.5. Focus of this review

Here, we provide an in-depth presentation of DI-QKD, while also introducing Semi-device independent methods, including standard SDI-QKD, as well as MDI-QKD (see Fig. 4(a)), receiver DI-QKD (RDI-QKD), and one-sided DI-QKD (1SDI-QKD). As shown in Fig. 3, this review integrates DI-QKD theoretical proofs [34,53,69–98], and experimental challenges [99–104] (with BI loopholes), resulting in fully DI-QKD experiments [54–56] (see Fig. 4(b)). We present simulations that bridge the gap with experiments in [105–107], as well as advanced mathematical methods, such as entropy accumulation and bounds in [29,85,108–111]. DI randomness generation (theory [112–114], experiments [115–117]), and broader DI-QKD versions (theory [42,118–121], experiments [122–127], are also discussed. A number of very nice review papers have covered theoretical, experimental and implementation aspects of QKD and DI-QKD [1–3,16,36,128–132]. As the DI framework relies on Bell nonlocality, we also refer the reader to reviews on this subject [133–135]. In the present review, we have attempted to build on this previous work by including the most recent results, and providing alternative approaches when possible. For example, the topic of Bell nonlocality in Section 2 is presented using the modern approach of causal structures. While touching upon mathematical and technological advancements, our review, starting with a pedagogical focus, remains concise, without claiming to cover all developments exhaustively, but providing references to relevant details in references, as well as a repository of simulations and tutorials, which we have made available online [20].

2. Nonclassicality in quantum cryptography

Not all entangled states violate a BI (see Fig. 2(b), [136]). Indeed, different types of non-classical behavior lead to distinct communication tasks. In this section, we introduce the ones related to DI cryptography.

2.1. Bell nonlocality

In 1862, Boole laid out conditions for probabilities and logical constraints that any consistent probability theory should follow [137] a.k.a. *Boole's conditions of "possible experience"*, or *causal instruments* [138] . Boole's work was essentially about the constraints on observable correlations, an early classical analogue to BI's constraints on local and realistic correlations [139]. A Bell test, in its simplest form, involves two random measurement settings X[3] and Y assuming values $x, y \in \{0, 1\}$, with dichotomous outcomes A and B with values $a, b \in \{0, 1\}$ for Alice ($\mathcal{A}$) and Bob ($\mathcal{B}$), who are space-like separated, as illustrated in Fig. 2. Generally, the measurement process is denoted as $M_{A|X}$, a map depending on the specific $X = x$ and $A = a$. A Bell test serves as a causal instrument, represented by an inequality that must be satisfied to ensure the compatibility of certain causal structures, e.g. in Fig. 5 with the statistics $\boldsymbol{p}$ in the 8 dimensional affine subspace of correlations [20] (e.g. replace $\boldsymbol{p}$ from Fig. 2(b) in Eq. (5) gives Eq. (52)).

$$\boldsymbol{p} = \{p(ab|xy)\} = \begin{array}{|c|c|c|c|c|} \hline ab\backslash xy & 00 & 01 & 10 & 11 \\ \hline 00 & p_{00|00} & p_{00|01} & p_{00|10} & p_{00|11} \\ \hline 01 & p_{01|00} & p_{01|01} & p_{01|10} & p_{01|11} \\ \hline 10 & p_{10|00} & p_{10|01} & p_{10|10} & p_{10|11} \\ \hline 11 & p_{11|00} & p_{11|01} & p_{11|10} & p_{11|11} \\ \hline \end{array} \in [0, 1]^{16}. \tag{5}$$

To explain how the causal structures in Fig. 5 work, let us consider 5(a) a.k.a *Local Hidden Variable (LHV) model*. The node A (B) represents the output random variable and is influenced only by classical random variables X and Λ (Y and Λ). Therefore $p_{A|X\Lambda}$ and $p_{B|Y\Lambda}$ are the probability distributions associated with variables A and B, influenced respectively by X, Λ and Y, Λ. The distributions P_X, P_Y, and P_Λ represent the probability distributions of X, Y, and Λ, respectively. BI

---
[3] We refer with the capital letter to the random variable and its lower case the values that it can assume.

can be obtained from the causal structure in 5(a). *Locality* means that no arrow occurs between the two cones of Fig. 2, i.e. between $\{A, X\}$ and $\{B, Y\}$. Then:

$$p_{AB|XY\Lambda} = p_{A|BXY\Lambda}\, p_{B|XY\Lambda} \overset{\text{Loc}}{=} p_{A|X\Lambda}\, p_{B|Y\Lambda}. \tag{6}$$

Note that this condition also implies *no-signaling*

$$p_{A|XY} \overset{\text{NS}}{=} p_{A|X}, \qquad p_{B|XY} \overset{\text{NS}}{=} p_{B|Y}. \tag{7}$$

Therefore the entries of the *local* correlation $\boldsymbol{p}$ are the marginal of $p_{AB\Lambda|XY} = p_{AB|XY\Lambda}p_\Lambda$. From (6)

$$\boldsymbol{p} \equiv p_{AB|XY}(ab|xy) = \sum_\lambda p_{A|X\Lambda}(a|x,\lambda)p_{B|Y\Lambda}(b|y,\lambda)\,p_\Lambda(\lambda). \tag{8}$$

The common source is described by a joint probability distribution $P_\Lambda(\lambda) = P_{\Lambda_A\Lambda_B}(\lambda_A, \lambda_B)$. Note that, local correlations $p_{AB|XY}$ can be reproduced by parties equipped only with shared randomness in p_Λ so that Alice (Bob) samples from the distribution $P_{A|X\Lambda}$ ($P_{B|X\Lambda}$). Λ can be any system with arbitrary dimension but for $A, B, X, Y \in \{0, 1\}$, the cardinality of Λ is 16 (see [141] min. 48:30).

Definition 1 (*Realism*). The outcome of A represents an element of reality, namely it satisfies the realism condition if it is pre-determined by a function $f(X, \Lambda_A) \overset{\text{real}}{=} A$. This can be rewritten as $\lambda_A(X) = A$ once redefining $f = \lambda_A$ as a pre-existing outcome of Λ_A.

The role of the measurement process, once X is chosen, is to select a specific function $M_{A|X} = \lambda_A(X) = A$. Given that X is dichotomous, $\lambda_A \in \{r_0, r_1, \text{fp}, \text{id}\}$ represents all possible deterministic functions (discard and replace $a \mapsto r_k(a) = k$, flip $a \mapsto \bar{a}$ and identity $a \mapsto a$) unveiling a pre-defined element of reality. Similarly, for $N_{B|Y} = \lambda_B(Y) = B$, thus with the assumption of *realism*, Eq. (8) becomes:

$$p_{AB|XY}(ab|xy) \overset{\text{Loc,real}}{=} \sum_{\lambda_A, \lambda_B} \delta_{A,\lambda_A(X)}\delta_{B,\lambda_B(Y)}P_{\Lambda_A\Lambda_B}(\lambda_A, \lambda_B). \tag{9}$$

With $\lambda_A, \lambda_B \in \{r_0, r_1, \text{fp}, \text{id}\}$, and denoting $P_Z(z) = p_z$, we have:

$$p_{00|00} = q_{r_0,r_0} + q_{\text{id},r_0} + q_{r_0,\text{id}} + q_{\text{id},\text{id}}$$
$$p_{00|01} = q_{r_0,r_1} + q_{\text{id},r_1} + q_{r_0,\text{fp}} + q_{\text{id},\text{fp}}$$
$$\vdots$$
$$p_{11|11} = q_{r_1,r_1} + q_{\text{id},r_1} + q_{r_1,\text{id}} + q_{\text{id},\text{id}}. \tag{10}$$

These 16 equations, along with the 16 constraints of probabilities of applying specific λ_A, λ_B, $0 \le q_{\lambda_A\lambda_B} \le 1$ represent a *linear quantifier elimination* on the 16 probabilities q. It satisfies the *no-signaling* relations of Eq. (7) that denies superluminal causal arrows (from node X to B in Fig. 5(c)), and characterize the polytope $\mathcal{L}$ by the following type of Clauser–Horne–Shimony–Holt (CHSH) inequalities[4][141,143]:

$$\hat{\beta} = \sum_{xy=0}^{1}(-1)^{xy}M_{A|x}N_{B|y}, \qquad \beta = \beta_\uparrow - \beta_\downarrow = \sum_{x,y=0}^{1} p(a \oplus b = xy|xy) - p(a \oplus b \ne xy|xy) \le 2 \tag{11}$$

where $\beta = \langle\hat{\beta}\rangle$ and $\beta_\uparrow = 4 - \beta_\downarrow$.

Definition 2 (*Optimal CHSH Quantum Strategy*). Let Alice and Bob share the singlet state $|\psi^-\rangle_{AB} = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$. Choose dichotomic observables $A_0 = \sigma_z$, $A_1 = \sigma_x$ for Alice and $B_0 = (\sigma_z + \sigma_x)/\sqrt{2}$, $B_1 = (\sigma_z - \sigma_x)/\sqrt{2}$ for Bob, which results in the outcome projectors $M_{a|x} = \frac{1}{2}(\mathbf{1} + (-1)^a A_x)$ and $N_{b|y} = \frac{1}{2}(\mathbf{1} + (-1)^b B_y)$, therefore, $p(ab|xy) = \langle\psi^-|M_{a|x} \otimes N_{b|y}|\psi^-\rangle$ achieves the maximal quantum value $\beta(p) = 2\sqrt{2}$ for the CHSH expression in Eq. (11).

Other Bell states also reach this maximum value, provided the measurement settings are adjusted accordingly. CHSH can be rewritten as

$$\beta_\uparrow = p_{a=b|00} + p_{a=b|01} + p_{a=b|10} + p_{a\ne b|11} \le 3 \quad \vee \quad \beta_\downarrow \ge 1, \tag{12}$$

Note that each CHSH inequality corresponds to a facet of the local polytope $\mathcal{L}$. This motivates the following definition

Definition 3. A Bell inequality is *tight* (or *facet-defining*) if the hyperplane it defines corresponds to a facet of the local polytope $\mathcal{L}$.

---

[4] Specifically, there are eight CHSH inequalities correspond to the 8 frustrated 4-node networks [141]. By taking the absolute value, only 4 CHSH inequalities are relevant and they can be represented in a tetrahedron [133,142].

The CHSH inequality can also be understood as a *non-local game*: once Alice and Bob receives $x, y \in \{0, 1\}$ they cannot communicate. They respond with bits $a, b \in \{0, 1\}$ and win if $a \oplus b = x \cdot y$. The correlator expression $\langle M_{A|x} N_{B|y} \rangle = p_{a=b|xy} - p_{a \neq b|xy}$, where $p_{a=b|xy} = \sum_{a=b} p_{ab|xy}$, elucidates the relationship between β, $\beta_\uparrow$, and $\beta_\downarrow$. Classically, $P_{\text{win}} = \sum_{x,y} p(x, y) \sum_{a,b} p(a \otimes b = xy|xy) = 3/4$. Notably, from the behavior $\tilde{\boldsymbol{p}}$ in Fig. 2(b), we have $\beta = 4v$. For $v \leq 1/2$, $\tilde{\boldsymbol{p}} \in \mathcal{L}$, consistent with the causal structure in Fig. 5(a). However, for $v > 1/2$, $\tilde{\boldsymbol{p}} \notin \mathcal{L}$ and cannot be derived from Eq. (9), which holds under the assumptions of locality and realism.

In quantum theory, neither locality nor realism is assumed. Instead of Eq. (9), the Born rule determines the entries of the conditional probability distribution $\boldsymbol{p}$. Given a quantum state $\rho \in \mathcal{D}(\mathcal{H}_A \otimes \mathcal{H}_B)$, where $\mathcal{H}_A \cong \mathbb{C}^{d_A}$ and $\mathcal{H}_B \cong \mathbb{C}^{d_B}$, and local measurements described by POVMs $M_{A|x} = \{M_{a|x}\}_a \in \mathcal{B}(\mathcal{H}_A)$ and $N_{B|y} = \{N_{b|y}\}_b \in \mathcal{B}(\mathcal{H}_B)$, the Born rule yields

$$\boldsymbol{p} \equiv \{p_{AB|XY}(ab|xy)\}_{abxy} = \{\text{Tr}\left(M_{a|x} \otimes N_{b|y} \rho\right)\}_{abxy} \in \mathcal{Q}. \tag{13}$$

These behaviors are consistent with the causal structure in Fig. 5(b) and with $\tilde{\boldsymbol{p}}$ in Fig. 2(b) for $v \leq 1/\sqrt{2}$. If we use Eq. (13) there exists ρ, $M_{A|X}$ and $N_{B|Y}$ such that $p_{\text{win}} \approx 0.85$.

The Hilbert space structure and the non-commutativity of observables imply $\mathcal{L} \subsetneq \mathcal{Q} \subsetneq \mathcal{NS}$.[5] In fact, certain $\tilde{\boldsymbol{p}}$ for $1/\sqrt{2} < v \leq 1$ can satisfy the no-signaling constraints ($\boldsymbol{p} \in \mathcal{NS}$) while still not belonging to $\mathcal{Q}$.[6] There is ongoing research into fundamental physical principles that could explain why $\mathcal{Q} \subsetneq \mathcal{NS}$. One example is the *information causality principle*[147,148]. It states that the amount of information that one party ($\mathcal{B}$) can gain about another party's ($\mathcal{A}$'s) data, even using shared correlations, cannot exceed the amount of classical communication exchanged between them. This principle is respected only for $\boldsymbol{p} \in \mathcal{Q}$, as it imposes limits compatible with Tsirelson's bound $v = \sqrt{2}$ (for details see [20] and the review on $\mathcal{Q}$ [149]). In conclusion, behaviors outside the no-signaling polytope contradict special relativity as shown in Fig. 5(d).

In general, $\dim \mathcal{L} = \dim \mathcal{Q} = \dim \mathcal{NS}$ and the extremal points of $\mathcal{L}$ is a finite subset of the set of infinite extremal points of $\mathcal{Q}$. BI violation remains a necessary condition to detect Eve and ensures secure communication [90]. It turns out that the shared state ρ must necessarily be entangled. Unlike entanglement witnesses, which rely on assumptions about Hilbert space structure, BI violation is a stronger test for witnessing entanglement of ρ by $\boldsymbol{p} \in \mathcal{Q} \setminus \mathcal{L}$. It depends *solely* on the observed statistical behaviors $\boldsymbol{p}$, making protocols device-independent. If the measurement outcomes of entangled particles violate BI, it guarantees that the correlations are genuinely quantum. Eve cannot reproduce these correlations without being detected, ensuring the security of the key. Indeed, let $\beta_{\mathcal{E}\mathcal{A}}$ be the CHSH value between Eve and Alice, and $\beta_{\mathcal{A}\mathcal{B}}$ between Alice and Bob, then quantum theory predicts that $\beta_{\mathcal{A}\mathcal{B}}^2 + \beta_{\mathcal{E}\mathcal{A}}^2 \leq 8$ [150]. Therefore if $\beta_{\mathcal{A}\mathcal{B}} > 2\sqrt{2} \implies \beta_{\mathcal{E}\mathcal{A}} < 2$.

Next, we analyze the numerical and experimental tool to assert that $\boldsymbol{p} \in \mathcal{Q} \setminus \mathcal{L}$.

2.2. The Navascués–Pironio–Acín hierarchy

The Navascués–Pironio–Acín (NPA) hierarchy is a systematic approach to check if $\boldsymbol{p} = p(ab|xy) = \text{Tr}(\rho M_{a|x} N_{b|y}) \in \mathcal{Q} \setminus \mathcal{L}$ [151,152]. It provides a sequence of increasingly tighter outer approximations to the set of quantum correlations $\mathcal{Q}_1 \supseteq \cdots \mathcal{Q}_k \supseteq \cdots \supseteq \mathcal{Q}$, where each kth level in the hierarchy defines the following semidefinite programming (SDP) relaxation:

$$\text{maximize}\{\varphi| \; \text{Tr} \, \Gamma^k J^i = 0, \; \text{Tr} \, \Gamma^k \Phi^i = p_i, \; \Gamma^k - \varphi \mathbf{1} \geq 0, \; \Gamma \succeq 0\} \tag{14}$$

where J^i and Φ^i are linked to the moment matrix Γ^k, which encodes the constraints derived from quantum mechanics: *(i) Definition of the moment matrix Γ^k* – for a given level k in the hierarchy,

$$\Gamma_{i,j}^k = \text{Tr} \, \rho (\tau_i^k)^\dagger \tau_j^k, \quad \tau^1 = \{\mathbf{1}, M_{a|x}, N_{b|y}\}_{abxy}, \quad \tau^{k+1} = \{\tau^k, \tau_i^k \tau_j^1\}_{ij}$$

where $\tau^k = \{\tau_i^k\}$ is the set of monomials of measurement operators up to degree k, e.g., consisting of products like $M_{a|x} N_{b|y}$ or $M_{a'|x} M_{a|x}$. The size of Γ grows with k, encompassing higher-order correlations between measurement operators.

(ii) Constraints − The condition $\text{Tr} \, \Gamma^k J^i = 0$ and $\text{Tr} \, \Gamma^k \Phi^i = p_i$ with opportune J and Φ suitably rewrite the constraints that $\boldsymbol{p} \in \mathcal{Q}_k$ only if $\exists \Gamma \succeq 0$ with $\boldsymbol{p} = \{p_i\}_i$ and (similarly for $N_{b|y}$)

$$M_{a|x} M_{a'|x} = \delta_{a,a'} \mathbf{1}, \qquad \sum_a M_{a|x} = \mathbf{1}, \qquad [M_{a|x}, N_{b|y}] = 0.$$

---

[5] In relativistic quantum field theory the set of quantum correlation is $\tilde{\mathcal{Q}} \supseteq \mathcal{Q}$. The question $\tilde{\mathcal{Q}} \equiv \mathcal{Q}$? is named *Tsirelson problem* and the answer is no, unless finite dimensional Hilbert spaces [144–146].

[6] These correlations can, in principle, violate the monogamy of entanglement, which asserts that if two parties ($\mathcal{A}$ and $\mathcal{B}$) are maximally entangled, neither can be maximally entangled with a third party ($\mathcal{C}$). Nonetheless, in quantum theory, non-local correlations must still respect monogamy of entanglement.

These constraints are incorporated into the structure of Γ, imposing relations between the matrix elements and reducing the affine subspace of the possible correlations.

(iii) Feasibility − If a feasible Γ that solves the ST problem exists at level k, then $\boldsymbol{p} \in \mathcal{Q}_k$ is "k-quantum", meaning it can be approximated by a quantum behavior up to kth hierarchy level. If $\boldsymbol{p} \in \mathcal{Q}_{k+1} \implies \boldsymbol{p} \in \mathcal{Q}_k$ since Γ^k is a sub-matrix of Γ^{k+1}. In the limit $\lim_{k\to\infty} \mathcal{Q}_k = \mathcal{Q}$, therefore if $\boldsymbol{p} \notin \mathcal{Q} \implies \exists k$ s.t. the problem is unfeasible.

(iv) Generalization − The NPA hierarchy can be seen as a specific instance of a more general framework for optimizing polynomial expressions over noncommuting variables. This generalized formulation was developed in [153], where the moment matrix Γ^k is understood as a noncommutative moment matrix, and the SDP relaxation is extended to arbitrary Hermitian polynomial constraints over operator variables. In this setting, one defines a sequence $y = \{y_w\}$ indexed by words w in the measurement operators, where $y_w = \langle \phi, w(X)\phi \rangle$ for some Hilbert space $\mathcal{H}$, state $\phi \in \mathcal{H}$, and operator tuple $X = (X_1, \ldots, X_n)$. The feasibility conditions $\Gamma^k \succeq 0$ and the constraints encoded by moment and localizing matrices ensure that the hierarchy of SDPs converges to the global optimum under an Archimedean condition on the constraint set.

This formulation subsumes the NPA hierarchy by treating quantum constraints (e.g., projection, completeness, commutation) as polynomial equalities or inequalities. Notably, it includes methods to detect when a given hierarchy level already yields the global optimum and to extract an explicit quantum realization $(\mathcal{H}, X, \phi)$ from the SDP solution, as shown in [153, Theorem 2].

In practice, the NPA hierarchy offers a tractable approximation of the quantum set via a sequence of SDPs, each solvable by efficient algorithms, though the computational cost increases with the level k. For many applications, low levels (e.g., $k = 2$ or 3) already yield tight enough bounds. Intermediate levels, such as $\tau^{1+AB} = \tau^1 \cup \{M_a^x N_b^y\}_{abxy}$, are also commonly used. Replacing the objective function φ with any linear function of the elements in τ^k, the NPA hierarchy becomes a powerful computational tool − e.g., for estimating min-entropy in security proofs (see Section 5). Additional methods for DI applications are discussed in [154–156] and in the SDP review [157].

2.3. Self-testing

In particular cases, DI-protocols not only identify $\boldsymbol{p} \in \mathcal{Q} \setminus \mathcal{L}$, but from the behaviors $\boldsymbol{p}$ can also infer the *input state and measurements realization* $R = (|\tilde{\psi}\rangle_{AB}, \tilde{M}_{A|X}, \tilde{N}_{B|Y})$ adopted in the experiment up to some local invariance Φ (Fig. 2(a)). When this is possible, we say that the behaviors self-test the realization, $\boldsymbol{p} \overset{\text{self-test}}{\mapsto} \Phi(R)$ [58,158].

Definition 4. Let identically and independent distributed (iid) $\boldsymbol{p} = \{p_{AB|XY}(ab|xy)\} \equiv p_{ab|xy}$ with locality and measurement-dependence loophole closed (Section 2.4), then $\forall \dim \mathcal{B}(\mathcal{H}_A), \dim \mathcal{B}(\mathcal{H}_A)$

$$\Sigma : \boldsymbol{p} \overset{\text{self-test}}{\mapsto} (\tilde{\psi}_{AB}, \tilde{M}_{A|X}, \tilde{N}_{B|Y}) \implies \exists | \Sigma^{-1}(\tilde{\psi}_{AB}, \tilde{M}_{A|X}, \tilde{N}_{B|Y}) = \langle \tilde{\psi} | \tilde{M}_{A|X} \otimes \tilde{N}_{B|Y} | \tilde{\psi} \rangle = p_{AB|XY} \tag{15}$$

up to some *gauge of freedom* characterized by the following local invariance $\Phi = \Phi_A \otimes \Phi_B$:

(i) $\tilde{M}_{A|x} \mapsto U\tilde{M}_{A|x}U^\dagger, \tilde{N}_{B|y} \mapsto V\tilde{N}_{B|y}V^\dagger, |\tilde{\psi}\rangle \mapsto U \otimes V|\tilde{\psi}\rangle$

(ii) Given $|\psi\rangle_{ABE} \in \mathcal{H}_{ABE}, \{M_{A|x}\}_x \in \mathcal{B}(\mathcal{H}_A), \{N_{B|y}\}_y \in \mathcal{B}(\mathcal{H}_B)$, exists

$$\Phi : \mathcal{H}_{AB} \mapsto \mathcal{H}_{\tilde{A}\bar{A}\tilde{B}\bar{B}E} \text{ s.t. } |\psi\rangle_{AB} \mapsto |\psi\rangle_{\tilde{A}\tilde{B}} |\text{junk}\rangle_{\bar{A}\bar{B}E} \tag{16}$$

and

$$\Phi_A : \mathcal{B}(\mathcal{H}_A) \mapsto \mathcal{B}(\mathcal{H}_{\tilde{A}} \otimes \mathcal{H}_{\bar{A}}) \qquad\qquad \Phi_B : \mathcal{B}(\mathcal{H}_B) \mapsto \mathcal{B}(\mathcal{H}_{\tilde{B}} \otimes \mathcal{H}_{\bar{B}})$$

$$M_{a|x} \overset{\Phi_A}{\mapsto} \tilde{M}_{a|x} \otimes \mathbf{1}_{\bar{A}} \qquad\qquad N_{b|y} \overset{\Phi_B}{\mapsto} \tilde{N}_{b|y} \otimes \mathbf{1}_{\bar{B}} \tag{17}$$

such that

$$(\Phi_A \otimes \Phi_B \otimes \text{id}_E)(M_a^x \otimes N_b^y \otimes \mathbf{1}_E |\psi\rangle_{ABE}) = (\tilde{M}_{a|x} \otimes \tilde{N}_{b|y} |\tilde{\psi}\rangle_{\tilde{A}\tilde{B}}) \otimes |\text{junk}\rangle_{\bar{A}\bar{B}E}. \tag{18}$$

A simple case of self-testing is given by the maximal violation of CHSH of Eq. (11). It is easy to observe that any realization such that $\beta = 2\sqrt{2}$ consists of anticommuting operators on the support of the state $|\psi\rangle$, $\{M_{A|0}, M_{A|1}\}|\psi\rangle = \{N_{B|0}, N_{B|1}\}|\psi\rangle$. Indeed, let $M_{A|\pm} = \frac{M_{A|0}\pm M_{A|1}}{\sqrt{2}}$, the sum-of-square (SOS) decomposition of the shifted CHSH operator assures that:

$$2\sqrt{2}\mathbf{1} - \hat{\beta} = \frac{(M_{A|+} - N_{B|0})^2 + (M_{A|-} - N_{B|1})^2}{\sqrt{2}} \succeq 0. \tag{19}$$

Then the anticommutation comes from $\beta = 2\sqrt{2} \implies M_{A|+} = N_{B|0}|\psi\rangle$ and $M_{A|-}|\psi\rangle = N_{B|1}|\psi\rangle$. The explicit isometry of Eq. (16) is given in the circuit 6(a). Analogously for the isometries on the measurements of Eq. (17). Similar calculations

(a) Isometry of Eq. (16)   (b) Selftesting as retrodictive task
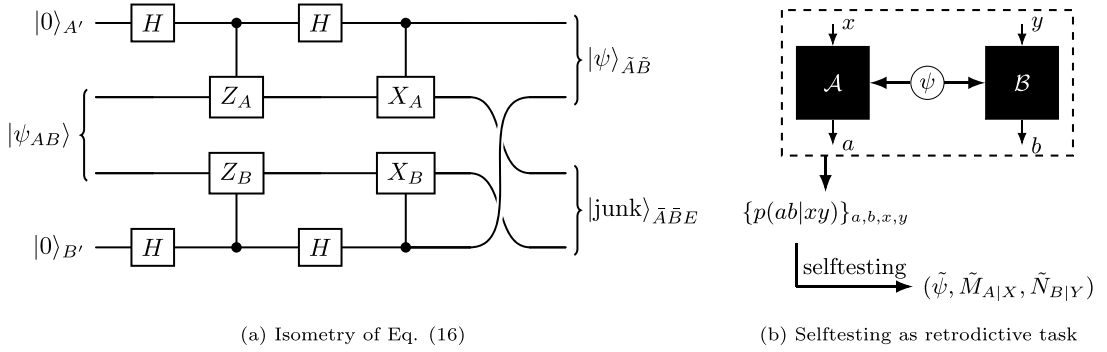
Fig. 6. In Fig. 6(a) an explicit implementation of the isometry (details in Ref. [161]) that characterizes the realization $(\tilde{\psi}, \tilde{M}_{A|X}, \tilde{N}_{B|Y})$ inferred only from $\boldsymbol{p} = \{p_{AB|XY}(a, b, |x, y)\}_{a,b,x,y}$ treating the labs as black boxes 6(b)–2(a).

hold when only one detector is inefficient [159] (see Section 2.4.1 putting $\alpha_B = 0$ in (27)) and the tilted Bell operator can be obtained, i.e. $\hat{\beta} + \alpha_A M_{A|0}$ (see Eq. (27)) such that

$$\sqrt{2 + \alpha_A^2}\mathbf{1} - (\hat{\beta} + \alpha_A M_{A|0}) = \sum_i P_i^\dagger P_i \tag{20}$$

in terms of polynomials $P_i \in \{\mathbf{1}, M_{A|x}, N_{B|y}, M_{A|x} \otimes N_{B|y}\}$. SOS decomposition allows to prove that if maximal violation $\beta_\mathcal{Q} = \sqrt{2 + \alpha_A^2}$ is obtained then the optimal realization $(|\psi\rangle_{AB}, M_{A|\pm}, N_{B|y})$ is *self-tested* [160,161], with

$$|\psi\rangle_{AB} = \cos\theta|00\rangle + \sin\theta|11\rangle, \quad N_{B|0} = \sigma_z, \quad N_{B|1} = \sigma_x, \quad M_{A|\pm} = \cos\mu\,\sigma_z \pm \sin\mu\,\sigma_x \tag{21}$$

where $\alpha_A = 2/\sqrt{1 + 2\tan^2 2\theta}$, $\tan(\mu) = \sin(2\theta)$. If the polynomials P_i are written in terms of the operators of *any* optimal realization, then $\forall i\ P_i|\psi\rangle = 0$. These conditions implies the existence of operators $\{Z_A, X_A, Z_B, X_B\}$ satisfying

$$Z_B|\psi\rangle_{AB} = Z_B|\psi\rangle_{AB}, \quad \sin\theta X_A(\mathbf{1} + Z_B)|\psi\rangle_{AB} = \cos\theta X_A(\mathbf{1} - Z_A)|\psi\rangle_{AB}. \tag{22}$$

In turn, Eq. (22) ensures the existence of local isometries Φ_A and Φ_B such that

$$\Phi_A \otimes \Phi_B|\psi\rangle_{AB} = |\psi\rangle_{\tilde{A}\tilde{B}} \otimes |\text{junk}\rangle_{\bar{A}\bar{B}E}$$
$$\Phi_A \otimes \Phi_B(M_{A|x} \otimes N_{B|y}|\psi\rangle_{AB}) = M'_{A|x} \otimes N'_{B|y}|\psi\rangle_{\tilde{A}\tilde{B}} \otimes |\text{junk}\rangle_{\bar{A}\bar{B}E}. \tag{23}$$

Self-testing can be made *robust* in the sense that in a neighborhood of the maximal quantum value $\mathcal{I}_{\beta_\mathcal{Q}}$, there exists a physical realization R that is close — up to a local isometry — to the ideal realization $R_\mathcal{Q}$ (see numerical SWAP technique in [162,163]). The most general case involving two inefficient detectors, the SOS decomposition is analyzed with NPA hierarchy (see Section 2.2) without finding a simple expression for the polynomial P_i, unless the inefficiency of the detectors is the same [164]. The solution in this case is obtained with Jordan's lemma [134] and Groebner basis.

Lemma 1 (*Jordan's Lemma*). *In CHSH, $\{M_{a|x}\}_{a,x=0,1}$ and $\{N_{b|y}\}_{b,y=0,1}$ can be projective w.l.o.g., then there must exist a local unitary transformations that simultaneously block-diagonalize the observables $M_{A|x}, N_{B|y}$, with blocks of size 1 or 2. But, to compute $\langle M_{A|x}\rangle_\psi, \langle N_{B|y}\rangle_\psi$ we can always complete a one-dimensional block by adding to it a projector over a state in the null space of the corresponding reduced state $\rho_{A(B)} = \text{Tr}_{B(A)}|\psi\rangle\langle\psi|$. We can thus assume all blocks to be two-dimensional and write Alice's measurement operators as*

$$M_{A|0} = \bigoplus_i M_{A|0}^{(i)} = \bigoplus_i \sigma_Z, \quad M_{A|1} = \bigoplus_i M_{A|1}^{(i)} = \bigoplus_i(\cos\theta_i^A\,\sigma_Z + \sin\theta_i^A\,\sigma_X), \tag{24}$$

where index i iterates over the Jordan blocks. Similarly, for Bob's observables.

Using Jordan's lemma, one can decompose the Bell operator as $\hat{\beta} = \bigoplus_i \hat{\beta}_i$, where each $\hat{\beta}_i$ acts on a two-dimensional subspace. This decomposition implies that *self-testing is independent of the local Hilbert space dimensions* $\dim \mathcal{B}(\mathcal{H}_A)$ and $\dim \mathcal{B}(\mathcal{H}_B)$, being invariant under local isometries $\Phi_A \otimes \Phi_B$ that preserve physical predictions. This leads to the so-called *qubit reduction argument*, a key security feature of device-independent QKD: although the actual devices may operate in high-dimensional spaces, only two-dimensional subspaces contribute to the Bell inequality violation. Suppose the state decomposes as $\rho = \bigoplus_i p_i\rho_i$, then the observed value is $\beta = \text{Tr}(\rho\hat{\beta}) = \sum_i p_i\langle\hat{\beta}_i\rangle$. Each $\hat{\beta}_i$ is bounded above by Tsirelson's bound $2\sqrt{2}$. If ρ is entirely supported on the block achieving this bound, the full violation is maximal. Otherwise, contributions from blocks with lower eigenvalues reduce the total violation. *This dilution effect makes the security proof robust against dimension attacks*, where an adversary might try to hide extra information in higher-dimensional components (see Section 1.3.2). Consequently, the derivation of bounds on the adversary's information —

such as bounding the guessing probability from the observed Bell violation — becomes *independent of the internal structure of the devices*, which can be treated as black boxes. The existence of a map $\Sigma : \boldsymbol{p} \mapsto R$ (via Jordan's lemma) is sufficient to certify private randomness extraction. Specifically, condition (18) implies:

$$\sigma_{AE} = \sum_a |a\rangle\langle a| \otimes \mathrm{Tr}_{AB}\left[(\tilde{M}_{a|x} \otimes \mathbb{I}_B \otimes \mathbb{I}_E)|\psi\rangle\langle\psi|\right] = \left[\sum_a p_A(a|x)|a\rangle_{\tilde{A}}\langle a|\right] \otimes \sigma_E,$$

where $\sigma_E = \mathrm{Tr}_{\tilde{A}\tilde{B}}|\mathrm{junk}\rangle\langle\mathrm{junk}| \in \mathcal{H}_{\tilde{A}\tilde{B}E}$, and $p_A(a|x) = \sum_b p(a, b|x, y)$ is Alice's marginal. Thus, *Alice's outcomes are completely random from Eve's perspective* [98], and for any correlation satisfying condition (18), one may optimize over Bob's measurements accordingly. A comprehensive review of self-testing is given in [161], and a geometric characterization of self-testing via nonlocal extremal points $\boldsymbol{p}$ is presented in [149,165]. In the next section, we examine how to account for *experimental imperfections* in Bell tests.

2.4. Experimental loopholes

Experimental validation that $\boldsymbol{p} \in \mathcal{Q} \setminus \mathcal{L}$ requires careful treatment of imperfections in Bell tests. Such imperfections — typically due to transmission losses, detector inefficiencies, or other technical limitations — can open *loopholes* that allow an LHV model to reproduce data that would otherwise appear nonlocal. These loopholes undermine the assumption that the observed statistics $\boldsymbol{p}$ truly violate the causal constraints illustrated in Fig. 5(a) [166,167]. Although this may seem like a conspiratorial behavior of nature, in practice, an adversary could exploit such loopholes to forge fake BI violations using only classical resources [168], potentially compromising device-independent cryptographic protocols. Below, we briefly summarize the main loopholes (see Refs. [166,167] for a detailed discussion).

2.4.1. Detection efficiency loophole

Consider the ideal scenario depicted in Fig. 2(a), where the behavior $\boldsymbol{p} = \{p(ab|xy)\}$ satisfies $\beta(\boldsymbol{p}) = 2\sqrt{2}$ as in Eq. (11). Detection is illustrated as "eyes" observing which lamp turns on, but in reality, it involves two detectors that click with respective probabilities $\eta_A, \eta_B < 1$. For simplicity, let us consider only Bob's detector, then he measures only a set $\mathcal{D}$ of detected particle from a set $\mathcal{E}$, of emitted particle, where $\eta = |\mathcal{D}|/|\mathcal{E}|$.[7] The most general way of accounting for no-click events is to consider an additional outcome, which enlarges the Bell scenario[8] [169,170]. As a results, characterizing the sets $\mathcal{L}$ and $\mathcal{Q}$ becomes considerably more complex [171–173]. To remain in the same Bell scenario, Bob fixes an outcome b to assign at each no-click event with probability $q_B(b|y)$. Similarly, Alice assigns a with probability $q_A(a|x)$.[9] An affine map $\hat{\boldsymbol{p}} = \Omega_{\eta_A\eta_B}(\boldsymbol{p}) = \{\hat{p}(ab|xy)\}$ describes the events of both detectors: both, only one, or none of them click with related probabilities $\eta_A\eta_B$, $\eta_A(1 - \eta_B)$ or $(1 - \eta_A)\eta_B$, and $(1 - \eta_A)(1 - \eta_B)$, such that

$$\hat{p}(ab|xy) = \eta_A\eta_B p(ab|xy) + \eta_A(1 - \eta_B)p_A(a|x)q_B(b|y) + (1 - \eta_A)\eta_B q_A(a|x)p_B(b|y)$$
$$+ (1 - \eta_A)(1 - \eta_B)q_A(a|x)q_B(b|y). \tag{25}$$

Taking into account also the "no click" events, the inequality (11) turns out to be $\beta(\hat{\boldsymbol{p}}) < 2$. It is well known that optimal local assignment gives $\beta(p_A(a|x)q_B(b|y)) = 2\langle M_{A|0}\rangle$, $\beta(q_A(a|x)p_B(b|y)) = 2\langle N_{B|0}\rangle$, and $\beta(q_A(a|x)q_B(b|y)) = 2$. This yields

$$\beta(\hat{\boldsymbol{p}}) = \eta_A\eta_B\beta(\boldsymbol{p}) + 2\eta_A(1 - \eta_B)\langle M_{A|0}\rangle + 2(1 - \eta_A)\eta_B\langle N_{B|0}\rangle + 2(1 - \eta_A)(1 - \eta_B) \leq 2. \tag{26}$$

This can be rewritten as ($\alpha_A = 2(1 - \eta_B)/\eta_B$ and $\alpha_B = 2(1 - \eta_A)/\eta_A$)

$$\beta_\mathcal{Q} \equiv \beta(\boldsymbol{p}) + \alpha_A\langle A_0\rangle + \alpha_B\langle B_0\rangle \leq 2 + \alpha_A + \alpha_B \equiv \beta_\mathcal{L} \leq 4. \tag{27}$$

The last inequality comes from $\mathcal{L} \subset \mathcal{NS}\ (\beta(\boldsymbol{p}_{\mathrm{NL}}) = 4)$. Therefore $\alpha_A + \alpha_B \leq 2$ (or equivalently, $\eta_A^{-1} + \eta_B^{-1} > 3$) $\implies \mathcal{Q}\setminus\mathcal{L} = \emptyset$. There is no room for quantum violation as shown in Fig. 2(d) as the local vertex is moving up towards what is known as the *critical detection efficiency* (CDE) (observe in Fig. 7(b) that $\beta_\mathcal{Q}$ approaches the local bound). Graphically, one can imagine that the plane of Figs. 2(c) and 2(d) with the local vertices approaches the no-signaling vertex $\boldsymbol{p}_{\mathrm{NL}}$ (more geometrical details are in Refs. [171,174–176]).

Definition 5. The open detection loophole refers to the implication $\beta(\boldsymbol{p}) > 2 \implies \boldsymbol{p} \in \mathcal{Q} \setminus \mathcal{L}$ mistakenly (assuming $\boldsymbol{p} = \hat{\boldsymbol{p}}$) ignoring the "no click" events.

---

[7] Here η is the probability that a photon emitted by the source is indeed detected. A discussion on the experimental parameters that contribute to η is provided in 7.3.

[8] This approach can be used to describe null events for analyzers with a number of outcomes that span the space associated to the degree of freedom of interest, such as two-outcome polarizing beam splitters, for example.

[9] This approach is best suited for experiments using "pass/fail" measurement devices, such as a polarization filter, where one cannot distinguish a null event from a projection onto the state that does not pass through the filter.

(a) *maximum quantum value*   (b) *correlations with inefficient detectors*
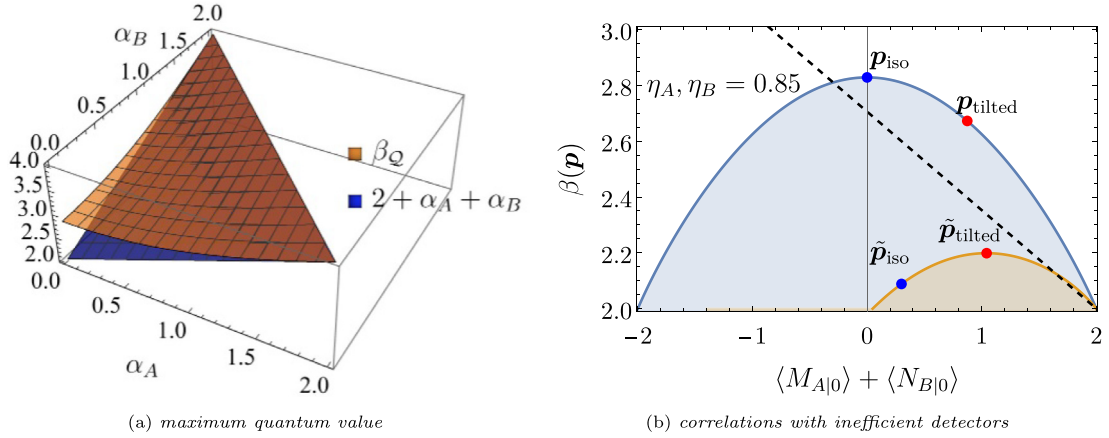
Fig. 7. CHSH with inefficient detectors − Fig. 7(a) encapsulates the optimal value of $\beta_{\mathcal{Q}}$ at given value of $\alpha_A + \alpha_B \leq 2$. The Fig. 7(b) illustrates the impact of detector inefficiencies on nonlocal quantum correlations within the simplest Bell scenario. The blue region represents the set of quantum correlations $\boldsymbol{p} \in \mathcal{Q}$ in ideal conditions. With the detection efficiencies $\eta_A = \eta_B = 0.85$, and the local assignment strategy $q_A(a|x) = \delta_{a,0}$, $q_B(b|y) = \delta_{b,0}$, the effective quantum correlations $\tilde{\boldsymbol{p}} = \Omega_{\eta_A \eta_B}(\boldsymbol{p})$ are constrained to the smaller orange subset (see Fig. 2(d)). The blue dot on the blue curve corresponds to the isotropic behavior $\boldsymbol{p}_{iso}$ that maximally violates the CHSH inequality, $\beta(\boldsymbol{p}_{iso}) = 2\sqrt{2}$, in ideal conditions, while the corresponding effective behavior (blue dot on the orange curve) $\tilde{\boldsymbol{p}}_{iso} = \Omega_{\eta_A \eta_B}(\boldsymbol{p}_{iso})$ no longer attains the maximum violation of the CHSH inequality, $\beta(\tilde{\boldsymbol{p}}_{iso}) \approx 2.08854$. Instead, the red dot on the blue curve corresponds to the quantum behavior $\boldsymbol{p}_{tilted}$ which maximally violates the doubly-tilted CHSH inequality (dashed black line) [20,164].

In many cases, local models can be constructed that are compatible with the experimental data [177]. It has been shown that manipulation of measurement devices can not only lead to fake violations of BI [168] but also to violations of Tsirelson's bound $2\sqrt{2}$ [178]. In DI-QKD, low values of η_A and η_B allow Eve to intercept and hide herself more effectively because many "no-click" events would already occur naturally due to losses from attenuation and imperfect detectors. On the contrary, high detection efficiency $\eta \lesssim 1$ helps to distinguish Eve's attacks from natural losses by maintaining a high value of $\beta_{\mathcal{Q}} - \beta_{\mathcal{L}}$, which translates to a reliable measure of nonlocality.

Definition 6. The detection loophole is closed on the test $\beta_Q = \beta(\hat{\boldsymbol{p}}) > \beta_{\mathcal{L}}$ as genuinely implies (if all other loopholes are closed) $\hat{\boldsymbol{p}} \in \mathcal{Q} \setminus \mathcal{L}$.

The problem of low detection efficiencies in Bell tests had been noted earlier [177], but it was Eberhard in 1993 [179] who first derived a Bell-type inequality specifically optimized for overcoming this loophole. His approach used only the probabilities of conclusive outcomes and allowed for non-maximally entangled states to minimize the critical detection efficiency. Originally it was written as

$$S_E = p(11|00) + p(11|01) + p(11|10) - p(11|11) - p(1|10) - p(1|01) \leq 0, \tag{28}$$

It is a limiting case of Eq. (27), obtained by setting $\alpha_A = \alpha_B = 1$ and expressing the expectation values through raw detection probabilities.

Proposition 1. *A necessary condition to close the detection loophole in Bell experiments implies $\eta > \eta^*$, where η^* is the CDE. (see a representation in Fig. 2(d)).*

Indeed, η^* is a characteristic of an ideal nonlocal correlation, below which $\mathcal{Q} \setminus \mathcal{L} = \emptyset$, and limits the distance across which nonlocality can be operationally (quantum) certified. In the simplest Bell scenario of Fig. 2, the quantum strategy maximally violating Eq. (11) (in ideal conditions) ceases to yield $\boldsymbol{p} \in \mathcal{Q} \setminus \mathcal{L}$ for CDE below $\eta^* = 2\sqrt{2} - 2 \simeq 0.82$ [180]. This comes from Eq. (26) for $\eta_A = \eta_B$, independent on the measurement nor on each other. Then $\langle M_{A|0} \rangle = 0 = \langle N_{B|0} \rangle$ because the results will be uncorrelated (the detected particle is in a maximally mixed state). It follows a list of less recent achievements: *(i)* The CDE is lowered to $2/3 \simeq 0.66$ [179], which comes at the cost of very low robustness to background noise as the state is almost separable (see Fig. 7(b)). *(ii)* For more general scenarios, involving more measurements, the extra-outcome approach presents lower CDEs [174].

(iii) Overall, if $\rho \in \mathcal{B}(\bigotimes_{i=1}^{n} \mathbb{C}^d)$ is used, then higher d and/or n implies lower (exponentially) CDE [181], but at the costs of more experimental complexity. For example, an improvement for CHSH is only for $d \gtrsim 1600$. In asymmetric (symmetric) Bell tests $\eta^* \sim \frac{1}{d}$ ($\eta^* \sim 61.8\%$) [182]. *(iv)* For the BI I_{3322}, with one ideal detection efficiency ($\eta_A = 1$), a CDE is $\eta_B = 43\%$ (or $\eta_B = 66.7\%$) for non-maximally (or maximally) entangled states [183]; *(v)* an LHV model cannot describe $\boldsymbol{p} \in \mathcal{Q}$ when the number of measurement settings at each site m_A and m_B satisfy [184,185]

$$\eta \geq \frac{m_A + m_B - 2}{m_A m_B - 1}. \tag{29}$$

Below more recent achievements: *(i)* a family of n-party BI with binary outcomes and $m > 2$ measurement settings per party can obtain BI violation with lower CDE [186]; *(ii)* BI using multiple copies of the two-qubit maximally entangled state and Pauli measurements, defining a Bell setup with $m = 2^n$ settings and 2^n outcomes reduces the CDE below 0.8214 for $n \geq 2$ [187]; *(iii)* An exponential reduction of CDE was demonstrated in [188] by violating N BI in parallel using N entangled states shared by a single particle pair. *(iv)* the BI I_{4422}^4 is experimentally violated using four-dimensional entangled photons closing the detection loophole with $\eta \sim 71.7\%$ [189].[10]

(v) to experimentally increase detection efficiency (qubits constructed in trapped ions, atoms, or nitrogen-vacancy (NV) centers in diamond) is also used an "event-ready" setup, in which the presence of particles at the measurement stations is heralded by an additional event-ready protocol [190–192] (more detail in Section 7.4.2). In point-to-point photonic experiments, both link losses and detector losses are more difficult to overcome. Superconducting single-photon detectors (SNSPDs), achieving efficiencies of over 90%, have been instrumental in recent loophole-free experiments [193–195].

Fair sampling loophole. — The losses that naturally appear (e.g., in optical fibers) and affect the particles independently of the measurement settings, are solely responsible for $|\mathcal{D}| \ll |\mathcal{E}|$. The *fair sampling assumption* (FSA) is often invoked to justify ignoring the detection loophole.

Definition 7. A Bell tests in which $|\mathcal{D}| \ll |\mathcal{E}|$ invoked FSA when it imposes that $p(\mathcal{D}) \simeq p(\mathcal{E})$.

Eve can exploit the fair sampling loophole by applying a biased coarse-graining μ_{DL} to the distribution $p(\mathcal{E})$, resulting in $p(\mathcal{D}) = \mu_{DL}[p(\mathcal{E})] \neq p(\mathcal{E})$. This manipulation skews the observed data $\boldsymbol{p}$, making it falsely appear that $\boldsymbol{p} \in \mathcal{Q} \setminus \mathcal{L}$, as if BI were violated. She can achieve this by influencing detection efficiency, introducing selective transmission losses, or tampering with data processing. For instance, Eve may ensure that only particles with hidden variables producing strong correlations are detected, while others are discarded.

Proposition 2. *Although high-efficiency detectors, with $|\mathcal{D}|/|\mathcal{E}| \simeq 1$, limit Eve's manipulation, they do not guarantee $p(\mathcal{D}) \simeq p(\mathcal{E})$.*

Even in experiments with $\eta \sim 1$, hidden mechanisms can bias which particles are detected based on certain hidden variables (e.g., emission angle or polarization). These variables could correlate with measurement settings in a way that skews the detected sample to favor results violating BI. Thus, while nearly all particles are detected (addressing the detection loophole), the sample may still not represent the full emitted set (leaving the fair sampling loophole open). To avoid such bias, careful calibration is crucial like using space-like separation and random detector calibration [196]. However, $\eta \sim 1$ [197] makes it easier to verify that the detected pairs are a fair representation of the emitted set, helping to close the fair sampling loophole, e.g. in Ref. [197].[11]

2.4.2. Locality and measurement-dependence loophole

Definition 8 (*Space-like Separation*). For two events in Alice and Bob's lab respectively with coordinates (t_A, x_A) and (t_B, x_B) in Minkowski spacetime are *causally space-like separated* iff the invariant spacetime interval $\Delta s^2 = c^2(t_A - t_B)^2 - |x_A - x_B|^2 < 0$, or equivalently Eq. (6) holds, which implies that the spatial distance between the events is greater than the distance light could travel in the time interval separating them.

Because no causal influence (which is limited by the speed of light) can bridge a space-like interval, there is no possible way for one event to affect the other. Fig. 2(a) shows two black boxes $\mathcal{A}$ and $\mathcal{B}$ representing the Alice and Bob's laboratories *causally space-like separated* in causal cones to prevent any influence the other detector's measurement from the other lab.

Definition 9 (*Locality Loophole*). The locality loophole is open if Eq. (6) is not certified.

To close the locality loophole the Bell experiment must be realized such that the entire measurement process, consisting of the random choice of basis, the adjusting the analyzer, and the detection of the particle satisfied the space-like separation condition [198]. Locality loophole was certified in the late "90s using *(i)* entangled photons from SPDC sources, *(ii)* increasing the space-like separation between the analyzers to tens of km [199,200], *(iii)* employing fast, unpredictable and random switching of measurement settings to further eliminate the possibility of communication between the detectors *(iv)* using fast electronics and quantum random number generators (QRNG) to choose the settings of the analyzers [196].

The first Bell test to close both the detection and locality loopholes was reported in 2015 [100]. It used electron spins that were entangled using an event-ready protocol [190–192]. The experiment demonstrated the first statistically significant BI violation without relying on additional assumptions such as fair sampling.

---

[10] In an atom–photon system for example, the atomic system can have η_A, η_B near the unity (see Section 7).

[11] Despite the detection loophole in Ref. [197] is closed, but the separation distance was not sufficient to close the locality loophole.

Definition 10 (*Measurement-dependence Loophole*). The measurement-dependence loophole, also known as the *freedom-of-choice* or *the free-will loophole*, questions whether the choices of measurement settings could be influenced by hidden variables, i.e. $P_X = P_{X|\Lambda}$?, $P_Y = P_{Y|\Lambda}$?

This arises from the observation that the local and realistic causal structure in Fig. 5(a) implicitly assumes $P_X = P_{X|\Lambda}$ and $P_Y = P_{Y|\Lambda}$ that there is no common cause between the local settings X and Y and the source Λ. A small amount of correlation is required to produce a false BI violation, therefore, a Bell test must use QRNGs to randomly determine the measurement settings in real-time, ensuring that no prior knowledge could influence the results, hence closing the measurement dependence loophole [201]. In 2017, a groundbreaking experiment, known as the "Cosmic Bell Test" the light from distant stars was used to choose measurement settings, arguing that the light had traveled for hundreds of years and thus could not be influenced by hidden variables [202].

Other loopholes. Coincidence-Time Loophole — Coincidence windows can create spurious correlations if the time window for considering detection events as part of the same pair is too wide. Then, nanosecond-level timing precision are used for tight synchronization and narrow coincidence time windows [203]. Future quantum networks employing repeater stations and tight coincidence timing windows will further ensure the proper pairing of entangled photons [204].

Memory Loophole — The memory loophole arises if detectors have some form of memory from previous trials, which could influence future results. Experiments must randomized trials and reset the system after each trial to avoid memory effects [197] (see Section 3.15).

Finally, *super-determinism* is a theoretical loophole that challenges the assumption of *free will* in choosing measurement settings [205]. Although superdeterminism is not directly testable in the traditional sense, the scientific consensus generally assumes that randomness and independence in quantum processes are valid. However, for DI-QKD its significance is largely philosophical — if all variables were predetermined, any "key" would already be known —. In contrast, for DI quantum random number generation, whose aim is to certify fresh randomness, the loophole poses a more substantive concern. A concise review of this philosophical loophole can be found in Ref. [206].

2.4.3. Experimental breakthroughs

The timeline in Fig. 3 refers to the first definitive closure of the detection and locality loopholes, simultaneously referred to as "loophole-free" Bell tests. In 2015, the first experiment was reported, using entangled photons and electrons in NV centers located at a distance of about 1.3 km [100]. All photonic experiments were also reported that same year: Ref. [194] used high-efficiency photon detectors and random measurement settings, and similarly, the experiment in Ref. [195] used highly efficient detectors and a large spatial separation between detectors. Compared to previous Bell tests using entangled photons, the critical component here was high-efficiency superconducting photo-detectors, which permitted the realization of experiments above the CDE.

A loophole-free Bell test using an event-ready setup with entangled neutral atoms in [207], where atom–photon entanglement and entanglement swapping to prepare entangled spin states of two atoms separated by 398 m; In Ref. [208], all three major loopholes were addressed using randomness from photons emitted by cosmic sources to determine the measurement settings. This approach effectively closes the locality loophole by ensuring that the measurement settings are not influenced by any local hidden variable by using events that occurred 11 years prior (see Section 7 for experimental details).

2.5. Other notions of nonclassicality that can power cryptography

Quantum steering. Similarly to the LHV framework introduced, we can define a Local Hidden State (LHS) model. The operational diagrams are [209]

$$p(ab|xy) = \begin{array}{c} a \\ M_{A|x} \\ x \end{array} \begin{array}{c} b \\ N_{B|y} \\ \Lambda \quad y \end{array} \; , \qquad \sigma_{a|x} = \begin{array}{c} a \\ M_{A|x} \quad \rho_\Lambda \\ x \quad \Lambda \end{array} \tag{30}$$

The left-hand side of Eq. (30) represents an LHV model for the Bell test. We note that such graphical equations follow the framework introduced in [210].

Definition 11 (*Local Hidden State (LHS) Model*). Let us consider Alice's measurements with the POVM $M_{A|x} = \{M_{a|x}\}_a$ on $\rho_{AB} \in \mathcal{B}(\mathbb{C}^{d_A} \otimes \mathbb{C}^{d_B})$, such that the update conditional state on Bob's side is given by

$$\rho_{a|x} = \frac{\sigma_{a|x}}{p_{A|X}(a|x)}, \qquad \sigma_{a|x} = \mathrm{Tr}_A[(M_{a|x} \otimes \mathbf{1}_B)\rho_{AB}], \qquad p_{A|X}(a|x) = \mathrm{Tr}\sigma_{a|x} > 0. \tag{31}$$

The collection $\{\sigma_{a|x}\}_{a,x}$, a.k.a. assemblages, is said to admit a LHS model if there exists: (i) a classical random variable λ with probability distribution $p(\lambda)$, (ii) a set of conditional probability distributions $p(a|x, \lambda)$, (iii) a collection of normalized quantum states $\{\sigma_\lambda\}_\lambda \in \mathcal{B}(\mathcal{H}_B)$, such that the following decomposition holds (discrete case):

$$\sigma_{a|x} = \sum_\lambda p_\Lambda(\lambda) p_{A|X\Lambda}(a|x, \lambda) \sigma_\lambda, \quad \wedge \quad \rho_B = \mathrm{Tr}_A[\rho_{AB}] = \sum_a \sigma_{a|x} \quad \forall x, a. \tag{32}$$

Bob performs full tomography of the quantum state $\rho_{a|x}$ that is effectively prepared in his lab after Alice's action. Then the LHS correlations are:

$$p(a, b|x, y) = p_{B|Y}(b|y, \sigma_{a|x}) = p_{A|X}(a|x)p_{B|Y}(b|y, \rho_{a|x}) = \sum_\lambda p_{A|X\Lambda}(a|, \lambda)p_{B|Y}(b|y\rho_{a|x}\lambda)p_\Lambda(\lambda), \tag{33}$$

where Bob's conditional probability is $p_{B|Y,\rho}(b|y, \rho) = \mathrm{tr}[N_{b|y}\rho]$, for $\rho \in \{\sigma_{a|x}\}_{a,x}$.

Definition 12 (*Quantum Steering*). A bipartite quantum state ρ_{AB} is said to be unsteerable (from Alice to Bob) if Eq. (32) holds, otherwise is said to be steerable (from Alice to Bob), $\rho_{AB} \in \mathcal{S}_{A\to B}$.

In other words, quantum steering is exhibited when the correlations between Alice's outcomes and Bob's conditional states cannot be explained by a classical mixture of preexisting states on Bob's side (in the diagram rather than Λ is required ρ_{AB}). Notice that steering is directional ($\rho_{AB} \in \mathcal{S}_{A\to B} \wedge \rho_{AB} \notin \mathcal{S}_{B\to A}$). Whether in DI-QKD the nonlocal correlation $\boldsymbol{p} \in \mathcal{Q}\setminus\mathcal{L} \implies$ Alice and Bob are untrusted (their measurement devices are "black boxes" − unknown to the experimenter), a *certification* of a steering state (Steering Inequality SI violation) allows *one-sided DI-QKD (1SDI-QKD)*: only Alice can be trusted (her measurement devices are well-characterized), while Bob's devices remain untrusted [211] (see Section 6.5). Specifically, $\boldsymbol{p}(\rho_{AB}) \in \mathcal{Q} \setminus \mathcal{L} \implies \rho_{AB} \in \mathcal{S}_{A\to B} \implies \rho_{AB}$ entangled, but the *only if* does not hold. Follows a series of interesting facts: *(i)* SI violation requires a lower CDE than its analogous BI violation. Indeed for loophole-free steering with qubits and N measurement settings $\eta^* \propto 1/N$ [119,212,213]. *(ii)* SI are easier to test than BI using continuous-variable (CV) systems, due to the fact that high-efficiency Gaussian measurements (such as homodyne) are not sufficient to violate BIs in Gaussian states [214]. This is not an issue for demonstration of quantum steering, and indeed the first demonstration was realized in 1992 using homodyne measurements on entangled optical fields [215]. Since then, a series of experiments have demonstrated one-way Gaussian steering [216] and non-Gaussian steering [217]. *(iii)* Loophole-free SI violations in discrete-variable (DV) systems were demonstrated in 2012 using polarization–entangled photon pairs and superconducting detectors for high detection efficiency [218–220]. Ref. [218] closed the detection loophole with superconducting detectors; Ref. [220] achieved steering over 1 km of optical fiber despite lower efficiencies. Ref. [219] simultaneously closed detection, locality, and measurement-dependence loopholes using measurements 48 m apart. See also [221,222] and Section 7.

Contextuality. Rooted in the Kochen–Specker (KS) paradox, contextuality, another nonclassicality notion, reveals the impossibility of *realism* of 1, i.e. assigning pre-existing values to quantum observables independently of measurement context. A contextuality-based DI-QKD scheme, exemplified by the Peres–Mermin square [223,224], uses a bipartite system satisfying KS paradox conditions locally while exhibiting perfect distant correlations [225]. This ensures secure key extraction, as any eavesdropping attempt by Eve introduces detectable errors. Unlike Bell-based methods, contextuality relies on the trade-off between information gain and disturbance, tied to quantum uncertainty [226,227] and wave–particle duality [228,229]. Variants like *generalized contextuality* [52], hyperbits [230], Kirkwood–Dirac distribution [231], witwords [211], and overall Generalized Probabilistic Theories [232,233] highlight quantum advantages for DI cryptography.

3. Fully Device Independent Quantum Key Distribution (DI-QKD)

We discussed that device-dependent cryptography permits *inventa fraus* [13]; *facta lexia*, DI-QKD eliminates them via BI violation or other nonclassical notions. In this section, we are going to introduce the DI protocols that are powered by *quantum theory* to enhance security.

3.1. Equivalence principle for simulation-based security

DI-QKD protocols are analyzed in *simulation-based security*, where the real execution of a protocol is compared to an ideal one: if no adversary can distinguish the two, then the real protocol is considered secure.

Definition 13 (*Indistinguishable Protocols*). Let Π A protocol which take inputs and produce outputs. Let $\Pi_1 = \mathcal{Z}_1(\Pi)$ and $\Pi_2 = \mathcal{Z}_2(\Pi')$ the protocols affected by the presence of an external environments. We define an equivalence relation $\Pi_1 \sim_{\epsilon(n)} \Pi_1$ if for all probabilistic polynomial-time (PPT) environment $\mathcal{Z}_1, \mathcal{Z}_2$, there exists a negligible function $\epsilon(n)$ (in the security parameter n) such that

$$\mathrm{Adv}(\Pi_1, \Pi_2) \le \epsilon(n), \qquad \mathrm{Adv}(\Pi, \Pi') := \left| \Pr[\Pi_1 = 1] - \Pr[\Pi_2 = 1] \right|. \tag{34}$$

where Adv is the distinguishing advantage function.

In other words, no efficient environment can tell Π apart from Π' with more than the negligible advantage $\epsilon(n)$.

Definition 14 (*Simulation Security*). We denote a real protocol executed among parties which may be corrupted by a real adversary $\mathcal{E}_R$ as a function $\mathcal{E}_R(\Pi^R)$ and an ideal protocol Π^I that receives inputs from the parties and returns outputs that are guaranteed to satisfy the security properties in the presence of a simulated adversary (simulator) $\mathcal{E}_S$ also as a function $\mathcal{E}_S(\Pi^I)$. The protocol $\mathcal{E}_R(\Pi^R)$ is said to securely realize the ideal functionality Π^I if for every PPT adversary $\mathcal{E}_R$ there exists a PPT simulator $\mathcal{E}_S$ such that $\mathcal{E}_S(\Pi^I) \sim_{\epsilon(n)} \mathcal{E}_R(\Pi^R)$.

This definition captures the intuition that any attack on Π^R in the real world can be simulated in the ideal world, so that no environment can distinguish the two executions except with negligible probability. In practice, protocols are rarely executed in isolation. The following UC framework requires that security be preserved even when the protocol is composed with an arbitrary set of other protocols.

Definition 15 (*Universal Composable (UC) Security [234–239]*). A protocol Π^R UC-realizes an ideal functionality Π^I if for every PPT adversary $\mathcal{E}_R$ even in the presence of arbitrary concurrent protocol executions $\{\Pi_i\}_i$ there exists a PPT simulator $\mathcal{E}_S$ such that for every PPT environment $\mathcal{Z}$, $\mathcal{Z} \circ \mathcal{E}_{\mathcal{R}}(\Pi^R, \{\Pi\}_i) \sim_{\epsilon(n)} \mathcal{Z} \circ \mathcal{E}_S(\Pi^I, \{\Pi\}_i)$, that is

$$\left| \Pr\left[\mathcal{Z} \circ \mathcal{E}_R \left(\Pi^R, \{\Pi\}_i \right) = 1 \right] - \Pr\left[\mathcal{Z} \circ \mathcal{E}_S \left(\Pi^I, \{\Pi\}_i \right) = 1 \right] \right| \leq \epsilon(n). \tag{35}$$

Here, the environment $\mathcal{Z}$ is allowed arbitrary interactions with all components (including Π as a subroutine, and any other concurrently running protocols $\{\Pi_i\}_i$), and the security guarantee must hold regardless of the surrounding context and any efficient environment. In the context of DI-QKD, this indistinguishability principle is operationalized via the following question: *Can Eve distinguish whether she is interacting with the real protocol executed with untrusted, potentially malicious quantum devices, or with an ideal protocol that outputs a uniformly random secret key independent of her side information?* If no efficient test exists that can tell the difference, then the protocol is deemed secure. The security of the protocol is ensured by the fact that Eve's intervention breaks the expected equivalence, which is detected in the security check step of Box 1 (Section 1.3.1) through the *lack* of BI violation.

3.2. Bell inequalities bound eavesdropper's knowledge

The *statistical security check step* notifies Eve's presence. Indeed, her action with the protocol is modeled by a non-signaling distribution $p = \prod_{i=1}^n p_{A^1B^1E^1|X^1Y^1Z^1}(a_i, b_i, e_i|x_i, y_i, z_i)$, or among n rounds with $p = p_{A^nB^nE^nT|X^nY^nZ^n}(\{a_i, b_i, e_i\}_i, t| \{x_i, y_i, z_i\}_i)$ including $T = \{(a_i, b_i, x_i, y_i), \text{hash}\}_i$ and hash is the collection of post-processing functions for error correction and privacy amplification. The simulator's job (security proof) is then to construct a hypothetical ideal non-signaling distribution p^I that matches Eve's observations, but where the secret key is perfectly secure. It must hold for any possible initial non-signaling distribution p where only the marginal $\boldsymbol{p} = p_{AB|XY}$ is used by Alice and Bob for the *security check* that estimate Eve's knowledge by a function of the Bell value (e.g. (12)) $f[\beta_{\mathcal{Q}}(\boldsymbol{p})]$. Given that, a DI-QKD protocol can be realized as a transformation of the form

$$p \mapsto \Pi_{K_A^n, K_B^n, f, T, E^n | X^n Y^n Z^n} \tag{36}$$

and it is sub-routine that satisfy UC-security [240] (35) when warrantees that the composed scheme that uses QKD is secure as if an ideal secret key were used instead

$$\sum_{K_A, K_B, t} \max_z \sum_e |p^R_{K_A, K_B, T, E|Z} - p^I_{K_A, K_B, T, E|Z}| = \mathcal{O}(1/N), \qquad p^I_{K_A K_B T E | Z} = \frac{1}{2^{N_S}} \delta_{k_A, k_B} p^R_{TE|Z}. \tag{37}$$

Th transformation (36) captures the operational steps of the protocol in Box 1 of Section 1.3.1. Importantly, this modular perspective separates the description of the protocol from the security proof: the protocol defines how the classical and quantum data are processed, while the security proof (the simulator) analyzes the transformation's outcome under the appropriate assumptions. This modularity highlights that the protocol structure can be independently specified without requiring the proof to be embedded in its definition. However, each protocol is secure by simulating an adversary constrained to perform specific attacks [29].

Definition 16 (*Simulation Attacks*). Given a global probability distribution $\boldsymbol{p}$ during the data generation step, an attack is simulated by computing Eve's knowledge about the outcome, let us say, b if Bob measures $Y = y_1$, by the optimal guessing probability

$$p_{\text{g}}(b|E) = \max_z \sum_e \boldsymbol{p}, \qquad \boldsymbol{p} = \begin{cases} p_{B^1E^1|Y^1Z^1}(b, e|y = y_1, z), & \text{individual} \\ \prod_{i=1}^n p_{A^1B^1E^1T|X^1Y^1Z^1}(a_i, b_i, e_i, t|x_i, y_i, z_i), & \text{collective} \\ p_{A^nB^nE^nT|X^nY^nZ^n}(\{a_i, b_i, e_i\}_i, t|\{x_i, y_i, z_i\}_i), & \text{coherent} \end{cases} \tag{38}$$

- *Individual attack* − before the public discussion (PD), Eve tries to guess at each round performing an identical operation on each qubit on the quantum channel and keeps only classical information Z. Shannon entropy measures p_g;

- *Collective attack* — after the PD the protocol Π^R has already generated the keys k_A, k_B and Eve's can read all the public discussion in T. Memorylessness via space-like separation (Definition 8) of devices *at each run* implies the factorization. Eve keeps quantum information but still performs the same operation on every round. Von Neumann entropy measures p_g
- *Coherent attack* — Eve has a (classical or quantum) memory to correlate inter-round communication. To measure p_g see Section 5.
- *Non-signaling attack* (a.k.a known as *post quantum attack*) — Eve can prepare p^λ, where λ is a post-quantum state allowing correlations stronger than quantum, as shown in Fig. 5(c).

Though memorylessness is impractical, in reality, Alice and Bob reuse single devices with a refresh routine to cancel memory effects. However, confined Eve to quantum collective attacks is already far weaker than (non-DI) QKD assumptions, because all these attacks are bounded by a functional f of the Bell value $P_g(b|E) < f[\beta_Q(\boldsymbol{p})]$ regardless of how $\boldsymbol{p} = p_{AB|XY}$ is produced.

Proposition 3. *Given a specific power to Eve that fix the simulation, a real and an ideal protocol Π^R Π^I satisfy a given simulation security iff $p_g(b|E) < f[\beta_Q(\boldsymbol{p})]$ with $\boldsymbol{p} \in \mathcal{NS} \setminus \mathcal{L}$.*

Apart from protocol in Ref. [71] that shows a security proof in a post-quantum theory, let us relate p_g with theoretical information quantities within quantum theory.

Definition 17. Let $\rho_{BE} = \sum_b p_b |b\rangle\langle b| \otimes \rho_{b|E} \in \mathcal{B}(\mathcal{H}_B \otimes \mathcal{H}_E)$ a cq-state the quantum,

- conditional min-entropy of B given E is (last equality for binary outcomes):

$$H_{\min}(B|E)_\rho := \sup\{\lambda > 0 : 2^{-\lambda}\mathbf{1}_B \otimes \sigma_E - \rho_{BE} \succeq 0, \ \sigma_E \in \mathcal{B}(\mathcal{H}_E)\} = -\log_2 p_g(b|E) \tag{39}$$

- Conditional ϵ-smoothed min-entropy [108], $\varepsilon \in [0, 1]$ is

$$H_{\min}^\varepsilon(B|E)_\rho := \sup_{\tilde\rho_{BE} \in \mathcal{B}^\varepsilon(\rho_{BE})} H_{\min}(B|E)_{\tilde\rho} = -\log \inf_{\tilde\rho \in \mathcal{B}_\varepsilon(\rho_{BE})} \inf_{\sigma_E \in \mathcal{B}(\mathcal{H}_E)} \| \ \tilde\rho_{BE}^{\frac{1}{2}} \sigma_E^{-\frac{1}{2}} \ \|_\infty^2, \tag{40}$$

$$\mathcal{B}_\varepsilon(\rho_E) = \{\tilde\rho | \tilde\rho \succ 0, \operatorname{Tr}\tilde\rho < 1, \sqrt{1 - \|\sqrt{\rho_{BE}}\sqrt{\tilde\rho}\|_1^2} \le \varepsilon\}. \tag{41}$$

$H_{\min}(B|E)$ is a worst-case entropy measure used for UC-security proofs. It quantifies Eve's maximum ability to guess Bob's value b given access to the quantum system E, by bounding ρ_{BE} above by a scaled product state $\mathbb{I}_B \otimes \sigma_E$. The smoothed version $H_{\min}^\varepsilon(B|E)_\rho$ accounts for finite-size effects by optimizing over subnormalized states $\tilde\rho$ within purified distance ε of ρ_{BE}. Operationally, $H_{\min}^\varepsilon(K|E)_\rho$ determines the maximum number of secret bits extractable from raw data K, secure against an adversary holding E, up to error ε. Unlike von Neumann entropy, which captures average uncertainty, smoothed min-entropy provides tight bounds reflecting worst-case adversarial knowledge.

Proposition 4. *In the iid asymptotic limit, this entropy converges (after smoothing) to the conditional von Neumann entropy:*

$$\lim_{\varepsilon \to 0} \lim_{n \to \infty} \frac{1}{n} H_{\min}^\varepsilon(B^n|E^n) = H(B|E), \qquad H(B|E) = H(\rho_{BE}) - H(\rho_E), \quad H(\rho) = -\operatorname{Tr}\rho \log \rho,$$

where the von Neumann entropy $H(\rho)$ generalized the Shannon entropy $H(X) = -\sum_i p_X(x_i) \log_2 p_X(x_i)$ of a classical variable X with probability distribution p_X.

$H_{\min}^\varepsilon(K|E)_\rho$ is related to the achievable key length, i.e. the number of uniform secret bits that can be extracted from the raw key K, given the adversary's quantum side information E, up to ε. In the finite-key regime, the secret key rate r and the extractable key length ℓ are bounded as

$$r = \eta\frac{\ell}{n}, \qquad \ell \le H_{\min}^\varepsilon(K|E)_\rho - \text{leak}_{EC} - \mathcal{O}(\log\frac{1}{\varepsilon}) = \begin{cases} n(1 - h(\text{QBER})) - \mathcal{O}(\log\frac{1}{\varepsilon}) & \text{QKD} \\ n(1 - h(\text{QBER}) - f(\beta_Q)) - \mathcal{O}(\log\frac{1}{\varepsilon}) & \text{DI-QKD} \end{cases} \tag{42}$$

where h is the binary entropy, leak_{EC} accounts for information revealed during error correction, $\eta = \eta_{\text{link}} + \eta_d$ modifies the effective number of rounds contributing to key generation where $\eta_l = 10^{-ad}$ represents line losses (transmittivity) over a distance d with attenuation coefficient a and η_d is the efficiency of the detectors (see Section 7). The last equality holds for one-way error correction and ideal privacy amplification[12] . $f(\beta_Q)$ upper bounds Eve's information as a function of $\beta_Q(\boldsymbol{p})$ such that $\boldsymbol{p} \in \mathcal{Q} \setminus \mathcal{L}$. The QBER may still appear due to experimental imperfections, or alternatively the bound

---

[12] In one-way postprocessing "error correction and privacy amplification" T flows only from Bob to Alice or vice-versa, efficient in terms of secret key rate; in two-way postprocessing "advantage distillation" T flows from both Alice and Bob. This is inefficient for small errors but tolerating larger errors (see 3.4.2).

Table 1
Summary of DI-QKD protocols. QT: quantum theory; p_g: Eve's guessing probability of k_i, the sifted bit; 1-w: one-way public discussion (PD); UC: universal composite security; r: secure key rate; CV: continuous variables; η^* = critical efficiency. We discuss the advanced security proof started from 2014 in Section 5.

Protocol	Description
E91 3.3 [53]	Within QT, E91 uses CHSH for secrecy without quantifying p_g
BHK "05 3.4.1 [71]	p_g via post-quantum individual attacks is bounded by chain inequality, but no rate is computed.
CHSH "06 3.4.2 [34,72]	First key rate r is computed bounding p_g via post-quantum individual attacks using CHSH and CGLMP in 1w and 2w PD.
Chain "06 3.4.3 [69]	Improvement of r bounding p_g via post-quantum individual attacks enlarging Bell scenario in 1w PD via chain inequality (UC-security [240], CV version [241] in "14).
$CHSH_\chi$ "07 3.5 [70]	Improvement of r bounding p_g obtained with post-quantum collective attacks via Holevo quantity χ in 1-w PD (rigorous proof in "09 [73], UC-secure in "09 [242]).
$CHSH_{p_g}$ "10 3.6 [76,77]	r improved bounding p_g in 1-w PD from coherent attacks (only independent devices assumed — memory attacks "13 [78]) via H_{min} achieving Q = 7.1% ($\beta_Q = 2.423$). 2-w PD secure in "20 [84], $\eta^* = 0.891$.
$CHSH_T$ "20 3.7 [243]	Implement Entropy Accumulation theorem (EAT) (see Section 5) for the bound on r robust under coherent attacks reducing $\eta^* = 0.832$.
$CHSH_\ell$ "13 3.8 [79]	Detection loophole is closed by performing a CHSH test entirely within Alice's lab using causally independent devices.
CH-SH "21 3.9 [86,87]	p_g bounded from refined CHSH data using either asymmetric expressions or full "$(X = CH, Y = SH)$" statistics; both improve r and match $\eta^* = 0.826$.
$CHSH_{IMD}$ "21 3.10 [85]	Rényi-like quantities — the iterated-mean divergences — to with tighter entropy bounds than previous numerical techniques.
$CHSH_{2e}$ "21 3.11 [88]	r improved by doubling the events for the raw key in a single round under quantum collective attacks in 1-w PD achieving Q = 8.2% ($\beta_Q = 2.362$).
$CHSH_{p\mathcal{V}_p}$ "22 3.12 [89]	r improved under quantum collective attacks using random postselection of raw key bit in 1-w PD, reducing the effect of no-detection events. $\eta^* = 0.685$ 5.
MPG "23 3.13 [91]	A protocol based on the Mermin–Peres magic square game, surpassing CHSH-based approaches in regimes of high state visibility and detection efficiency.
rDI-QKD "24 3.14 [92–97]	Introduces routing-based Bell tests to enable long-range DI-QKD; security relies on witnessing long-range nonlocality. Routed Bell inequalities certified even under loss or weak detection, achieving critical efficiency $\eta_{A_1} > 1/2$, with exponential robustness in parallel repetition.

may depend only by β_Q. The *secret key rate r* is defined as the number of secret bits extracted per use of the quantum channel. In the asymptotic limit, it reduces to the Devetak–Winter bound

$$r \geq \sup_T I(A:B) - I(A:E) = \sup_T H(K|E) - H(K|B), \tag{43}$$

showing consistency between one-shot and large-scale QKD analyses. I is the mutual information and T represents *preprocessing*[13]

In the next, we discuss the developments and the ideas in the variants of protocol in Box 1 listed in Table 1. We are interested on the *data generation* and the *statistical security check* to focus only on the term $f(\beta_Q)$ in Eq. (42) since the *raw key validation*, that involves perfect correlated outcomes, is the same of all QKD protocols. Recall that in DI-QKD Eve controls the source and the fabrication of Alice and Bob's devices, therefore for the users the preparations and measurements becomes merely input and output classical labels.

3.3. Ekert (1991) — bell inequality for secrecy without bound

E91 is the first quantum key distribution (QKD) protocol leveraging Bell inequality violation for security [53], but with no bound on Eve's knowledge.

Protocol — *Data generation.* Alice and Bob select $x, y \in \{0, 1, 2\}$ obtaining $a, b \in \{0, 1\}$. In QT $M_{A|x} = \{\Pi_{0|x}, \Pi_{1|x}\}$ and $N_{B|y} = \{\Pi_{0|y}, \Pi_{1|y}\}$:

$$\Pi_{a|x} = U_{\theta_x}|a\rangle\langle a|U_{\theta_x}^\dagger, \quad U_\theta = e^{-i\frac{\theta}{2}\sigma_y}, \quad \theta_{x=(0,1,2)} = \left(\frac{\pi}{2}, \frac{\pi}{4}, 0\right), \quad \theta_{y=(0,1,2)} = \left(\frac{\pi}{4}, 0, -\frac{\pi}{4}\right). \tag{44}$$

PD and raw key validation. They publicly announce x, y. For $(x, y) = (0, 2)$ they evaluate $\beta_Q(\boldsymbol{p})$ and abort if $\beta_Q(\boldsymbol{p}) \leq 2$. But when settings match: $(x, y) = (1, 0) \vee (2, 1)$, they use the outcomes to extract the key. If they share $|\phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ they exploit perfect outcome correlations.

---

[13] In QKD, preprocessing denotes any local operation applied to the raw key *before* information reconciliation and privacy amplification, with the aim of improving security or noise tolerance. For the specific noisy-preprocessing scheme used in this work, see Section 3.7.

Security − in the absence of eavesdropping, E91 predicts $\beta_{\mathcal{Q}}(\boldsymbol{p}) = 2\sqrt{2}$. If Eve attempts to eavesdrop, she must interact with the system, inevitably introducing disturbances that degrade the observed nonlocal correlations. Any such unnoticed tampering constrains the statistics $\boldsymbol{p}$ to admit a local hidden variable (LHV) model, for which $\beta_{\mathcal{Q}}(\boldsymbol{p}) \leq 2$. More precisely, all LHV strategies can be written as convex mixtures over deterministic outcomes defined by hidden variables n_a, n_b:

$$\langle A_x B_y \rangle = \int \rho(n_a, n_b)(a_x \cdot n_a)(b_y \cdot n_b)\, \mathrm{d}n_a \mathrm{d}n_b.$$

This class of models forms the local polytope $\mathcal{L}$, and defines the boundary of what is attackable without to be noticed. Hence, a violation $\beta_{\mathcal{Q}}(\boldsymbol{p}) > 2 \implies \boldsymbol{p} \notin \mathcal{L}$ guarantees no eavesdropper.

Although the E91 protocol does not address the detection loophole caused by no-click events (see Section 2.4.1), it pioneered the principle that a Bell inequality violation enables secrecy independently of device trust, by certifying entanglement without assuming a specific Hilbert space structure. This insight paved the way to later protocols that guarantee security even beyond quantum correlations, i.e., for behaviors $\boldsymbol{p} \in \mathcal{NS} \setminus \mathcal{Q}$.

More recently, proofs based on the (Generalized) Entropy Accumulation Theorem have established a rigorous, finite-size, composable security proof of E91 against coherent attacks. For details of this analysis and explicit bounds, we refer the reader to Section 5.2.1.

3.4. DI-QKD secure against no-signaling adversaries

We start with presenting the earliest DI-QKD protocols that achieve security against a general non-signaling adversary — that is, an eavesdropper constrained only by the no-signaling principle, rather than by the laws of quantum mechanics (see Definition 16). These adversaries may exploit post-quantum correlations, including those stronger than any quantum strategy, provided they do not enable faster-than-light communication. Security proofs in this regime rely on monogamy properties of non-local correlations, typically quantified via Bell inequality violations. The protocols discussed here preceded the development of entropy-based techniques and thus typically achieve limited key rates, but they remain important foundational milestones in the theory of device-independent cryptography.

3.4.1. Barrett–Hardy–Kent (2005) — bound on Eve's knowledge without positive rate

Once the correlations $\boldsymbol{p} \notin \mathcal{L}$ are information-theoretic resource [71] a protocol the first protocol is derived with a security proof (against collective no-signaling) bounding Eve's knowledge with $f[\beta_{\mathcal{Q}}(\boldsymbol{p})]$ but without computing the secrete key rate [71].[14]

Protocol. *Data generation* – Alice and Bob select $x, y \in \{0, \ldots, m-1\}$ obtaining $a, b \in \{0, 1\}$. In QT $M_{A|x} = \{\Pi_{0|x}, \Pi_{1|x}\}$ and $N_{B|y} = \{\Pi_{0|y}, \Pi_{1|y}\}$:

$$\Pi_{a|x} = U_x |a\rangle \langle a| U_x^\dagger, \qquad U_x = e^{-i\frac{\pi x}{2m}\sigma_y}.$$

PD and raw key validation – given $n = Mm^2$ with $M \in \mathbb{N}$, the protocol continues if

(i)

$$2Mm \leq \sum_{x=0}^{m-1} \sum_{c=-1}^{1} \mathcal{M}_{x,c}, \qquad \mathcal{M}_{x,c} := \left| \left\{ j : X_j = x, Y_j = x + c \right\} \right|. \tag{45}$$

(ii) $\forall j = 1, \ldots, s-1, s+1, \ldots, \mathcal{M}_{x,c}$ rounded that reveals the outcomes $(X_j, Y_j) = (x, x+c)$

(iii) Let $X_j \in \{0, \ldots, m-1\}$ Alice's input at round j and Bob's input $Y_j \in \{x-1, x, x+1\}$ for a given $X_j = x$. For all j the following BI (a variant of the chained Bell inequality [177,244]) must be violated:

$$\beta_j(\boldsymbol{p}^\lambda) = \frac{1}{3m} \sum_{c=-1}^{1} \sum_{x=0}^{m-1} p^\lambda(a_j = b_j \mid X_j = x, Y_j = x + c) \leq 1 - \frac{2}{3m} \tag{46}$$

The outcomes are kept private only for a designated setting pair $(X_s, Y_s) = (x, x+c)$, with $c \in \{-1, 0, 1\}$. The secret bit is then derived from the outcomes of this unrevealed round, defined as $a_s = b_s$.

Security Proof. For her collective attack Eve prepares a post-quantum state λ so that she keeps a subsystem for her and 2n subsystems where at each run Alice and Bob believe to share a state as in E91. Thus, λ defines joint probability distributions $p^\lambda_{A^n B^n E X^n Y^n Z}$, where $X^n = (X_1, \ldots, X_n)$, $Y = (Y_1, \ldots, Y_n)$ are the players' measurement choices, and $E = \{E_1\}$ is Eve's *time-independent* measurement. This means that Eve's choice and statistics do not depend on the players' measurement rounds, preventing adaptive attacks. Otherwise, the theory would be pathological, even if it respects the no-signaling principle [245].

---

[14] Ref. [71]. Tested in QT, it uses anticorrelation from $|\psi\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$, here we keep $|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ as in E91.

Then, for any partition $X = X^1 \cup X^2$, $Y = Y^1 \cup Y^2$, and $E = E^1 \cup E^2$, the no-signaling condition (see Eq. (7)) imposes:

$$p^\lambda_{X^1 Y^1 E^1} = p^\lambda_{X^1 Y^1 E^1 | X^2 Y^2 E^2}.$$

This expresses that no local measurement on one subsystem can transmit information to a distinct subsystem.

Let $(X_j, Y_j) = (x, y)$ be a random measurement pair chosen with uniform probability $1/m^2$, yielding outcomes $(a_j, b_j) \in \{0, 1\}^2$. From (46):

$$\beta_j(\boldsymbol{p}^\lambda) \leq 1 - \frac{2}{3m} \equiv \beta_{\mathcal{L}}(m) \implies \boldsymbol{p}^\lambda \in \mathcal{L}, \qquad \beta_j(\boldsymbol{p}^\lambda) = 1 - \mathcal{O}(1/m^2) \equiv \beta_{\mathcal{NS} \setminus \mathcal{L}}(m) \implies \boldsymbol{p} \notin \mathcal{L}. \tag{47}$$

For $m \gg 1$, the gap $\beta_{\mathcal{NS} \setminus \mathcal{L}}(m) > \beta_{\mathcal{L}}(m)$ is detectable, computed either:(i) using the Born rule in QT: $p^\lambda(a, b \mid x, y) = \mathrm{Tr}\left[\rho_\lambda \left(\Pi_{a|x} \otimes \Pi_{b|y}\right)\right]$, or in any no-signaling probability model (Hahn–Banach theorem[15]): $p^\lambda(a, b \mid x, y) \in \mathcal{NS} \setminus \mathcal{Q}$.

This gap is used to infer limits on Eve's knowledge. Specifically, she cannot simultaneously satisfy: (a) Passing the Bell test (i.e., the protocol does not abort), (b) Possessing high confidence in the value of the secret bit $a_s = b_s$.

Lemma 2. *If the protocol passes with probability $p^\lambda(\text{pass}) > \epsilon$, then the correlation of the secret bit is bounded:*

$$1 - \frac{1}{2Mm\epsilon} < p^\lambda(a_s = b_s \mid \text{pass}). \tag{48}$$

From (48), the no-signaling constraint and chain rule:

$$1 - \frac{1}{2Mm\epsilon} < \beta_s(\boldsymbol{p}^\lambda). \tag{49}$$

The maximum probability that Eve guesses correctly that $a_s = b_s$ (the secret bit), conditioned on her outcome e, for a fixed input setting pair $(x, x + c)$ p^λ_g, defined as:

$$p^\lambda_g(b|E) := \max_e p^\lambda(a_s = b_s \mid X_s = x, Y_s = x + c, e),$$

Assume that Eve has partial information about the secret bit. That is, there exists an outcome e_0 occurring with probability $\delta > 0$ (i.e. how likely it is for Eve to land on a "lucky" outcome — one that gives her some knowledge), such that her guessing probability is strictly better than random:

$$p^\lambda_g(b|E = e_0) = p^\lambda(a_s = b_s \mid X_s = x, Y_s = x + c, e_0) > \frac{1 + \delta'}{2}, \qquad \delta' > 0.$$

δ' is the bias in Eve's knowledge, i.e., how much better than random she is at guessing the secret bit when she obtains outcome e_0.[16] This implies that the conditional distribution $p^\lambda(a_s, b_s \mid X_s = x, Y_s = x + c, e_0)$ is biased towards equal outcomes, allowing Eve to guess $a_s = b_s$ with success probability greater than $1/2$.

Proof. From the derivation in [71], one can use the triangle inequality and the no-signaling property to propagate this bias across the chained Bell expression. The result is a *reduction* in the observed Bell value:

$$\beta^\lambda_s(\boldsymbol{p}) \leq 1 - \frac{\delta \delta'}{3m},$$

where the factor $\delta \delta'/3m$ quantifies the average amount of correlation that is lost due to Eve's biased knowledge. On the other hand, if the protocol passes (i.e., the observed Bell value is high), we have a previously established lower bound (49) from Lemma 2, which assumes that the test was passed with probability at least ϵ. We now reach a contradiction if both bounds are applied at once. Specifically, if:

$$\frac{1}{2Mm\epsilon} < \frac{\delta \delta'}{3m} \implies \text{Contradiction:} \quad p^\lambda_g > \frac{1 + \delta'}{2} \quad \text{is incompatible with} \quad \beta^\lambda_s(\boldsymbol{p}) > 1 - \frac{1}{2Mm\epsilon}.$$

In short, if the observed value of the chained Bell parameter is high enough, Eve's guessing probability must remain close to $1/2$, meaning she gains vanishing information about the secret bit. Thus, we can write the final conclusion as:

$$p^\lambda_g \leq f(\beta^\lambda_s) := \frac{1}{2} + \mathcal{O}\left(1 - \beta^\lambda_s\right),$$

where f is a function that decreases as the BI violation increases, and vanishes as $m \to \infty$ [173,246]. $\square$

However, this protocol has zero key rate (defined in Section 3.4.2) ascribing correlations with noiseless states. In the following protocol, we describe a more practical scheme, but without tackling the most powerful adversary. It was proposed in [34] (extended version [72]) and improved with higher noise tolerance and key rate in [69].

---

[15] Exists always an hyperplane that separate a point from a convex set such as $\mathcal{L}$ and $\mathcal{Q}$ (both contained in $\mathcal{NS}$).

[16] By considering both δ and δ', the bound becomes robust and general. Even if Eve's knowledge is good but rare (large δ', small δ), or frequent but weak (small δ', large δ), the product $\delta \delta'$ controls her effective information.

3.4.2. CHSH protocol (2006) − from polytopes to positive rates

The idea is to generate a protocol from the geometry of $\mathcal{L}$, $\mathcal{Q}$, $\mathcal{NS}$ and the specific Eve's attacks. In fact, suppose that Eve prepare $\lambda = \sum_i c_i \lambda_i$ such that $\boldsymbol{p}^\lambda \in \mathcal{NS}$ [34,71]. If Alice and Bob observe a Bell violation (e.g., $\beta > \beta_\mathcal{L}$), then: $\boldsymbol{p}^\lambda = \sum_i c_i \boldsymbol{p}^{\lambda_i} \notin \mathcal{L}$. So at least one λ_i must generate a distribution $\boldsymbol{p}^{\lambda_i} \notin \mathcal{L}$. But this alone does not guarantee security: such $\boldsymbol{p}^{\lambda_i}$ could still be *deterministic* or even *signaling*. This leads to three possibilities:

- $\boldsymbol{p}^{\lambda_i} \in \mathcal{L} \Longrightarrow$ contradiction as no BI violation is observed;
- $\boldsymbol{p}^{\lambda_i} \in \mathcal{NS} \setminus \mathcal{L}$. Eve's hidden variable λ_i is no-signaling but nonlocal. Such correlations are monogamous: Nonlocality cannot be shared *freely* with a third party without violating no-signaling [71,246]. Therefore, Eve cannot simultaneously reproduce the nonlocal statistics between Alice and Bob and retain side-information allowing her to predict outcomes. Otherwise, her model would allow signaling. Let us explain what *freely* means:

  1. Given $|\text{EPR}\rangle_{AB}$, $|\text{EPR}\rangle_{AC}$, $|\text{EPR}\rangle_{BC}$, the state of the 3 subsystems we cannot really talk about tripartite entanglement because the correlations are always between any two of the three parties. When Alice and Bob share $\rho_{AB} = |\text{EPR}\rangle\langle\text{EPR}|_{AB}$, being a pure maximally entangled state, it has eigenvalues $\lambda_1 = 1$ and $\lambda_k = 0$ ($k > 1$). For Uhlmann theorem any $\rho_{ABC} = \rho_{AB} \otimes \rho_C$ still has eigenvalues $\lambda_1 = 1$ and $\lambda_k = 0$ ($k > 1$), but the Schmidt rank across the partition AB : C is 1, thus $\rho_{AB|C}$ is not entangled, hence cannot share any correlation with $|\text{EPR}\rangle_{AB}$, not only that, the subsystem C does not know nothing about A since $\rho_{AC} = \frac{1}{2} \otimes \rho_C$.
  2. Given $|\text{GHZ}\rangle_{ABC} = \frac{1}{2}(|000\rangle + |111\rangle)$ this has genuine entanglement in all the partition AB : C, AC : B, BC : A but the entanglement is not maximal if one qubit is dropped, e.g. ρ_{AB} is separable.

  Consider a *3-players CHSH game*. The referee selects 2 players to perform the *CHSH game* of Section 2.1. If Alice is selected, she does not know who will be her partner. Therefore, she does not know what to choose $|\text{EPR}\rangle_{AB}$ or $|\text{EPR}\rangle_{AC}$. Or maybe $|\text{GHZ}\rangle_{ABC}$? But its marginals ρ_{AC}, ρ_{AB} are separable. Therefore the classical strategy is also the quantum one.

- $\boldsymbol{p}^{\lambda_i} \notin \mathcal{NS}$. If Eve uses such a λ_i, the associated strategy enables faster-than-light signaling. This is physically excluded: such distributions violate relativistic causality [247] (see Figs. 2(c) and 5(d)).

Let us study the simplest scenario with $x, y \in \{0, 1\}$, $a, b \in \{0, 1\}$, and individual attacks

$$p_{ABE|XYZ} = p_{E|XYZ} p_{AB|XYZE} = p_{E|Z} p_{AB|XYZE} \tag{50}$$

such that

$$p(ab|xy) = \sum_e p(abe|xyz) \sum_e p(ab|xyze)p(e|z). \tag{51}$$

The no-signaling condition in Eq. (7) is applied in $p_{E|XYZ} = p_{E|Z}$. Being $\mathcal{NS}$ a convex polytope, $p_{AB|XYZE}$ can be expressed as a convex combination of extremal points, but in Eq. (50), $p_{AB|XYZE}$ is taken extremal because individual attacks satisfy two key properties:

  (i) the interconvertibility property [171,172] ensures that extremal points $p(ab|xyze)$ describe the most general individual attack;
  (ii) local operations and public communication between Alice and Bob do not enhance their security.

For binary a, b the extreme points $\{p_{AB|XYZE}\} = \boldsymbol{p}_{\text{ext}} \in \mathcal{NS}$ are fully characterized (binary input [172,173], arbitrary input [171]). For binary input and output Eve's strategy is sketched in Fig. 2(c). Let us analyze it in detail.

Proposition 5. *For $\boldsymbol{p} \in \mathcal{NS}$ with binary input and output the no-signaling conditions requires that $\sum_a p(ab|xy) = p(b|y)$ and $\sum_b p(ab|xy) = p(a|x)$ so that*

  (i) *$\exists \boldsymbol{p}_{\text{NL}} = \frac{1}{2}\delta_{a\oplus b, yx}$ isotropic correlation (as in Fig. 2(b) with $v = 1$) know as Popescu–Rohrlich–Tsirelson box [173,248,249], or nonlocal machine [250], or unit of nonlocality [171,172] and it is the vertex on the top in Fig. 2(c)*

$$\boldsymbol{p}_{\text{NL}} = \begin{array}{|c|c|c|c|c|} \hline ab\backslash xy & 00 & 01 & 10 & 11 \\ \hline 00 & 1/2 & 1/2 & 1/2 & 0 \\ \hline 01 & 0 & 0 & 0 & 1/2 \\ \hline 10 & 0 & 0 & 0 & 1/2 \\ \hline 11 & 1/2 & 1/2 & 1/2 & 0 \\ \hline \end{array} \tag{52}$$

  (ii) *As in Fig. 2(c), $\exists$ 8 extreme points $\boldsymbol{p}_{\text{L}}^{j,r}$ with entries $p_{\text{ext}}(ab|xy) = \delta_{a,\lambda_A(x)}\delta_{b,\lambda_B(y)}$ (satisfying 1) s.t. $\beta_\uparrow = 3$ defined as*

$$\boldsymbol{p}_{\text{L}}^{j,r} : (x, y) \in \{0, 1\}^2 \mapsto \{0, 1\}^2 \ni \boldsymbol{p}_{\text{L}}^{j,r}(x, y) = (a(x), b(y)) \tag{53}$$

  where at each $j \in \{1, \ldots, 4\}$, and $r = 0, 1$ the output $(a(x), b(y))$ are

$\boldsymbol{p}_{\text{L}}^{1,0}$	$\boldsymbol{p}_{\text{L}}^{1,1}$	$\boldsymbol{p}_{\text{L}}^{2,0}$	$\boldsymbol{p}_{\text{L}}^{2,1}$	$\boldsymbol{p}_{\text{L}}^{3,0}$	$\boldsymbol{p}_{\text{L}}^{3,1}$	$\boldsymbol{p}_{\text{L}}^{4,0}$	$\boldsymbol{p}_{\text{L}}^{4,1}$
$(0, 0)$	$(1, 1)$	$(x, 0)$	$(x + 1, 1)$	$(0, y)$	$(1, y + 1)$	$(x, y + 1)$	$(x + 1, y)$

$$\tag{54}$$

for example

$$
\boldsymbol{p}_{\mathrm{L}}^{1,0} =
\begin{array}{|c|c|c|c|c|}
\hline
ab\backslash xy & 00 & 01 & 10 & 11 \\
\hline
00 & 1 & 1 & 1 & 1 \\
\hline
01 & 0 & 0 & 0 & 0 \\
\hline
10 & 0 & 0 & 0 & 0 \\
\hline
11 & 0 & 0 & 0 & 0 \\
\hline
\end{array}
, \quad
\boldsymbol{p}_{\mathrm{L}}^{4,1} =
\begin{array}{|c|c|c|c|c|}
\hline
ab\backslash xy & 00 & 01 & 10 & 11 \\
\hline
00 & 0 & 0 & 1 & 0 \\
\hline
01 & 0 & 0 & 0 & 1 \\
\hline
10 & 1 & 0 & 0 & 0 \\
\hline
11 & 0 & 1 & 0 & 0 \\
\hline
\end{array}
, \quad etc.
\tag{55}
$$

(iii) If $\boldsymbol{p} \in \mathcal{L} \implies$ Eve knows a_0, a_1, b_0, b_1

(iv) If Alice and Bob would observe $\boldsymbol{p} = \boldsymbol{p}_{\mathrm{NL}} \implies$ Eve cannot be correlated (perfect monogamy [173])

To mimic the marginal $\boldsymbol{p} = p_{AB|XY}$ of Eq. (51) observed by Alice and Bob, Eve's optimal attack $\boldsymbol{p}_{\mathcal{E}}$ with entries $\{p(abe|xyz)\}$ from Eq. (50) then consists of the combination of the 9 extreme points with the minimal $p_{\mathrm{NL}} = 1 - p_L = 2v - 1$ (see Fig. 2(c)):

$$
\boldsymbol{p}_{\mathcal{E}} = \sum_{j=1}^{4} \sum_{r=0}^{1} p_j^r \boldsymbol{p}_{\mathrm{L}}^{j,r} + p_{NL}\boldsymbol{p}_{NL}, \quad \text{with} \quad \sum_{j=1}^{4} \sum_{r=0}^{1} p_j^r = p_L.
\tag{56}
$$

We label the Eve input $z \in \{1, \ldots, 9\} \mapsto \{v_i\}$ with $\{v_i\} \in \{\boldsymbol{p}_{\mathrm{L}}^{j,r}\} \cup \{\boldsymbol{p}_{\mathrm{NL}}\}$ which provides the following knowledge $e \in \{(a, b), (a, ?), (?, ?)\}$ at given x and y. Then, resulting marginal probability distribution $p(ab|xy) = \sum_e p(abe|xyz)$ reads as

$$
\begin{array}{|c|c|c|c|c|}
\hline
ab\backslash xy & 00 & 01 & 10 & 11 \\
\hline
00 & \frac{p_{\mathrm{NL}}}{2} + \sum_{j \neq 4} p_j^0 & \frac{p_{\mathrm{NL}}}{2} + \sum_{j \neq 3} p_j^0 & \frac{p_{\mathrm{NL}}}{2} + p_1^0 + p_3^0 + p_4^1 & p_1^0 \\
\hline
01 & p_4^0 & p_3^0 & p_2^1 & \frac{p_{\mathrm{NL}}}{2} + p_2^1 + p_3^0 + p_4^0 \\
\hline
10 & p_4^1 & p_3^1 & p_2^0 & \frac{p_{\mathrm{NL}}}{2} + p_2^0 + p_3^1 + p_4^0 \\
\hline
11 & \frac{p_{\mathrm{NL}}}{2} + \sum_{j \neq 4} p_j^1 & \frac{p_{\mathrm{NL}}}{2} + \sum_{j \neq 3} p_j^1 & \frac{p_{\mathrm{NL}}}{2} + p_1^1 + p_3^1 + p_4^0 & p_1^1 \\
\hline
\end{array}
\tag{57}
$$

From the bipartite distribution $p(ab|xy)$ in (57) the best procedure to extract the secret key is unknown. The CHSH protocol [34,72] is a good candidate because it provides high correlations between Alice and Bob and reduces Eve's information. From (57) we see that Alice and Bob are highly anticorrelated only for $x = y = 1$. It is therefore natural to devise the following procedure that transforms these anticorrelations into correlations (see tutorial [20]), this is done in the *Pseudosifting* step, which is the only variant from Box 1 to discuss.

CHSH protocol (*Pseudosifting*) − Alice reveals $x = 0$ or $x = 1$ and Bob without announcing the value of y, if $(x, y) = (1, 1) \implies b \mapsto \bar{b}$. The anticorrelation becomes correlations and the distribution $p(ab|xy)$ in Eq. (57) is updated to $p(ab|x = 0, y = k)$ and $p(ab|x = 1, y = k)$ conditioned to the knowledge of x and outcome probability $p(y = k) = \xi_k$.

$$
\begin{array}{|c|c|}
\hline
ab & x = 0, \; p(y = k) = \xi_k \\
\hline
00 & \frac{p_{\mathrm{NL}}}{2} + p_1^0 + p_2^0 + \xi_0 p_3^0 + \xi_1 p_4^0 \\
\hline
01 & \xi_1 p_3^0 + \xi_0 p_4^0 \\
\hline
10 & \xi_1 p_3^1 + \xi_0 p_4^1 \\
\hline
11 & \frac{p_{\mathrm{NL}}}{2} + p_1^1 + p_2^1 + \xi_0 p_3^1 + \xi_1 p_4^1 \\
\hline
\end{array}
\qquad
\begin{array}{|c|c|}
\hline
ab & x = 1, \; p(y = k) = \xi_k \\
\hline
00 & \frac{p_{\mathrm{NL}}}{2} + \xi_0 p_1^0 + \xi_1 p_2^1 + p_3^0 + p_4^1 \\
\hline
01 & \xi_1 p_1^0 + \xi_0 p_2^1 \\
\hline
10 & \xi_1 p_1^1 + \xi_0 p_2^0 \\
\hline
11 & \frac{p_{\mathrm{NL}}}{2} + \xi_0 p_1^1 + \xi_1 p_2^0 + p_3^1 + p_4^0 \\
\hline
\end{array}
\tag{58}
$$

To maximize Eve's uncertainty $\xi_k = 1/2$. An interesting property for the pseudosifting about all the eight local points is that Alice's outcome a from Eq. (53) is always known to Eve because x is publicly announced, and if one $\boldsymbol{p}_{\mathrm{L}}$ provides the knowledge of b to Eve for $x = 0$, the same point leaves Eve ignorant for $x = 1$ and vice-versa. For example, given Eve's strategy in (56) she knows (a, b) if she sent out $\boldsymbol{p}_{\mathrm{L}}^{1,0}$ (with probability p_1^0) and Alice announces $x = 0$, then $\forall y \in \{0, 1\} \implies b = 0$. In this case, Eve's uncertainty on Bob's symbol is null, we write it as $H(b|E = \boldsymbol{p}_{\mathrm{L}}^{1,0}, x = 0) = 0$. But if Eve sent out $\boldsymbol{p}_{\mathrm{L}}^{1,0}$ and Alice announces $x = 1$, then $y = 0 \implies b = 0$ and $y = 1 \implies \bar{b} = 1$. Since Eve does not know y the uncertainty is maximum $H(b|E = \boldsymbol{p}_{\mathrm{L}}^{1,0}, x = 1) = 1$. Because of pseudosifting, she does not know if Bob's outcome is $b = 0$ or $\bar{b} = 1$, and at the same time, the outcomes are correlated $a = b$ when $x = y = 1$. Given the above distributions $p(ab|x = 0, y = k)$ and $p(ab|x = 1, y = k)$ in Eq. (58), then $p(a \neq b|0) = \frac{1}{2}(p_3^0 + p_3^1 + p_4^0 + p_4^1) \equiv e_{AB|0}$ and $p(a \neq b|1) = \frac{1}{2}(p_1^0 + p_1^1 + p_2^0 + p_2^1) \equiv e_{AB|1}$ (with $\xi_k = 1/2$). Then Eve's uncertainty on b is the conditional Shannon entropy:

$$
H(B|E, X) = \sum_e P(E = e, X = x)H(b|E = e, X = x) = 1 - 2e_{AB|x+1},
\tag{59}
$$

with fixed $x \in \{0, 1\}$ and e determined by the values of z that chooses the strategies $\{v_i\} = \{\boldsymbol{p}_{\mathrm{L}}^{j,r}, \boldsymbol{p}_{\mathrm{NL}}\}$. This is the first evidence of an analogue of quantum mechanical uncertainty relations in a generic no-signaling theory. The pseudosifting process is optimized to extract correlations from the nonlocal strategy $\boldsymbol{p}_{\mathrm{NL}}$, but it also affects deterministic strategies differently. In particular, for $\boldsymbol{p}_{\mathrm{L}}^{1,r}$ and $\boldsymbol{p}_{\mathrm{L}}^{2,r}$, pseudosifting yields no errors when $x = 0$, and Eve fully learns Bob's outcome

b, since $b(y)|_{y=0} = b(y)|_{y=1} = a$. However, when $x = 1$, errors occur in half of the cases, and Eve gains no information about b, as $b(y)|_{y=0} \neq b(y)|_{y=1}$. The reverse holds for $\boldsymbol{p}_\mathrm{L}^{3,r}$ and $\boldsymbol{p}_\mathrm{L}^{4,r}$ [72].

Quantitative security. To compute the key rate, the so-called *depolarization procedure* (individual attacks) transform w.l.o.g. Eve's strategy of Eq. (56) into the isotropic distribution (cf. Appendix C of [72])

$$\boldsymbol{p}_\mathcal{E} = p_L \mathbf{1} + p_\mathrm{NL} \boldsymbol{p}_\mathrm{NL}, \quad \text{with } p_j^r = \frac{p_L}{8}.$$

This leads to the probability distributions in Eq. (58)

$$p(ab|x = 0, y = k) = p(ab|x = 1, y = k) = \sum_e p(abe|X = x, Y = k, z = \boldsymbol{p}_\mathcal{E}),$$

and the tripartite distribution:

$$p(abe|0, k, \boldsymbol{p}_\mathcal{E}) = \begin{array}{|c|c|c|c|}
\hline
ab \backslash e & (?, ?) & (a, ?) & (a, b) \\
\hline
00 & \frac{p_\mathrm{NL}}{2} & \frac{p_L}{8} & \frac{p_L}{4} \\
\hline
01 & 0 & \frac{p_L}{8} & 0 \\
\hline
10 & 0 & \frac{p_L}{8} & 0 \\
\hline
11 & \frac{p_\mathrm{NL}}{2} & \frac{p_L}{8} & \frac{p_L}{4} \\
\hline
\end{array} \tag{60}$$

One-way classical postprocessing. – The tapescript $T(q)$ flow goes from Alice to Bob and from the distribution in (60) Bob's error probability is $\epsilon_\mathrm{AB} = p_L/4$, after preprocessing, the quantity to be corrected in error correction is $e'_\mathrm{AB} = (1 - q)e_\mathrm{AB} + q(1 - e_\mathrm{B})$ while Eve's information is $I(A : E) = p_L/2(1 - h(q))$. Therefore Eq. (43) yields [20]

$$r(D) = \max_{q \in [0, 1/2]} \left(1 - h(e'_\mathrm{AB}) - \frac{p_L}{2}(1 - h(q)) \right), \quad \text{with } p_\mathrm{NL} = \sqrt{2}(1 - 2D) - 1. \tag{61}$$

The critical disturbance D characterizes the properties of the channel linking Alice and Bob. $r(p_\mathrm{NL}) > 0$ is obtained with optimal preprocessing at $p'_\mathrm{NL} \gtrsim 0.236$ ($D \lesssim 6.3\%$) and without preprocessing at $p''_\mathrm{NL} \gtrsim 0.318$.

Since $\boldsymbol{p}_\mathcal{E}(p_\mathrm{NL}) \in \mathcal{Q} \iff p_\mathrm{NL} \leq \sqrt{2} - 1 \simeq 0.414$, both $p'_\mathrm{NL}, p''_\mathrm{NL} \in \mathcal{Q}$ (see Fig. 8(a)).

Definition 18 (*Bell Limit*). A family of distributions $\boldsymbol{p} = p(ab|xy)$ reach the Bell limit if leads to a secret key $r > 0$ for any amount of nonlocality.

Remark 1. In the case of $p_1^0 = p_2^0$, $p_1^1 = p_2^1$, and $p_3^r = p_4^r = 0$, even neglecting preprocessing $p_\mathrm{NL} > 0 \implies r = 1 - \frac{h(p_L/2)}{2} - \frac{p_L}{2} > 0$. Notice that, $\exists \boldsymbol{p}$ reaching the Bell limit, despite the fact $\boldsymbol{p} \notin \mathcal{Q}$ hence it cannot be broadcasted using quantum preparations (solid orange line in Fig. 8(a)). Indeed $\mathcal{L} \subsetneq \mathcal{Q} \subsetneq \mathcal{NS}$ and $\sum_{j,r} p_j^r \boldsymbol{p}_\mathrm{L}^{j,r} = 0 \iff \forall p_j^r = 0$ (see Ref. [72] sec.III.E.3).

Only in 2024, Refs. [98] show a protocol that for $\boldsymbol{p} \in \mathcal{Q}$ a quantum strategy reaches the Bell limit extending the BI scenario beyond CHSH. Exploiting a family of d-outcome Bell inequalities and the additivity of the von Neumann entropy, they obtained the analytic relation $H(A|E) = H(A)$, which gives the key-rate bound $r \geq \log d$, so that $\log d$ bits of secret key can be extracted for every integer $d \geq 3$. In other words, *unbounded DI key rates can be certified from correlations exhibiting arbitrarily small non-locality*. Wooltorton et al. [251] obtained the same result by examining a family of three-parameter Bell inequalities [149], whose maximal quantum violations self-test a unique state and measurement settings. Within this family, there exist nonlocal correlations — across a range of CHSH violations, including those arbitrarily close to the classical bound — that exhibit the remarkable property of producing outputs arbitrarily close to a perfect key for a specific pair of inputs. Additionally, they extended this result by demonstrating the existence of quantum correlations capable of generating both perfect key and perfect randomness simultaneously, while exhibiting arbitrarily small CHSH violations.

Two-way classical postprocessing: repetition code advantage distillation. – In two-way postprocessing, no optimal procedure or tight bound analogous to Eq. (43) is known. The most common method, *Advantage Distillation* (AD) [239,252,253], especially in the form of repetition-code AD, say that

$$\exists \tilde{B}, \tilde{E} \text{ s.t. } I(A : B) < I(B : E) \overset{AD}{\Longrightarrow} I(\tilde{A} : \tilde{B}) > I(\tilde{B} : \tilde{E}) \tag{62}$$

enabling one-way postprocessing on $\tilde{B}, \tilde{E}$. While repetition-code AD is often introduced as a classical two-way step, the so-called B-step from entanglement purification is typically described in terms of bilateral CNOT operations. However, as explained in Section 6.1 of [254], these quantum operations can be commuted with the final measurements and reduce to classical parity (XOR) operations on the raw data [253]. Thus, repetition-code AD and the B-step are operationally equivalent at the level of classical data processing, even though their derivations originate from different viewpoints. Below, we follow the AD terminology for consistency.

In AD, Alice publicly reveals N instances where her bits are equal, i.e., $a_{i_1} = a_{i_2} = \cdots = a_{i_N} = a$. Bob checks his corresponding bits and announces whether all his bits are also equal. If Bob's bits are all equal, Alice and Bob keep one of these instances, (a_{i_k}, b_{i_k}); otherwise, they discard the N instances. The error rate between Alice and Bob after this process, denoted as $\tilde{e}_{AB}$, becomes exponentially smaller:

$$\tilde{e}_{AB} = \frac{e_{AB}^N}{(1 - e_{AB})^N + e_{AB}^N},$$

where e_{AB} is the initial error rate between Alice and Bob. As $N \to \infty$, $\tilde{e}_{AB} \to 0$, meaning that Alice and Bob almost always share identical bits after a sufficiently large number of instances.

The probability that Eve makes an error on Bob's symbols after AD is approximated by

$$\tilde{e}_E \gtrsim C[f(e_{AB})]^N,$$

where $f(\cdot)$ is a function that depends on the probability distribution and C is a constant. As long as the condition $f(e_{AB}) > e_{AB}/(1 - e_{AB})$ is satisfied, Eve's error increases exponentially with N. There is always a finite value of N such that Eve's error becomes greater than Bob's, ensuring that a secret key can be extracted.

The bound on the tolerable error after AD is derived by solving this inequality and provides the necessary condition for secrecy extraction. Without preprocessing $p_{NL} \gtrsim 0.2$; with preprocessing (allowing Alice and Bob to flip some bits before AD) $p_{NL} \gtrsim 0.09$ [239]. It remains an open question if in two-way postprocessing, a Bell limit can be reached. Although one might consider that a two-way communication would increase interceptions, overall AD is more noise tolerant (lower p_{NL}) than one-way post-processing, by iteratively improving correlations and discarding mismatched rounds to reduce error rates. Preprocessing enhances this by scrambling Eve's knowledge before AD.

Intrinsic information. Given a tripartite probability distribution $\tilde{\boldsymbol{p}} = \{p_{ABE|XYZ}(abe|xyz)\}_{a,b,e}$, the intrinsic information $I_\downarrow = I(A : B \downarrow E) = \min_{E \to \bar{E}} I(A : B|\bar{E}) \geq r$ [255]. This upper bound represents the mutual information between Alice and Bob conditioned on Eve's knowledge. $I_\downarrow < 0 \implies r = 0$ witness the impossibility of secret correlations in $\tilde{\boldsymbol{p}}$. The vice-versa is unknown [256–258]. Furthermore, $\exists \, \tilde{\boldsymbol{p}}$ with a $I_\downarrow > 0$ but $r = 0$, indicating the presence of bound information (similarly to bound entanglement). While bound information has been proven in multipartite settings, its existence in bipartite scenarios remains unknown.

For the CHSH protocol, $I(A : B|E) = p_{NL}$ when Alice and Bob are perfectly correlated (see Fig. 8(b)). In other cases, they are uncorrelated. A conjectured optimal map for minimizing this conditioned mutual information is introduced, supported by numerical evidence giving

$$I_\downarrow = (1 - p_L/2)[1 - h(p_L/(4 - 2p_L))]. \tag{63}$$

This conjectured intrinsic information remains positive for $p_{NL} > 0$, which leads to two possibilities: (i) $r > 0 \, \forall \tilde{\boldsymbol{p}} \notin \mathcal{L}$ (ii) In the Bell limit ($p_{NL} \simeq 0$) $\tilde{\boldsymbol{p}}$ might represent bipartite bound information.

The CHSH protocol in quantum theory (Alice and Bob share a quantum state of two qubits, agreeing on specific measurements, while Eve holds a purification) is shown to be equivalent to the BB84 protocol with added classical preprocessing, having the same robustness to noise. However, BB84 achieves a higher secret key rate at low error rates but cannot be used for device-independent proofs, as its security becomes compromised if the Hilbert space dimensionality is unknown.

Then how to improve the rate in DI-QKD? For example, CHSH protocol admits larger-dimensional outcomes generalization using CGLMP inequalities with more extractable secrecy as the outcomes increase (see Ref. [72] sec.IV) or via chain BI (Section 3.4.3). The former is a tight family of BI, while chain BI, though not tight, can be efficiently implemented in the next protocol (see definition 3 for tight BI).

3.4.3. Chain protocol (2006) — enlarged Bell scenario

The previous protocol considered the simplest CHSH scenario with inputs and outputs $x, y, a, b \in \{0, 1\}$, providing a preliminary step towards key-rate estimation. In this section, we begin by revisiting a slightly extended CHSH-based analysis, where Alice's input x can take three values, $x \in \{0, 1, 2\}$. We then generalize this setting to the more powerful chained Bell inequalities (CHAIN), introduced in [69], which offer improved key rates and greater noise tolerance while remaining secure against individual no-signaling adversaries.

(3,2)–CHSH protocol. *Data generation.* Alice selects $x \in \{0, 1, 2\}$ with probability $q, (1 - q)/2, (1 - q)/2$, Bob selects $y \in \{0, 1\}$ with probability $q', 1 - q'$. They obtain $a, b \in \{0, 1\}$. In QT $M_{A|x} = \{\Pi_{0|x}, \Pi_{1|x}\}$ and $N_{B|y} = \{\Pi_{0|y}, \Pi_{1|y}\}$:

$$\Pi_{a|x} = U_{\theta_x}|a\rangle\langle a|U_{\theta_x}^\dagger, \quad U_\theta = e^{-i\frac{\theta}{2}\sigma_z}, \quad \theta_{x=(0,1,2)} = \left(\frac{\pi}{4}, 0, \frac{\pi}{2}\right), \quad \theta_{y=(0,1)} = \left(\frac{\pi}{4}, -\frac{\pi}{4}\right). \tag{64}$$

acting on the Werner state ρ_W of Fig. 2(b) with $P_+ = |\phi^+\rangle\langle\phi^+|$.

PD and raw key validation. They publicly announce x, y. For $x \in \{1, 2\}$ they evaluate $\beta_{\downarrow Q}(\boldsymbol{p}) = 2 - \sqrt{2}p$ and abort if $\beta_{\downarrow Q}(\boldsymbol{p}) \geq 1$. When the settings unmatch: $(x, y) = (0, 1)$, the outcomes are uncorrelated and they reject the round, instead

(a) *CHSH protocol*   (b) *Intrinsic information in CHSH protocol*
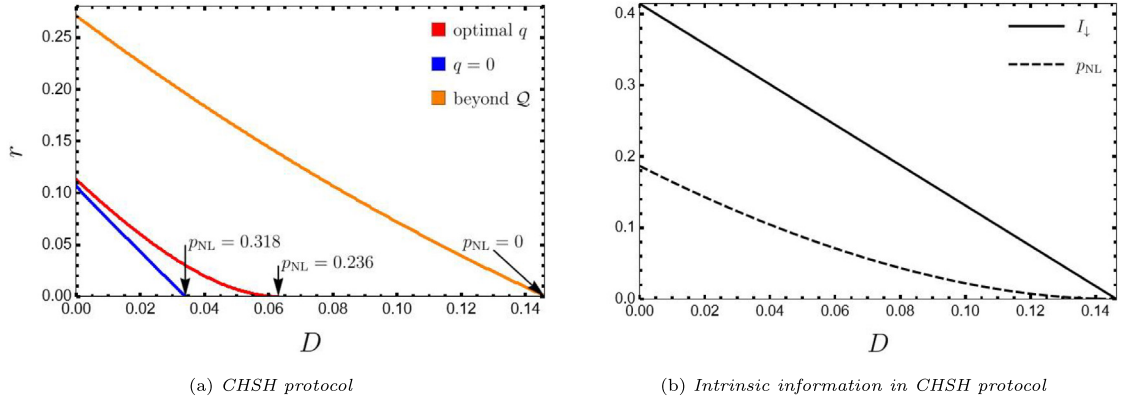
Fig. 8. Key rate versus noise in individual attack − In 8(a), key rate for one way PD of Eq. (61), with preprocessing (red); without preprocessing (blue); without preprocessing, but using a distributions compatible with CHSH protocol but that cannot be broadcasted using quantum states. In 8(b) Eq. (63) is positive $\forall p_{\mathrm{NL}}$.

Table 2
Eve's extremal strategies for $(x, y) = (0, 0)$ with probability p_i (details in [69]).

	Strategies	S_*	$\langle C \rangle_\rho$	$H(A|E)$	$H(B|E)$	$I(A : B|E)$
p_1	(D,D)	≥ 1	≤ 1	0	0	0
p_2	(D,R)	≥ 0	0	0	1	0
p_3	(R,R)	≥ 0	≤ 1	1	1	1

for $(x, y) = (0, 0)$ they quantify the correlation $\langle C \rangle_\rho \equiv P(a_0 = b_0) - P(a_0 \neq b_0) = v$ and extract the key. If they share $|\phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ they exploit perfect outcome correlations.

Security In Eve's strategy [69], for each Alice's measurement, there might be output: predetermined (D) $p(a|x) = \delta_{a, \lambda_A(x)}$ or uniformly random (R) $p(a|x) = 1/2$. Similarly for Bob. If $y = 0$ is (D), then all the measurements are (D). Eve's strategies can be classified as in Table 2 into three sets, according to whether $(x, y) = (0, 0)$ yields predetermined (D) or uniformly random outcomes (R). For each strategy a bound on the *security check* $\beta_{\downarrow\mathcal{Q}}(\boldsymbol{p})$ and *raw key validation* $\langle C \rangle$ is computed:

$$r \geq \sqrt{2}v - 1 - h\left(\frac{1 + v}{2}\right), \qquad r \leq I_\downarrow \leq \langle C \rangle_\rho - \beta_{\downarrow\mathcal{Q}}(\boldsymbol{p}) = (1 + \sqrt{2})v - 2. \tag{65}$$

Proof. (1) From Table 2, $I(B : E) \leq I(A : E)$ then the privacy amplification goes from Bob to Alice, thus $r = I(A : B) - I(B : E)$. The mutual information is $I(A : B) = 1 - h(\frac{1+v}{2})$, where h is the binary entropy and

$$I(B : E) = H(B) - \sum_{k=1}^{3} p_k H_k(B|E) = p_1 \leq \beta_{\downarrow\mathcal{Q}}(\boldsymbol{p}), \quad \text{where } H(B) = 1. \tag{66}$$

This follows from $p_k \geq 0$, $\sum_k p_k = 1$ and measured values of $\beta_{\downarrow\mathcal{Q}}(\boldsymbol{p})$ and $\langle C \rangle$.

(2) The intrinsic information $I_\downarrow$ is upper-bounded, since $I(A : B \downarrow E) \leq I(A : B|E)$, thus $I_\downarrow \leq \sum_{k=1}^{3} p_k I_k(A : B|E) = p_3$. Additionally $p_1 + p_3 \geq \langle C \rangle_\rho$ concludes the proof. □

Whether a key can be extracted from such data, and if it can, what is the best protocol for achieving it, remains an open challenge.

(M+1,M)– chain protocol. As the performance depends on the BI, a generalization extends from $(3, 2) \to (M + 1, M)$ settings

$$\theta_{x=0} = \frac{\pi}{2M}, \quad \theta_{x>0} = \frac{x\pi}{2M}, \qquad \theta_y = -\frac{\pi(y + 1/2)}{M}, \text{ for } x, y = 1, \ldots, M. \tag{67}$$

Similarly, for $(x, y) = (0, 0)$ the measurement gives highly correlated bit used for the secret key, the other choices are used to violate the chain BI (used in (47) with a quantum state ρ_{AB} from a post-quantum tripartite λ) from [177,244,260] based on Franson interferometer [261] where it is known [262,263] that the CHSH is insufficient as a security test. Full security can be reestablished with [264,265]

$$\beta_{\downarrow\mathcal{Q}}^M(\boldsymbol{p}) = \sum_{i=1}^{M} (p(a_i \neq b_{i-1}) + p(a_i \neq b_i)) = \begin{cases} 2(M - 1) & \boldsymbol{p} \in \mathcal{L} \\ M\left(1 - v\cos\left(\frac{\pi}{2M}\right)\right) & \boldsymbol{p} \notin \mathcal{L} \end{cases} \tag{68}$$

(a) $(3, 2)$–CHSH vs. CHSH protocol rate   (b) $(M, M + 1)$–chain protocol rate
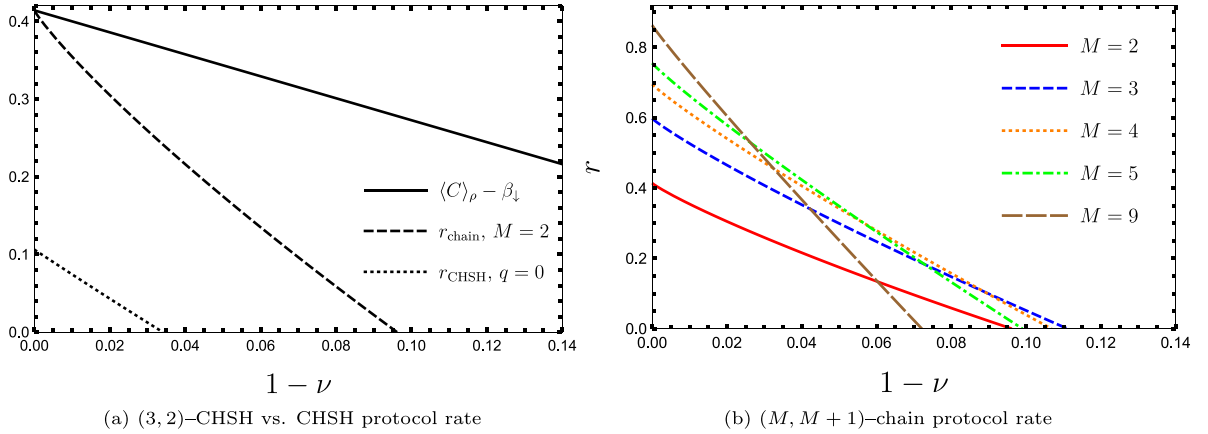
Fig. 9. In 8(a) the rate of $(3, 2)$-CHSH protocol in Eq. (65) vs. the rate of CHSH protocol without preprocessing where $1 - \nu$ in ρ_W in 2(b) in one-way communication protocols bounded via $\beta_{\downarrow Q}(\boldsymbol{p})$ of Eq. (12). If Eve saturates the inequalities of Table 2 the rate is saturated. Without noise $r|_{\nu=1} \geq \sqrt{2} - 1 \simeq 0.414$ and $r = 0$ for $\nu = 0.9038$; upper-bounded by intrinsic information $I_\downarrow$ using two-way key distillation protocols [255] For $\nu = 2/(1 + \sqrt{2}) \simeq 0.8284 \implies r \leq I_\downarrow = 0$, however CHSH is violated for $p \geq 0.7071$ always with $I_\downarrow > 0$ [259]. In 9(b) Eq. (69) generalized $M = 2$.

where $b_M \equiv b_0 = 1 \mod 2$. One-way privacy amplification lower bounds as (see Fig. 9(b))

$$r_M \geq 1 - h\left(\frac{1+\nu}{2}\right) - M\left(1 - \nu \cos\left(\frac{\pi}{2M}\right)\right). \tag{69}$$

A variant with pre-processing from Ref. [266] improves the noise-resistance. For M increase, $r_M \gtrsim 1 - \pi^2/8M$ and $\boldsymbol{p} = \sum_i c_i \boldsymbol{p}_i$ become maximally non-local with any local component: Eve must always use non-local strategies for which has zero knowledge about Bob's outcome $I(B : E) = 0$ (see end of Section 3.4.1). Each BI provides a different estimation of Eve's knowledge so that for M large, the corresponding protocols are very sensitive to noise, but in the absence of noise, Alice and Bob extract one secret bit per e-bit asymptotically. For a post-quantum and quantum individual attacks, the maximal value of the resistance to noise are respectively $\nu = 0.86$ and $\nu = 0.75$. However, the chain protocol originally did not take into account the detection loophole that would lower such values to certify security (see Section 2.4.2) nor collective attacks, but nowadays we know the following.

Theorem 1. $\forall p_{A,B,E|X,Y,Z}$ *there always exists* hash *such that the transformed distribution* $P_{K_A,K_B,BI,T,E|Z}$ *via the* $(M+1, M)$–chain *protocol is universal composable secure* [240].

3.5. CHSH$_\chi$ protocol secured by Holevo quantity

Instead of extending the Bell scenario, to improve the key rate, a tighter bound that relates β_Q with Holevo quantity χ, itself related to $p_g(B|E)$ can be derived against *quantum* collective attacks [70,73]. Specifically, given n the number of instances, the state prepared by Eve is the same at each instance $|\Psi\rangle = |\psi\rangle^{\otimes n} \in \mathcal{H}_{ABE}$ and Alice and Bob receive $\rho_{AB} = \text{Tr}_E(|\Psi\rangle\langle\Psi|) = \sum_c p_c \rho_{AB}^c$ without unknowing dim $\mathcal{H}_{AB}$ for Alice and Bob similarly to Eqs. (50)–(51) for individual attacks. Because of *Jordan's lemma* 1 (any pair of binary measurements can be decomposed as the direct sum of pairs of measurements acting on two-dimensional spaces) $\rho_{AB}^c \in \mathcal{B}(\mathbb{C}^2 \otimes \mathbb{C}^2)$ without restrictions. At each ρ_{AB}^c, the classical ancilla c known to Eve determines which measurements Alice and Bob choose.

CHSH$_\chi$ protocol. *Data generation*. The same as CHSH protocol (Section 3.4.2), but a variant allows Bob's choices $y \in \{0, 1\}$ (or $y \in \{0, 1, 2\}$ as in E91 3.3 and [80]) so that $M_{A|0} = N_{B|1} = \sigma_z$, $N_{B|2} = \sigma_x$, $M_{A|x} = (\sigma_z \pm \sigma_x)/\sqrt{2}$ for $x = 1, 2$; the raw key is extracted from the pair $(x, y) = (0, 1)$, and QBER $= Q = p(a \neq b|01)$ (from Eq. (4)).

Security 1 way PD. As detailed in [70,73] (see Section 5.6) Eq. (43) valid for in the asymptotic $n \to \infty$ one-way public discussion (PD) gives,

$$r_{\text{CHSH}} = 1 - h(Q) - h\left[\frac{1}{2} + \frac{1}{2}\sqrt{\left(\frac{\beta_Q}{2}\right)^2 - 1}\right] \leq r_{\text{BB84}} = 1 - h(Q) - h\left(\frac{\beta_Q}{2\sqrt{2}} + Q\right), \quad \beta_Q = 2\sqrt{2}(1 - 2Q). \tag{70}$$

Eq. (70) is obtained as $r = I(a : b|x = 0, y = 1) - \max\{I(a : E|x = 0), I(b : E|y = 1)\}$ where $I(a : b|x = 0, y = 1) = 1 - h(Q)$ is computed assuming uniform marginals and $\max\{I(a : E|x = 0), I(b : E|y = 1)\} = \chi(b : E|y = 1)$ (PD from

(a) *CHSH protocol improvement* (b) *CHSH protocol vs detection efficiency*
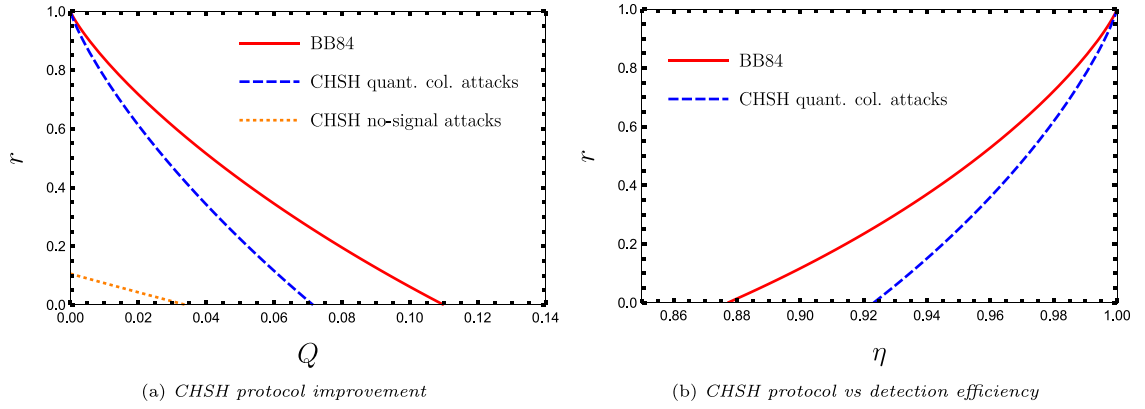
Fig. 10. In 10(a) *Key rate versus noise–* The noise in orange dotted line is $Q = D$ as in Eq. (61) obtained for the CHSH protocol under no-signaling individual attacks. Within quantum collective attacks, r_{CHSH} is enhanced in Eq. (70) (dashed blue) and compared with standard QKD BB84 (solid red). In 10(b) $Q = \eta(1-\eta)$ and $\beta_Q = 2\sqrt{2}\eta^2 + (1-\eta)^2$ following the discussion below Eq. (26).

Alice to Bob) can be tightly upper bounded by the binary entropy h

$$\chi(b:E|y=1) \equiv H(\rho_E) - \frac{1}{2}\sum_{b=0}^{1} H(\rho_{E|b}) \leq h\left[\frac{1}{2} + \frac{1}{2}\sqrt{\left(\frac{\beta_Q}{2}\right)^2 - 1}\right] \equiv \chi_0(\beta_Q). \tag{71}$$

The Holevo quantity upper bounds the amount of classical information (about the variable b (when $y = 1$) that can be extracted by any measurement on the quantum state $\rho_{E|b}$. In other words, if you encode classical information b in quantum states $\rho_{E|b}$, then the accessible information (mutual information between b and the outcome of any measurement E is at most $\chi(b:E|y=1)$. The expression is valid for $\beta_Q > 2$.[17] In short, r_{CHSH} of Eq. (70) reads as

$$r = 1 - h(Q) - \chi_0(\beta_Q). \tag{72}$$

Eve's guessing measurement p_G^M. If Eve has some probability p_g^M of making a correct guess on the choice of measurement settings (a flag $f = 1$ so that she fixes a priori the players' outcomes engineering

$$\beta'_Q(\boldsymbol{p}) = 4p_g^M + (1 - p_g^M)\beta_Q(\hat{\boldsymbol{p}}), \text{ to mimic } \beta'_Q(\boldsymbol{p}) \in [2, 2\sqrt{2}] : p_g^M \in [0, \sqrt{2} - 1], \tag{73}$$

(otherwise her guess is uncorrelated, $f = 0$), then Eq. (72) becomes [267],

$$r = 1 - h(Q) - p_g^M - (1 - p_g^M)\chi_0(\beta'_Q) \tag{74}$$

To take into account the detection loophole, the key rate in Eqs (74) must be computed on $\hat{\boldsymbol{p}}$ rather than the ideal $\boldsymbol{p}$ (with $\eta_A = \eta_B = 1$) as discussed in Eq. (25) of Section 2.4.1, therefore for $\eta_A = \eta_B = \eta$, $Q = \eta(1-\eta)$ and $\beta(\hat{\boldsymbol{p}}) = 2\sqrt{2}\eta^2 + 2(1-\eta)^2$ ($\langle M_{A|0}\rangle = \langle N_{B|0}\rangle = 0$ in Eq. (26)) .

Fig. 11(a) shows $r \to 0 \implies \eta > 0.924$ at $p_g^M = 0$.

A variant of $CHSH_\chi$ protocol that instead of $M_{A|0} = \{M_{a|0}\}_{a=0}^{1}$ assume $M_{A|0} = \{M_{a|0}\}_{a=0}^{3}$ reduces $\eta^* = 0.909$ [268]. Ref. [269] shows an analogue of Eq. (70) for coherent attacks with memoryless measurement devices.

$CHSH_\chi$ protocol vs. BB84. For the entanglement-based BB84, r_{BB84} in Eq. (70) has $\chi'(b:E|y=1) \leq h(\beta_Q/(2\sqrt{2}) + Q)$ with β_Q computed on $\rho_{AB} = \sum_{j=\pm}(1 + jC)/2|\Phi_j\rangle\langle\Phi_j|$, where $C = \sqrt{(\beta_Q/2)^2 - 1}$ is the concurrence that maximize β_Q at a given amount of entanglement. The measurements defined by Eve are σ_z, σ_x, fr $y = 1, 2$, and $\frac{1}{1+C^2}\sigma_z \pm \frac{C}{1+C^2}\sigma_x$ for $x = 1, 2$. Under collective attack, with this realization (state and settings), $CHSH_\chi$ protocol saturates Holevo bound and BB84 turns out *unsafe*. Indeed, not only ρ_{AB}, but also guessing Alice's measurements depend explicitly on the observed values β_Q and Q.

CV - $CHSH_\chi$ protocol. The encoding of $CHSH_\chi$ protocol (see Section 3.5 and [70]) is possible with continuous variable (CV) [241]. Typically, CV adopts Gaussian states that alone cannot violate a BI [270]. As a result, non-Gaussian states or measurements are necessary, though they are harder to produce experimentally. This poses challenges for developing a CV-based version of DI-QKD, as most current CV-QKD protocols rely on Gaussian states. This challenge, however, can be addressed by utilizing, for instance, a single mode of the electromagnetic field as the harmonic oscillator by *GKP encoding* (Gottesman, Kitaev, Preskill): embedding a two-level Hilbert space into the full infinite-dimensional space [271]. A qubit

---

[17] Note that in Section 3.4.3 $\beta_{\downarrow Q} = 2 - \sqrt{2}p$, then $\beta_Q C = 2\sqrt{2}p$, then $Q = (1 - p)/2$.
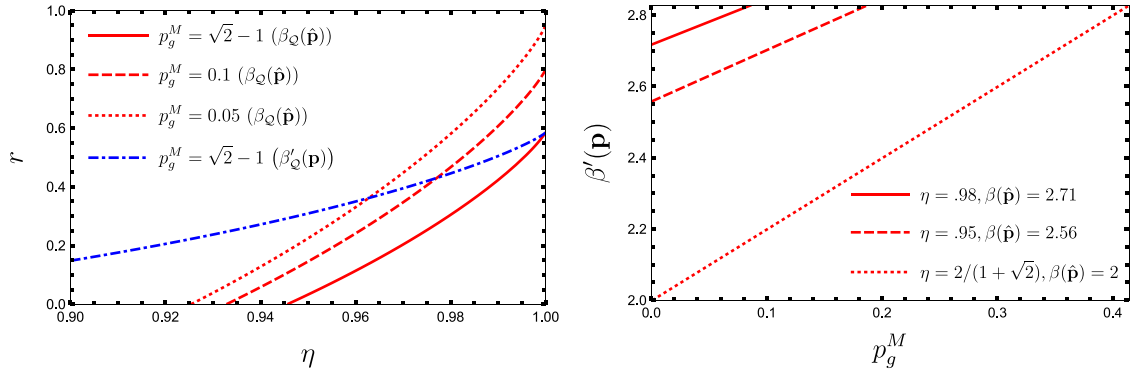
Fig. 11. In 11(a) − Eve's guessing probability p_g open the detection loophole (dash-dotted blue line) where $\beta_\mathcal{Q}(\hat{\boldsymbol{p}}) = 2$, but $\beta'_\mathcal{Q}(\boldsymbol{p}) \in (2, 2\sqrt{2}]$. To close this loophole for large values of p_g a higher critical detection efficiency η^* is required. In 11(b) higher is $\beta_\mathcal{Q}(\hat{\boldsymbol{p}})$ less manoeuvre is left to Eve to mimic BI violation by $\beta'_\mathcal{Q}(\boldsymbol{p})$.

is encoded in the infinite-dimensional space of an oscillator, allowing protection against arbitrary but small shifts in the canonical variables such as position and momentum.

However, this result is possible in 2-input and 2-output scenarios thanks to the *qubit reduction argument* (Jordan's lemma). Do similar results exist for more complex scenarios for m measurements of d outcomes [152]? Along this line, some progress for $n = 2, m \to \infty$ in [272,273] conjectured in [274].

We analyzed CHSH protocol under the no-signaling attack and recalled it CHSH_χ under quantum collective attacks by related the key rate to Holevo quantity χ. In the next section, instead, the key rate is obtained via $H_{\min} = -\log_2 p_g$ as we discussed above, and we recall the protocol CHSH_{p_g}.

3.6. CHSH_{p_g} protocol − bounding the attacks with $H_{\min}$ assuming independent measurement devices

It is remarkable to highlight the issues due to memory effects in the data generation [78]. **CHSH_{p_g} protocol**. *Data generation*. Alice and Bob select $x, y \in \{1, \dots, M\}$ to generate a raw key $K_A = K_B \in \{0, 1\}^n$ with $n = M$ via separate pair of commuting measurements [76,77]

$$[M_{a|x}, N_{b|y}] = 0, \qquad [M_{a|x}, M_{a'|x'}] = [N_{b|y}, N_{b'|y'}] = 0, \quad x, y = 1, \dots, M. \tag{75}$$

The commutation relations can be satisfied by either using the devices in parallel where the n bits of the raw key are generated by n separate and non-interacting devices or using in a sequential way in which the raw key is generated by repeatedly performing measurements provided that the functioning of the devices do not depend on any internal memory storing the quantum states and measurement results obtained in each round so that $\boldsymbol{p}$ has only one entry

$$p(a_1, \dots, a_N, b_1, \dots, b_N | x_1, \dots, x_N, y_1, \dots, y_N) = \text{tr}\left(\rho_{AB} \prod_{i=1}^{N} M_{a_i|x_i} N_{b_i|y_i}\right), \tag{76}$$

where $\rho_{AB} = \text{tr}_E(\rho_{ABE})$. After Alice's n systems have been measured, $\rho_{AE} = \sum_{\boldsymbol{a}} p(\boldsymbol{a}|\boldsymbol{x}_{raw})|\boldsymbol{a}\rangle\langle\boldsymbol{a}| \otimes \rho_{E|a}$ where $\rho_{E|a}$ is the reduced state of Eve conditioned on Alice measuring outcome $\boldsymbol{a}$[18] In the protocol Alice always uses a particular measurement x_{raw} (call it a_0) to produce the sifted key bit.

Security 1 way PD [76,77]. After PD Eve possesses some (possibly huge-dimensional) quantum system E. Whatever coherent processing she performs, she must end with a single classical guess $\hat{a} \in \{0, 1\}$ for Alice's bit a_0. In each round Eve wants to maximize her success probability $p_{\text{succ}} = p(\hat{a} = a_0 \mid x_{raw})$. The best she can do is always output the most likely value of a_0. Therefore the optimal success probability is $p_g = \max_{a \in \{0,1\}} P(a \mid x_{raw})$, (For a binary outcome variable this coincides with the operationally meaningful smooth min-entropy $H_{\min}(A|E) = -\log_2 p_g$ as expressed in Eq. (39)). Because the two outcomes are encoded as ± 1, p_g can be rewritten as $p_g = (1 + |\langle a_0\rangle|)/2$. Again, via Jordan's lemma it is enough to consider $|\psi 0\rangle = \cos\theta|00\rangle + \sin\theta|11\rangle$ where $\theta \in [0, \frac{\pi}{4}]$ determine the amount of the entanglement. Then, $|\langle a_0\rangle| = \cos 2\theta \equiv \alpha \implies p_g = (1 + |\cos 2\theta|)/2$ with $M_{A|0} = \sigma_z$ and $M_{A|1} = \sigma_x$. It is known (and easy to verify by direct optimization) that Bob should measure $N_{B|y} = \cos\mu\,\sigma_z + (-1)^y \sin\mu\,\sigma_x$ (inverting the role of the players in Eq. (21)), with μ chosen to maximize the CHSH value. A straightforward calculation gives [276]

$$\beta_\mathcal{Q}(\alpha, \mu) = 2(\cos 2\theta \cos\mu + \sin 2\theta \sin\mu) = 2(\alpha \cos\mu + \sqrt{1 - \alpha^2} \sin\mu). \tag{77}$$

---

[18] In a parallel execution the devices receive all inputs $\boldsymbol{x}, \boldsymbol{y}$ simultaneously, and return the outputs $\boldsymbol{a}, \boldsymbol{b}$ at once. The security proof is equivalent to the sequential execution [275], but experimentally more challenging as higher-dimensional entanglement is required.

Table 3

Why the guessing-probability proof improves on the Holevo-χ approach.

Aspect	CHSH$_{p_g}$ [76,77]	CHSH$_\chi$ [73]
Attack	Arbitrary (coherent) attacks on *any* dimension, only causally independent uses assumed	Collective IID attacks only
Security metric	Smooth min-entropy $\Rightarrow$ *explicit* upper bound on Eve's success probability, implies universally composable secrecy	Holevo information $\chi(b{:}E\vert y=1) \Rightarrow$ bound on *average* quantum information; extra steps needed for composability
Technique	Direct operator inequality gives $p_g \leq f(\beta_\mathcal{Q})$ that is concave, tight, and easily generalized to other Bell inequalities	Two-qubit reduction, optimization over eigenvalues and entropic inequalities
Generality	Same machinery works for any Bell inequality once $f(\beta_\mathcal{Q})$ is computed (via SDP)	Tailored to CHSH; extending to other inequalities is non-trivial
Noise threshold	More conservative (5% QBER) because the proof holds for stronger adversaries	Higher tolerance (7.1% QBER) but under weaker assumptions
Conceptual clarity	Security expressed in *operational* terms: "Eve cannot guess the raw bit better than $f(\beta_\mathcal{Q})$"	Security expressed via χ, which is less intuitive and only bounds Eve's *knowledge in principle*

Maximizing the right-hand side over μ yields

$$\beta_\mathcal{Q}(\alpha) = 2\sqrt{2-\alpha^2} \Longrightarrow p_g = \frac{1}{2}\big(1+\vert\alpha\vert\big) \leq \frac{1}{2}\bigg(1+\sqrt{2-\tfrac{\beta_\mathcal{Q}^2}{4}}\bigg) = f(\beta_\mathcal{Q}). \tag{78}$$

For n independent rounds (the "no memory" or "causal-independence" assumption), p_g translates into a smooth min-entropy $H_{\min}(A\vert E) = -\log_2 p_g^n = -n\log_2 f(\beta_\mathcal{Q})$. The amount of public communication needed to reconcile Bob with Alice is $n\,H(A\vert B) = n\,h(Q)$. Privacy amplification therefore yields the asymptotic key rate

$$r \geq \frac{1}{n}\Big[H_{\min}(A\vert E) - n\,h(Q)\Big] = -\log_2 f(\beta_\mathcal{Q}) - h(Q) = 1 - h(Q) - \log_2\bigg[1+\sqrt{2-\tfrac{\beta_\mathcal{Q}^2}{4}}\bigg]. \tag{79}$$

Last step uses $h\left(\frac{1}{2}(1+x)\right) = 1 - \log_2(1+x)$. For the usual depolarized noise ($\beta_\mathcal{Q} = 2\sqrt{2}\,\nu$, $Q = (1-\nu)/2$),

$$r(\nu) \geq 1 - h\Big(\tfrac{1-\nu}{2}\Big) - \log_2\Big[1+\sqrt{2(1-\nu^2)}\Big], \tag{80}$$

this rate vanishes at $Q \simeq 5\%$ (visibility $\nu \simeq 0.95$) (see Table 3).

Security 2-w PD [84]. *advantage distillation* (AD, see Eq. (62)), improves the tolerable imperfections of quantum devices. The security proof is fully composable and phrased in the *min-entropy* framework: for every set of observed correlators, a level-two NPA semidefinite programme is used to upper-bound the trace distance $d(\rho_{E\vert 00}, \rho_{E\vert 11}) = \frac{1}{2}\Vert\rho_{E\vert 00} - \rho_{E\vert 11}\Vert_1$ between Eve's conditional states when Alice and Bob both obtain outcome 0 or 1. A sufficient condition for security is then provided by Corollary 1 in [84], which states that $1 - d > \varepsilon/(1-\varepsilon)$, where ε is the bit-error rate after advantage distillation. This replaces earlier security analyses based on the Holevo quantity χ, and yields direct bounds on the smooth min-entropy $H_{\min}(A\vert E)$, which governs universally composable key extraction. The authors analyze two noise models: *(i)* depolarizing noise, parameterized by $q \in [0, 1/2]$, where the observed distribution is $\boldsymbol{p} = (1-2q)\boldsymbol{p}_T + q/2$ for an ideal target distribution $\boldsymbol{p}_T$; and *(ii)* detection inefficiency, where each outcome is independently flipped by a σ_z channel with probability $1-\eta$, for efficiency $\eta \in [0, 1]$. In both cases, advantage distillation raises the noise tolerance and lowers the detection threshold (see Table 4). Because the SDP formulation depends only on observed Bell correlators, the method is general and adaptable to other inequalities and more advanced Bell tests.

3.7. CHSH$_T$ — noisy preprocessing

Noisy preprocessing denotes the deliberate random flipping of raw key bits prior to information reconciliation and privacy amplification. When appropriately tuned, this strategy reshapes the trade-off between Eve's information and the observed error rate, thereby increasing the tolerable noise level for a given Bell violation and improving finite-size key rates. In the following, we focus on the CHSH$_T$-based realization, which provides a concrete and widely studied implementation of this idea.

Protocol. *Data generation*. If Bob applies the preprocessing T of Eq. (43) (see [69,266]) generating a new raw key $T(K_B)$ by flipping each bit independently with probability q before the post-processing [243].

Security. The secret key rate is derived using a min-entropy uncertainty relation that bounds Eve's knowledge about Bob's (post-processed) raw key $\widehat{B}_1$ in terms of the observed CHSH violation $\beta_\mathcal{Q}$. The rate takes the form: $r \geq H_{\min}(\widehat{B}_1\vert E) -$

Table 4

Noise thresholds for advantage distillation in various DI-QKD scenarios. $\boldsymbol{p}_T$ is the ideal target distribution, q_t is the tolerated depolarizing noise, and η_t is the minimum detection efficiency under which a positive key rate is provable [84].

Description of $\boldsymbol{p}_T$	State and measurements for $\boldsymbol{p}_T$	q_t	η_t
(i) Achieves maximal CHSH value with the measurements A_0, A_1, B_1, B_2.	$A_0 = B_0 = \sigma_z, A_1 = \sigma_x, B_1 = (\sigma_x + \sigma_z)/\sqrt{2}$, $B_2 = (\sigma_x - \sigma_z)/\sqrt{2}$.	6.0%	93.7%
(ii) Modification of a distribution exhibiting the Hardy paradox for improved robustness against limited detection efficiency.	$\lvert\psi\rangle = \sqrt{\kappa}(\lvert 01\rangle + \lvert 10\rangle) + \sqrt{1 - 2\kappa}\lvert 11\rangle$, with $\kappa = (3 - \sqrt{5})/2$; the 0 outcomes correspond to projectors onto: $\lvert a_0\rangle = \lvert b_0\rangle \propto (\sqrt{1 + 2\kappa} - \sqrt{1 - 2\kappa})\lvert 0\rangle + 2\sqrt{\kappa}\lvert 1\rangle$, $\lvert a_1\rangle = \lvert b_1\rangle \approx 0.37972\lvert 0\rangle + 0.92510\lvert 1\rangle$, $\lvert a_2\rangle = \lvert b_2\rangle \approx 0.90821\lvert 0\rangle + 0.41851\lvert 1\rangle$.	3.2%	92.0%
(iii) Includes the Mayers–Yao self-test and the CHSH measurements.	$A_0 = B_0 = \sigma_z, A_1 = B_1 = (\sigma_x + \sigma_z)/\sqrt{2}, A_2 = B_2 = \sigma_x$, $A_3 = B_3 = (\sigma_x - \sigma_z)/\sqrt{2}$.	6.8%	92.7%
(iv) Achieves maximal CHSH value with the measurements A_0, A_1, B_0, B_1.	$A_0 = \sigma_z, A_1 = \sigma_x, B_0 = (\sigma_x + \sigma_z)/\sqrt{2}, B_1 = (\sigma_x - \sigma_z)/\sqrt{2}$.	7.7%	91.7%
(v) Similar to (iv), but with measurements optimized for robustness against depolarizing noise.	Measurements are in the x-z plane at angles: $\theta_{A_0} = 0.42, \theta_{A_1} = 1.79, \theta_{B_0} = 0.86, \theta_{B_1} = 2.63$.	9.1%	90.0%
(vi) Similar to (iv), but states and measurements maximizing CHSH for each value of detection efficiency η.	$\lvert\psi\rangle = \cos\Omega\lvert 00\rangle + \sin\Omega\lvert 11\rangle$, with $\Omega = 0.6224$; 0 outcomes correspond to projectors onto states of the form: $\cos(\theta/2)\lvert 0\rangle + \sin(\theta/2)\lvert 1\rangle$, with $\theta_{A_0} = -\theta_{B_0} = -0.36, \theta_{A_1} = -\theta_{B_1} = 1.15$.	7.3%	89.1%

$H(\widehat{B}_1|A_0)$, where the first term is bounded via a refined uncertainty relation, and the second is the conditional Shannon entropy (the error correction cost). The bound on $H_{\min}(\widehat{B}_1|E)$ is obtained using the *entropy accumulation theorem (EAT)*, and incorporates the effect of Bob's deliberate bit-flip preprocessing (probability q) through the function $I_p(S)$. This function is not a Holevo quantity, but rather a derived bound on min-entropy that depends concavely on the CHSH violation β_Q and reads [243]

$$I_p(\beta_Q) = \chi_0(\beta_Q) - h\left(\frac{1 + \sqrt{1 - q(1-q)(8 - \beta_Q^2)}}{2}\right), \quad (p_g^M = 0). \tag{81}$$

so that the asymptotic rate becomes

$$r \geq 1 - h(Q) - I_p(\beta_Q), \qquad Q = \frac{1}{2}\left(1 - \frac{\beta_Q}{\sqrt{2}}\right), \tag{82}$$

where we model $H(\widehat{B}_1|A_0) = h(Q)$ with a binary key $\widehat{B}_1$ and four-valued outcome $A_0 \in \{0, 1, 2, 3\}$ (representing 0-click, 1-click-left, 1-click-right, 2-click), this entropy is:

$$H(\widehat{B}_1|A_0) = \sum_{a=0}^{3} p_{A_0}(a) \cdot h\left(p(\widehat{B}_1 = 1|A_0 = a)\right) = h(Q),$$

where $p_{A_0}(a)$ is the empirical probability distribution of Alice's outcome A_0, $p(\widehat{B}_1 = 1|A_0 = a)$ the empirical conditional probability of Bob's bit being 1 given $A_0 = a$ and assuming binary errors with some effective QBER $Q(\beta_Q)$. Again, including the artificial pre-processing noise q to K_B damages both the correlation between Alice and Bob and the correlation to Eve. However, since the possibility of generating a key depends on the difference between the strengths of these correlations, the net effect is positive. Optimization over q therefore lowers the security threshold without changing the physical devices or the Bell test itself. The security proof applies to arbitrary, memory-free devices and is fully composable. A realistic performance analysis for a pulsed SPDC source, non–photon-number-resolving detectors and finite-mode multiplexing shows a dramatic improvement: the global detection-efficiency threshold drops from 92.7% (original CHSH protocol) to 90.9% when four-outcome error correction is used, and further to 83.2% once the noisy pre-processing is included − an effective 78% relative gain that approaches the fundamental Bell limit of 82.8%. At unit efficiency the protocol still produces nearly one secret bit per entangled pair despite multi-pair emissions, and for $\eta > 0.85$ the predicted key rate is within a factor $\lesssim 2$ of the BB84 Shannon limit because the only extra requirement is software-level bit-flipping advances a near-term DI-QKD photonic demonstration. This represents an improvement compared to the efficient post-processing method described in [268].
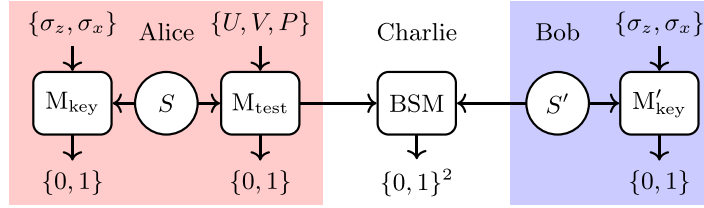
Fig. 12. The CHSH$_\ell$ protocol [79], inspired by the time-reversed BB84, introduces an untrusted party, Charlie, who performs a Bell-state measurement on ρ sent by Alice and Bob. He outputs a pass or fail indicating success, and if successful, provides two bits for Alice to apply bit-flip corrections.

3.8. CHSH$_\ell$ protocol - DI-QKD with local test and entanglement swapping

A *local Bell-test* approach is introduced to close the detection loophole arising from the lossy channel between Alice and Bob [79] (see Fig. 12).

Protocol. *Data generation.* The CHSH test is performed entirely inside Alice's lab using a setup composed of three separate devices: a source device $\mathcal{S}$ that generates entangled systems ρ, and two measurement devices $\mathcal{M}_{\text{key}}$ and $\mathcal{M}_{\text{test}}$. The device $\mathcal{M}_{\text{key}}$ implements two settings $\{\sigma_x, \sigma_z\}$ to generate the raw key, while $\mathcal{M}_{\text{test}}$ has three settings — two used to evaluate $\beta_\mathcal{Q}$, and one to send ρ into the quantum channel towards Charlie. Bob operates a similar setup with measurement $\mathcal{M}'_{\text{key}}$ and source $\mathcal{S}'$. A Bell-state measurement (BSM) is then performed by Charlie on qubits A' and B'; when a successful detection occurs in orthogonal spatial modes, bosonic symmetry implies a collapse into the antisymmetric Bell state $|\psi^-\rangle_{A'B'}$, which by entanglement swapping also projects the remaining qubits AB into $|\psi^-\rangle_{AB}$. This clever scheme ensures the overall detection efficiency $\eta = \eta_\ell + \eta_d$ has $\eta_\ell = 0$ due to the post-selected BSM (see Section 2.4.1), effectively closing the detection loophole that plagues long-distance DI-QKD.

Security. The security proof is proven via an entropic-uncertainty framework that links the observed local CHSH value $\beta_\mathcal{Q}$ to the incompatibility of Alice's measurement bases, yielding a lower bound on the smooth min-entropy of the raw key. This distinguishes the protocol from standard DI-QKD schemes, which rely on the monogamy of nonlocal correlations. The asymptotic secret key rate is

$$r = \frac{\ell}{m_x} = 1 - 2h(Q) - \log_2\left(1 + \frac{\beta_\mathcal{Q}}{4\eta}\sqrt{8 - \beta_\mathcal{Q}^2}\right).$$

where ℓ is the secret key length, m_x is the number of sifted key bits, and $\beta_\mathcal{Q}, \eta, Q$ are the tolerated CHSH value, Bell-state measurement efficiency, and quantum channel error rate, respectively. This rate is independent of transmission losses and matches that of BB84 in the ideal limit $\beta_\mathcal{Q} \to 2\sqrt{2}$. Ref. [84] shows how the key rate degrades with decreasing η for visibility $v = 0.99$ and 0.999, yet still allows key generation at the channel transmission $t \simeq 45\%$ (about 17 km of optical fiber), demonstrating remarkable robustness under realistic visibilities.

3.9. CH-SH protocol — splitting CHSH parameter estimation

CH-SH protocol [86,87], so-called because Eve's knowledge is bounded by the quantity X and Y obtained by splitting the parameter estimation of $\beta_\mathcal{Q}$ more finely than the single CHSH score:

$$X = \langle A_0 \otimes (B_0 + B_1)\rangle, \qquad Y = \langle A_1 \otimes (B_0 - B_1)\rangle.$$

Apart from that, the protocol is the same as CHSH$_\chi$ protocol. Keeping the two CHSH sub-sums separate and derive a tight, closed-form lower bound $H(A_0|E) \geq 1 - h_q(z)$ with $z = \frac{1}{2}\left(\frac{Y}{\sqrt{4-X^2}} + 1\right)$ and the noisy-pre-processing parameter q. Because the full pair (X, Y) is used, the bound is always as good as — and often strictly better than — the CHSH-only bound. Indeed, the set of points (X, Y) where Eve's conditional entropy is bounded below by a constant is convex. Consequently, combining two quantum models into a new one results in Eve's conditional entropy being bounded by the weighted sum of the individual models' entropy bounds. Using this fact and considering all possible quantum models (ψ_{ABE}, A_x, B_y) where $X_{\text{model}} \geq X$ and $Y_{\text{model}} \geq Y$, it is equivalent to bound Eve's conditional entropy with the following linear constraint:

$$\frac{\cos(\Omega)}{2}X_{\text{model}} + \frac{\sin(\Omega)}{2}Y_{\text{model}} \geq \beta, \tag{83}$$

where $\beta = \frac{1}{2}(\cos(\Omega)X + \sin(\Omega)Y)$ is deduced from the quantities X and Y. An improved bound on Eve's knowledge can be obtained in two identified regimes: $\Omega \leq \frac{\pi}{4}$ and $\Omega > \frac{\pi}{4}$. In the first regime, $\Omega \leq \frac{\pi}{4}$, the optimal value is given by $\cot(\Omega) = \frac{XY}{4-X^2}$, and it is verified that the bound in this regime is better than the CHSH formula if $\frac{4-X^2}{XY} < 1$. The regime $\Omega > \frac{\pi}{4}$ is more complicated, but numerical evaluation shows the advantage of the generalized CHSH inequality (83).

When applying this result to photonic implementations of DI-QKD using an SPDC source, the key rate improved by up to 37% with $\eta = 1$ while the efficiency threshold ($\approx 82.8\%$ for photon-loss-limited optics) is unchanged with $T = $ fp [243]. The analysis remains analytic thanks to the *qubit reduction argument* and shows that the advantage is largest when the correlations lie far from the line $X(X+Y) = 4$ (where usual CHSH attacks are optimal).

Ref. [87] tackles the complementary mismatch that only Alice's measurement A_1 is used for key generation although the CHSH expression is symmetric. They introduce an *asymmetric* CHSH family $\beta_\alpha = \alpha\langle A_1 B_1\rangle + \alpha\langle A_1 B_2\rangle + \langle A_2 B_1\rangle - \langle A_2 B_2\rangle$ and, combining a qubit decomposition with BB84-type techniques, derive the exact conditional-entropy bound $H(A_1|E) \geq \bar{g}_{q,\alpha}(S_\alpha)$ valid for every α and any noise q. Optimizing α and q raises the tolerable depolarizing error from 7.15% to 8.34%, and pushes the loss-only detection-efficiency threshold for maximally-entangled qubits from 90.8% down to 90.0%. In the high-loss regime still larger gains arise when Bob re-optimizes his bases; conversely, in realistic noisy channels the two refinements (asymmetric tests + noise pre-processing) are most beneficial at moderate to high visibilities where they deliver the best device-independent key rates reported so far without changing the implementation.

3.10. CHSH$_{IMD}$ protocol-conditional entropies via iterated-mean divergences

The CHSH$_{IMD}$ [85] exploits a new family of Rényi-like quantities — the iterated-mean divergences — to certify secret key directly from CHSH statistics with tighter entropy bounds than previous numerical techniques.

Protocol. *Data generation.* This stage is identical to the CHSH setting, but the rate analysis departs from min-entropy methods. Alice and Bob use their raw correlation sample to solve an SDP that outputs the IMD-based conditional entropy under the observed CHSH β. This bound is evaluated at a low hierarchy level (degree 3), making the computation fast enough to be iterated in real time while the experiment runs. Optimizing measurement angles within this loop raises the certified asymptotic key rate by 15–35% in the high-violation, low-noise regime and reaches the analytic maximum of two bits of global randomness already with qubit systems.

Security Security against collective quantum and general non-signaling attacks follows because every IMD conditional entropy lower bounds the true von Neumann entropy. By deriving affine trade-off functions from the SDP dual, this approach enables a plug-and-play use of EAT. As a result, finite-key analysis inherits the same modular proof structure as modern BB84 protocols. Importantly, the new technique lowers the minimal global detection efficiency for two-qubit CHSH DI-QKD without noisy preprocessing to $\eta_{\rm crit} = 0.843$. See the mathematical technique of the protocol in Section 5.8.

3.11. CHSH$_{2e}$ protocol — random key basis

We name the CHSH$_{2e}$ protocol in Ref. [88] a variant of CHSH$_{p_g}$ protocol because it provides an extra Bob's choice that doubles the event to generate the raw key for $x = y = 0, 1$.

Protocol. *Data generation.* Alice selects $x \in \{0, 1\}$ with probability weight $p, 1 - p$. The same of CHSH protocol, but Bob selects $y \in \{0, 1, 2, 3\}$, with probability respectively $qp, q(1-p), (1-q)/2, (1-q)/2$. The extra Bob's choice doubles the event to generate the raw key for $x = y = 0, 1$. This enhances the security besides BI violation as decreases p_g^M, i.e. Eve does not even know the pair (x, y) used to generate the key anymore.

Security 1-w PD. In CHSH$_{2e}$ protocol Eq. (74) yields

$$r = \max_\lambda p_s \left[\lambda H(A_0|E) + (1-\lambda)H(A_1|E) - \lambda h(Q_0) - (1-\lambda)h(Q_1) \right], \tag{84}$$

with $p_s = q(p^2 + (1-p)^2) = p(x = y)$ is the matching basis probability; Q_0 and Q_1 is the QBER to generate the key when $x = y = 0$ and $x = y = 1$ respectively (in the depolarizing noise, $Q_0 = Q_1 = \frac{1}{2}\left(1 - \beta_Q/\sqrt{8}\right)$), $\lambda = p^2/p_s$, and E is Eve's variable gathered before the error correction step with the quantum side-information. To estimate the LHS of Eq. (84) with a function $C^\star(\beta_Q)$ depending only on β_Q the first step is to consider in the asymptotic limit regime $q \to 1$ (CHSH$_{2e} \to$ CHSH) and reformulate the tripartite problem among Alice, Bob, and Eve into a bipartite one so that the conditional entropy $H(A_i|E) \mapsto H(T_X(\rho_{AB})) - H(\rho_{AB}) = D(\rho_{AB} \| T_X(\rho_{AB}))$ is mapped into the *quantum relative entropy*, as well as the entropy production of the quantum channel T_X on ρ_{AB}, e.g. the *pinching channel* $T_X(\rho) = \sum_{a=0}^{1}(M_{a|x} \otimes \mathbf{1})\rho(M_{a|x} \otimes \mathbf{1})$. Eve's action mix $\rho_{AB} \in \mathcal{B}(\mathbb{C}^2 \otimes \mathbb{C}^2)$, as $q \to 1$, and CHSH$_{2e} \to$ CHSH the same argument (see Section 3.4.2, Jordan's Lemma 1) applies here. It implies that

$$C^\star \geq \inf_\mu \int_2^{2\sqrt{2}} C^\star_{M_{\mathbb{C}}(4)}(\beta_Q)\,\mu(\mathrm{d}\beta_Q), \quad \text{s.th.}: \mu([2, 2\sqrt{2}]) \leq 1, \ \mu \geq 0, \ \int_{\beta'_Q=2}^{2\sqrt{2}} \beta'_Q\,\mu(\mathrm{d}\beta'_Q) = \beta_Q, \tag{85}$$

yielding

$$C^\star(\beta_Q) := 1 - h\left(\frac{1 + \frac{\beta_Q}{2\sqrt{2}}}{2}\right), \qquad \xi(S) := \begin{cases} \frac{1}{2} & \text{for } S \leq 2.5, \\ 1 & \text{for } S > 2.5, \end{cases} \implies r = \xi(S)\left[C^\star(\beta_Q) - h\left(Q(\beta_Q)\right)\right]. \tag{86}$$

A direct computation of the 4×4 complex operator $\hat{\beta}_Q$ is still an open problem as no known proof techniques can be applied. To that end, a refined version of Pinsker's inequality formulates the SPD problem in terms of trace norm, i.e. $D(\rho \parallel T(\rho)) \geq \log 2 - h(1/2 - \|\rho - T(\rho)\|_1/2)$, obtaining a closed, efficiently computable expression for the one-way secret fraction in the asymptotic IID regime. The optimization involves similar methods discussed in Sections 2.2 and 2.3 (see details in Ref. [88] and Section 5) to estimate the lower bound of uncertainty relations. Most importantly, their bound is *near-optimal*: for CHSH violations $S \lesssim 2.5$ the choice $\lambda = \frac{1}{2}$ (fully random basis) maximizes Eve's conditional entropy $H(Z|E\Theta)$ essentially up to the linear algebraic limit, while for $S \gtrsim 2.5$ the protocol smoothly reverts to the original single-basis variant ($\lambda = 1$). Thus the family interpolates between minimal and maximal entropy production without sacrificing simplicity or implementability.

Assuming isotropic depolarizing noise, the new protocol tolerates QBER up to $Q = 8.2\%$, corresponding to a critical CHSH value of $\beta_Q = 2.362$, whereas the CHSH$_{p_g}$ [77] ceased to produce key beyond $Q = 7.1\%$ $\beta_Q = 2.423$). This ~15% noise-budget increase brings today's loophole-free, event-ready Bell experiments firmly into the positive-rate region: the 2015 NV-center test by Hensen et al. [100] and its 2017 cold-atom successor by Rosenfeld et al. [207] both admit asymptotic key rates of order 10^{-2}–10^{-1} bits per channel use. A finite-key analysis based on EAT shows that 10^8–10^{10} rounds suffice to beat finite-size overheads against *coherent* attacks, squarely within reach of next-generation entanglement-swapping platforms. In contrast, all-photonic loophole-free experiments still fall short, primarily due to detector inefficiencies, but the authors' Monte-Carlo study indicates that threshold efficiencies could drop below the often-quoted 94% mark once modest multiplexing or precertification techniques mature. Overall, the random-basis variant narrows the gap between theory and experiments.

3.12. CHSH$_{pV_p}$ protocol — random postselection pre-processing

Ref. [89] introduces a simple yet powerful modification of the standard two-basis/three-setting DI-QKD protocol.

Protocol. *Data generation.* After the usual CHSH rounds, Alice and Bob keep only those *key-generation* outcomes for which at least one detector clicks, and they do so *independently at random*. Formally, every raw bit pair (a, b) obtained with inputs $(\bar{x}, \bar{y}) = (1, 3)$ is accepted with weight $\omega_{ab} \in \{1, p, p, p^2\}$, where p is the local post-selection probability and $V_p = \{(a, b)|(a, b) = (0, 0), (0, 1), (1, 0), (1, 1)\}$ the set of potentially retained events. Because the secrecy analysis still uses the *complete* detection statistics — including all double-clicks and no-clicks — the postselection does *not* re-open the detection loophole (Section 2.4.1), yet it strips away the high-error, low-correlation data that would otherwise dominate the error-correction cost.

Security. The authors cast Eve's optimal attack as a semidefinite programme (see 5.8) over the *unnormalized* quantum behaviors $p_e^0(a, b|x, y)$ compatible with the observed distribution $p(a, b|x, y)$, and bound her information through the conditional min-entropy $H_{\min}(A|E, V_p)$ of the postselected string.

Then, in the asymptotic IID regime and against collective attacks, the extractable secret key rate per *channel use* obeys the Devetak–Winter lower bound and yields

$$r \geq p_{V_p}\Big[H_{\min}\big(A \mid E, V_p\big) - H\big(A \mid B, V_p\big)\Big]. \tag{87}$$

Here $H_{\min}(A|E, V_p) = -\log_2 p_g(A|E, V_p)$ is the guessing probability of Alice's bit A by an eavesdropper Eve, *conditioned on* the fact that the round was retained (i.e., passed the postselection V_p),[19] while $H(A|B, V_p)$ is the (classically estimated) one-way error-correction cost for the retained bits. All three quantities — p_{V_p}, $H_{\min}$ and $H(A|B)$ — are directly computable from the experimentally observed correlations and the chosen postselection parameter p. Specifically, the usual secrecy term is multiplied by the *sifting factor* p_{V_p},

$$p_{V_p} = \sum_{(a,b)\in V_p} \omega_{ab}\, p(a, b \,|\, \bar{x}, \bar{y}), \qquad \omega_{00} = 1,\ \omega_{01} = \omega_{10} = p,\ \omega_{11} = p^2, \tag{88}$$

denote the probability that a key-generation round survives the random postselection. Numerical optimization over the quantum realization (quantum state, measurement settings and the single parameter p) shows that a positive key rate is already achieved for a global detection efficiency of $\eta \simeq 68.5\%$ — a dramatic improvement over the 92.4% required by CHSH$_{p_g}$ [77] and the 82.6% achieved by noisy preprocessing. At $\eta = 80\%$ the protocol cuts the Shannon error-correction term from 0.65 to 0.033 bits per retained round and *simultaneously* raises Eve's uncertainty, yielding $r \approx 7.9 \times 10^{-5}$ bits per *attempted* channel use — two orders of magnitude better than without postselection (see Table 5).

Remark. As we emphasized, the security proof above is against collective attacks. More recently, it was shown in [278] that CHSH-based DI-QKD protocols with random post-selection are vulnerable to coherent attacks. This vulnerability, however, is specific to the random post-selection variant and does not extend to standard DI-QKD protocols such as E91, which do not employ post-selection.

---

[19] Formally, it is defined as: $p_g(A|E, V_p) = \max_{\{E_e\}} \sum_{a\in\{0,1\}} p(A = a, \hat{A}_E = a \mid V_p)$ where: $\{E_e\}$ is the POVM Eve applies to her system; $\hat{A}_E$ is Eve's guess based on her measurement outcome; the probability is conditioned on the postselected events $V_p = \{00, 01, 10, 11\}$; the overall state is a classical–quantum (cq) state of the form $\rho_{AE} = \sum_a p_a|a\rangle\langle a| \otimes \rho_E^a$ after the postselection.

Table 5
A comparison of critical detection efficiency η^* among different methods for DI-QKD.

Protocols	Method	η^*
$CHSH_{p_g}$	Standard analysis [73]	92.4%
$CHSH_{p_g}$	Efficient post-processing [268]	90.9%
$CHSH_{p_g}$	Advantage distillation [84]	89.1%
$CHSH_{IMD}$	Iterated mean divergence [85]	84.5%
$CHSH_T$	Noisy preprocessing [243]	83.2%
CH-SH	Asymmetric inequality [86,87]	82.6%
$CHSH_T$	Quasi-relative entropy [277]	80.5%
$CHSH_{p_v p}$	Random Postselection [89]	68.5%
rDI-QKD	Routed BI [92]	50%
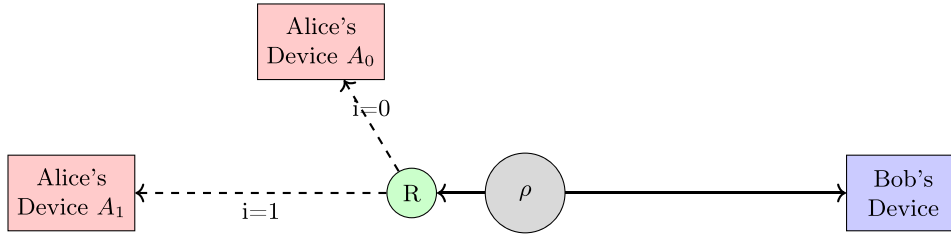
Fig. 13. A schematic of routed Bell experiment introduced in [92]. In each round of experiment, Alice transmits her choice of $i \in \{0, 1\}$ to the relay switch, R, which then transmits the quantum system from the source to either the measurement device, A_0, placed close to the source or A_1, placed further away, based on i.

3.13. Mermin–peres magic square game-based DI-QKD

Ref. [91] proposes a DI-QKD protocol based on the Mermin–Peres Magic Square Game (MPG) [223,224]. In this game, there are two players, Alice and Bob, who are forbidden to communicate with each other. In each round of the game, a referee generates two random 'trits' $x, y \in \{0, 1, 2\}$ and sends the index x to Alice and the index y to Bob. Alice and Bob then reply to the referee with $[a_0^x, a_1^x, a_2^x]$ and $[b_0^y, b_1^y, b_2^y]$ under the conditions that $a_2^x = a_0^x + a_1^x$ and $b_2^y = b_0^y + b_1^y \oplus 1$. The winning condition is when $a_{i=y}^x = b_{j=x}^y$. After the game, the referee decides whether Alice and Bob win or not according to the average winning probability

$$\omega = \frac{1}{9} \sum_{x,y} p(a_y^x = b_x^y | x, y) \tag{89}$$

where $p(a_y^x = b_x^y | x, y)$ is the winning probability of Alice and Bob with respect to (x, y). The MPG DI-QKD in [91] is based on the fact that for all classical strategies $\omega \le \frac{8}{9}$ and since all classical strategies are equal to local hidden variables, then $\omega \le \frac{8}{9}$ is actually a Bell inequality that some quantum strategies can violate [279,280].

Protocol. Alice and Bob initially generate data by playing the MPG. They announce their inputs and record the overlapped bits. To estimate parameters, Alice communicates to Bob which part of the bits serves as raw keys, with the remaining part of the bits announced to play the MPG. If the average winning probability estimated from the announced data is less than an expected value, they abort the protocol; otherwise, they perform data reconciliation on raw keys to obtain the final keys.

Security. The security analysis is against collective attacks in the asymptotic scenario and showed that if $\omega > 0.9575$, it generates higher secret keys than the CHSH-based protocol for ρ_p of Fig. 2(b) with $v > 0.978$ ($\eta = 1$) or $\eta \ge 0.982$ ($v = 1$). Later in [281], this protocol is generalized to the finite-round regime under general attacks.

3.14. rDI-QKD: DI-QKD based on routed Bell tests

The current state-of-the-art combination of detection efficiency and visibility v 2(b) (see Section 7) is achieved only for distances less than 400 m. For DI-QKD to become a widely adopted near-term technology, operationally certifiable robust nonlocal correlations must be sustained over distances that are orders of magnitude greater ($\gg$100 km). Due to the high sensitivity inherent in traditional approaches for establishing nonlocal quantum correlations, these methods prove ineffective for long-distance DI-QKD. Consequently, developing alternative methods to establish nonlocality over large distances is essential.

An approach to extending nonlocal correlations over large distances involves generalizing standard Bell experiments to the *routed Bell experiments* introduced in [92]. In a routed Bell experiment, as illustrated in Fig. 13, the measuring parties randomly select the location of their measurement in each round (the relay R in Fig. 14).
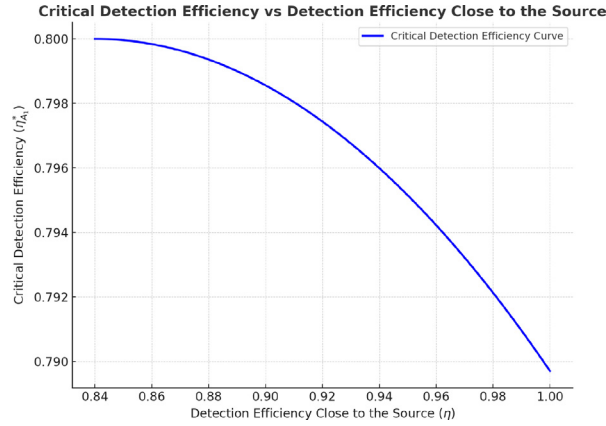
Fig. 14. The detection efficiency $\eta_{A_1}^*$ versus detection efficiency η obtained by Eq. (101) in symmetric case where A_0 and B are equidistance from the source [92].

For a general quantum strategy, the correlations in a routed Bell experiment can be expressed as follows [93]

$$p(a, b|x, y, i) = \mathrm{Tr}[C_i \otimes \mathcal{I}(\rho_{AB})M_{a|xi} \otimes M_{b|y}] = \mathrm{Tr}[\rho_{AB}\tilde{M}_{a|xi} \otimes M_{b|y}], \tag{90}$$

where C_i is the CPTP map describing the transmission of Alice's system on the short-path ($i = 0$) or the long-path ($i = 1$), and $\tilde{M}_{a|xi} = C_i^\dagger(M_{a|xi})$ are the elements of a valid POVM. Thus general correlation in a routed Bell experiment coincides with those of regular bipartite Bell experiment where Alice has $m_0 + m_l$ inputs (m_0 and m_1 are the number of measurement settings at short-distance $i = 0$ and long-distance $i = 1$, respectively). Various subsets of general quantum correlations $\mathcal{Q}$ then can be defined as follows [93]:

Definition 19.

- **Short-range quantum correlations:** denoted as $\mathcal{Q}_{SR}$, short-range quantum (SRQ) correlations refer to the correlations achieved without the distribution of any entanglement to A_1. For these correlations, C_1 is an entanglement-breaking channel $C_1(\rho) = \sum_\lambda \mathrm{Tr}[N_\lambda \rho]\rho_\lambda$, where N_λ's are the elements of a POVM. Therefore, the POVM elements of $M_{a|y_1}$ are maps to

$$\tilde{M}_{a|x_1} = \sum_\lambda p(a|x, \lambda)N_\lambda, \quad \text{where} \quad p(a|x, \lambda) = \mathrm{Tr}[\rho_\lambda M_{a|x_1}], \tag{91}$$

  which is equivalent to the statement that the measurement $M_{a|x1}$ are jointly-measurable. Therefore, the SRQ correlations can be expressed as

$$p(a, b|x, y, i) = \begin{cases} \mathrm{Tr}[\rho_{AB}\tilde{M}_{a|x0} \otimes M_{b|y}] & \text{if } i = 0, \\ \sum_\lambda p(a|x, \lambda)\mathrm{Tr}[\rho_{AB}N_\lambda \otimes M_{b|y}] & \text{if } i = 1. \end{cases} \tag{92}$$

  This operationally means that if the relay selects the short path $i = 0$, the correlations are obtained by measuring a shared entangled state ρ_{AB} as in a regular Bell experiment. If it selects the long path $i = 1$, a fixed measurement N_λ is performed on Alice's system, yielding a classical outcome λ with the probability distribution $p(a|x, \lambda)$, and transmit it to A_1.

- **Fully quantum marginal correlations:** denoted as $\mathcal{M}_{qq}$, the fully quantum marginal correlations are where the source prepares on Alice's side a pair of systems $A = (A_0, A_1)$ and if $i = 0$ ($i = 1$) the relay routes the first subsystem to the device A_0 (A_1). The resulting correlations can be encompassed to the bipartite marginals of qqq-correlations

$$p(a_0, a_1, b|x_0, x_1, y) = \mathrm{Tr}[\rho_{A_0 A_1 B}M_{a|x,0} \otimes M_{a|x,1} \otimes M_{b|y}]. \tag{93}$$

- **Quantum–classical marginal correlations:** denoted as $\mathcal{M}_{qc}$, the quantum–classical marginal correlations can be obtained by further restricting the state $\rho_{A_0 A_1 B}$ to be a qqc-state as

$$\rho_{A_0 A_1 B} = \sum_\lambda p(\lambda)\rho_{A_0 B} \otimes |\lambda\rangle\langle\lambda|_{A_1}. \tag{94}$$

All the above correlations can be written as

$$p(a, b, i) = \mathrm{Tr}[\rho M_{a|xi}M_{b|y}], \tag{95}$$

where $M_{a|xi}$ and $M_{b|y}$ are projectors that satisfy the following commutation relations for each subset

$$[M_{a|xi}, M_{b|y}] = 0, \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \text{if } p \in \mathcal{Q}, \qquad (96)$$

$$[M_{a|xi}, M_{b|y}] = 0, \quad [M_{a|x1}, M_{a'|x'1}] = 0, \qquad\qquad\qquad\qquad \text{if } p \in \mathcal{Q}_{SR}, \qquad (97)$$

$$[M_{a|xi}, M_{b|y}] = 0, \quad [M_{a|x0}, M_{a'|x'1}] = 0, \qquad\qquad\qquad\qquad \text{if } p \in \mathcal{M}_{qq}, \qquad (98)$$

$$[M_{a|xi}, M_{b|y}] = 0, \quad [M_{a|x0}, M_{a'|x'1}] = 0, \quad [M_{a|x1}, M_{a'|x'1}] = 0, \quad \text{if } p \in \mathcal{M}_{qc}. \qquad (99)$$

which follows from the fact that each of the tensor products between subsystems in definition 19 can be replaced by commutation relations.

As a result, the above representation fits in the framework of non-commutative polynomial optimization, which means that the sets defined in 19 can be outer-approximated through SDP hierarchies.

Trade-off relations between β_0 and β_1. Consider a realistic CHSH scenario in which the source and measurement devices are imperfect. Considering the situation described in Fig. 13, when $i = 0$ Alice places her measurement device A_0 close to the source achieving effective detection efficiencies, η_{A_0}, while when $i = 1$, she places her device A_1, further away from the source, therefore $\eta_{A_1} \leq \eta_{A_0}$. Similarly, for effective visibilities $v_{A_1} \leq v_{A_0}$, which result in the following quantum state shared between (A_i, B)

$$\rho(v_i) = v_{A_i} v_B |\psi\rangle\langle\psi| + v_{A_i}(1 - v_B)\left(\rho_B \otimes \frac{I}{2}\right) + (1 - v_{A_i})v_B\left(\frac{I}{2} \otimes \rho_A\right) + (1 - v_{A_i})(1 - v_B)\frac{I_4}{4}, \qquad (100)$$

where $\rho_{A(B)} = \text{Tr}_{B(A)}(|\psi\rangle\langle\psi|)$. Treating $i \in \{0, 1\}$ as an additional Alice's input, denoting the location of her measurement device, the CHSH value is also dependent on i, which we denote by β_i. The following theorem captures the tradeoffs between β_0 and β_1 [92]

Theorem 2. *If a loophole-free nonlocal correlation between (A_0, B) is witnessed i.e. $\beta_0 > 2$, then loophole-free nonlocal correlations between (A_1, B) can be certified whenever the following inequality is violated*

$$\beta_1 \leq \sqrt{8 - \beta_0^2}. \qquad (101)$$

Proof. The short-range correlations that were considered in [92] are represented as

$$p(a, b|x, y, i) = \begin{cases} \sum_\lambda p(\lambda)\text{Tr}[\rho_{A_0 B}^\lambda M_{a|x0} \otimes M_{b|y}] & \text{if } i = 0, \\ \sum_\lambda p(\lambda)p(a|x, \lambda)p(b|y, \lambda) & \text{if } i = 1. \end{cases} \qquad (102)$$

The intuition for the proof is as follows: for simplicity, consider the case where $\beta_0 = 2\sqrt{2}$. Then, by standard self-testing result 2.3, it can be inferred that the measurement $\{B_{b|x}\}$ corresponds to a Pauli measurement on a two-dimensional subspace of B that is maximally entangled with A_0. In particular, the Bob's measurement outcomes must be fully random and uncorrelated with the classical instructions λ shared with B which result in $p(b|y, \lambda) = p(b|y) = \frac{1}{2}$ for all λ's which gives $\beta_1 = 0$ Although the assumption that $\beta_0 = 2\sqrt{2}$ is too strong, for any value $\beta_0 > 2$ there is a bound on how much the outcomes of POVM $\{B_{b|y}\}$ can be correlated to other systems besides. Particularly $p(b|x, \lambda) \leq \frac{1}{2}(1 + \frac{\sqrt{8 - \beta_0^2}}{2})$ for all λ [75], which result in the bound (101). $\square$

Since $\sqrt{8 - \beta_0^2}$ is a monotonically decreasing function of β_0, the inequality (101) implies that any amount of loophole-free violation of the CHSH inequality between (A_0, B) ($\beta_0 > 2$), results in reducing the threshold value of the CHSH expression β_1

The significance of this result depends on the assumptions underlying the derivation of the bound (101) (see proof in [92]). Specifically, it relies on the interpretation of *nonlocality* and *ruling out classical models* in routed Bell experiments, since the local variable model can already be excluded by performing a simple CHSH test between (A_0, B). The main purpose is that by observing the nonlocality in (A_0, B) one can conclude about the classicality or nonclassicality of the observed outcomes of the remote device A_1. Therefore, Theorem 2 provides a convenient tool to estimate the critical parameters, $(\eta_{A_1}^*, v_{A_1}^*)$, required for the loophole-free certification of nonlocal correlation between (A_1, B). Given a tuple of experimental parameters $(\eta_B, \eta_{A_0}, v_B, v_{A_0})$, the critical parameters $(\eta_{A_1}^*, v_{A_1}^*)$ are those that saturate inequality (101).

Considering both asymmetric and symmetric cases, if the parties share a maximally nonlocal isotropic strategy, the following results hold:

1. **Asymmetric Case**: Suppose B is placed extremely close to the perfect source, such that $\eta_B = 1$, and all devices exhibit perfect visibilities. In this scenario:

$$\beta_0 = 2\sqrt{2}\eta_{A_0}, \quad \beta_1 = 2\sqrt{2}\eta_{A_1}.$$

The violation of (101) yields:

$$\eta_{A_1} > \sqrt{1 - \eta_{A_0}^2} = \eta_{A_1}^*.$$

This result highlights a central insight: the closer A_0 is placed to the source, the higher its effective detection efficiency, η_{A_0}, becomes. Consequently, the critical detection efficiency of η_{A_1} decreases, allowing A_1 to be placed further from the source while still retaining loophole-free non-local correlations with B.

2. **Symmetric case**: (A_0, B) are equidistant from the source, such that $\eta_B = \eta_{A_0} = \eta$ and in the presence of perfect visibility for all devices, then

$$\beta_0 = 2\sqrt{2}\eta^2 + 2(1 - \eta)^2,$$
$$\beta_1 = 2\sqrt{2}\eta_{A_1}\eta + 2(1 - \eta_{A_1})(1 - \eta). \tag{103}$$

where a loophole-free violation can be observed for $\eta \in (\frac{2}{1+\sqrt{2}}, 1]$. Fig. 14 shows the detection efficiency values $\eta_{A_1}^*$ versus η. The critical detection efficiency starts to decline after η exceeds the threshold value, $\eta = \frac{2}{1+\sqrt{2}} \approx 0.828$.

Consider now a strategy where the source, Bob's measurement device, the relay R, and the measurement device A_0 all behave as in CHSH expectations. Thus, any $\beta_0 \in [0, 2\sqrt{2}]$ can be obtained by tuning η_{A_0}. For $i = 0$, consider the case where at some point between R and A_1 (before A_1) the second qubit is measured on the basis z, yielding a binary result λ. This classical outcome is then transmitted to A_1 through some purely classical channel and upon receiving it, A_1 outputs it, irrespective of the input x. Therefore, we have $p(\lambda) = \frac{1}{2}$, $p(a|x, \lambda) = \delta_{a,\lambda}$, and $p(b|y, \lambda) = \text{Tr}(\rho_\lambda B_y)$ (B_y is the corresponding observable for Bob's measurement) where $\rho_0 = |0\rangle\langle 0|$ and $\rho_1 = |1\rangle\langle 1|$ are the reduced states for Bob conditioned upon λ. Inserting in (102), one gets the value $\beta_1 = 2$, which gives a violation of (101) while A_1 is fully classical. This shows that the form of non-classicality defined as (102) is weaker than $\mathcal{Q}_{SR}$ 19.

Lobo, Pauwels, and Pironio showed that there exist stronger versions of tradeoffs between long path (LP) and short path (SP) correlations in which, instead of CHSH, they considered the following Bell expression for LP [93]

$$J_1^\theta = \tan\theta\langle A_{01}B_0\rangle + \langle A_{11}B_0\rangle + \langle A_{01}B_1\rangle - \tan\theta\langle A_{11}B_1\rangle, \tag{104}$$

satisfying the following local and quantum bound

$$J_1^\theta \overset{L}{\le} 2 \overset{Q}{\le} 2/c_\theta, \tag{105}$$

where $c_\theta = \cos\theta$ ($\theta \in [0, \frac{\pi}{4}]$). For the case of observing the maximal CHSH violation for SP ($\beta_0 = 2\sqrt{2}$), SRQ correlations defined in 19 satisfy the following bound

$$J_1^\theta \le \frac{\sqrt{2}}{c_\theta}, \tag{106}$$

The intuition of finding the bound (106) is that when Alice and Bob observe $\beta_0 = 2\sqrt{2}$, by self-testing the LP correlators are associated with the Pauli expectations i.e. $\text{Tr}(PA_{x1})$ where $P \in \{\mathbb{I}, \sigma_x, \sigma_z\}$, of the observables A_{x1} and as a result, performing tomography of these observables is restricted to ZX plane. In the case $\theta = 0$ it was found that $\frac{1}{2}[\text{Tr}(\sigma_x A_{11}) + \text{Tr}(\sigma_z A_{01})] \le \sqrt{2}$ [282]. Therefore, the bound (106) can be obtained by rotation $R_\theta = \begin{bmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{bmatrix}$ in the ZX plane.

For any value $0 \le \theta < \frac{\pi}{4}$, the bound obtained (106) is strictly smaller than the local bound, which means that the SP CHSH test weakens the condition of witnessing a long-range quantum correlation based on J_1^θ. This weakening is maximal in the case $\theta = 0$, yielding

$$J_1 = \langle A_{1L}B_0\rangle + \langle A_{0L}B_1\rangle \le 2, \tag{107}$$

which coincides with the quantum bound in (105). Although the above inequality in the standard case (without any relay R) does not demonstrate a violation and may not appear to be a proper Bell inequality, in a routed Bell scenario equipped with a strategy that achieves $\beta_0 = 2\sqrt{2}$, the local bound is replaced by the SRQ bound (106).

$$J_1 = \langle A_{1L}B_0\rangle + \langle A_{0L}B_1\rangle \overset{L}{\le} \sqrt{2} \overset{Q}{<} 2, \tag{108}$$

which is smaller than the quantum bound, making it a proper witness for long-range nonlocality ($J_1 = J_1^{\theta=0}$). Therefore, since the SP CHSH is maximally violated, long-range quantum correlations can be witnessed whenever $J_1^\theta > \frac{\sqrt{2}}{c_\theta}$ instead of the more constraining criterion $J_1^\theta > 2$.

The maximal SP CHSH violation S_0 is too strong and unrealistic in experimental settings, so deriving bounds based on non-maximal cases is important. For the case $\theta = 0$ the following analytical tradeoff between J_1 and β_0 can be proved [93]

Theorem 3. *For any SRQ correlation defined in* 19, *the following inequality holds for* $\beta_0 \in [2, 2\sqrt{2}]$

$$J_1 \le \frac{\beta_0 + \sqrt{8 - \beta_0^2}}{2}. \tag{109}$$

For other values of θ, an SRQ bound of J_1^θ can be obtained numerically using the NPA hierarchy 2.2.

Universal bounds on critical detection efficiency. Similarly to the case of the regular Bell experiment, lower bounds on critical detection efficiency can be obtained in routed Bell scenarios. The detection efficiencies in a routed Bell experiment can be denoted by the vector $\vec{\eta} = (\eta_{A_0}, \eta_{A_1}, \eta_B)$. In [93] it was proved that there exists an SRQ model if the following condition is satisfied.

$$\eta_{A_1} \leq \frac{\eta_B(m_B - 1)}{\eta_B(m_{A_1} m_B - 1) - (m_{A_1} - 1)}, \tag{110}$$

which is independent of the number of measurement settings m_{A_0}. For the special case $m_{A_0} = 0$, this bound can be applied to the standard Bell experiment. Therefore, this bound places fundamental limits on the distance at which nonlocal correlations can be observed for both regular and routed Bell experiments. Since the right-hand side of (110) is always greater than $1/m_{A_1}$, the detection efficiency of the remote device A_1 cannot be lower than $1/m_{A_1}$, even if the other detectors are perfect.

Although the bound in (110) applies to both standard and routed Bell experiments, this does not mean that the Routed Bell experiment cannot be more robust to photon losses than the regular ones. To see this, consider a protocol that the nearby detectors have the same efficiency $\eta_{A_0} = \eta_B = \eta_S$ and the remote detector has a lower one $\eta_{A_1} \leq \eta_S$. Assuming the case that produces maximal CHSH violation ($\beta_0 = 2\sqrt{2}$ for $\eta_S = 1$), and following anticommuting measurement settings for A_1

$$A_{01} = s_\theta \sigma_x + c_\theta \sigma_z, \quad A_{11} = c_\theta \sigma_x - s_\theta \sigma_z. \tag{111}$$

Considering the standard Bell experiment between (A_1, B) by ignoring the relay R in Fig. 13. The violation of CHSH inequality is then implied

$$\beta_1 = 2\eta_B(c_\theta + s_\theta) > 2 \longrightarrow \eta_B > \frac{1}{c_\theta + s_\theta}, \tag{112}$$

for the routed Bell inequality using Eq. (106), one can get the following bound for all values of θ

$$\eta_B \geq \frac{1}{\sqrt{2}} \approx 0.71, \tag{113}$$

Considering that $\frac{1}{c_\theta + s_\theta} \geq 0.71$ (the equality holds for $\theta = \frac{\pi}{4}$), for values $\theta \in (0, \frac{\pi}{4}]$ the routed Bell experiment can tolerate higher losses compared to standard Bell inequality. The critical efficiency can be further reduced by the following LP inequality.

$$\begin{aligned} J_1^{\theta_+, \theta_-} &= (c_{\theta_+} + s_{\theta_-} s_{\theta_+})\langle A_{01} B_1 \rangle + (c_{\theta_+} - s_{\theta_-} s_{\theta_+})\langle A_{11} B_1 \rangle \\ &\quad + (s_{\theta_+} - s_{\theta_-} c_{\theta_+})\langle A_{01} B_0 \rangle + (s_{\theta_+} + s_{\theta_-} c_{\theta_+})\langle A_{11} B_0 \rangle \\ &\quad + c_{\theta_-}(\langle A_{0L} \rangle + \langle A_{1L} \rangle) \leq 2 \end{aligned} \tag{114}$$

where the SRQ bound $J_1^{\theta_+, \theta_-} \leq 2$ is obtained assuming $\beta_0 = 2\sqrt{2}$ [93]. By considering the general projective measurements for A_1 of the form $A_{01} = s_{\theta_0} \sigma_x + c_{\theta_0} \sigma_z$ and $A_{11} = s_{\theta_1} \sigma_x + c_{\theta_1} \sigma_z$ the following lower bounds can be obtained for standard and routed Bell strategies

$$\eta_{A_1} > \begin{cases} \frac{1}{c_{\theta_+}(c_{\theta_-} + s_{\theta_-})} & \text{Standard Bell test,} \\ \frac{1}{1 + c_{\theta_-}} & \text{Routed Bell test .} \end{cases} \tag{115}$$

As $\theta \to 0$, the critical efficiency in routed Bell scenario approaches $\frac{1}{2}$, which saturates the universal lower bound (110). There exist an explicit SRQ bound when $\eta_{A_L} = \frac{1}{1 + c_{\theta_-}}$ implying that the above bound is tight [93].

Sekatski et al. [96] consider another test of nonlocality between (A_1, B) where A_1 has a continuous number of settings $A_1 \equiv \theta \in [0, 2\pi)$ and they evaluate the following LP quantity

$$C = \int \frac{d\theta}{2\pi} \sum_{a_1, b=0, 1} (-1)^{a+b}(c_\theta p(a_1, b|\theta, 0, b) + s_\theta p(a_1, b|\theta, 1, b)) \tag{116}$$

and satisfy the Bell inequality $C \leq \frac{2\sqrt{2}}{\pi} \sin(\pi \frac{\mathcal{T}}{2})$ where $\mathcal{T} = \int \frac{d\theta}{2\pi} \sum_{a_1=0, 1} p(a_1|\theta)$ is the average click probability of A_1 detector. Thanks to this Bell inequality, a strong routed Bell inequality can be proved as follows [96]

Theorem 4. *All SRQ correlations satisfy the following tight routed Bell inequality*

$$C \leq \frac{2}{\pi} \sin\left(\frac{\pi}{2}\mathcal{T}\right) \begin{cases} \frac{\beta_0 + \sqrt{8 - \beta_0^2}}{2\sqrt{2}} & \beta_0 > 2 \\ \sqrt{2} & \beta_0 \leq 2 \end{cases} \tag{117}$$

The proof of this theorem is based on a steering scenario. Specifically, we first apply the SP-CHSH test to gather information about Bob's measurement settings, which is then used to determine whether the correlations observed in the LP are compatible with an SRQ model (92). For instance, when $\beta_0 = 2\sqrt{2}$, one can certify that the shared state ρ_{AB} is a two-qubit Bell state and Bob's measurement settings correspond to the Pauli operators σ_z and σ_x. In this case, Eq. (92) becomes equivalent to a steering scenario in which Bob's states are remotely prepared by A_1 measurements, i.e., the assemblage $\rho_{A_1|\theta}$ admits a LHV model of the form $\rho_{A_1|\theta} = \sum_\lambda p(a_1|\theta, \lambda)\rho_\lambda$. If one can show that $\rho_{A_1|\theta}$ does not admit such a model, then it exhibits steering and therefore belongs to the set $\mathcal{M}_{qqq}$. Consequently, the violation of any steering inequality certifies that the full correlations are genuinely quantum. The complete proof of this theorem in [96] uses such steering inequalities to derive Eq. (117).

If $\beta_0 = 2\sqrt{2}$, and A_1 perform all real projective qubit measurements of the form $c_\theta\sigma_z + s_\theta\sigma_x$, then $\mathcal{C} = \mathcal{T} = \eta_l$ where η_l is the transmission rate of the *LP* link (see Section 7.3). Putting these together, there is a violation of the inequality (117) that happens when

$$\mathcal{C} = \eta_l > \frac{2}{\pi}\sin\left(\frac{\pi\eta_l}{2}\right), \tag{118}$$

which can be satisfied for any $\eta_l > 0$. As a result, *the routed Bell inequality expressed in* 4 *can be violated for arbitrary transmission $\eta_l > 0$, offering a dramatic advantage in terms of robustness to loss compared to standard Bell tests.* Even when the source and detectors are not ideal but sufficiently reliable, quantum nonlocal correlations can still be established for arbitrarily low transmission, provided that the number of measurement settings on A_1 (n_{A_1}) satisfies condition $n_{A_1} > \frac{1}{\eta_l}$.

Parallel repeated routed Bell experiments. The repeated routed Bell experiments introduced in [97] work as follows: consider a Bell experiment where Alice and Bob both have N-bit strings $\boldsymbol{x} = (x_j)_{j=1}^N$ and $\boldsymbol{y} = (y_j)_{j=1}^N$ as inputs and produce N-bit strings $\boldsymbol{a} = (a_j)_{j=1}^N$ and $\boldsymbol{b} = (b_j)_{j=1}^N$. In the routed version, based on an additional input $i \in \{0, 1\}$, Alice decides to direct the transmission from the source to her measurement device A_i. The source prepares a $2^N \times 2^N$ dimensional state $|\Phi^+\rangle^{\otimes N}$, and the devices close to the source, (A_0, B) perform the following measurements

$$A_{a|x} = \bigotimes_{j=1}^N A_{a_j|x_j}, \quad B_{b|y} = \bigotimes_{j=1}^N B_{b_j|y_j}, \tag{119}$$

where

$$A_{a_j|x_j} = \frac{1}{2}\left[\boldsymbol{I}_2 + (-1)^{a_j}\left(\delta_{x_j,0}\sigma_z + \delta_{x_j,1}\sigma_x\right)\right] \quad B_{b_j|y_j} = \frac{1}{2}\left[\boldsymbol{I}_2 + \frac{(-1)^{b_j}}{\sqrt{2}}\left(\delta_{y_j,0}(\sigma_x + \sigma_z) + \delta_{y_j,1}(\sigma_x - \sigma_z)\right)\right]$$

This strategy achieves the maximal violation of the N-product CHSH inequality defined as

$$C_{A_0B}^N = \frac{1}{2^{2N}}\sum_{\boldsymbol{x},\boldsymbol{y},\boldsymbol{a},\boldsymbol{b}}(\Pi_{j=1}^N\delta_{x_jy_j=a_j\oplus b_j})\,p(a, b \mid x, y, 0) = \alpha^N, \tag{120}$$

where $\alpha = \frac{1}{2}(1+\frac{1}{\sqrt{2}})$. A penalized version of this equation with the penalty parameter q can be obtained as a generalization of the LP inequality in (104) (Also see equation (63) in [93])

$$C_{A_1B}^N(q) = C_{A_1B}^N - q\frac{1}{2^N}\sum_{\boldsymbol{x},\,\boldsymbol{a}\in\{0,1\}^N} p_A(\boldsymbol{a} \mid \boldsymbol{x}, 1), \tag{121}$$

where $q \in [0, \frac{1}{2^N}(1 + \frac{1}{\sqrt{2}})^N]$. For a strategy with A_1 clicking with efficiency η gives

$$C_{A_1B}^N(q) = (\alpha^N - q)\eta. \tag{122}$$

It is shown in [97] that when A_1 and B witness the maximal quantum violation of (120) the maximal attainable value of the q-penalized N-product CHSH inequality (121) with joint measurable measurements in A_1 satisfies the following upper bound

$$C_{A_1B(q)}^N \le \frac{1}{2^N}\left(\alpha^N - q\right), \tag{123}$$

for $q \in [\alpha^{N-1}\beta, \alpha^{N-1}]$ where $\beta = \frac{1}{8}(2 + \sqrt{2} + \sqrt{4\sqrt{2} - 2})$. Then the following result is immediately obtained

Theorem 5. *The q-penalized N-product CHSH inequality* (121) *can be violated by the strategy achieving* (123) *for $q \in [\alpha^{N-1}\beta, \alpha^{N-1}]$ whenever $\eta > \frac{1}{2^N}$.*

As a result, the threshold detection efficiency of the distant device, needed to certify non-jointly-measurable measurements, a prerequisite of secure DI-QKD, decreases exponentially with the number N of parallel repetitions.
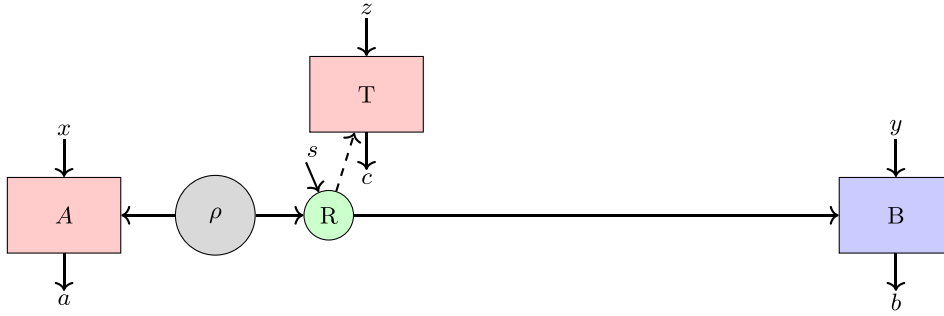
Fig. 15. rDI-QKD Protocol: Alice (*A*) and Bob (*B*) aim to establish a secret key over a long distance using the routed Bell setting. The relay (*R*) receives an input $s \in 0, 1$ and, based on its value, sends the particle from the source to either the nearby device *T* ($s = 0$) or the distant device *B* ($s = 1$).

rDI-OKD: DI-QKD based on the routed Bell test. The routed Bell scenario introduced in 3.14 exhibits features that enhance its applicability to DI-QKD and, in certain cases, provides advantages over standard Bell tests. For example, the BB84 correlations, which can be generated from a maximally entangled two-qubit state by performing measurements in the σ_x and σ_z bases, can be reproduced classically in a standard Bell setup which makes these correlations unsuitable for standard DI-QKD. However, their quantum nature can be demonstrated in a routed Bell scenario by performing random CHSH tests in the (*A*, *T*) configuration. Consider the case in Fig. Fig. 15 where *A* and *T* are two devices close to the source and the device *B* is located far from the source and the purpose is to establish a key between *A* and *B*. As in standard DI-QKD, all components including the relay *R* are untrusted. The only assumption is that they obey certain no-signaling constraints preventing them from signaling arbitrarily to each other.

Unlike standard DI-QKD, some particles emitted from the source are routed to the testing device *T* instead of *B*. The output of these cases always contributes to parameter estimation and cannot be used to generate a key.

The rDI-QKD protocol introduced in [95] as follows: in each round of the protocol, Alice generates independent random variables $X_i \in \mathcal{X}$ and $s_i \in \{0, 1\}$ and feed them to her device *A* and the relay *R*, respectively. Based on the value of s_i, two cases can occur:

1. $s_i = 0$: Bob's quantum particle is routed to *T*, in this case, Alice generates a random variable *Z* and feeds it to *T*. She records the output variable A_i and publicly announces S_i.
2. $s_i = 1$: Bob's quantum particle is routed to *B* where Bob generates a random variable $Y_i \in \mathcal{Y}$, feeds it on his device, and records the output B_i.

After all rounds, Alice and Bob check the date for which $s_i = 0$ to see if they violate a routed Bell inequality. On the other hand, they agree on a subset of the rounds to generate the raw key. Finally, if the test of violating a routed Bell inequality is passed, they apply error correction and privacy amplification to extract the secret key.

An important condition must be satisfied for the security of rDI-QKD. This condition is captured in the following theorem [95].

Theorem 6. *Long-range quantum correlation as defined in* 19 *is necessary for the security of rDI-QKD.*

Proof. The proof can be done by contradiction. Let us consider that Alice and Bob only generate the SRQ correlation of the form (92), then Eve can perform the parent POVM $N = \{N_\lambda\}$ on the public channel between *R* and *B*. Since Eve can keep a copy of the classical outcome λ, the correlation between *A* and *B* was factorized when conditioned on Eve's information, i.e. $p(a, b|x, y, \lambda) = p(a|x, \lambda)p(b|y, \lambda)$, implying that no secure key can be extracted between *A* and *B* when only an SRQ correlation exists in the protocol. □

General behavior of eavesdropper in rDI-QKD. Based on the location of the relay *R*, the device *T*, and the source, two situations can be considered: first, consider them as being outside Alice's and Bob's labs and in full control of the eavesdropper, and the second option is to assume that the relay *R* and the device *T* are all situated in Alice's lab by imposing the condition that they cannot arbitrarily communicate their private input to Alice's device. Clearly, security in the first case also implies security in the second case, since in the first case, the eavesdropper has more power. The protocol in [95] considered the first case in which Eve has the measurement device *T* that performs a measurement $T_z = \{T_{c|z}\}$ that acts jointly on the subsystems *B* and *E* when $s = 0$, as this is the most general thing she can do to simulate the honest correlation between *A* and *T*. Considering this behavior for Eve, the secret key rate can be calculated using the method explained in Section 5.2.2.

To conclude the list of the CHSH-like protocol, in the following, we update the list of critical detection efficiency from Ref. [89].

DI-QKD protocols beyond binary inputs and outputs. Up to now, we have discussed DI-QKD protocols with two inputs and two outputs. It is worth mentioning some results beyond this scenario: Ref. [283] for BI I^4_{4422} (also in [284]); Ref. [279] for BI I_{234} with $T = \mathrm{id}$. Both of these protocols perform better than the CHSH_χ protocol [73], but not as good as the $\mathrm{CHSH}_{p_{\nu_p}}$ protocol with $T = \mathrm{fp}$ [89]. This motivates the research to characterize any Bell scenario [285–289]. Given a Bell scenario, find the largest gap $\beta_\mathcal{Q} - \beta_\mathcal{L}$ is promising, but does not guarantee a good QKD performance as many aspects needs to be further addressed. Among them, *memory loophole*.

3.15. DI-QKD memory loopholes

We discussed the theoretical security proofs of (fully)-DI-QKD. However, to satisfy the definition of *universal composable security* the theory demands many different devices at each run to close *memory attack loophole*, i.e. a leakage of information due to correlated subsequent outputs [78,240,290]. This is experimentally critical. Suppose that Alice and Bob have only one device each. Then a memory attack is possible: the protocol is run on day i, generating $K^i_A = K^i_B$, while informing Eve on day $i = 1$ of the hash functions used by Alice for postprocessing.

Eve can instruct the devices to proceed as follows. On day 2, Eve modulates ρ^c_{AB} where c is a classical ancilla to carry new instructions to the device in Alice's lab as discussed in *collective attacks in QT*. These instructions tell the device the hash functions used on day 1, allowing Eve to compute $K^1_A = K^1_B$. The classical ancillae also instruct the device to bias the protocol for randomly selected inputs by producing specified bits from this secret key as outputs for example by programming the device to announce one key bit of day 1 as an output of some specified input. If any of these selected outputs are among those announced in the parameter estimation step, Eve learns the corresponding bits of day 1's secret key. But, Alice or Bob might abort the protocol any day, thus, by waiting long enough, Eve can program them to communicate some or all information about their day 1 key to obtain N secret bits from day 1 and then program it to abort on the day $N + 2$ since from this day Alice and Bob do not have any secret key available. This type of attack is called an *abort attack* and cannot be detected until it is too late. To defend against these attacks *(i)* all quantum data and public communication come only from Alice, even if, Eve can still program Alice's device to leak K^1_A or K^i_A, $i = 1, 2, \dots$ via the abort attack; *(ii)* encrypt $c_\mathcal{Q}$ with some initial preshared seed randomness, even if fails if an abort attack involves communication with multiple users who may not be trustworthy; *(iii)* additional independent measurement devices close memory attack loophole, but leave open the imposter attack [78].

4. Other device-independent protocols

The device-independent framework can be extended to other cryptographic primitives that rely on similar physical assumptions and security techniques. In this section, we briefly discuss three such protocols: device-independent quantum random-number generation, quantum secret sharing, and quantum secure direct communication. In the same fashion as DI-QKD, these protocols exploit BI violations to achieve secure operation with untrusted devices, and their security analyses often rely on comparable tools such as entropy accumulation and randomness extraction.

4.1. DI quantum random number generation (DIQRNG)

The fact that the decay of the isotope that kills Schroedinger's cat is an intrinsically random event means that the cat is in the superposition state $|\mathrm{cat}\rangle = \alpha|\mathrm{alive}\rangle + \beta|\mathrm{dead}\rangle$. This is in contrast to simple ignorance of the observer, who would describe the cat in the statistical mixture $\rho_{\mathrm{cat}} = \alpha\rho_{\mathrm{alive}} + \beta\rho_{\mathrm{dead}}$. Both examples give a probabilistic prediction concerning the status of the cat. However, it is only in the former case that true unpredictability is present. Associating random bits to the clicks of a Geiger counter, already in the 1940s, is based on this idea [291]. However, in practice, the ontological quantum randomness, appearing in the superposition state $|\mathrm{cat}\rangle$, is difficult to distinguish from the randomness due to the "classical ignorance" present in the mixture ρ_{cat} [292].

Realism in Bell's hypothesis (Definition 1) rules out any intrinsic randomness. Therefore, a Bell-inequality violation not only produces randomness but also − in a device-independent way − certifies that this randomness cannot be mimicked by a classical mixture [293,294]. More quantitatively, for iid trials the *conditional smooth min-entropy*

$$H^\varepsilon_{\min}(AB|XYE) \geq nf(\beta_\mathcal{Q}) \equiv -n\log_2\left(\frac{1}{2} + \frac{1}{2}\sqrt{\frac{\beta^2_\mathcal{Q}}{4} - 1}\right), \tag{124}$$

where E denotes the adversary's quantum side information, n is the number of rounds is tight for CHSH [112,153]. Eq. (124) lower-bounds the number of uniform bits that can be extracted with a strong randomness extractor. The Bell tests use initial classical randomness for the choice of the settings, DIQRNGs *expand* randomness rather than *produce* it. Since then, the terms *randomness expansion* and *randomness generation* have been used in the DIQRNG literature interchangeably. A DIQRNG consumes a short, uniformly-random seed R_{in} to choose the settings (X, Y), and − upon observing a BI violation − outputs a longer string R_{out}; the expansion factor is $|R_{\mathrm{out}}|/|R_{\mathrm{in}}|$. Unbounded expansion is possible using two interleaved devices that alternately supply fresh settings for each other [295]. Finite-size analyses must account for statistical fluctuations (via, e.g., Azuma–Hoeffding inequalities) and possible memory attacks that correlate different rounds. The theoretical and experimental challenges follows:

Table 6
Key milestones in DIQRNG and certified randomness. Only experiments that reported a full finite-size analysis and extractor implementation are listed.

Platform	β_Q value	Net random bits
Photonic (heralded) "10 [153]	2.41 ± 0.10	42 bits
Photonic time-bin "18 [296]	2.63 ± 0.04	6×10^6
Photonic (NV centers) "18 [297]	2.34 ± 0.18	1.02×10^7
Photonic (SNSPD, spot-checking) "21 [300]	2.75 ± 0.02	1.18×10^9
Superconducting qubits "23 [301]	2.0747 ± 0.0033	$\sim 10^5$
Photonic two-photon interference "23 [302]	2.62 ± 0.03	$\sim 10^6$
Trapped-ion processor (cloud) "25 [303]	RCS,*	7.1×10^4

Random circuit sampling certificate rather than CHSH.

- **Detection & locality loopholes.** A DIQRNG must simultaneously close the detection and locality loopholes; otherwise an adversary can fake a violation and inject deterministic bits. This demands overall detection efficiencies $\eta \gtrsim 90\%$ and space-like separation of the measurement events.
- **Finite-key effects.** High Bell values are necessary but not sufficient; one must also accumulate a sufficiently large dataset before the entropy rate in (124) becomes positive.
- **Rate versus security trade-off.** Short gate times and high-brightness entangled sources improve rates but exacerbate multi-pair noise, which lowers S.
- **Contrast with DI-QKD.** In DI-QKD, the raw outcomes A and B are further processed into a shared secret key. Besides randomness, one must bound the *Holevo information* $\chi(E : K)$ leaked to an eavesdropper, perform information reconciliation, and authenticate classical communication, which reduces the asymptotic key rate per run to $R_{\text{key}} \leq H_{\min}(AB|E) - H_{\max}(A|B)$. Moreover, DI-QKD typically requires distributing entanglement over *kilometer* scales, whereas DIQRNG may keep both measurement stations on a single optical table. Conversely, DI-QKD is tolerant to *loss* (lost events are simply discarded) but highly sensitive to *phase noise*, while DIQRNG demands near-unit detection efficiency but can operate with smaller spacings.

The first experimental demonstration of randomness expansion was presented in [75]. The experiment there was based on the violation of CHSH in a setup which used heralded entanglement generation through entanglement swapping. Later, experiments also based on CHSH but involving direct production of entanglement were performed [296–300]. Table 6 compiles the most influential experimental demonstrations to date.

Device-independent protocols continue to push both theoretical and technological boundaries [304]. Near-term goals include (i) giga-bit-per-second DIQRNG via multiplexed sources and feed-forward switching, (ii) metropolitan-scale DI-QKD combining satellite links with ground-based quantum repeaters, and (iii) hybrid protocols that merge computation-based certification (as in random circuit sampling) with Bell-test randomness to relax detection efficiency requirements.

4.2. Device-independent quantum secret sharing

Quantum secret sharing (QSS), introduced first in [305], is a multiparty communication protocol where a dealer tries to share a secret among a number of participants in such a way that a set of participants is needed to recover the secret. Each QSS includes three stages: Data gathering, Parameter estimation, and Key extraction.

The first device-independent quantum secret sharing (DI-QSS) protocol was introduced in [306], based on an N-partite d-dimensional XOR game; however, it was limited to cases where d is an even number. Almost simultaneously, it was shown in [307] that in a three-party protocol, a maximal violation of Svetlichny's inequality [308] guarantees that an untrusted receiver cannot obtain any information about the secret unless they collaborate with the other parties. In cases of non-maximal violation, the adversary's access to the secret can still be limited. The advantage of using Svetlichny's inequality lies in its ability to certify a stronger form of nonlocality, one that even an untrusted party (as in three-party QSS) cannot simulate. The security analysis robust individual and collective attack is respectively in [307,309]. Suppose that three separated parties, Alice, Bob, and Charlie, measure their photons with their binary measurement settings x_i, y_j, and z_k, respectively, where $i, k \in \{0, 1\}$, and $j \in \{0, 1, 2\}$ and obtain the outcomes a_i, b_j, and c_k, (all with binary outcomes -1 and 1); therefore, the Svetlichny polynomial S_{ABC} can be written as the combination of the CHSH polynomials

$$S_{ABC}^{\text{Svetlichny}} = \langle S_{AB}^{j=2,3} c_2 \rangle + \langle S_{AB}' c_1 \rangle, \tag{125}$$

where $S_{AB}^{j=2,3}$ is the CHSH value between Alice and Bob with $y_j = \{2, 3\}$ measurement settings, and S'_{AB} is obtained from $S_{AB}^{j=2,3}$ by mapping $b_2 \to b_3$ and $b_3 \to -b_2$. As a result of (125), the violation of the Svetlichny inequality for three users is equal to the violation of the CHSH inequality for Alice and Bob. Consequently, the security proof of DI-QSS is similar to the one for DI-QKD given in Section 3.5 (see equation (70)). By assuming that each user successfully detects the transmitted

photon with a global detection efficiency η and considering the white noise model with the fidelity F for photon loss and decoherence ($\rho = F|GHZ\rangle\langle GHZ| + \frac{1-F}{8}I$), the following lower bound can be obtained [309]

$$r \geq 1 - h\left(\frac{\sqrt{2F^2\eta^6 - 1}}{2} + \frac{1}{2}\right) - h\left(1 - \frac{1}{2}\eta^3 - \frac{1}{2}\eta^3 F\right). \tag{126}$$

A positive value of r requires high global detection efficiency and fidelity. For example, with no decoherence ($F = 1$), the detection efficiency threshold is 96.32%; at $F = 0.95$, it increases to 97.57%. The minimum tolerable fidelity is 85.1%. Below either threshold, no key can be generated.

The high detection efficiency thresholds in DI-QSS arise from the need to distribute multiphoton entanglement among multiple parties through noisy quantum channels. Photon loss in each channel can destroy the entanglement, making DI-QSS especially vulnerable to such losses. Consequently, it is crucial to develop methods that reduce the global detection efficiency requirement and improve noise tolerance for practical implementations. Similar techniques such as noise preprocessing and random postselection used for DI-QKD have been shown to enhance DI-QSS performance [309]. Building on this, Ref. [310] combined these techniques with a random key generation basis (see Section 3.11) and demonstrated that the global detection efficiency can be reduced to 93.41%.

4.3. Device-independent quantum secure direct communication

Unlike QKD, quantum secure direct communication (QSDC) enables the sender to transmit secret messages directly to the receiver without first establishing a shared key. The QSDC protocol was introduced in Ref. [311], leveraging quantum entanglement and block transmission techniques. In QSDC protocols, photons are transmitted in two rounds. Therefore, to achieve device-independent QSDC (DI-QSDC), a security check based on the BI violation is performed after each transmission round. A more robust security against collective attacks, instead, is in Ref. [312]. The protocol works as follows: Alice has three measurement settings $x \in \{0, 1, 2\}$ and Bob has two measurement settings $y \in \{0, 1\}$ same as CHSH$_\chi$ protocol. Alice prepares n EPR pairs, divides them into two sequences and sends one to Bob. They perform the first security check (a CHSH test) by measuring a subset of EPR pairs. If the security check passes, Alice selects a subset of photons as checking photons and does not perform any operation on them. For the rest of them, she uses four operations, I, σ_x, σ_y, and $i\sigma_z$ to encode the message and then sends all of her photons to Bob and reveals the position of each message photon and each checking photon through a classical channel. Bob performs the second security check on checking photon pairs on his own. If the second security check passes, Bob can read Alice's message by performing a Bell measurement on the message pairs.

Since in DI-QSDC there is no key generation between two parties, to study the security of the DI-QSDC, the communication efficiency E_c is defined [312] as the amount of transmitted correct secure information qubits divided by the total amount of information qubits. Similar as the DI-QKD, for collective attacks it can be lower-bounded by the Devetak–Winter rate (74). Since both security checking processes of the DI-QSDC are the same as that of DI-QKD, the following lower bound can be obtained

$$E_c \geq 1 - h(Q) - h\left(\frac{1 + \sqrt{(\frac{\beta_1}{2})^2 - 1}}{2}\right) - h\left(\frac{1 + \sqrt{(\frac{\beta_2}{2})^2 - 1}}{2}\right), \tag{127}$$

where β_1 and β_2 are the CHSH values for the first and second security checks, respectively. Since DI-QSDC requires two rounds of photon transmission, the influence of environmental noise and eavesdropping on DI-QSDC is more serious than DI-QKD. To compensate for these negative effects, the methods entanglement-based noiseless linear amplification and entanglement purification protocols can be applied to DI-QSDC. In a modified protocol with both of these methods, Alice and Bob can have a near-perfect entanglement channel where the secure communication is effectively extended and Eve cannot steal any secure information without being detected.

Other DI-QSDC protocols have been proposed since then. A one-step DI-QSDC protocol was proposed in [313], wherein Bob prepares a large number of polarization-spatial mode hyperentangled photon pairs, transmit one photon from each pare to Alice in a single round, performs CHSH tests on both degrees of freedom, and Alice encodes her message in the polarization mode. Combining it with the hyperentanglement heralded amplification and the hyperentanglement purification can eliminate the message loss and the message error caused by the channel noise. A DI-QSDC protocol based on single-photon sources and the heralded Bell state measurement was introduced in [314], where Alice and Bob each have two photon sources send one photon to a third party who performs a Bell state measurement, and if the measurement is successful, then they have an entanglement channel that can be used to send the message. The DI-QSDC protocol with hyper-encoding technique was studied in [315], and non-Markovian dynamics have been shown to enhance protocol security compared to their Markovian counterparts significantly [316].
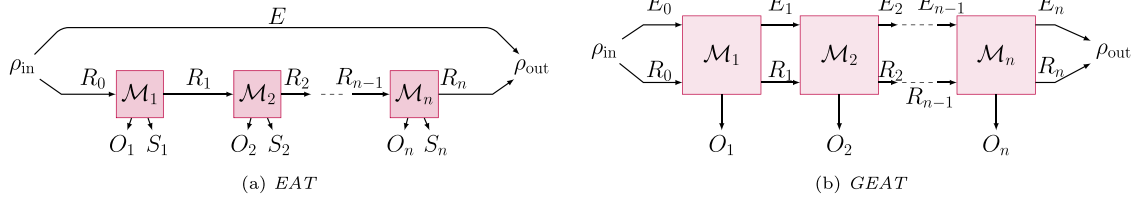
Fig. 16. (Generalized) Entropy accumulation theorem − 16(a) sequential processes $\bigcirc_{i=1}^n \mathcal{M}_i \otimes \mathrm{id}$ with $\mathcal{M}_i : R_{i-1} \mapsto R_i O_i S_i C_i$, and its generalization $\bigcirc_{i=1}^n \mathcal{M}_i$ with $\mathcal{M}_i : R_{i-1} E_{i-1} \mapsto R_i E_i O_i S_i C_i$ in 16.

5. Mathematical techniques for advanced security proofs

In the previous section, we examined a secure protocol for generating a secret key K, along with its associated security proof, treating it as an independent *module*. We analyzed lower bounds on Eve's uncertainty or randomness under various types of attacks − individual, collective, and coherent − to establish robust security guarantees. While Section 3 demonstrated the feasibility of such protocols, our current focus is on optimizing the key rate by considering correlations across protocol rounds. Broadly, there are two categories of protocols: those based on the (Generalized) Entropy Accumulation Theorem and Quantum Probability Estimation, as well as complementarity-based methods. These are typically used in *sequential implementations*, where each round of the protocol depends on the outcomes of previous rounds. This contrasts with *parallel approaches*, which require distinct analytical techniques. In this section, we explore advanced mathematical methods for constructing such security proofs in real-world settings.

5.1. Entropy accumulation theorem (EAT)

Let us begin with some key definitions required for a formal description of EAT.

Definition 20 (*Sequential Process*). We call *sequential process* the composition map $\mathcal{M} = \bigcirc_{i=1}^n \mathcal{M}_i$, where $\mathcal{M}_i : R_{i-1} \mapsto R_i O_i S_i C_i$ are CPTP maps that transform the state on R_{i-1} (quantum registers) into R_i, with output quantum system O_i (readout observed outcome), S_i (side information), C_i (classical check), and where the composition $\bigcirc_{i=1}^n \mathcal{M}_i$ is defined as $\mathcal{M}_n \circ \cdots \circ \mathcal{M}_1$, acting sequentially on the quantum registers.

As in Fig. 16(a), in the ith round, the internal state in the input memory R_{i-1} is updated to the output memory R_i ensuring that the state at the step i depends on the previous one (non-iid). At each i, the quantum output system in the register O_i *accumulates* the entropy of Eve. The leaked information (about the measurements or outcomes) is in the partial state on the support of S_i and the environment "controlled" by Eve in the Hilbert space E. The conditional entropy $H(O_1^n|S_1^n E)$ quantifies how much uncertainty remains about the update post-measurement state outputs O_1^n after Eve learns the side information S_1^n and external system E. The quantity X_1^n refers to the whole process of n rounds where each round i is isomorphic the $i = 1$. The protocol is considered secure if the entropy in Eq. (40) is higher than a lower bound from parameter estimation that is computed by other output $c_i^{(j)}$ or simply $c_i \in C_i$ stored in a classical register $C_i = \{c_i^{(j)}\}_j$ with probability distribution $p_i^{(j)} = p(c_i^{(j)})$ such that $\sum_j p_i^{(j)} = 1$, $p_i^{(j)} \geq 0$. This is derived from the system $\rho_{O_i S_i}$ and used for BI violation.

Definition 21 (*Markovianity*). Given $\mathcal{M}$ a sequential process from 20. It is *Markovian* iff $O_{i-1} \leftrightarrow S_{i-1} E \leftrightarrow S_i$, i.e. the mutual information $I(O_{i-1} : S_i | S_{i-1} E) = 0$

Definition 22 (*Trade-off Functions*). The following quantum state set

$$\Sigma_i(p_{i_j}) = \{\rho_{R_i O_i S_i C_i E} = \mathcal{M}_i(\rho_{R_{i-1}} E) | \rho_{C_i} = \rho_{c_{i_j}} = p_{i_j} \in C_i\} \tag{128}$$

with ρ_{C_i} defines in the classical register C_i the probability distribution with weight $p_{i_j} = \langle c_{i_j} | \rho_{C_i} | c_{i_j} \rangle \geq 0$ and $\sum_j p_{i_j} = 1$ on the possible classical output c_{i_j} in the ith round. Given p_{i_j}, then real functions $f_{\min}$ and $f_{\max}$ are called *min(max)–tradeoff function* for $\mathcal{M}_i$ if respectively

$$f_{\min}(p) \leq \inf_{\rho \in \Sigma_i(p)} H(O_i|S_i E)_\rho, \qquad f_{\max}(p) \geq \sup_{\rho \in \Sigma_i(p)} H(O_i|S_i E)_\rho \tag{129}$$

The function f is adequate to quantify the accumulated entropy in a single step of the process because it balances between overly optimistic and pessimistic entropy estimates. A naive approach might use the conditional von Neumann entropy $H(O_2|O_1)$, which averages the entropy over all states and overestimates the extractable randomness. On the other hand, a worst-case min-entropy $H_{\min}^{\mathrm{w.c.}} = \min_{o_1, o_2}[-\log \Pr(o_2|o_1)]$ is too pessimistic, as it fails to capture the realistic entropy when the systems are independent. The correct definition considers the worst-case state o_1 but averages the entropy contribution $-\log \Pr(o_2|o_1)$ over o_2, leading to $\min_{o_1} \mathbb{E}_{o_2}[-\log \Pr(o_2|o_1)] = \min_{o_1} H(O_2|O_1 = o_1)$.
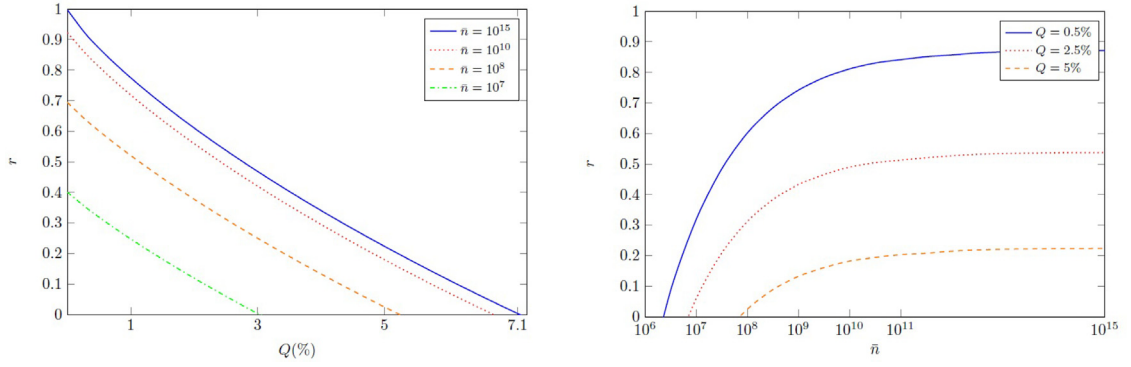
Fig. 17. Figure from [105]. (left) The expected key rate versus the QBER is lower for finite n and with a security proof against coherent attacks than the one against individual and collective attacks. (Right) The expected key rate as a function of the number of rounds $\bar{n}$.

Definition 23 (*Events on Classical Registers*). The classical registers C_i defines the following classical probability space $(\Omega, \mathcal{B}(\Omega), p)$ where the sample set

$$\Omega = \{\omega = (c_1, \ldots, c_n) | \forall i, \ c_i \in \{c_{i_j}\}_j\} \subseteq C_1 \times \ldots \times C_n \equiv C^n \tag{130}$$

contains the results from each step extracted by $\rho_{O_i S_i}$ for $i = 1, \ldots, n$ so that the updated final state reduced to the classical registers C^n is the probability distribution $\rho_{C^n} = p(\omega)$, with $\omega \in \Omega$. The updated final state at the output of the sequential process conditioned by the event ω is denoted as $\rho_{|\omega} \in \bigotimes_{i=1}^n \Sigma_i(p_i) \subseteq \bigotimes_{i=1}^n R_i O_i S_i C_i E = R_1^n O_1^n S_1^n C_1^n E$ (denoting, e.g. $R^n \equiv R^{\otimes n}$). With this notation, each register is isomorphic to the corresponded register at round $i = 1$. $\mathcal{B}(\Omega)$ is the Borel σ–algebra.

Note that the trade-off functions applied for the probabilities $p(\omega)$ have consistent bound from all the other quantum output $O_1, \ldots, O_n \equiv O_1^n$ and similarly S_1^n. For instance $\inf_{\rho_{|\omega}} H(O_1^n | S_1^n E)_{\rho_{|\omega}} \geq f_{\min}(p(\omega))$. Using these definitions, EAT can be stated as the following theorem.

Theorem 7 (Entropy Accumulation Theorem). *Given a Markovian sequential process $\mathcal{M} = \bigcirc_{i=1}^n \mathcal{M}_i \otimes \mathrm{id}$ (see Fig. 16(a)) such that the output state is $\rho_{|\omega} = \mathcal{M}(\rho_{\mathrm{in}})$, a convex $f_{\min}(p(\omega)) \geq t$ with $t \in \mathbb{R}$, and $\varepsilon \in (0, 1)$, then*

$$H_{\min}^{\varepsilon}(O_1^n | S_1^n E)_{\rho_{|\omega}} \geq nt - \nu\sqrt{n}, \qquad \nu = 2\left(\log(1 + 2\dim O_i) + \lceil \| \nabla f_{\min} \|_\infty \rceil\right)\sqrt{1 - 2\log(\varepsilon p(\omega))}. \tag{131}$$

Proof (*Details in Refs. [108,109]*). The smooth min-entropy $H_{\min}^\epsilon$ is related to the sandwiched Rényi entropy H_α for some parameter $\alpha > 1$ used to decompose the entropy of the full sequence into a sum of conditional entropies for each round: $H_\alpha(O_1^n | S_1^n E) \approx \sum_{i=1}^n H_\alpha(O_i | S_i E)$. The Markovianity ensures that each term $H_\alpha(O_i | S_i E)$ depends only on the previous rounds and not the entire sequence. Now, H_α can be bounded by the von Neumann entropy $H(O_i | S_i E)$ using properties of the Rényi entropy $H_\alpha(A_i | B_i R) \approx H(A_i | B_i R) - \mathcal{O}(\alpha - 1)$. Combining this with the tradeoff function $f_{\min}$, which lower bounds $H(O_i | S_i E)$, we get: $H_\alpha(A_i | B_i R) \geq f(p(\omega)) - \mathcal{O}(\alpha - 1)$. The distribution $p(\omega)$ of the classical outcomes is used to bound the entropy of the sequence. The observed event Ω ensures that $f(p(\omega)) \geq t$, i.e. the entropy rate averaged over all rounds is at least t. The finite-size effects arise because n is finite and $f_{\min}$ depends on the second order statistical fluctuations $\nu\sqrt{n}$ in the observed data. The sandwiched Rényi entropy H_α is converted to the smooth min-entropy $H_{\min}^\epsilon$. Thus, the total smooth min-entropy grows approximately *linearly* with n, up to finite-size corrections. $\square$

Finite key analysis with EAT. Thanks to EAT, the key rate r of CHSH protocol versus the QBER Q can be predicted at finite n (see Fig. 17). For $n = 10^{15}$, the curve nearly overlaps the asymptotic iid case 3.5, which was shown to be optimal allowing the protocol to tolerate up to $Q = 0.071$. Instead, for non-iid coherent attack analysis, the key rate obtained in [81] remains well below the lowest curve presented in Fig. 17, even if the number of signals approaches infinity, with a maximum noise tolerance of only 1.6%.

Fig. 17 shows the key rate as a function of the number of rounds n, for different values of Q. Evidently, the rates achieved are significantly higher than those without EAT, and are comparable to the key rates of the practical device-dependent QKD with the difference that the device-independent one requires a larger n. Indeed, the finite-key analysis in Ref. [105] shows that the experiments [100,207] require, respectively, $n = 10^8$ and $n = 10^{10}$ rounds against coherent attacks for $r > 0$. This analysis involves noisy preprocessing, random key measurements, and modified CHSH inequalities. While this is a marked improvement wrt the basic protocol in [73] (Section 3.5) (which yields zero asymptotic key rates for those experiments), the values of n are still impractical. Therefore, two modifications were applied: (*i*) a pre-shared key, which results in a net key generation rate approximately double that of the original protocol; (*ii*) relax the protocol by considering the collective-attacks assumption to alter its structure and enhance the key rate. However, despite the drop in $n \sim [10^6, 10^7]$ the required number of rounds remains impractically large.

Entropy accumulation theorem with improved second order. EAT theorem provides tight bounds only at the first order. The second-order term can be improved in many protocols of interest, where the entropy is estimated by testing positions with probability $O(n^{-1})$. Since $v_1 \propto \| \nabla f_{\min} \|_\infty \propto O(n)$, this gives $v_1\sqrt{n} \gg tn$. Ref. [317] show the correction, $H^\varepsilon_{\min}(K_1^n \mid S_1^n E) \geq nt - (v_1\sqrt{n} + v_2)$, with v_2, a functions of ε, the maximum dimensions of the systems K_i (d_K), and the variance of the function f. This further improvement contributes to reducing n. In recent works on DI-QKD [54] and randomness expansion [299,318], the improved second-order term is explicitly employed to derive positive key rates and certify randomness with realistic experimental resources. Without this advancement, the required number of Bell test rounds would be orders of magnitude larger, making such protocols infeasible with current technology.

5.2. Generalized entropy accumulation theorem

EAT is incompatible with prepare-and-measure protocols because it assumes Markovianity, where side information ρ_{S_i}, once output, cannot be updated so that the total side information is in ρ_{ES^n}. But in prepare-and-measure protocols, Eve intercepts ρ_i at the ith round and updates her side information $\rho_{S_1,\dots,S_i}$ so that the total side information is higher than the one in $\rho_{ES_1^n}$. Although Markovianity allows estimating the smoothed min-entropy from a single round, it conflicts with the dynamic nature of side information in prepare-and-measure scenarios. For these protocols, to apply EAT one must first convert the protocol to an Entanglement-based one. To illustrate what could happen without Markovianity, consider a case where K_i is classical and no side information is output in the first $n-1$ rounds. Consider the side information of the last round in ρ_{S_n} that contains a copy of the systems A_n which can be passed along during the process in the systems R_i. Then, $H^\epsilon_{\min} = 0$ while for the previous $n-1$ rounds, each single-round entropy bound that only considers the system K_i and S_i can be positive. To address these issues, the *Generalized Entropy Accumulation Theorem (GEAT)* replaces the Markov condition with a natural non-signaling condition between past outputs and future side information [29].

Definition 24 (*Non-signal Process*)**.** Given $\mathcal{M}$ a sequential process from 20. It is *non-signal* if

$$\forall \mathcal{M}_i \qquad \exists \mathcal{R}_i : E_{i-1} \to E_i \text{ CPTP s.t} \qquad \mathrm{Tr}_{K_i R_i} \circ \mathcal{M}_i = \mathcal{R}_i \circ \mathrm{Tr}_{R_{i-1}}. \tag{132}$$

Let us consider the systems R_{i-1} and $R_i K_i$ as the inputs and outputs on "Alice's side" of $\mathcal{M}_i$, and E_{i-1} and E_i as the inputs and outputs on Eve's side, then Eq. (132) states that the marginal of the output on Eve's side cannot depend on the input on Alice's side. This is exactly the non-signaling condition of Eq. (7) in non-local quantum games.

Theorem 8. *Given a non-signal sequential process $\mathcal{M} = \bigcirc_{i=1}^n \mathcal{M}_i$ with $\mathcal{M}_i : R_{i-1}E_{i-1} \to R_i K_i C_i E_i$ (see Fig. 16) such that the output state is $\rho_{|\omega} = \mathcal{M}(\rho_{\mathrm{in}})$, an affine min-tradeoff f such that $t = \min f(p(\omega))$, $\varepsilon \in (0,1)$, $\alpha \in (1, \frac{3}{2})$, then*

$$H^\epsilon_{\min}(K^n|E_n)_{\rho_{|\omega}} \geq n\left(t - \frac{\alpha-1}{2-\alpha}\frac{\ln 2}{2}V^2 - \left(\frac{\alpha-1}{2-\alpha}\right)^2 K'(\alpha)\right) - \frac{g(\epsilon) - \alpha \log p(\omega)}{\alpha-1}, \tag{133}$$

where $p(\omega)$ is the probability of observing event ω, and

$$g(\epsilon) = -\log(1 - \sqrt{1-\epsilon^2}), \quad V = \log(2d_A^2 + 1) + \sqrt{2 + \Delta_f}, \quad K'(\alpha) = \frac{(2-\alpha)^3 \ln^3(2^\beta + e^2)}{6(3-2\alpha)^3 \ln 2} 2^{\frac{\alpha-1}{2-\alpha}(\beta + \log d_A)} \tag{134}$$

with $d_A = \max_i d_{A_i}$, $\Delta_f = \mathrm{Var} f$ and $\beta = \log d_A + Max(f) - Min_\Sigma(f)$

The GEAT deals with a sequence of channels $\mathcal{M}_i$ that can update both the internal memory register R_i and the side information register E_i (subject to the no-signaling condition of Eq. (132)), while EAT sequential channels *do* not update from each round the side information in the next rounds. As a result, GEAT is strictly more general than the EAT [29]. The B92 protocol and BB84 decoy-state protocol, lacking direct conversion to an entanglement-based form, cannot use EAT for security proof but it is based on GEAT [94,319].

Before (G)EAT the security proof bounds utilized de Finetti-type theorems combined with the QAEP, but with several drawbacks: (i) applicable only under specific assumptions regarding the symmetry of the protocols robust only against specific attacks; (ii) limited in the practically finite-size analysis; (iii) limited in a device-independent context. Entropy Accumulation Theorem (EAT) [108,317,320] applied for DI-QKD [321] solve these drawbacks. However, if condition (i) is satisfied, the security of DI-QKD against coherent attacks follows from security under the iid assumption. Moreover, the dependence of the key rate on the number of rounds, n, is the same as that in the iid case, up to terms that scale like $\frac{1}{\sqrt{n}}$. As a consequence, one can extend tight results known for DI-QKD, under the iid assumption, to the most general setting. This yields the best rates known for any protocol for a DI cryptographic task as shown in Fig. 17 for $n = 10^{15}$.

5.2.1. Security of E91 with (G)EAT

To study the security of E91 (introduced in Section 3.3), we consider a simplified version where, in each round $i \in [n]$, Alice and Bob independently choose basis bits $x_i, y_i \in \{0,1\}$ such that $\Pr[x_i = y_i = 1] = \mu$ (diagonal basis) and $\Pr[x_i = y_i = 0] = 1 - \mu$ (computational basis). Defining $x^n := (x_1, \dots, x_n)$ and $y^n := (y_1, \dots, y_n)$, they announce

their bases and keep the subset $S = \{i : x_i = y_i\}$, with Alice's sifted string denoted A_S and Eve's total side information represented by E.

Using EAT, one obtains the finite-size bound (Dupuis et al. [108] Theorem 5.1)

$$H_{\min}^{\varepsilon}\big(A_S \mid x^n y^n E\big)_{\rho_{|\omega}} \geq n\big(1 - 2\mu - H(e)\big) - O(n), \tag{135}$$

where e is the observed phase-error rate on rounds with $x_i = y_i = 1$.

Information reconciliation leaks at most $n\vartheta_{\mathrm{EC}}$ syndrome bits, so privacy amplification produces a κ-bit secret key whenever

$$\kappa \leq H_{\min}^{\varepsilon}\big(A_S \mid x^n y^n E\big)_{\rho_{|\omega}} - n\vartheta_{\mathrm{EC}} - O(1). \tag{136}$$

Dividing (136) by n and inserting (135) yield the finite-size key-rate condition,

$$r = \frac{\kappa}{n} < 1 - h(e) - \vartheta_{\mathrm{EC}} - 2\mu. \tag{137}$$

In the asymptotic limit $n \to \infty$ with sampling fraction $\mu \to 0$, all finite-size terms vanish and (137) reduces to

$$r_{\infty} = 1 - h(e) - \vartheta_{\mathrm{EC}}. \tag{138}$$

When applying GEAT to the same E91 protocol, it can be seen explicitly that the single-round trade-off function and testing step do not change, and the remainder of the security proof is exactly as EAT. As a result, GEAT does not change the key rate obtained by EAT; however, GEAT drops the Markov assumption, so one can treat protocols (e.g. prepare-and-measure or ones with device memory) that EAT could not handle at all.

5.2.2. Security of rDI-QKD with GEAT

An rDI-QKD protocol introduced in 3.14 mainly differs from DI-QKD in the quantum measurement phases $\mathcal{M}_i$. To see it more clearly, let us focus on each step i. Conditioning on the input classical variables x_i, s_i, z_i, and y_i, each $\mathcal{M}_i$ can be described as a CPTP map $\mathcal{M}_i : \mathcal{Q}_{A_{i-1}}\mathcal{Q}_{B_{i-1}}E_{i-1} \to A_i B_i C_i \mathcal{Q}_{A_i}\mathcal{Q}_{B_i}E_i$ that takes as input the quantum registers $\mathcal{Q}_{A_{i-1}}$ (Alice's private measurement device A), $\mathcal{Q}_{B_{i-1}}$ (B's private measurement device B), and E_{i-1} (Eavesdropper Eve) and outputs the classical variables A_i, B_i, C_i along with updated quantum registers $\mathcal{Q}_{A_i}$, $\mathcal{Q}_{B_i}$, and E_i. By including the additional data in rDI-QKD (compared to DI-QKD) i.e. random inputs S_i, z_i, and the outcome c_i into the Eve's side information E, the non-signal condition in (132) remains unaffected and GEAT can be applied for the security proof of the protocol.

An rDI-QKD protocol introduced in 3.14 can be shown by a tuple $\mathcal{Q}_r = \{\rho_{AB}, A_x, B_y, T_z\}$ which gives rise to the correlations $p(a, b|x, y)$ and $p(a, c|x, z)$. Based on the above discussion, as in the standard DI-QKD, the asymptotic key rate can be calculated by the iid Devetak–Winter rate $r = H(A|XE) - H(A|B)$. To lower-bound the term $H(A|XE)$, considering that the source initially produces a state ρ_{ABE}, without loss of generality, one can assume that this state is a pure state $|\Psi_{ABE}\rangle$ and all the measurement settings are projective. The possible quantum strategies that Eve can use are fully characterized by the pure state $|\psi_{ABE}\rangle$ and the projective measurements $\{A_{a|x}\}$, $B_{b|y}$, and $T_{c|z}$ conditioned to the fact that they return the honest correlations

$$p(a, c|x, z) = \langle \Psi_{ABE}|A_{a|x} \otimes T_{c|z}|\Psi_{ABE}\rangle,$$
$$p(a, b|x, y) = \langle \Psi_{ABE}|A_{a|x} \otimes B_{b|y} \otimes \boldsymbol{I}_E|\Psi_{ABE}\rangle, \tag{139}$$

where $T_{c|z}$ acts jointly on subsystems B and E. To each strategy, one can associate the post-measurement state $\sigma_{AXE} = \sum_{a,x} p(x)|ax\rangle\langle ax| \otimes \sigma_E^{a,x}$ where $\sigma_E^{a,x} = \mathrm{tr}_{AB}(|\Psi_{ABE}\rangle\langle \Psi_{ABE}|(A_{a|x} \otimes \boldsymbol{I}_B \otimes \boldsymbol{I}_E))$ is the unnormalized state held by Eve conditioned to Alice's inputs and outputs. The conditional min-entropy can then be computed as

$$H(A|XE) = \inf_{\hat{\mathcal{Q}}|p} H(A|XE)_{\sigma_{AXE}}, \tag{140}$$

where the optimization runs over all quantum strategies $\hat{\mathcal{Q}}$ compatible with the honest correlations (139). Notice that this optimization is almost identical to the optimization problem in a standard DI-QKD protocol where Bob performs the measurements $T_z \otimes B_y$, with a difference that the measurements T_z act on the joint systems BE, instead of just B. The method in Section 5.8 (see Theorem 15) then can be applied to lower bound the conditional entropy $H(A|XE)$ in rDI-QKD in almost the same way as in DI-QKD. For the rCHSH protocol which is the routed version of the DI-QKD CHSH protocol, if A and T have perfect detectors $\eta_A = \eta_B = 1$, the key rats are very robust as η_B decreases, remaining positive for $\eta_B \gtrsim 0.68$ [94]. However, this value is not robust when η_A and η_B are decreased for example, in the case where all devices have the same detection efficiency η, the key rate is positive for $\eta \gtrsim 0.96$ which is worse than standard CHSH based DI-QKD protocols.

5.2.3. GEAT and the security of monogamy-of-entanglement based DI-QKD

While some protocols, such as the generalized CHSH game 3.9 and the magic square game 3.13, have also been considered, most of the protocols studied so far have been based on the CHSH game due to its simplicity of implementation. So, here an important question arise: *Is it possible to explicitly prove secrecy of a DI-QKD protocol using an arbitrary monogamy-of-entanglement game?* This question was tackled in [281].

Let us start by defining *a non-local game.*

Definition 25. A two-party nonlocal game is a tuple $G_2 = (\pi, \mathcal{X}, \mathcal{Y}, \mathcal{A}, \mathcal{B}, V)$, where π is a probability distribution over input pairs $(x, y) \in \mathcal{X} \times \mathcal{Y}$, and $V : \mathcal{X} \times \mathcal{Y} \times \mathcal{A} \times \mathcal{B} \to \{0, 1\}$ is the winning predicate. Alice and Bob receive input (x, y), respond with output $a \in \mathcal{A}$, $b \in \mathcal{B}$, and win if $V(x, y, a, b) = 1$. Similarly, a three-party game G_3 is defined as one in which a third player (Eve) also contributes by receiving (x, y) and outputs a bit $c \in \{0, 1\}$.

Using this definition, the main theorem in [281] is expressed as the following theorem.

Theorem 9. *Consider a DI-QKD protocol based on a two-player non-local game G_2 between Alice and Bob, with quantum winning probability ω_2. Suppose an adversary (Eve) holds quantum side information and may launch general coherent attacks, which can be modeled by extending the game to a three-party non-local game G_3 with quantum winning probability $\omega_3 < \omega_2$. Then, there exists an affine min-tradeoff function $f : [0, 1] \to \mathbb{R}$, defined for any $\beta \in [\omega_3, \omega_2]$ by*

$$f(p) = \frac{p - \beta}{\ln 2}(1 - \beta + \omega_3) - \log(1 - \beta + \omega_3), \tag{141}$$

such that the smooth min-entropy of Alice's raw key conditioned on Eve's quantum side information and public communication, satisfies

$$H_{\min}^{\varepsilon}(A|E) \geq nf(p_{\exp}) - O(\sqrt{n}), \tag{142}$$

where $p_{\exp} \in [0, 1]$ is the observed winning probability in the testing rounds.

The monogamy-of-entanglement property in this setting is reflected in the fact that the optimal quantum winning probability ω_2 of the two-player non-local game (played between Alice and Bob) exceeds the tripartite quantum winning probability ω_3 of the extended game, in which a third party receives both inputs and attempts to guess the key bit produced by Alice and Bob.

Theorem 9 implies that it is indeed possible to construct DI-QKD — and prove their security — from any two-player non-local game that exhibits a sufficiently large gap $\omega_2 > \omega_3$ between the two-party and three-party instances of the game.

5.2.4. (G)EAT vs. iid and non-iid techniques

(G)EAT is more general in the sense that it does not need to assume that the rounds of the experiment are *independent and identically distributed* (iid). This, in particular, implies that (*i*) the measurement devices are memoryless, i.e. they behave independently and in the same way in every round of the protocol;(*ii*) the distributed state is the same for every round $\rho_{A_1^n B_1^n E} = \rho_{ABE}^{\otimes n}$. The iid simplification can be justified, for example, in experimental setups where Alice and Bob control, to some extent, the source and measurement devices, but do not have a full characterization of their working devices. In this case, $H_{\min}^{\varepsilon}(K_1^n \mid E_1^n)$ can be directly related to the single-round conditional von Neumann entropy $H(K_i|E_i)$ and (G)EAT is equivalent to the quantum asymptotic equipartition property (AEP) [322] yielding

$$H_{\min}^{\varepsilon}(K_1^n \mid E_1^n) \geq nH(K_i \mid E_i) - c_{\varepsilon}\sqrt{n}, \tag{143}$$

where c_{ε} is dependent only on ε and $H(K_i \mid E_i) \leq 1 - \chi_0$ of Eq. (??) for CHSH protocol.

(G)EAT improves the traditional DI-QKD security proofs under coherent attacks [81,82]. This, in particular, assumes that Eve exploits all degree of freedoms of the quantum systems, applying global operations across all protocol rounds $\rho_{ABE} = \rho_{A^n B^n E}$ and a global measurement $\mathcal{M}_E$ on ρ_E. Let us consider CHSH protocol with abortion threshold $S \leq 2\sqrt{2}(1 - 2Q)$, then

$$H_{\min}^{\varepsilon}(A \mid E)_\rho > -6(1 - \tau') \log\left(\frac{11}{12} + \frac{3}{8}\sqrt{\frac{Q}{1 - \tau}}\right) - O\left(\frac{\log(1/\varepsilon)}{2Q^2 n}\right), \qquad \forall \tau + \tau' > 1, \tag{144}$$

with n the rounds and Q the QBER. After postprocessing $r \geq H_{\min}^{\varepsilon}(A|E) - h(Q)$, as in Eq. (43). Eq. (144) relies on *quantum reconstruction paradigm* (QRP) [323].

However, the key rate is lower compared to security proofs obtained via (G)EAT.

(G)EAT vs. Rényi-divergence method

Before the development of the EAT, one of the most complete finite-key security proofs for robust DI-QKD was introduced by Miller and Shi [295]. Their approach was based on bounding a Rényi-divergence that decreases linearly with the number of rounds, relying on a game-specific uncertainty relation for strong self-testing XOR games and an intricate induction technique using partially trusted measurements. This allowed them to achieve notable milestones such as a polylogarithmic seed length, constant quantum memory requirements for the honest parties, and explicit exponential soundness error bounds. However, their proof was highly specialized and tightly coupled to the particular structure of the underlying nonlocal game, making it difficult to generalize or adapt to new protocols, statistics, or noise models. In contrast, the (G)EAT framework generalizes this type of entropy accounting by providing a universal accumulation statement: once a suitable min-tradeoff function is established, the conditional smooth min-entropy grows predictably and additively, regardless of whether the device behavior is iid or exhibits arbitrary non-stationary correlations. This shift

delivers sharper finite-size bounds, native composability, and a modular, game-independent toolkit that can be applied across a wide range of DI-QKD, DI-randomness expansion, and other sequential quantum protocols without rederiving core security proofs. As such, (G)EAT is widely regarded as the natural successor to the Rényi-divergence-based method for modern device-independent security analysis.

5.3. Quantum probability estimation method

Another useful method for proving security in device-independent protocols is to employ the quantum probability estimation method, which was introduced in [324,325]. The analysis in [325] enables a full security analysis for DIQRNG. Similarly to (G)EAT, in QPE, inputs and outputs are determined in a sequence of n time-ordered trials, where the i trial has input Z_i and output C_i, so $\boldsymbol{Z} = (Z_i)_{i=1}^n$ and $\boldsymbol{C} = (C_i)_{i=1}^n$. QPE introduces a flexible tool called a Quantum Estimation Factor (QEF), which quantifies certifiable randomness in quantum experiments, even in the presence of quantum side information. QEF is defined as

Definition 26 (*Quantum Estimation Factor*)**.** Let C and Z be classical random variables that represent, respectively, the output (e.g., measurement result) and input (e.g., measurement setting) in a quantum experiment, and let E be a quantum system that may hold quantum side information by an adversary. Then a function $F : \text{Rng}(C) \times \text{Rng}(Z) \to \mathbb{R}_{\geq 0}$ is called a Quantum Estimation Factor (QEF) with power $\beta > 0$ if, for every valid classical–quantum state ρ_{CZE}, the following inequality holds:

$$\sum_{c \in \text{Rng}(C)} \sum_{z \in \text{Rng}(Z)} \text{Tr}\left[\rho_E(c, z)\right] \cdot F(c, z) \cdot \hat{R}_\alpha \left(\rho_E(c, z) \parallel \rho_E(z)\right) \leq 1, \tag{145}$$

where $Rng(A)$ is the value space of a classical variable A and

- $\alpha = 1 + \beta$,
- $\rho_E(c, z)$ is the (possibly subnormalized) quantum state of the adversary's system E conditioned on observing $C = c$ and input $Z = z$,
- $\rho_E(z) = \sum_c \rho_E(c, z)$ is the marginal quantum state for input z,
- $\hat{R}_\alpha(\rho \parallel \sigma)$ is the normalized sandwiched Rényi power of order α, defined as:

$$\hat{R}_\alpha(\rho \parallel \sigma) = \frac{1}{\text{Tr}[\rho]} \cdot \text{Tr}\left[\left(\sigma^{-\frac{\beta}{2\alpha}} \rho \, \sigma^{-\frac{\beta}{2\alpha}}\right)^\alpha\right]. \tag{146}$$

Using this definition, the following lower bound on quantum smooth min-entropy can be proved [325].

Theorem 10 (*Lower Bound on Quantum Smooth Min-Entropy via QEFs*)**.** *Suppose that the experiment is repeated for n rounds. For each round i, let $F_i : \text{Rng}(C) \times \text{Rng}(Z) \to \mathbb{R}_{\geq 0}$ be a QEF with power $\beta > 0$. By defining the total QEF value as $f = \prod_{i=1}^n F_i(c_i, z_i)$ and any desired soundness error $\epsilon \in (0, 1]$, if $f \geq \left(\frac{2^{-k} \cdot \epsilon^2}{2}\right)^{-\beta}$, then the smooth conditional min-entropy of the output string $\boldsymbol{C}$ with given inputs $\boldsymbol{Z}$ satisfies:*

$$H_{\min}^\epsilon(C \mid ZE) \geq k. \tag{147}$$

The above theorem states that at least k bits of the output string are private and unpredictable, which can be safely extracted using a quantum-proof randomness extractor.

Since certifying quantum smooth conditional min-entropies is a central task in QKD, QPE can be adapted to enhance the finite-data efficiency of DI-QKD. To achieve this, it is necessary to certify the quantum smooth conditional min-entropy evaluated on a classical–quantum state following the error-correction step, similar to the approach used in security proofs of DI-QKD via the EAT [109] (see Section 5.1).

5.4. Complementarity-based security for DI-QKD

So far, DI-QKD security proofs have primarily relied on entropic techniques such as the (G)EAT. While powerful, these methods are technically demanding and typically require large data sizes, limiting their experimental feasibility.

A different security proof for DI-QKD was proposed by Zhang et al. [326] by employing a *complementarity-based* approach. They recast the DI-QKD security problem as a form of *quantum error correction* against **phase errors**, drawing on principles already familiar from standard device-dependent QKD [327–329].

The central insight in [326] is that a BI violation can be used to upper-bound the adversary's information via a *phase error probability* derived from complementary observables and provide an operational connection between the Bell value and phase error rate using sample-entropy techniques together with a composable, finite-size security proof under coherent (non-iid) attacks. This leads to the following main result:

Theorem 11. *In a CHSH-based DI-QKD protocol with memoryless devices executed over n rounds, let m rounds be used for key generation. If the observed average Bell value is $\bar{\beta} > 2$, then, except with small failure probability, the number of secure key bits that can be extracted is approximately:*

$$k \approx m \cdot \left[1 - h(e_b) - h\left(e_p(\bar{\beta}) \right) \right], \tag{148}$$

where

$$e_p(\bar{\beta}) = \frac{1 - \sqrt{(\bar{\beta}/2)^2 - 1}}{2}$$

is the phase error probability inferred from the Bell violation β.

Simulation results demonstrate that the complementarity-based approach significantly improves the finite-size performance of DI-QKD. For example, in an ion-trap experiment with $\beta = 2.64$ and $Q = 1.8\%$, approximately 3.16×10^5 measurement rounds are required to generate a secure key, which is less than one-third of the rounds required by EAT methods. This substantial reduction in data size makes the protocol more practical for experimental platforms with low entangled-pair rates, such as cold atoms and nitrogen-vacancy centers. Moreover, it was shown that advantage distillation can be applied without assuming iid behavior [326], lowering the thresholds for required transmittance and fidelity and expanding the range of conditions under which secure DI-QKD is possible.

5.5. Security proof of parallel DI-QKD

The original security proof for parallel DI-QKD relates collision entropy of the raw key to the success probability in a derived game. By showing that even entangled strategies cannot win this game with high probability, they obtain the bound:

$$H_{\min}^\epsilon(A|E) - H_{\max}^\epsilon(A|B) \geq R(n) \tag{149}$$

where $R(N)$ is the extractable key rate, and $R(N) \in \Omega(N)$ means it grows at least linearly with the number of rounds N.

Soon after, Vidick [330] provided a simplified security proof for such protocols relying on two powerful and general tools from quantum information theory, the immunization technique and anchored parallel repetition. The immunization method ensures that even entangled adversaries cannot win a modified "guessing" version of the Magic Square game with certainty, introducing unavoidable uncertainty that translates into key entropy. The anchored parallel repetition theorem then guarantees that this uncertainty accumulates exponentially with the number of rounds, even under coherent attacks. By combining these ideas, he shows that a positive key rate can be securely extracted with a far more direct and modular argument. Further improvement was done by Jain et al. [290] by introducing the direct product theorem. They show that it is possible to do DI quantum cryptography without the assumption that devices do not leak any information. By applying it to parallel DI-QKD, they showed that when the protocol is carried out with devices that are compatible with n copies of the Magic Square game, it is possible to extract $\Omega(n)$ bits of key from it, even in the presence of $O(n)$ bits of leakage.

5.6. Analytical bounds

5.6.1. 2-Input/2-output protocols

The first analytical bound, as mentioned in Section 3.5, was established in Ref. [70] against collective attacks.

Theorem 12. *Let $|\psi_{ABE}\rangle$ be a quantum state for a $CHSH_c$ protocol. Then, the following upper bound holds for the Holevo quantity:*

$$\chi(B_1 : E) \leq h\left(\frac{1 + \sqrt{(\beta/2)^2 - 1}}{2} \right),$$

For the proof of this theorem, we use the following lemma, which we put here without proof.

Lemma 3. *For a Bell-diagonal state with eigenvalues λ ordered as $\lambda_{\Phi^+} \geq \lambda_{\psi^-}$ and $\lambda_{\Phi^-} \geq \lambda_{\psi^+}$ and for measurements in the xz plane, the following bound holds for the Holevo quantity $\chi_\lambda(B_1|E)$*

$$\chi_\lambda(B_1|E) \leq F(\beta_\lambda) \leq h\left(\frac{1 + \sqrt{(\beta_\lambda/2)^2 - 1}}{2} \right),$$

where β_λ is the largest violation of the CHSH inequality by the state ρ_λ.

Using this lemma, the proof of the theorem can be established.

Proof. As stated at the beginning of Section 3, suppose that Eve sends to Alice and Bob a mixture $\rho_{AB} = \sum_c p_c \rho^c_{AB}$ of two-qubit states with a classical ancilla known to her which carries on the information about measurement settings on Alice and Bob side. Two measurements on Alice and Bob can be assumed as von Neumann measurements (if necessary by including ancillas in ρ_{AB}). Thus the measurements $A_{1,2}$ are Hermitian d-dimensional operators. Using the Jordan Lemma 1 one can show that A_1 and A_2 are block diagonal, with blocks of size 1×1 or 2×2 i.e. $A_j = \sum_c P_c A_j P_c$ with P_c's as projectors of rank 1 or 2. Therefore, from Alice's standpoint, $A_{1,2}$ amounts at projecting in one of the at most two-dimensional subspaces defined by the projectors p_c followed by a measurement on the reduced state observable $P_c A_i P_c$. The same argument holds for Bob. As a result, one can conclude that in each round of the protocol Alice and Bob receive a two-qubit state.

Each state ρ^c_{AB} can be taken to be a Bell diagonal state $(\sum_\lambda p_\lambda \rho_\lambda)$, and the measurements of Alice and Bob to be measurements in the xz plane which result in $\chi(B_1 : E) = \sum_\lambda p_\lambda \beta_\lambda$ plane. Therefore, using Lemma 3 the concavity of function F

$$\chi(B_1 : E) \leq \sum_\lambda p_\lambda F(\beta_\lambda) \leq F\left(\sum_\lambda p_\lambda \beta_\lambda\right) \leq F(\beta),$$

the last inequality comes from the fact that F is a monotonically decreasing function. □

Based on this bound, the following lower bound for the key rate can be derived:

$$r \geq I(A_0 : B_1) - h\left(\frac{1 + \sqrt{(\beta/2)^2 - 1}}{2}\right), \tag{150}$$

The basic CHSH protocol based on the above lower bound is, however, not optimal in several respects. To address the drawbacks, Masini et al. [331], introduced a new and versatile approach to bound the conditional entropy in the 2-input/2-output device-independent setting that is conceptually and technically relatively simple. The starting point is to use Jordan's lemma to reduce the analysis to convex combinations of qubit strategies.

The next step, as in a standard qubit QKD protocol like BB84, is to bound the conditional entropy of Alice's key-generating measurement, A_1, through an uncertainty relation involving the correlations $\langle \bar{A}_1 \otimes B \rangle$ where $\bar{A}_1$ is an orthogonal measurement on Alice's subsystem and B is a binary observable on Bob's system. Considering the situation where Alice's raw key bit A_1 is obtained as the outcome of the measurement, then we have the following bounds which are qubit uncertainty relations of the standard entanglement-based BB84 protocols its variants:

BB84 entropy bound [332]	$H(A_1|E) \geq 1 - \phi\left(|\langle \bar{A}_1 \otimes B \rangle|\right)$
BB84 bound with noisy preprocessing [87,333]	$H(A_1^q|E) \geq f_q\left(|\langle \bar{A}_1 \otimes B \rangle|\right)$
BB84 with noisy preprocessing and bias [331]	$H(A_1^q|E) \geq g_q\left(|\langle A_1 \rangle|, |\langle \bar{A}_1 \otimes B \rangle|\right)$
Two-basis bound [87,331]	$H(A_X^q|E) \geq f_q\left(\sqrt{p\langle \bar{A}_1 \otimes B \rangle^2 + (1-p)\langle \bar{A}_2 \otimes B' \rangle^2}\right)$

where $\phi(x) = h(\frac{1}{2} + \frac{1}{2}x)$ and $h(x)$ is the binary entropy. Moreover, $f_q(x) = 1 + \phi(\sqrt{(1-2q)^2 + 4q(1-q)x^2}) - \phi(x)$, and $g_q(z, x) = \phi(\frac{1}{2}(R_+ + R_-)) - \phi(\sqrt{z^2 + x^2})$, with $R_\pm = \sqrt{(1-2q \pm z)^2 + 4q(1-q)x^2}$. The second step approach consists in deriving a constraint on these correlators in terms of correlators involving only the observables A_1, A_2, B_1, B_2 measured by the devices

CHSH correlation bound [87]	$|\langle \bar{A}_1 \otimes B \rangle| \geq \sqrt{\beta^2/4 - 1}$
Asymmetric CHSH correlation bound [87]	$|\langle \bar{A}_1 \otimes B \rangle| \geq E_\alpha(\beta_\alpha)$
Two-basis correlation bound [331]	$p\langle \bar{A}_1 \otimes B \rangle^2 + (1-p)\langle \bar{A}_2 \otimes B' \rangle^2 \geq E_p(\beta)^2$

where

$$E_\alpha(\beta_\alpha) = \begin{cases} \sqrt{\frac{\beta_\alpha^2}{4} - \alpha^2}, & \text{if } |\alpha| \geq 1, \\ \sqrt{1 - \left(1 - \frac{1}{|\alpha|}\sqrt{(1 - \alpha_2)\left(\frac{\beta_\alpha^2}{4} - 1\right)}\right)^2}, & \text{if } |\alpha| < 1. \end{cases} \tag{151}$$

and $E_p(\beta)^2$ is the solution of a polynomial optimization problem of five real variables which for the case $p = \frac{1}{2}$ can be solved analytically [331].

By combining the aforementioned correlation bounds with the entropy bounds, one can derive device-independent bounds on conditional entropy. For instance, by integrating the BB84 bound with the CHSH correlation bound, the bound in (150) can be obtained.

Similarly, using the asymmetric CHSH correlation bound within the BB84 noisy preprocessing framework, the bound from [87] can be derived:

$$H(A_1^q|E) \geq f_q(E_\alpha(\beta_\alpha)), \tag{152}$$

Moreover, by combining the CHSH correlation bound with BB84, incorporating noisy preprocessing and bias, the following bound is obtained [331]:

$$H(A_1^q|E) \geq g_q(|\langle A_1 \rangle|, \sqrt{\beta^2/4 - 1}), \tag{153}$$

Finally, if we denote $\tilde{E}_p(\beta)^2$ as any lower bound on $E_p(\beta)^2$, another bound can be expressed as [331]:

$$H(A_X^q|XE) \geq f_q(\tilde{E}_p(\beta)), \tag{154}$$

where $\tilde{E}_p(\beta)$ is defined as $\tilde{E}_p(\beta) = \sqrt{\tilde{E}_p(\beta)^2}$.

Since the obtained bounds are convex, they can be extended to give fully device-independent bounds in arbitrary dimensions.

5.7. Rényi-entropy bounds for CHSH

Building on the analytical CHSH bounds for the von Neumann entropy and the min-entropy/guessing-probability approach, Hahn et al. [334] derive closed-form trade-off functions that relate a device's observed CHSH violation $\beta \in [2, 2\sqrt{2}]$ directly to Rényi conditional entropies. Their main result provides tight entropy rate functions for a wide range of Rényi entropies.

Before stating the theorem, we introduce the relevant definition:

Definition 27 (*H Rate Function for CHSH*). Let H be a conditional entropy and $\beta \in [2, 2\sqrt{2}]$. A function

$$f_H : [2, 2\sqrt{2}] \rightarrow \mathbb{R}$$

is a tight H rate function for the CHSH Bell inequality if

$$f_H(\beta) := \inf_{\mathcal{E}} H(A \mid X = 0, E) \quad \text{subject to} \quad \beta_{\text{CHSH}}(\mathcal{E}) = \beta,$$

where the infimum is over all quantum strategies $\mathcal{E}$.

The following analytical bounds hold for the sandwiched Rényi conditional entropies $\tilde{H}_\alpha^\uparrow(A \mid E)$ and $\tilde{H}_\alpha^\downarrow(A \mid E)$ for any order $\alpha > 1$:

Theorem 13. *For any $\alpha > 1$, the rate functions take the form:*

$$f_{\tilde{H}_\alpha^\uparrow}(\beta) = 1 + \frac{2\alpha - 1}{1 - \alpha} \log \varphi_{\frac{\alpha}{2\alpha-1}}(\beta), \tag{155}$$

$$f_{\tilde{H}_\alpha^\downarrow}(\beta) = 1 + \frac{\alpha}{1 - \alpha} \log \varphi_{1/\alpha}(\beta), \tag{156}$$

where

$$\varphi_\mu(\beta) = \left(\frac{1 - \sqrt{\beta^2/4 - 1}}{2} \right)^\mu + \left(\frac{1 + \sqrt{\beta^2/4 - 1}}{2} \right)^\mu.$$

These bounds recover known results in the limits $\alpha \to 1$ (von Neumann entropy) and $\alpha \to 2$ (min-entropy).

Notably, the minimum entropy is achieved by a single optimal eavesdropping strategy independent of α. Alice measures $A_0 = \sigma_z$ and $A_1 = \sigma_x$, while Bob measures

$$B_{0/1} = \frac{\sigma_z \pm g_\beta \sigma_x}{\sqrt{1 + g_\beta^2}}, \quad \text{where } g_\beta = \sqrt{\beta^2/4 - 1}.$$

These observables act on a partially entangled Bell state dependent only on β.

The new rate function $f_{\tilde{H}_\alpha^\downarrow}$ can significantly enhance finite-key DI-QKD performance. For example, in the loophole-free demonstration of [54], it improves the extractable key length by up to a factor of three for $n \sim 10^9$ rounds, and raises the positive-rate noise threshold to approximately $Q \approx 8.4\%$ depolarizing noise.

5.7.1. Entropy bound for multiparty DI cryptography

Ribeiro et al. [335] and Grasselli et al. [336] extended DI protocols to multipartite scenarios by proposing a DI conference key agreement (DI-CKA) among N parties. The security of their protocol relies on the violation of a Mermin–Ardehali–Belinskii–Klyshko (MABK) inequality [337–339], a generalization of the CHSH inequality. Specifically, they focused on the three-party case involving Alice, Bob, and Charlie. In this context, the MABK inequality is expressed as:

$$m = \langle M_3 \rangle = \text{Tr}[M_3 \rho] \overset{\text{CI}}{\leq} 2 \overset{\text{GME}}{\leq} 2\sqrt{2} \overset{\text{Q}}{\leq} 4, \tag{157}$$

where $M_3 = A_0 \otimes B_0 \otimes C_1 + A_0 \otimes B_1 \otimes C_0 + A_1 \otimes B_0 \otimes C_0 - A_1 \otimes B_1 \otimes C_1$ is the MABK operator. Here, A_x, B_y, and C_z represent Alice's, Bob's, and Charlie's observables, respectively. A violation beyond the GME threshold implies that the parties share a genuine multipartite entangled (GME) state.

They derived the following bound on the conditional entropy as a function of the observed MABK violation m :

$$H(A_0|E) \geq 1 - h\left(\frac{1}{2} + \frac{1}{2}\sqrt{\frac{m^2}{8} - 1}\right).$$

By proving that this bound on the conditional entropy of a party's outcome is tight at the GME threshold, it can be concluded that genuine multipartite entanglement is essential to ensure the privacy of a party's random outcome in any device-independent protocol based on the MABK inequality.

Grasselli et al. [340] advance the field by deriving tight analytical bounds on entropy as a function of the violation of the Holz inequality, a multipartite generalization of the CHSH inequality introduced in [103]. The Holz inequality was specifically designed for DI-CKA protocols. In the tripartite case, the inequality takes the form:

$$\beta_H = \langle A_1 B_+ C_+ \rangle - \langle A_0 B_- \rangle - \langle A_0 C_- \rangle - \langle B_0 C_- \rangle \overset{L}{\leq} 1 \overset{Q}{\leq} \frac{3}{2}, \tag{158}$$

where $B_\pm = \frac{1}{2}(B_0 \pm B_1)$ and $C_\pm = \frac{1}{2}(C_0 \pm C_1)$.

If Alice, Bob, and Charlie test this inequality and obtain an expected Bell value β_H, the following tight analytical bound on the conditional entropy of Alice's outcome A_0 can be derived:

$$H(A_0|E) \geq 1 - h\left[\frac{1}{4}\left(\beta_H + 1 + \sqrt{\beta_H^2 - 3}\right)\right]. \tag{159}$$

Moreover, the authors demonstrate that the entropy bounds for the Holz inequality remain non-zero below the GME threshold set by the MABK inequality. This implies that GME might not be a strict requirement for certifying the privacy of a single party's outcome when testing multipartite Bell inequalities.

5.8. Numerical techniques

The main theoretical problem in QKD is calculating how much of a secret key can be extracted by a given protocol. A crucial practical issue is that the QKD protocols that are easiest to implement with existing technology do not necessarily coincide with the protocols that are easiest to analyze theoretically. Furthermore, existing analytical methods for calculating the key rate are highly technical and often limited in scope to particular protocols, and invoke inequalities that introduce looseness into the calculation. Therefore, putting efforts into numerical methods, which are inherently more robust to device imperfections and protocol structure changes, is necessary.

At the technical level, the key rate problem is an optimization problem, since one must minimize the well-known entropic formula $H(A|E)$ over all states ρ_{AB} that satisfy Alice's and Bob's experimental data.

$$r := \min_{\rho_{AB} \in \mathcal{C}} [H(R_A \mid E) - H(R_A \mid R_B)], \tag{160}$$

where $\mathcal{C}$ is the set of all states ρ_{AB} consistent with the observed experimental data. Coles et al. [341] showed that the key rate r can be lower bounded with the use of the dual problem by the following maximization problem

$$r \geq \frac{\Theta}{\ln 2} - H(A \mid B), \tag{161}$$

where $\Theta = \max_{\vec{\lambda}} \left(- \parallel \sum_i A_{a_i|\bar{x}} R(\vec{\lambda}) A_{a_i|\bar{x}} \parallel - \vec{\lambda} \cdot \vec{\gamma}\right)$ ($\bar{x}$ is the key generating measurement) and $R(\vec{\lambda}) = \exp(-\boldsymbol{I} - \vec{\lambda} \cdot \vec{\Gamma})$. $\vec{\Gamma} = \{\Gamma_i\}$ where Γ_i are bounded Hermitian operators dependent on the observed experimental data and $\vec{\lambda} = \{\lambda_i\}$ ($\lambda_i = \text{Tr}(\rho_{AB}\Gamma_i)$). The key rate also can be lower bounded by applying direct optimization (primal problem) [342]

$$r \geq \alpha - p_{\text{pass}}\text{leak}^{EC}, \tag{162}$$

such that $\alpha = \min_{\rho \in \mathcal{C}} f(\rho)$ where $f(\rho)$ is a convex function of ρ and leak^{EC} denotes the number of bits Alice publicly reveals during error correction.

To apply the EAT, as discussed in the previous section, a trade-off function must be computed that lower-bounds the amount of randomness produced in a single round. Existing results for the CHSH game [73] are highly specific to this case, with limited generalizability to other games. A particularly promising approach involves using SDP relaxations [152,343] provide valuable techniques for studying classical and quantum advantages in DI and SDI protocols (see also [344]). Often, these methods can provide exact solutions to the problems at hand. However, the complexity of these techniques imposes limitations, especially when studying protocols involving higher-dimensional quantum systems.

Lower bounds on the min-entropy. A straightforward way to derive numerical lower bounds for von Neumann entropy minimization is through the use of min-entropy, as demonstrated in [345,346]. The corresponding optimization of min-entropy can be formulated as a noncommutative polynomial over measurement operators. This problem can be relaxed into a semidefinite program (SDP) using the NPA hierarchy 2.2, which can then be solved efficiently. While this method provides a simple and effective way to lower bound the rates of various device-independent (DI) tasks, the min-entropy is generally much smaller than the von Neumann entropy. As a result, this approach often yields suboptimal outcomes. Therefore, to achieve optimal bounds, obtaining upper bounds on von Neumann entropy is both more efficient and essential.

Lower bounds on the conditional von Neumann entropy. Tan et al. [347] approach the DI security problem with a universal computational toolbox that directly bounds the von Neumann entropy using the complete measurement statistics of a device-independent cryptographic protocol. Suppose that the protocol estimates parameters of the form $l_j = \sum_{abxy} c_{abxy}^{(j)} p(ab|xy)$ for some coefficients c_{abxy}^j. These parameters could be Bell inequalities in a DI scenario. Thanks to the Naimark theorem, one can assume all measurements as projective measurements, $P_{a|x}$ for Alice's side and $P_{b|y}$ for Bob's side, in a higher but finite dimension space. The task is to find lower bounds on $\inf H(A_0 \mid E)$ such that $\langle L_j \rangle = l_j$ where $L_j = \sum_{abxy} c_{abxy} P_{a|x} \otimes P_{b|y}$ and the infimum takes place over ψ_{ABE} and any uncharacterized measurements. The central result of Tan et al. [347] is expressed as the following theorem

Theorem 14. *For a DI scenario, the minimum value of $H(A_0|E)$ subject to constraints $\langle L_j \rangle = l_j$ is lower-bounded by*

$$\sup_{\vec{\lambda}} \left(\sum_j \lambda_j l_j - \ln \left(\sup_{\substack{\rho_{AB}, P_{a|x}, P_{b|y} \\ \text{s.t. } \langle L_j \rangle_{\rho_{AB}} = l_j}} \langle K \rangle_{\rho_{AB}} \right) \right), \tag{163}$$

where

$$K = T \left[\left| \int_{\mathbb{R}} dt \, \beta(t) \right| \prod_{xy} \sum_{ab} e^{\kappa_{abxy}} P_{a|x} \otimes P_{b|y} \Big|^2 \right] \tag{164}$$

with $T[\sigma_{AB}] = \sum_a (P_{a|0} \otimes \mathbb{I}_B) \sigma_{AB} (P_{a|0} \otimes \mathbb{I}_B)$, $\beta(t) = (\pi/2)(\cos(\pi t) + 1)^{-1}$, and $\kappa_{abxy} = (1 + it) \sum_j \lambda_j c_{abxy}^{(j)} / 2$.

The previous best bound on $H(A_0 \mid E)$ was established in [73] (see Section 5.6), where only the CHSH value was used instead of the full probability distribution. In contrast, the method proposed in Theorem 14 directly bounds $H(A_0 \mid E)$ using the complete input–output distribution. This approach yields results that are comparable to or slightly better than the bound in [73]. It also demonstrates that in scenarios with limited detection efficiency, better bounds on $H(A_0 \mid E)$ can be achieved by considering the full distribution rather than relying solely on the CHSH value. This suggests that optimizing experimental parameters to maximize the CHSH value may not be the most effective strategy; instead, optimizing a different Bell value could lead to further improvements.

The numerical results presented in [347] are very promising, providing significant improvements in the rates when compared to the min-entropy approach and also improving over the analytical results [73]. However, the approach is relatively computationally intensive requiring the optimization of a degree 6 polynomial in the simplest setting. To reduce the complexity, Brown et al. [85] take a different approach, defining a new family of quantum Rényi divergences, the iterated mean (IM) divergences which for the sequence $\alpha_k = 1 + \frac{1}{2^k - 1}$ for $k \in \mathbb{N}$ is defined as

$$D_{(\alpha_k)}(\rho \parallel \sigma) := \frac{1}{\alpha_k - 1} \log Q_{(\alpha_k)}(\rho \parallel \sigma), \tag{165}$$

where

$$Q_{(\alpha_k)}(\rho \parallel \sigma) = \max_{V_1, \dots, V_k, Z} \alpha_k \text{Tr} \left[\rho \frac{(V_1 + V_1^*)}{2} \right] - (\alpha_k - 1) \text{Tr}[\sigma Z] \tag{166}$$

such that

$$V_1 + V_1^* \geq 0, \quad \frac{V_2 + V_2^*}{2} \geq V_1^* V_1, \quad \cdots, \quad Z \geq V_k^* V_k. \tag{167}$$

The crucial property that makes these divergences well-adapted for device-independent optimization is the fact that $Q_{(\alpha_k)}(\rho \parallel \sigma)$ has a free variational formula as a supremum of linear functions in ρ and σ. Given a bipartite quantum state ρ_{AB} and a divergence $D_{(\alpha_k)}(\rho \parallel \sigma)$ the corresponding conditional entropy can be defined as $H_{\alpha_k}^{\downarrow} = -D_{(\alpha_k)}(\rho_{AB} \parallel I_A \otimes \rho_B)$ together with its optimized version $H_{\alpha_k}^{\uparrow} = \sup_{\sigma_B} -D_{(\alpha_k)}(\rho_{AB} \parallel I_A \otimes \sigma_B)$, then the following theorem gives an explicit characterization of $H^{\uparrow}$ for the iterated mean divergences

Theorem 15 (*BFF Method*). *For a bipartite state ρ_{AB}*

$$H_{\alpha_k}^{\uparrow}(A|B)_{\rho_{AB}} = \frac{1}{1 - \alpha_k} \log Q_{(\alpha_k)}^{\uparrow}, \tag{168}$$

where

$$Q_{(\alpha_k)}^{\uparrow} = \max_{V_1,\dots,V_k} \left(Tr[\rho_{AB} \frac{V_1 + V_1^*}{2}] \right)^{\alpha_k}, \tag{169}$$

such that

$$Tr[V_k^* V_k] \leq I_B, \quad V_1 + V_1^* \geq 0, \quad and \quad \begin{pmatrix} I & V_i \\ V_i^* & \frac{V_{i+1}+V_{i+1}^*}{2} \end{pmatrix} \geq 0,$$

where in the last constraint $1 \leq i \leq k - 1$.

Brown et al. [85] showed that for each α_k and any pair of ρ and σ, $D_{(\alpha_k)}(\rho \parallel \sigma) \geq \tilde{D}_{(\alpha_k)}(\rho \parallel \sigma)$ where $\tilde{D}_{(\alpha)}$ denotes the sandwiched Renyi divergence [348] which result in $H_{\alpha_k}^{\uparrow}(A|B) \leq \tilde{H}_{\alpha_k}^{\uparrow}(A|B) \leq H(A|B)$ for all $\alpha > 1$ that can be used to compute lower bounds on the rates of various device-independent protocols.

Both above methods improve upon the min-entropy method, but neither has been shown to give tight bounds on the actual rate of a protocol, and in general, there appears to be significant room for improvement. As such, the question remains as to whether one can give a computationally tractable method to compute tight lower bounds on the rates of protocols. To address this question, Brown et al. [277] derived a converging sequence of upper bounds on the relative entropy between two positive linear functionals on a von Neumann algebra and demonstrated how to use this sequence of upper bounds to derive a sequence of lower bounds on the conditional von Neumann entropy. The main technical result of their work is the following theorem

Theorem 16. *Assume that ρ and σ are two positive operators on a finite-dimensional Hilbert space and $\lambda > 0$ is such that $\rho \leq \lambda\sigma$. Then for any $m \in \mathbb{N}$ there exists a choice of $t_1, \dots, t_m \in (0, 1]$ and $\omega_1, \dots, \omega_m > 0$ such that*

$$D(\rho \parallel \sigma) \leq -c_m - \sum_{i=1}^{m-1} \frac{\omega_i}{t_i \ln 2} \inf_Z Tr[\rho Z + Z^* + (1-t_i)Z^*Z] + t_i Tr[\sigma ZZ^*], \tag{170}$$

$$s.t. \quad \|Z\| \leq \frac{3}{2} \max\{\frac{1}{t_i}, \frac{\lambda}{1-t_i}\}, \tag{171}$$

where $c_m = Tr[\rho](\sum_{i=1}^{m} \frac{\omega_i}{t_i \ln 2} - \frac{\lambda}{m^2 \ln 2})$. As $m \to \infty$, the right-hand side of the above equality converges to $D(\rho \parallel \sigma)$.

The Theorem 16 provides a convergent sequence of upper bounds on the relative entropy in the form of an optimization problem and can turn into SDP lower bounds on the rate of DI protocols. For the case of DI-QKD and for the devices are constrained by quantum theory the following noncommutative polynomial optimization problem gives a lower bound $H(A|E)$

$$c_m + \inf \sum_{i=1}^{m-1} \frac{\omega_i}{t_i \ln 2} \sum_a \langle \psi | (M_{a|x=x^*} x^* Z_{a,i} + Z_{a,i}^* + (1-t_i)Z_{a,i}Z_{a,i}^*) + t_i Z_{a,i} Z_{a,i}^* | \psi \rangle \tag{172}$$

such that

$$\sum_{abxy} c_{abxy}^j \langle \psi | M_{a|x} M_{b|y} | \psi \rangle \geq v_j, \tag{173}$$

and $[M_{a|x}, N_{b|y}] = [M_{a|x}, Z_{b,i}^{(*)}] = [N_{b|y}, Z_{a|i}^*] = 0$ where $M_{a|x}$ and $N_{b|y}$ are POVM elements of Alice and Bob measurements respectively which are bounded operators together with $Z_{a,i}$.

By applying the NPA hierarchy 2.2, this optimization can be relaxed into a sequence of SDPs that yield a converging series of lower bounds on the optimal value. This, in turn, provides a lower bound on the protocol's rate. When calculating key rates for DI-QKD, a significant improvement (below 0.8) in the minimum detection efficiency required to generate a secret key can be achieved, bringing it well within the capabilities of current device-independent experiments. Araujo et al. [349] adapt the same SDP hierarchy to the case of QKD with characterized devices.

5.9. Upper bounds

Up to this point, only the lower bounds on key rates have been explored for all the protocols mentioned. In this section, we address a different question:

What is a non-trivial upper bound on the secret key rate that can be extracted from a DI-QKD protocol?

Understanding upper bounds on key rates is crucial from a practical perspective, as it reveals the inherent limitations of an entire class of protocols rather than focusing on individual protocols and analyzing them in isolation.

This question was first posed by Kaur et al. [83], who introduced information-theoretic measures of nonlocality, termed intrinsic nonlocality and quantum intrinsic nonlocality. They demonstrated that these measures serve as upper bounds for DI-QKD protocols, specifically against no-signaling and quantum adversaries, respectively. Instead of using intrinsic

nonlocality, Arnon-Friedman et al. [350] examined a closely related information-theoretic quantity known as intrinsic information, which they employed to derive an upper bound on the key rates of DI-QKD protocols.

Winczewski et al. [351] initiated a systematic study of upper bounds on secret key rates within the no-signaling DI scenario. They introduced a computable function, termed squashed nonlocality, as one such bound. Their numerical analysis suggests that quantum devices with two binary inputs and two binary outputs can extract only a limited amount of key. Moreover, they found that isotropic devices with less than 80% of the Popescu–Rohrlich box weight are generally key-undistillable.

Since DI-QKD has a higher security demand than QKD, one has the trivial bounds $r^{\mathrm{DI}} \leq r^{\mathrm{DD}}$ (r^{DD} is the key rate of a standard device-dependent QKD protocol). Christandl et al. [352] use this fact to find an upper bound on a DI-QKD as follows: assume that the POVMs $\{A_{a|x}\}$ and $\{B_{b|y}\}$ are chosen such that the key-rate r is optimal, there might be different measurement $A'_{a|x}$ and $B'_{b|y}$ and state ρ' leading to the same distribution

$$p(a, b \mid x, y) := \mathrm{Tr}[(A_{a|x} \otimes B_{b|y})\rho] = \mathrm{Tr}[(A'_{a|x} \otimes B'_{b|y})\rho'], \tag{174}$$

the above equality is shown as $(\mathcal{M}, \rho) \equiv (\mathcal{M}', \rho')$. Since the maximal achievable key rate for ρ is also achievable for ρ' ($r^{\mathrm{DI}}(\rho) \leq r^{\mathrm{DI}}(\rho')$) then combining it with $r^{\mathrm{DI}}(\rho') \leq r^{\mathrm{DD}}(\rho')$ the following bound can be obtained [352]

$$r^{\mathrm{DI}}(\rho) \leq \sup_{\mathcal{M}} \inf_{\substack{(\mathcal{M}', \rho') \\ (\mathcal{M}, \rho) \equiv (\mathcal{M}', \rho')}} r^{\mathrm{DD}}(\rho'), \tag{175}$$

Consider that ρ is a PPT state $\rho^{\Gamma} \geq 0$ (Γ denotes partial transpose) because the transpose of a POVM element is a POVM element then one can find

$$r^{\mathrm{DI}}(\rho) \leq \min\{r^{\mathrm{DD}}(\rho), r^{\mathrm{DD}}(\rho^{\Gamma})\}, \tag{176}$$

The significance of the above result, can be seen by an example. Consider the $2d \times 2d$ state σ_d as

$$\sigma_d = \frac{1}{2} \begin{bmatrix} (1-p)\sqrt{XX^{\dagger}} & 0 & 0 & (1-p)X \\ 0 & pY & 0 & 0 \\ 0 & 0 & pY & 0 \\ (1-p)X & 0 & 0 & (1-p)\sqrt{XX^{\dagger}} \end{bmatrix}$$

where $Y = \frac{1}{d}\sum_{i=0}^{d-1}|ii\rangle\langle ii|$ and $X = \frac{1}{d\sqrt{d}}\sum_{i,j=0}^{d-1}u_{ij}|ij\rangle\langle ij|$, where u_{ij}'s are the elements of a unitary matrix such that $|u_{ij}| = \frac{1}{d}$. For this state, it has been found in [352] that for the case of $d = 2^{20}$, $r^{\mathrm{DD}}(\sigma_{2^{20}}) \geq 0.98$ and $r^{\mathrm{DD}}(\sigma_{2^{20}}^{\Gamma}) \leq \frac{1}{2^{10}+1}$. Therefore, we see that whereas in QKD, the obtained bit in this setting is secure, the upper bound tells us that this bit is not secure in a device-independent setting. Therefore the state, and any of its parts, cannot be tested independently of the device. This example can be also regarded as supported evidence for the revised Peres conjecture for DI-QKD in [350] which states that bound entangled states cannot be used as a resource for DI-QKD.

Kaur et al. [353] develop the above bounds by going beyond PPT states and arrive at the following upper bound for general DI-QKD protocols based on the relative entropy of entanglement [354]

$$r^{\mathrm{DI}}(\rho) \leq (1-p) \inf_{(\sigma^{NL}, \mathcal{N})=(\rho^{NL}, \mathcal{M})} E_R(\sigma^{NL}) + p \inf_{(\sigma_L, \mathcal{N})=(\rho^L, \mathcal{M})} E_R(\sigma^L), \tag{177}$$

where $\rho = (1-p)\rho^{NL} + p\rho^L$ such that $(\sigma^L, \mathcal{N}), (\rho^L, \mathcal{M}) \in$ LHV where LHV denoted the set of devices with locally realistic hidden variable models. For the CHSH-based protocols, with ω denoting the CHSH violation, the following analogous upper bound can be obtained

$$r^{\mathrm{DI}}(\rho) \leq (1-p) \inf_{\omega(\sigma^{NL}, \mathcal{N})=\omega(\rho^{NL}, \mathcal{M})} E_R(\sigma^{NL}), \tag{178}$$

One implication of this bound is that all PPT states satisfy the CHSH inequality, resulting in a zero device-independent key rate for CHSH-based protocols. This, in turn, proves the revised Peres conjecture for such protocols. It is important to note that while there exist bound entangled states from which a private key can be distilled in device-dependent protocols, these states are useless for DI-QKD in CHSH-based protocols. Furthermore, for CHSH-based protocols, they show that the convex hull of above-mentioned bounds is a tighter upper bound on the device-independent key rates.

Upper bounds based on convex-combination attacks. Farkas et al. [90] studied the problem of upper bounding the key rate of a DI-QKD problem by applying a convex combination attack. In a convex combination attack, Eve distributes local deterministic correlations with certain probabilities that give rise to a local correlation $p_{AB}^{L}(a, b|x, y)$ with overall probability q_L, and a nonlocal quantum correlation $p_{AB}^{NL}(a, b|x, y)$ with probability $1-q_L$. Eventually, the observed correlation of Alice and Bob takes the form

$$p_{AB}(x, y) = q_L p_{AB}^{L}(a, b|x, y) + (1 - q_L)p_{AB}^{NL}(a, b|x, y), \tag{179}$$

Since Alice and Bob announce their input for each round, Eve knows their results in all rounds in which she distributes a local correlation, so to gain more information about the key, she should maximize q_L for the given observed correlation
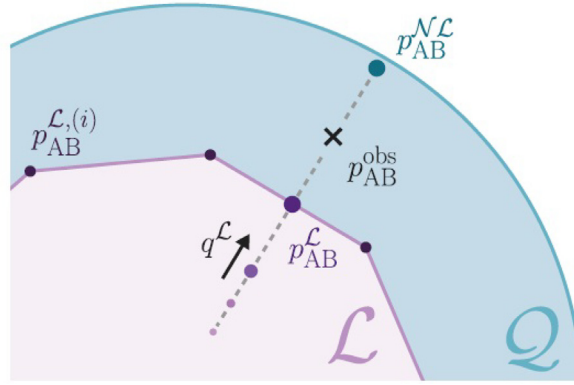
Fig. 18. Figure from [356]. Geometry formulation of the CC attack.

(179). By denoting e as the classical variable representing Eve's knowledge which $e = (a, b)$ when a local correlation was distributed and $e =?$ for the cases of nonlocal correlations were distributed. The corresponding joint probability of (179) distribution among Alice, Bob, and Eve is then written as

$$p_{ABE}(x, y, e) = q_L p_{AB}^L(a, b|x, y)\delta_{e,(a,b)} + (1 - q_L)p_{AB}^{NL}(a, b|x, y)\delta_{e,?}, \tag{180}$$

where δ is the Kronecker delta. Then, the following bound on the key rate can be obtained

$$r \leq \sum_{x,y} p_{xy} I_{xy}(A : B \downarrow E), \tag{181}$$

where p_{xy} is the probability of Alice and Bob choosing the settings x and y and $I_{xy}(A : B \downarrow E)$ is the intrinsic information of the distribution (180) which is defined as $I(A, B \downarrow E) = \min_{E \to F} I(A : B|F)$ where $I(A : B|F)$ is the conditional mutual information and the minimization is taken over all stochastic maps $E \to F$ that map the variable E to a new variable F such that the alphabet size of F is at most that of E.

The upper bound (181) resulted from a well-established result in classical cryptography that the asymptotic rate extractable from a distribution $p_{ABE}(a, b, f)$ is bounded by intrinsic information [355].

Additionally, Farkas et al. [90] investigate the problem by applying the upper bound on a standard protocol implemented on a two-qubit Werner state with visibility v using an arbitrary number of projective measurements. They showed that for a range of visibilities for which the Werner state is nonlocal the upper bound on the key rate is zero. This means that nonlocal quantum states exist that cannot be used for standard DI-QKD with projective measurements. Therefore, *the bell nonlocality is generally insufficient for the security of standard device-independent quantum key distribution protocols.*

To find the maximum value of q_L in (179), Lukanowski et al. [356] provided a geometric interpretation of the CC attack, which describes its optimization in terms of a linear program for determining the tightest upper bound on the key rate. A given correlation $p(a, b|x, y)$ represents a point within the probability space (Fig. 18). Maximizing q_L involves identifying two additional points that are collinear with this point: $p_{AB}^L(a, b|x, y)$, located within the local set $\mathcal{L}$, and p_{NL}, which lies outside the local set but within the quantum set $\mathcal{Q}$. The goal is to minimize the ratio of the distances from $p_{AB}^L(a, b|x, y)$ to $p_{AB}(a, b|x, y)$ and from $p_{AB}^{NL}(a, b|x, y)$ to $p_{AB}(a, b|x, y)$.

The assertion that Eve has perfect knowledge of all outcomes when distributing a local correlation to Alice and Bob is based on the fact that the local set $\mathcal{L}$ forms a convex polytope within the probability space. As such, any local correlation $p_{AB}^L(a, b|x, y)$ can be expressed as a combination of the extremal points of the polytope, which can be represented by the vector $\boldsymbol{p}^L = (p_i^L(a, b|x, y))_i$. Furthermore, in this geometric construction, maximizing the local weight q_L results in the optimal local correlation $p_{AB}^L(a, b|x, y)$ lying on the boundary of the local polytope $\mathcal{L}$, meaning it must always reside on one of the polytope's facets.

Analogous to $\boldsymbol{p}^L$, one can define the vector $\boldsymbol{q}^L = (q_i^L(a, b|x, y))_i$, which represents the probabilities assigned by Eve to each local correlation in the CC attack. Similarly, the average non-local correlation that Eve distributes can be modeled as a mixture of preselected non-local quantum correlations, forming the vector $\boldsymbol{p}^{NL} = (p_i^{NL}(a, b|x, y))_i$, with the corresponding probability vector $\boldsymbol{q}^{NL} = (q_i^{NL}(a, b|x, y))_i$ indicating the probabilities assigned by Eve to each non-local correlation.

To optimize the CC attack, Eve seeks a probability vector $\boldsymbol{q} = \boldsymbol{q}^L \oplus \boldsymbol{q}^{NL}$, ensuring that local correlations are distributed as frequently as possible. This requires solving the following linear program, which maximizes the overall probability of

sending any local boxes:

$$\boldsymbol{q}_{CC}[\boldsymbol{p}^{NL}, p(a, b|x, y)] = \arg\max \sum_i q_i^L,$$

subject to the following constraints:

$$\boldsymbol{q}^L \cdot \boldsymbol{p}^L + \boldsymbol{q}^{NL} \cdot \boldsymbol{p}^{NL} = p(a, b|x, y),$$

$$\sum_i q_i^L + \sum_j q_j^{NL} = 1,$$

$$\forall i, j : 0 \leq q_i^L, q_j^{NL} \leq 1.$$

The first condition is nothing but Eq. (179) and the other constraints ensure $\boldsymbol{q}$ is a valid probability vector. The set of extremal local correlation, $\boldsymbol{p}^L$, is a predetermined fixed collection fixed by the scenario.

To apply the CC attack and upper bound the key rate in a DI-QKD protocol, one must first specify the ideal correlation that would be shared by the parties in the absence of noise, denoted by $Q_{AB}(a, b|x, y)$. However, due to practical imperfections − such as finite detection efficiency η and visibility v − the actual noisy correlation observed is $p_{AB}(a, b|x, y)$. This correlation is then decomposed within the attack into local and nonlocal parts as Eq. (179).

The method in [356] works such that the eavesdropper must specify in advance the set of nonlocal correlations p_{NL} to be used in the convex decomposition and then apply the linear program to determine the local contribution. For a CHSH protocol involving maximally entangled states with finite detection efficiency η, the maximum local weight can be analytically determined as

$$q^L = (1 - \eta)(1 + (3 + 2\sqrt{2})\eta) \quad \text{for} \quad \eta \geq \eta_{\text{loc}},$$

where $\eta_{\text{loc}} = 2(\sqrt{2} - 1) \approx 82.8\%$ is the detection efficiency threshold, below which ($\eta < \eta_{\text{loc}}$) the correlation $p(a, b|x, y)$ becomes local.

As a result, the following bounds can be derived for the one-way and two-way protocols:

$$r_{\text{1-way}} \leq (3 + 2\sqrt{2})\eta^2 - 2(1 + \sqrt{2})\eta - \frac{\eta}{2} h(\eta) - (1 - \eta) h\left(\frac{\eta}{2}\right), \tag{182}$$

$$r_{\text{2-way}} \leq \eta \left(2(1 + \sqrt{2})\eta - 2\sqrt{2} - 1\right) \left(1 - h\left(\frac{1 - \eta}{1 - 2(1 + \sqrt{2})(1 - \eta)}\right)\right). \tag{183}$$

There are critical values for one-way ($\eta_{\text{1-crit}} \approx 89.18\%$) and two-way ($\eta_{\text{2-crit}} \approx 85.36\%$) protocols, below which the key rates become negative. This demonstrates that, for detection efficiencies in the range $\eta_{\text{loc}} \leq \eta \leq \eta_{\text{i-crit}}$, no DI-QKD protocol is feasible, even though the shared correlation remains nonlocal. The same result can be extended to the case of finite visibility ($v < 1$); i.e., there are critical visibilities that introduce nonlocal intervals in which no DI-QKD protocol is possible.

Zhang et al. [357] applied the CC attack to a two-way protocol by optimizing the non-local points in the CC decomposition using the NPA-hierarchy 2.2. They demonstrated that noise reduction can be achieved by employing the B-step procedure [253].

6. Semi-device-independent quantum key distribution

The implementation of fully DI-QKD schemes is hampered by the stringent hardware requirements that currently prohibit a reasonable key rate over practical distances. One way to make DI methods more viable is to slightly relax the notion of *device independence*, and establish a minimal set of reasonable assumptions. This approach, named semi-device-independent (SDI) QKD reduces hardware demands, so that a more reasonable key (or randomness) rate can be achieved with current technology [118]. Examples of these additional assumptions include (i) an upper bound on the system's dimension [118], (ii) shared randomness [358], or (iii) honest construction of part of the device [359]. Still other approaches within the general semi-DI philosophy include measurement-device independent (MDI) QKD [120] and one-sided DI-QKD (1SDI-QKD) [119]. In the following sections, we present these methods (see Table 7).

6.1. Prepare-measure semi-device-independence

In DI-QKD protocols, the security is based on testing non-locality between two parties. One question that can arise is whether such a strong form of security could be established for prepare and measure scenarios. This question is especially important since many commercially available QKD systems operate in one-way configurations, in which a transmitter (Alice) prepares a quantum state and sends it to a receiver (Bob). This question was first addressed by Pawłowski and Brunner in 2011 [118], in a scenario which they called semi-DI (SDI). In their approach, the Hilbert space dimension of the quantum system is known, but the quantum preparation and measurement devices are uncharacterized, such that the devices of Alice and Bob can be seen as black boxes. The assumptions of the SDI protocols are the following (see [118]):

Table 7
Overview of semi-device-independent QKD (SDI-QKD) protocols.

Protocol	Main assumption(s)	Key features	Security notes
P&M SDI-QKD	Known dimension of quantum states	One-way communication; black-box devices for Alice and Bob	Uses dimension witnesses; robust against individual attacks
RDI-QKD	Trusted sender; bounded overlaps $\gamma_{ij} = \langle\psi_i|\psi_j\rangle$	No assumptions on Bob's device	Resilient to side-channel attacks on Bob
MDI-QKD	Untrusted measurement devices; trusted sources	Bell-state measurement by untrusted third party	Removes detector-side channel attacks
DDI-QKD	Trusted preparation; black-box detection system	Uses single-photon Bell-state measurement	Simpler than MDI-QKD, but vulnerable to preparation attacks
1SDI-QKD	One trusted party; entanglement-based	Demonstrates quantum steering; asymmetric trust	Security linked to steering inequalities

---

SDI-QKD scenario [118]

1. Alice's black box is a "state preparator" which has the freedom to choose among a certain set of preparations $\rho_a \in \mathcal{B}(\mathbb{C}^d)$ with $a \in \{1, \ldots, N\}$ unentangled from Eve, but knows nothing about these quantum states apart from their dimensionality. She sends the prepared state to Bob.
2. Bob's measurement device is a black box. He can choose to perform an uncharacterized measurement M_y with $y \in \{1, \ldots, m\}$ and gets the outcome $b \in \{1, \ldots, k\}$.
3. The boxes may feature shared classical variables λ, known to Eve, but uncorrelated from the choice of preparation (measurement) made by Alice (Bob).
4. After repeating this procedure many times, Alice and Bob can estimate the probability distributions $P(b|a, y) = \text{Tr}(\rho_a M_y^b)$ which denotes the probability of Bob finding outcome b when he performed measurement M_y and Alice prepared ρ_a.
5. The protocol is restricted to individual attacks.

Notice that if Alice's preparations were entangled with Eve's system, then the communication capacity would be effectively doubled using dense coding [360].

To prove the security of SDI-QKD from the table of probabilities $P(b|a, y)$, a *dimension witness* can be used to estimate the minimal dimension of the state sent from Alice to Bob. Introduced by Gallego et al. [74], a dimension witness is defined as $W = \sum_{a,y,b} w_{aby}P(b|ay)$, where the real coefficients w are chosen such that one can derive lower bounds on the dimension of classical or quantum systems that is necessary to reproduce the measurement data. For example, in the simplest case of a two-dimensional system with three preparations and two binary measurements, for a classical system (i.e., a bit), they derived the witness I_3:

$$I_3 = |E_{11} + E_{12} + E_{21} - E_{22} - E_{31}| \leq 3, \tag{184}$$

where $E_{ij} = P(b = +1|ij) - P(b = -1|ij)$. To surpass the upper bound with a classical system, dimension of at least three (trits) is required, giving an algebraic maximum of $I_3 = 5$. Looking now to the quantum case, the same witness can be employed. After solving the maximization problem, one finds that $\max_{|\psi\rangle \in \mathcal{H}_2} I_3 = 1 + 2\sqrt{2}$, and the witness takes the form $I_3 \leq 1 + 2\sqrt{2}$.

The first four terms in (184) can be seen as a CHSH inequality (whose maximum is $2\sqrt{2}$), and the maximization does not involve the fifth term (E_{31}), which can be set to -1. Thus, the violation of (184) corresponds to the violation of the CHSH inequality and can be seen as a device-independent protocol by estimating the CHSH inequality. Moreover, the witness I_3 can be used to distinguish between bits and qubits. If the dimension witness W satisfy the following condition

$$C_d < W \leq Q_d, \tag{185}$$

where C_d and Q_d are the classical and quantum bounds respectively, for dim $\mathcal{H}_A = d$. Specifically, suppose Alice's device creates d–dimensional quantum systems, a value $W > C_d$ means that it becomes infeasible to replicate the quantum data table using d–dimensional classical systems, or equivalently quantum states emitted by Alice's device that are *orthogonal* to Bob's measurements. The inability to replicate the data table using d–dimensional classical systems, witnessed by $W > C_d$, confirms that Eve cannot access the full information about the system. Relaxing the assumption on the dimension would enable Eve to use a classical system with sufficient higher dimensions to reproduce such a table.

To prove the security of SDI-QKD in [118], following the geometrical method in [74], the authors utilize a dimensional witness as the main tool to assess the security of SDI-QKD. Consider that Alice's device prepares qubits and is limited to four specific preparations ($N = 4$), denoted by two bits, a_0 and a_1, while Bob's device can perform two binary measurements, and they can evaluate the correlators $E_{a_0 a_1, y}$. They can evaluate a dimension witness of the form

$$S = E_{00,0} + E_{00,1} + E_{01,0} - E_{01,1} - E_{10,0} + E_{10,1} - E_{11,0} - E_{11,1} \leq 2. \tag{186}$$

Applying this dimension witness to the states and measurements of the BB84 protocol yields $S = 2$, demonstrating the insecurity of the BB84 scheme. However, this conclusion is not limited to BB84, and in fact any protocol that utilizes the same states and measurements as BB84, such as the SARG protocol [361], is also insecure when viewed from this perspective. Rather, to obtain a positive key rate in the SDI scenario, Bob must perform measurements in a basis that is rotated with respect to the BB84 bases, as will be discussed below.

Security of SDI-QKD. A secret key can be extracted if a positive value for the key rate $r = I(A : B) - I(A : E)$ is obtained, where $I(A : X) = \sum_j 1 - h(P_X(a_{y_j}))$ represents the mutual information. Consequently, the sufficient condition for security is expressed as follows:

$$I(A : B) > I(A : E) \Longrightarrow P_B > P_E,$$

where $P_X = \frac{1}{2}(p_X(a_0) + p_X(a_1))$ denotes the average probability of party X correctly guessing when Alice sends the state $\rho_{a_0 a_1}$, based on the two random bits a_0 and a_1 that she generates. By evaluating Bob's success probability, it can be established that P_B is a function of S as given by:

$$P_B = \frac{S + 4}{8}.$$

Now, consider the following scenario: Alice receives an n-bit string as input, and Bob is tasked with guessing the value of a function from the set $\{F_n\}_n$ (where $\{F_n\}_n$ represents all Boolean functions on n-bit strings) after receiving s qubits from Alice. The average probability of Bob's success is bounded above by:

$$P_n \leq \frac{1}{2} \left(1 + \sqrt{\frac{2^s - 1}{2^n - 1}} \right).$$

For $n = 2$, the optimal probability of guessing a function F_n or its negation is equivalent. Thus, when Alice sends a single qubit to Bob ($s = 1$), we have:

$$P_B(a_0) + P_B(a_1) + P_B(a_0 \oplus a_1) \leq \frac{3}{2} \left(1 + \frac{1}{\sqrt{3}} \right),$$

which also holds when Bob collaborates with Eve. By utilizing the relationships $P_{BE}(a_i) \geq P_B(a_i)$ and $P_{BE}(a_i) \geq P_E(a_i)$, along with the inequality:

$$P_{BE}(a_0 \oplus a_1) \geq P_{BE}(a_0, a_1) \geq P_{BE}(a_0) + P_{BE}(a_1) - 1,$$

one can derive the following equation:

$$P_{BE}(a_0) + P_{BE}(a_1) + P_{BE}(a_0 \oplus a_1) \geq 2P_B(a_0) + 2P_E(a_1) - 1.$$

Using the earlier inequality, this leads to:

$$P_B(a_0) + P_E(a_1) \leq \frac{5 + \sqrt{3}}{4}.$$

A similar inequality can be derived by interchanging a_0 and a_1. This illustrates that when Eve attempts to guess a different bit than Bob, she will inevitably disturb Bob's statistical outcomes. From inequality $P_B(a_0) + P_E(a_1) \leq \frac{5+\sqrt{3}}{4}$ and its symmetry with respect to a_0 and a_1, we conclude:

$$P_B + P_E \leq \frac{5 + \sqrt{3}}{4}.$$

This implies that $P_B > P_E$ if:

$$P_B > \frac{5 + \sqrt{3}}{8} \approx 0.8415.$$

When Bob uses measurement operators $(\sigma_x \pm \sigma_z)/\sqrt{2}$, $P_B \sim 0.8536$ and the key rate is

$$r = I(A : B) - I(A : E) \approx 0.0581.$$

An additional conclusion can be drawn from the discussion above. In DI-QKD, nonlocality is necessary but not sufficient [90] (see 5.9). Similarly, we can deduce the analogous result: *mere violation of a dimension witness ($S > 2 \Longrightarrow P_B > 3/4$) is not sufficient to guarantee the security of SDI-QKD.*

In the ideal scenario where perfect detectors are assumed, meaning all systems leaving Alice's laboratory are detected by Bob, P_B is the sole security parameter. However, in the presence of losses, the average detection efficiency of Bob's detectors, denoted as η_B, becomes an additional security parameter. It is crucial to define how the parties handle rounds where no particle is detected. Chaturvedi et al. [362] chose the simplest case, where no-detection rounds are discarded from the statistics. This choice allows the parties to estimate the average success probability close to the optimal one in [118]. If we split Bob's detection efficiency as $\eta_B = \eta + \eta'$, where $\eta = P(\text{Click}|e \neq b)$ represents the detection efficiency when Eve's and Bob's inputs are different, and η' corresponds to the case where their inputs are the same, then Eve maximizes η' because she wants Bob's device to return outcomes as often as possible. Since Eve has no control over Bob's setting, this leads to $\eta_B = \frac{1+\eta}{2}$. Therefore, the condition for establishing a secret key is translated to

$$P_B(\eta) > P_E(\eta). \tag{187}$$

Chaturvedi et al. [362] studied security against two types of quantum eavesdroppers, those with and without access to quantum memory. They showed that, in the general case where Eve could control both Alice's and Bob's devices, the security condition for both cases (with and without memory) is

$$P_B > \frac{1}{2}\left(1 + \frac{1}{1+\eta}\right). \tag{188}$$

Moreover, they considered a minimal characterization of the preparation device, with the restriction that, while Eve can choose the states that leave Alice's laboratory, she cannot alter them during the protocol. This is a reasonable assumption, as manipulations inside Alice's laboratory are significantly more difficult for Eve. They found that the optimal states are mutually unbiased bases, and the security condition in this case is

$$P_B > \frac{1}{4}\left(2 + \cos\alpha_\eta + \frac{1-\eta}{1+\eta}\sin\alpha_\eta\right), \tag{189}$$

where $\alpha_\eta = \arctan\left(\frac{1-\eta}{1+\eta}\right)$. The fact that these conditions are the same for both cases, with and without memory, proves that access to a small quantum memory (a qubit) does not help the eavesdropper in attacking the SDI-QKD protocol.

Additionally, as a straightforward generalization of the original protocol [118], Chaturvedi et al. [362] presented a modified SDI-QKD protocol based on the $(3 \rightarrow 1)$ scenario. In this protocol, Alice is given three bits, and depending on them, she prepares a state and sends it to Bob, who has as input a classical trit $b \in \{0, 1, 2\}$ to select his measurement. Although the generalized protocol has lower key rates, the security requirements are significantly reduced.

Relation between SDI and DI. Just as the violation of a Bell inequality in the DI case tells us that the measured system cannot have a classical description, the violation of a dimension witness in the SDI case tells us that the communicated system cannot be a classical bit. In both cases, violation of the classical bound is a necessary (though not always sufficient) condition, with the difference residing in the form of the inequalities. Finding the correspondence between these two objects is equivalent to finding the correspondence between the scenarios. A typical bell inequality I can be written as $I = \sum_{a,b,x,y}\alpha_{a,b,x,y}P(a, b|x, y)$. Using the relation $p(a, b|x, y) = p(a|x, y)p(b|a, x, y)$, then I can be rewritten as $\sum_{a,b,x,y}\alpha_{a,b,x,y}p(a|x, y)p(b|a, x, y)$. By considering a as an input of Alice ($x' = (x, a)$), $p(a|x, y)$ can be seen as the part of Alice's input is a. Since in the parameter estimation phase of the protocol the inputs are chosen according to a uniform distribution, we set $P(a|x, y) = \frac{1}{A}$, where A is the size of the alphabet of a. Then, the Bell inequality I takes the form of a dimension witness. Using this method, the method for going from SDI to DI and vice versa was introduced in [363]. For going from SDI to DI, Alice's input x must be divided into a pair comprising a setting and an outcome. Let us consider the SDI randomness generation (based on $n \rightarrow 1$ quantum random access code q) where Alice input x' is a collection of n independent bits $a_0, \ldots, a_{n-1}$. For this case, Alice's input can be divided into pairs of outcome $a = a_0$ and setting $x = (a_1, \ldots, a_{n-1})$ and a family of Bell inequalities can be obtained which they were found useful to implement entanglement-assisted random access codes works in DI randomness and DI-QKD protocols. The other side is also possible, and one can show a DI protocol can be converted to an SDI protocol. The example of this conversion was also shown in [363].

Using a similar approach, Woodhead et al. [364] demonstrated that the fundamental bound on Alice's min-entropy in the DI setting also applies to the semi-DI setting. They achieved this by utilizing the PM version of the CHSH correlator, defined as $S = \frac{1}{2}\sum_{abxy}(-1)^{a+b+xy}P(b|axy)$, instead of Eq. (11). This result helps bring the semi-DI setting, where security proofs are still lacking, more in line with the established security results for DI-QKD.

SDI protocols based on other assumptions. In addition to the previously mentioned protocols, it is possible to introduce other SDI protocols based on alternative constraints. A prerequisite for developing any DI or SDI protocol is to examine the set of available correlations under the given assumptions. In light of this, Himbeeck et al. [365] introduced a general framework for SDI prepare-and-measure scenarios and modified it to account for a physical constraint, namely, the mean value of an observable. This results in a restriction on the quantum messages ρ_x, which can be expressed as a constraint on the corresponding mean values $H_x = \text{tr}(H\rho_x)$ of the observable.
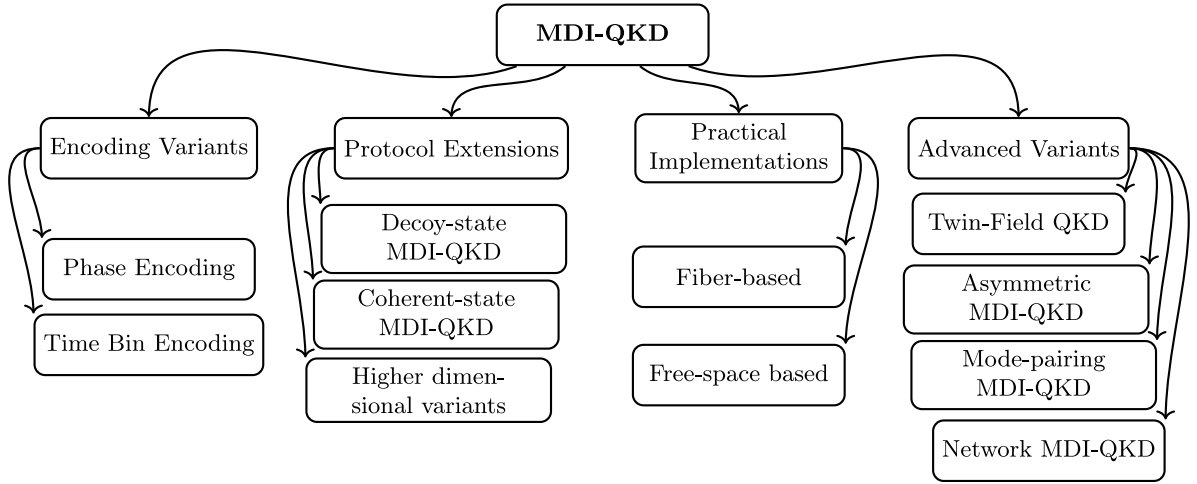
Fig. 19. Hierarchical overview of MDI-QKD advancements.

More specifically, Himbeeck et al. [365] considered two types of constraints on the mean values of H. The first, called the max-average assumption, assumes upper bounds on the mean values:

$$H_x = \text{tr}(H\rho_x) = \sum_\lambda p_\lambda \text{tr}(H\rho_x^\lambda) \leq \omega_x, \quad \forall x. \tag{190}$$

For example, if H is the photon-number operator, one can trust that, for all states ρ_x emitted by the source, the mean photon numbers H_x are below a certain threshold. If the states emitted by the source (Alice) vary from run to run according to some random parameter λ, the max-average assumption only bounds the mean value averaged over all possible values of $H_{x|\lambda} = \text{tr}(H\rho_{x|\lambda})$. However, it does not constrain the maximum values of $H_{x|\lambda}$, which could, in principle, be arbitrarily high. To address this, a stronger assumption, known as the max-peak assumption, was introduced:

$$\max_\lambda H_{x|\lambda} = \max_\lambda \text{tr}(H\rho_x^\lambda) \leq \omega_x, \quad \forall x. \tag{191}$$

Again, if H is the photon-number operator, this second condition still allows fluctuations in photon numbers within each state. It does not imply truncation of the Fock space, as the constraint only imposes a bound on the mean values $\text{tr}(H\rho_x^\lambda)$ of H for each ρ_x^λ. In particular, the states may still have non-zero amplitudes in any number-basis states.

The max-average assumption has the advantage of being verifiable externally by testing the average emitted states without requiring knowledge of the internal workings of the source. On the other hand, verifying the max-peak assumption typically depends on modeling the source. Its primary advantage is that it is more restrictive and can certify useful properties that would not be certified under the max-average assumption.

6.2. Measurement-device-independent QKD

The purpose of SDI-QKD is to eliminate the most serious possible hardware vulnerabilities at the expense of a minimum of security assumptions. The measurement devices and detectors used in QKD present considerable opportunities for side-channel attacks by Eve, in particular, due to the fact that Eve can both probe and/or manipulate the measurement system using external light, allowing her to determine measurement settings, blind a detector, or force a detector to "click". To combat this type of attack, Lo et al. proposed the idea of measurement-device-independent QKD (MDI-QKD) in 2012 [120]. Since its introduction, many variants and improvements of MDI-QKD have been proposed, a summary of which is shown in Fig. 19. In the following section, we present a brief overview of MDI-QKD.

6.2.1. Original MDI-QKD protocol

The main idea of the original MDI-QKD scenario [120] is sketched in Fig. 20. For simplicity, consider first that Alice and Bob each send a single photon to Charlie, who implements a linear-optical Bell-state measurement (BSM), which can be described by measurement operators Π_+, Π_-, Π_0 (see also Fig. 22). Here $\Pi_\pm$ is a rank-one projector onto one of the Bell states $|\psi^\pm\rangle = (|H\rangle_A|V\rangle_B \pm |V\rangle_A|H\rangle_B)/\sqrt{2}$, where H and V are the rectilinear polarization states. Π_0, on the other hand, is a rank-two projector onto the remaining two Bell states. When Alice and Bob prepare their pulses in either the H or V polarization state, a successful BSM ("$\Pi_\pm$" results) indicates that their pulses were prepared in orthogonal states. In the ideal scenario, they have an error rate of zero. These events can be used to generate a shared key — say — by defining $H_A \equiv$ "0" and $V_A \equiv$ "1", where Bob will flip all of his bits so that their bit strings are correlated. When the photons are prepared with diagonal polarization (states A, D in Fig. 20), a detection of the state ψ^- (ψ^+) occurs only when

A / B	H	V	D	A
H	Π_0	$\Pi_\pm$	X	X
V	$\Pi_\pm$	Π_0	X	X
D	X	X	Π_+, Π_0	Π_-, Π_0
A	X	X	Π_-, Π_0	Π_+, Π_0
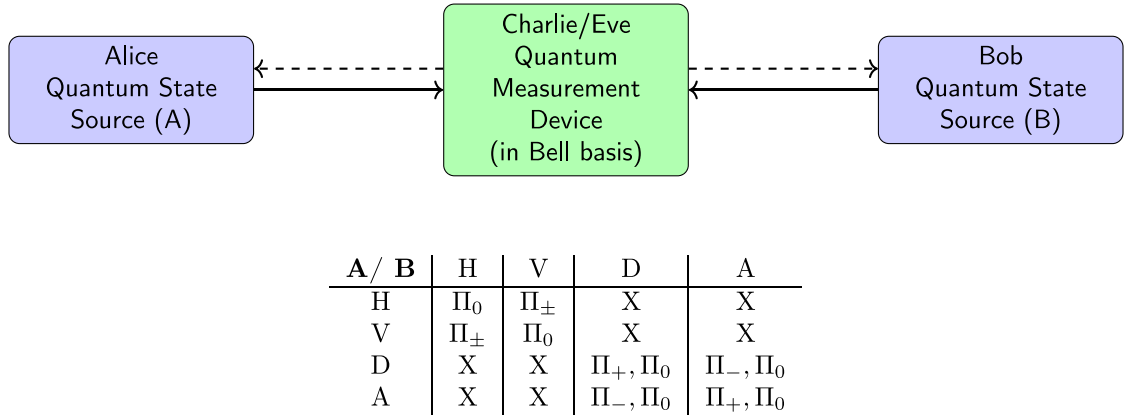
Fig. 20. Basic set-up of an MDI-QKD protocol. Alice and Bob each send a single photon to Charlie, who implements a linear-optical Bell-state measurement, which can be described by measurement operators Π_+, Π_-, Π_0. The tables includes expected detection results at BSM station in MDI-QKD. "X" refers to discarded results in which Alice and Bob chose different bases. H, V, D, A are horizontal, vertical, diagonal and anti-diagonal linear polarization states, respectively.

orthogonally (parallel) polarized pulses were prepared. An error in this case corresponds to detection events Π_+ (Π_+) when orthogonal (the same) diagonal polarization states are sent. With the error rates for both bases, post-processing steps similar to BB84 can be realized.

Remarkably, the same logic can be applied to the case when Alice and Bob use weak coherent pulses (WCP) [120]. To fully realize MDI-QKD, the pulses are prepared in one of the four polarization states, determined by random bit strings held by Alice and Bob, and then sent to Charlie, who publicly announces the results when the BSM is successful. Alice and Bob subsequently post-select their data, retaining only the outcomes with a successful BSM, and the same preparation bases were used. The data corresponding to the diagonal basis is used for assessing bit and phase error rates. If the error rates fall below a predetermined threshold, Alice and Bob proceed with classical error correction and privacy amplification processes to obtain a secure key; otherwise, they terminate the protocol. Most notably, MDI-QKD does not require a trusted measurement apparatus. To see this, notice that a successful BSM event $\psi^\pm$ does not provide any information about whether Alice and Bob prepared H_A, V_B (= secret bit value 0) or V_A, H_B (= secret bit value 1), and moreover there is no basis selection at the measurement device, so no information can be acquired if Eve somehow probes the BSM station. In addition, forcing BSM detectors to click, or announcing false results will inevitably lead to errors when diagonal states are sent.

Thus, MDI-QKD effectively mitigates all potential detector side channels, and in fact, the BSM station can be implemented by an untrusted third party and completely under Eve's control. However, one still needs to consider the imperfection of signal resources, such as the basis-dependent flaw that results in a decrease in achievable distance. Therefore, a generalization of [120] is essential for practical purposes.

Published back to back with Ref. [120], Braunstein et al. (2012) adopted a similar approach by devising a side-channel-free protocol to account for all potential side channels that might arise during a QKD implementation [42]. In its simplest form, this protocol corresponds to an entanglement-swapping experiment, where the dual teleportation channels serve as ideal Hilbert space filters to eliminate the possibility of side-channel attacks. To prevent any attempts at probing side channels within Alice's and Bob's laboratories, they implemented state-generation via partial measurement of a bipartite entangled state. This strategic move effectively isolates any external probes from the state-generation device. This approach ensures the complete protection of both Alice and Bob's private spaces against any potential side-channel attacks. In this protocol, the secret key rate can be lower bounded through the use of quantum memory and by calculating the entanglement distillation rate over the distributed state as follows:

$$r \geq I(A\rangle B|L') + \Delta. \tag{192}$$

Here, $I(A\rangle B|L')$ represents the coherent information conditioned on Eve's fake variable L' which Eve sends to both parties to mislead them, instead of the true variable L ($I(A\rangle B) = S(\rho_B) - S(\rho_{AB}) = -S(A|B)$) and Δ denotes the amount of classical cheating.

By modeling MDI-QKD as a special case of LOCC-assisted communication over a multiplex quantum channel, Das et al. [366] derived a tight strong-converse upper bound on the achievable key rate. The bound is expressed in terms of entanglement measures, such as the max-relative entropy of entanglement and, for teleportation-simulable channels, the relative entropy of entanglement of the effective channel's Choi state. For practical photon-based MDI-QKD setups (e.g., with erasure or depolarizing channels), their results account for both channel losses and imperfections at the measurement node, offering a more precise benchmark than earlier network-cut-based bounds.

Practical loopholes in MDI-QKD. Practical loopholes in MDI-QKD shift the focus from measurement device imperfections to state preparation or source flaws, as these can be exploited to compromise security. Liu et al. [367] demonstrated a hacking strategy leveraging modulation errors to obtain all key bits. One significant imperfection is the basis-dependent flaw arising from discrepancies in density matrices in BB84 states, while the birefringence effect in optical fibers highlights the practicality of phase encoding over polarization encoding. Tamaki et al. [368] addressed these issues with two MDI-QKD schemes: one using phase locking of separate lasers and a double BB84 protocol to control basis-dependent flaws, and another employing phase encoding for longer distances. Primaatmaja et al. [369] introduced a numerical technique using semidefinite programming to analyze phase-error rates, showing phase-encoding MDI-QKD's potential to outperform decoy-state MDI-QKD at short distances. Zhu et al. [370] improved analysis by modulating different intensities in key and test bases. Bourassa et al. [371] identified a time-dependent side channel in sources employing Faraday mirrors, showing divergences between three-state and BB84 protocols. Alternative schemes [372] simplified encoding and decoding with minimal performance compromise. Xu et al. [373] analyzed error sources like polarization misalignment and mode mismatch, showing that MDI-QKD tolerates up to 6.7% polarization misalignment at 0 km and 5% at 120 km, while mode mismatch tolerance decreases from 80% to 50% over the same range. Wang et al. [374] estimated gains, error rates, and key rates under arbitrary photon mixtures, while Li et al. [114] proposed a polarization-alignment method using fewer devices to reduce photon loss. Phase-randomized weakly coherent pulses (PR-WCPs), commonly used due to a lack of mature single-photon sources, introduce errors in the X basis. Li et al. [375] incorporated these errors into security analysis, showing equivalence between PR-WCPs and Poisson-distributed photon states, with a tighter key rate than [376]. Lu et al. [377] introduced an MDI-QKD protocol addressing modulation errors, achieving high performance despite X basis imbalances and asymmetric channel transmittances. Yin et al. [378,379] removed encoding state characterization assumptions, demonstrating practicality and tolerance for high loss and errors over 160 km. Hwang et al. [380] improved phase error estimation, and Zhou et al. [381] extended uncharacterized qubit protocols to weak coherent sources using decoy-state methods. Kang et al. [382,383] developed protocols with uncharacterized coherent states under collective attacks. Li et al. [384] proposed the CHSH-MDI-QKD protocol to mitigate state preparation assumptions, using the CHSH inequality and decoy states [385] to enhance accuracy in single-photon yield estimation, though increased parameter estimation complexity limited its effectiveness.

Finite-key analysis. Finite-key analysis of MDI-QKD was first conducted in [376,386], where they derived secure bounds under the influence of statistical fluctuations in relative frequency. This analysis applies to practical detectors with low efficiency and highly lossy channels. Their study demonstrates the possibility of achieving secure transmission over distances exceeding 10 km with a success rate of 10^{10} outcomes, making it directly applicable in practical implementations. However, when the number of successful outcomes falls below 10^8, achieving a nonzero key rate becomes impossible.

Both studies mentioned above focused on security assessments against specific types of attacks. The first study to explore security proofs within the finite-key regime against general attacks and to satisfy the composability definition was conducted by Curty et al. [387]. They utilized the principles of large deviation theory, specifically employing a multiplicative form of the Chernoff bound, for critical parameter estimation. This step was crucial in demonstrating the feasibility of implementing MDI-QKD over long distances and within a reasonable timeframe. Their findings demonstrated that even with the technology available at the time, an MDI-QKD protocol could be realized without the need for high-efficiency detectors. Importantly, they showcased the potential for long-distance MDI-QKD protocols, extending up to approximately 150 km, for finite-sized data sets ranging from 10^{12} to 10^{14} signals. This achievement was made possible using practical signal sources, such as WCPs.

6.2.2. Decoy-state measurement-device-independent QKD

The sources used in MDI-QKD must be trusted, necessitating a complete characterization of the source. Commonly, weak coherent sources replace perfect single-photon sources, though they remain susceptible to photon number splitting (PNS) attacks due to multiphoton fractions [388]. To counteract this, the decoy-state method was originally proposed by Hwang [389], with the first security proofs independently established by Wang [40] and by Lo, Ma, and Chen [390]. This method has since been adapted for MDI-QKD to estimate single-photon contributions efficiently [372]. Wang et al. [391] further optimized this by employing three-intensity decoy states, which addressed basis-dependent coding errors. Subsequent enhancements, such as vacuum and weak decoy states by Sun et al. [392], showed improved performance but highlighted the limitations of certain methods. Advances continued with modified coherent states introduced by Li et al. [393], reducing multiphoton distributions and enhancing key rates. Techniques to refine single-photon yield and phase error estimation, as demonstrated by Zhu et al. [394] and Ding et al. [395], increased the accuracy of MDI-QKD parameters and extended secure transmission distances. Other studies, such as those by Mao et al. [396], explored new decoy-state frameworks that surpassed prior methods, further enhancing both distance and key rates.

Incorporating heralded single-photon sources (HSPS) offers notable benefits, including reduced dark count rates and lower QBER [397]. Wang et al. [398] showed that combining triggered and non-triggered events in HSPS-based protocols enhances both key rates and transmission distances. Subsequent works [399] applied biased decoy-state schemes with HSPS, yielding superior results for small datasets. Similarly, Zhou et al. [400], introduced passive decoy methods to spontaneous parametric down-conversion (SPDC) sources, to minimize side-channel leaks and improve performance compared to weak coherent states. While SPDC sources offer advantages, challenges such as spectral entanglement were addressed by Zhan et al. [401], underscoring the need for high-purity sources.

Optimization of decoy-state parameters has played a pivotal role in enhancing MDI-QKD protocols. Techniques such as local search algorithms [402], statistical fluctuation considerations [403], and advanced joint constraints [404] have significantly improved key rates and extended transmission distances. Furthermore, protocols integrating memory-assisted techniques [405] and MDI-QKD mode-pairing [406–412] further push the boundaries of MDI-QKD capabilities. Asymmetric protocols (where Alice and Bob have different distances from the source) [413] and reference-frame-independent methods [414,415] address practical challenges like channel asymmetry and misalignment, making MDI-QKD more adaptable for real-world applications.

6.2.3. High-dimensional measurement-device-independent QKD

So far, all mentioned protocols were for two-dimensional encoding systems using Z and X bases. In this section, we review protocols developed for higher dimensions. Chau et al. [416] introduced the protocol which they called the mother-of-all QKD protocol and its MDI variants for qudits, including the round-robin differential phase protocol [417] and the Chau15 protocol [418]. However, these were experimentally infeasible due to challenges in realizing high-dimensional Bell states. Hwang et al. [419] proposed a d-dimensional MDI-QKD protocol, proven secure under the condition of zero QBER. Jo et al. [420] proposed a three-dimensional MDI-QKD (3d-MDI-QKD) protocol with mutually unbiased bases (MUBs) comprising time and energy bases [421]. Bell state measurements in 3d-MDI-QKD use nine maximally entangled states in a three-dimensional bipartite system, enabling a secret key rate of $\tilde{r} \geq \log_2 3 - 2Q - 2h(Q)$, where Q represents state error rate. This protocol achieves higher secret key rates than the original MDI-QKD for low transmission losses, suitable for short-distance communication, but faces feasibility challenges in realizing high-dimensional Bell state measurements with linear optics [422]. Sekga et al. [423] introduced a qutrit-based MDI-QKD protocol employing biphotons and Mach–Zehnder interferometers, achieving significant secret key rates for moderate distances. Dellantonio et al. [424] extended QKD to generalized Z and X bases in d dimensions, demonstrating unconditional security with improved performance in low dark-count scenarios. Cui et al. [425] proposed a high-dimensional MDI-QKD protocol utilizing hyper-encoded qudits with polarization and spatial-mode degrees of freedom, yielding a fivefold improvement in secret key rates. This was further extended by Yan et al. [426] and Li et al. [427] to multi-degree-of-freedom encoding. The limitations of long-distance QKD due to decoherence prompted solutions like quantum repeaters, as discussed by Erkilic et al. [428]. Their MDI-QKD protocol surpasses the PLOB bound [429] using high-dimensional states optimized for increased key rates at shorter distances, though these advantages diminish with greater transmission distances due to photon loss.

6.2.4. Continuous-variable measurement-device-independent QKD

While two-dimensional discrete protocols can achieve long-distance communication, they often suffer from low key rates, making them unsuited for metropolitan network requirements. A solution to this challenge can be found in adopting continuous-variable (CV) systems. One significant advantage of a CV-QKD protocol is its compatibility with standard telecommunication technology, particularly because it does not rely on single-photon sources, which are the most vulnerable to attacks in discrete-variable QKD (DV-QKD) protocols. Another significant advantage is that, in a typical QKD protocol, users often need to allocate a portion of their raw data to estimate communication channel parameters, such as the error rate. This results in a trade-off between the secret key rate and the accuracy of parameter estimation in the finite-size regime. However, it has been demonstrated that this constraint does not apply to continuous variable QKD. In continuous variable QKD, the entire set of raw keys can be utilized for both parameter estimation and secret key generation without compromising security [430]. In addition, CV-QKD systems might be more suitable to coexist with classical data transmission in optical fibers, since the local oscillator required for homodyne detection can act as a mode filter, reducing classical Raman noise from the quantum signal.

As such, there is considerable interest in continuous-variable MDI-QKD (CV-MDI-QKD). The first CV-MDI-QKD protocols were originally introduced by Pirandola et al. [125], Li et al. [431] and Ma et al. [432]. The protocol operates as follows: Alice and Bob randomly prepare coherent states, denoted as $|\alpha\rangle$ and $|\beta\rangle$, respectively, where the amplitudes α and β are modulated by Gaussian distributions with zero mean and sufficiently large variances. These prepared states are then sent to an intermediary party (Charlie) for measurement. To establish secret correlations, Charlie performs a CV Bell measurement and communicates the outcomes to Alice and Bob. This Bell measurement is executed by mixing the incoming modes using a balanced beamsplitter. The measurement corresponds to the quadrature operators $\hat{q}_- = (\hat{q}_A - \hat{q}_B)/\sqrt{2}$ and $\hat{p}_+ = (\hat{p}_A + \hat{p}_B)/\sqrt{2}$, and the classical outcomes are combined into a complex variable denoted as $\gamma = (q_- + ip_+)/\sqrt{2}$. The most general eavesdropping strategy involves a joint attack encompassing both Charlie's measurement device and the two communication links, namely Alice–Charlie and Charlie–Bob. Since the protocol is based on Gaussian modulation and the detection of Gaussian states, the optimal eavesdropping technique employs a Gaussian unitary approach [433]. By introducing a reconciliation efficiency factor denoted as $\epsilon \leq 1$, the secret key formula can be modified as follows:

$$r := \epsilon I(A:B) - I_E. \tag{193}$$

where I_E is the upper bound on Eve's information.

An investigation into the performance of the protocol under ideal reconciliation conditions ($\epsilon = 1$) reveals the potential for achieving remarkably high secret key rates, approaching one bit per use. Notable, symmetric configurations, where the transmissivities are the same between Alice–Charlie and Bob–Charlie, are not the most secure option, particularly

for longer distances. The optimal configuration is asymmetric, corresponding to minimal loss in Alice's link, which allows Bob's link to have a low transmissivity. Specifically, if Charlie's position can be situated close to Bob, the total transmission distance, i.e., the distance between Alice and Bob, can theoretically extend up to 80 km. Taking into account realistic reconciliation performance, the experimental rates closely approach the maximum theoretical predictions. In particular, with $\epsilon \approx 0.97$, the experimental rates can achieve remarkably high values over typical connection lengths within a metropolitan network.

Zhang et al. [434] introduced a CV-MDI QKD protocol using squeezed states and demonstrated that its secret key rate consistently surpasses the coherent-state-based protocol, particularly under collective attacks, with a total maximum transmission distance increase of 6.1 km under both perfect and imperfect detectors. The transmission distance further increases in asymmetric scenarios. In the extreme case where Charlie is on Bob's side, such that the coherent-state-based protocol achieves zero transmission distance, the squeezed-state protocol significantly outperforms it, especially with the introduction of optimal Gaussian noise levels on Bob's side, as determined for maximizing key rate and transmission distance under reverse reconciliation. Chen et al. [435] extended this protocol against general attacks using entropic uncertainty relations, yielding a composable security analysis and demonstrating the system's resilience to a maximum channel loss of 0.64 dB. One key limitation of Gaussian-modulated protocols is their low reconciliation efficiency in long-distance transmissions, which has driven interest in discrete modulation. Ma et al. [436] proposed a four-state discrete-modulated CV-MDI-QKD protocol, leveraging nonorthogonal coherent states for encoding bits, achieving longer transmission distances and simplified implementation compared to Gaussian modulation, with the eight-state protocol [437] further improving key rates and modulation variances. Wilkinson et al. [438] introduced postselection in long-distance CV-MDI-QKD, extending the communication range to 14 km over standard optical fiber, while protocols employing quantum catalysis [439,440], quantum scissors [441], and multimode signals [442] further improved performance by improving transmission distance and reducing noise. Practical implementation challenges, such as independent light sources, phase reference calibration, and external disturbances, require mitigation to prevent overestimation of key rates. Ma et al. [443] studied phase calibration imperfections and their thermal noise equivalence, proposing models for realistic security analysis, while Zhao et al. [437] introduced Bayesian phase-noise estimation to eliminate local oscillator transmission. Simplified implementations, such as the plug-and-play scheme [444,445], address synchronization issues by deriving local oscillators from a shared laser, reducing complexity and enhancing stability. However, imperfections in state preparation also introduce Gaussian noise, as modeled by Ma et al. [443], who explored intensity error impacts under various distributions and emphasized placing stable sources on the encoder's side for optimization. Countermeasures like Huang et al.'s one-time calibration method [446] and noise characterization approaches are critical for enhancing practical security. Addressing transmittance fluctuations, Zheng et al. [447] highlighted performance degradation under varying channel conditions, proposing Gaussian post-selection to mitigate risks of denial-of-service attacks, while Li et al. [448] studied the effects of non-ideal Bell detection due to angle errors, showing significant transmission distance reductions even with minor errors. Efforts to reduce CV-MDI-QKD complexity include self-referenced schemes [449], shared optical path methods [450], and unidimensional modulation [451], achieving comparable performance with reduced system demands. Semi-Quantum Key Distribution (SQKD), introduced by Boyer et al. [452], evolved into a continuous variable version [453], enabling secure communication between classical and quantum users, leveraging Charlie's full quantum capabilities to balance cost-effectiveness and security under various attack scenarios.

Finite-size effects. The impact of finite-size effects on the key rate of CV-MDI-QKD was initially investigated by Papanastasiou et al. [454], considering two-mode Gaussian attacks, and by Zhang et al. [455], examining collective attacks. To study the security of the protocol, a potent approach is to employ the entanglement-based representation, where the description of the dynamics occurs within an extended Hilbert space, allowing the use of pure states. The protocol is outlined as follows: Alice and Bob employ sources of coherent states, which are purified, assuming they start from two-mode squeezed vacuum states ρ_{aA} and ρ_{bB}, where modes A and B are transmitted over the communication links, while local modes a and b are heterodyned. The measurements project the traveling modes into pure coherent states. The attenuation of the channel on modes A and B is modeled using two beam splitters with transmissivities τ_A and τ_B, where $0 \leq \tau_A, \tau_B \leq 1$. These processes manipulate Alice and Bob's signals with a pair of Eve's ancillary systems $E1$ and $E2$, which generally belong to a broader reservoir of modes controlled by the eavesdropper.

The key rate, accounting for finite-size effects, is expressed as:

$$r^{\text{finite}} = \frac{n}{N} \left(r - \Delta(n) \right), \tag{194}$$

where n represents the number of signals used for key preparation, N is the total number of exchanged signals, and r denotes the asymptotic key rate. The correction function $\Delta(n)$ is employed to compensate for the utilization of the Holevo function in the context of a finite number of signals. It is a function that relies on the number of signals used for key preparation (n) and the probability of error associated with the privacy amplification procedure ϵ_{PA} ($\Delta(n) \sim \sqrt{\frac{1}{n} \log_2(2/\epsilon_{PA})}$).

Numerical results indicate that under realistic conditions and considering finite-size effects, CV-MDI-QKD is viable for metropolitan distances within experimental constraints. In particular, a total number of signals exchanged in the range of $N = 10^6$ to 10^9 is sufficient to achieve a high key rate of 10^{-2} bits per use over metropolitan distances, even in the presence of excess noise of approximately 0.01.

For the protocol considering collective attacks, the CV-MDI-QKD protocol with an asymmetric structure and finite-size effects can securely transmit over approximately 86 km under ideal reconciliation efficiency and optimal modulation variance conditions for $n = 10^{10}$ block size. When the reconciliation efficiency is 96.9%, the maximum transmission distance achievable is approximately 75 km.

Lupo et al. [430] studied the security proof for coherent attacks. The advantage of their study compared to the previous ones is that the correlations between Alice and Bob are generated through the variable Z announced by the relay which allows Alice and Bob to do parameter estimation with a negligible amount of public communication. Therefore, the whole raw key can be exploited for both parameter estimation and secret-key extraction. They first investigated the security against collective attacks by presenting an improved estimation of the conditional smooth min-entropy obtained by applying a new entropic inequality and found the following lower bound on the secret-key rate:

$$r^{\text{finite}} \geq r - \frac{1}{\sqrt{n}} \Delta_{\text{AEP}}(\frac{2}{3}p\epsilon_s, d) + \frac{1}{n} \log(p - \frac{2}{3}p\epsilon_s) + \frac{1}{n} 2 \log(2\epsilon), \tag{195}$$

where p is the probability of successful error correction, ϵ_s is the smoothing parameter entering the smooth conditional min-entropy and $\Delta_{\text{AEP}}(\delta, d)$ is a function of dimensionality d ($\Delta_{\text{AEP}}(\delta, d) \leq 4(d + 1)\sqrt{\log(2/\delta^2)}$).

The secret key rate for coherent attacks can be modified by applying the results of [456] as

$$r^{\text{finite}} \geq \frac{n-k}{k} r^{\infty} - \frac{\sqrt{n-k}}{n} \Delta_{\text{AEP}}(\frac{2}{3}p\epsilon_s, d) + \frac{1}{n} \log(p - \frac{2}{3}p\epsilon_s) + \frac{2}{n} \log(2\epsilon) - \frac{2}{n} \log\binom{K+4}{4}, \tag{196}$$

where k is the number of signals used for the energy test and $K \sim n$. Based on numerical examples, it is in principle possible to generate a secret key against the most general class of coherent attacks for block sizes of the order of 10^7–10^9, depending on loss and noise. In particular, this composable security analysis confirms that CV-MDI protocols allow for high QKD rates on the metropolitan scale, supporting the results of the asymptotic analysis of Pirandola et al. [125]. The viability of utilizing the entire raw key for both parameter estimation and key extraction was later demonstrated by Lupo et al. [457]. Their work CV-MDI-QKD revealed that parameter estimation in this scheme can be achieved with minimal public communication, as correlations are postselected by the central relay. Consequently, the public variable announced by the relay encompasses all the information regarding the correlations between Alice and Bob, making it sufficient, along with the local data, to estimate the covariance matrix. This crucial discovery eliminates the trade-off between the secret key rate and the accuracy of parameter estimation in the finite-size regime of CV-QKD. Similar results are presented in [458,459].

Non-Gaussian postselection, such as virtual photon subtraction from a coherent state source, improves CV-QKD protocols by enhancing secret key rates and tolerating excess noise over longer distances [460,461]. Zhao et al. [462] and Ma et al. [463] demonstrated its application in coherent-state CV-MDI-QKD, optimizing performance through Alice's photon subtraction with carefully chosen parameters while maintaining protocol security. Kumar et al. [464] showed that photon subtraction on two-mode squeezed coherent states extends transmission distances up to 68 km but reduces key rates compared to vacuum states. Practical applications, such as photon subtraction over fiber-to-water channels [465], further validate this approach. Recently, Papanastasiou et al. [466] and Ghalaii et al. [467] analyzed composable finite key generation, demonstrating secure CV-MDI QKD over free-space optical links under realistic conditions.

6.2.5. Measurement-device-independent multiparty quantum communication

Multiparty quantum communication protocols strive to ensure information-theoretic security in the realm of highly sensitive and confidential multiuser communication. Using the principles of quantum mechanics, these protocols exhibit superior physical performance compared to their classical counterparts. Their versatile applications encompass a spectrum of scenarios such as secret multiparty conferences, remote voting, online auctions, management of payment system master keys, collaborative scrutiny of accounts containing quantum money, and the facilitation of secure distributed quantum computation.

Specifically, Quantum Cryptographic Conferencing (QCC) is a protocol designed for multiparty Quantum Key Distribution. QCC ensures the secure sharing of a key among legitimate users, even in the presence of potential eavesdroppers. Another notable protocol, Quantum Secret Sharing (QSS), involves the fragmentation of a message into multiple parts distributed among a group of participants. Each participant is allocated a share of the secret, and consequently, the complete set of shares is required to comprehensively decipher the message. For instance, QSS can be employed to guarantee that no single individual possesses the capability to launch a nuclear missile or access a bank vault independently. Instead, the collective participation of all legitimate users is essential for these critical actions.

Discrete variable protocols. The Greenberger–Horne–Zeilinger (GHZ) entanglement is an important resource for multiparty quantum communication tasks, especially for the measurement-device-independent versions of QCC (MDI-QCC) and QSS (MDI-QSS). However, the practical applications of GHZ states are quite limited due to the lack of two important factors — (i) high-intensity sources and (ii) reliable distribution of the GHZ states. To tackle these limitations, Fu et al. [468] take advantage of postselected GHZ states among three legitimate users (typically called Alice, Bob, and Charlie) to perform secure multiparty quantum communication. As a typical MDI-QKD protocol, the postselecting measurement device here can be regarded as a black box that can be manipulated by anyone including the eavesdropper. Therefore, the scheme

is naturally immune to all detection-side attacks and can be regarded as the combination of time-reversed GHZ state distribution and measurement. Moreover, by employing the decoy-state method, the scheme can defeat photon-number-splitting attacks. The protocol in [468] is as follows: Alice, Bob, and Charlie independently and randomly prepare quantum states with phase-randomized weak coherent pulses in two complementary bases (Z basis and X basis). They send the pulses to the untrusted fourth party located in the middle node, David, to perform a GHZ-state measurement which projects the incoming signals onto a GHZ state. After performing the measurement, David announces the events through public channels whether he has obtained a GHZ state and which GHZ state he has received. Alice, Bob, and Charlie only keep the raw data of successful GHZ-state measurements and discard the rest. They post-select the events where they use the same basis in their transmission through an authenticated public channel. Notice that Alice performs a bit flip when Alice, Bob, and Charlie all choose X basis and David obtains a GHZ state $\frac{1}{\sqrt{2}}(|000\rangle - |111\rangle)$. The data of Z basis is used to generate the key, while the data of X basis are used to estimate errors. After classical error correction and privacy amplification, Alice, Bob, and Charlie extract secure cryptographic conferencing keys. In the asymptotic limit, the MDI-QCC key generation rate and the MDI-QSS key rate are given by

$$R_{QCC} = Q_{\nu}^{Z} + Q_{111}^{Z}[1 - H(e_{111}^{BX})] - H(E_{\mu\nu\omega}^{Z*})fQ_{\mu\nu\omega}^{Z}, \tag{197}$$

$$R_{QSS} = Q_{\nu}^{X} + Q_{111}^{X}[1 - H(e_{111}^{BZ})] - H(E_{\mu\nu\omega}^{X})fQ_{\mu\nu\omega}^{X} \tag{198}$$

where $Q_{\mu\nu\omega}^{Z}$ and $E_{\mu\nu\omega}^{Z*}$ ($Q_{\mu\nu\omega}^{X}$ and $E_{\mu\nu\omega}^{X}$)) are the gain and quantum bit error rate of Z (X) basis respectively. The subscripts μ, ν, and ω are the pulse intensities of Alice, Bob, and Charlie respectively. Q_{111}^{Z} (Q_{111}^{X}) is the gain of Z (X) basis and e_{111}^{BX} (e_{111}^{BZ}) is the bit error rate of X (Z) basis. The parameter f is the error correction efficiency.

Simulation results for QCC show that the estimation using two decoy states gives a secure key rate nearly the same as the corresponding one using infinite decoy states. In the case of asymptotic data with two decoy states, the secure transmission distance between Alice and the middle node of MDI-QCC is about 190 km for the detection efficiency of 40% (210 km for the detection efficiency of 93%). For MDI-QSS, the secure transmission distance is about 130 km for the detection efficiency of 40% (150 km for the detection efficiency of 93%) between the middle node and any user. Hua et al. proposed a similar scheme based on a GHZ entangled state, which is different from the above protocol and uses a GHZ entangled state and the polarization state prepared by users to execute BSM and realize multi-user sharing of a common secret key [469]. They derived the secure key rate when users employ an ideal single photon source and a weak coherent source and showed that the secure distance between each user and the measurement device can reach more than 280 km while reducing the complexity of the quantum network. Despite the efficiency of the protocol, its scalability diminishes exponentially with the number of users, and security issues in QSS protocols, such as in [468], remain underanalyzed, particularly for participant attacks [470]. To address these challenges, Li et al. [471] proposed an MDI-QSS protocol based on spatial multiplexing, achieving a transmission distance over 300 km and a secret key rate two orders of magnitude higher than [470], while addressing security concerns like participant attacks. Ju et al. [472] introduced a hyper-encoding MDI-QSS protocol using polarization and spatial-mode degrees of freedom for enhanced error resilience and achieved a key rate improvement of three orders of magnitude over the original MDI-QSS protocol under a 100 km transmission distance. Zhang et al. [473] developed a secure protocol against Trojan horse attacks. Memory-assisted MDI-QKD, combined with HSPS and the decoy-state method, was introduced in [474].

Chen et al. [475] demonstrated finite-key performance using a biased decoy-state approach, further extended by an asymmetric decoy-state method achieving secure communication over 43.6 km [476]. Protocols using W-states [477] and cluster states [478] showed feasibility for distances over 150 km and 280 km, respectively. MDI key agreement protocols are discussed in [479–481].

Continuous variable protocols. A continuous-variable Measurement-Device-Independent multiparty quantum communication protocol was initially explored by Wu et al. [482], utilizing squeezed states of light and homodyne measurements to optimize the secret key rate. To execute QCC and QSS communication protocols, they employ a Continuous-Variable GHZ state, a multipartite entangled state with squeezed uncertainties in relative position and total momentum [483]. In the case of the tripartite CV GHZ state, their positions and momenta satisfy the relations $\hat{X}_1 - \hat{X}_2 \to 0$, $\hat{X}_2 - \hat{X}_3 \to 0$, and $\hat{P}_1 + \hat{P}_2 + \hat{P}_3 \to 0$.

The security analysis in [482] addresses two types of attacks: entangling cloner and coherent attacks. Under the entangling cloner attack, the maximal transmission distances can be extended in scenarios of unbalanced distribution. In contrast, the coherent attack notably diminishes the maximum transmission distances. A coherent state-based MDI multiparty protocol was investigated in [484], demonstrating superior performance compared to the squeezed state-based MDI protocol in terms of experimental realizations.

The three-party CV GHZ state in [482] is not prepared and then distributed; instead, it is obtained through postprocessing using the concept of entanglement swapping. Conversely, Guo et al. [485] employ a four-party GHZ state to execute the CV-MDI QSS protocol. Specifically, the four participants prepare and transmit modulated states to a relay for the generation of a four-party GHZ state. In this protocol, three participants collaborate to acquire the fourth person's secret key by leveraging the GHZ state. Furthermore, given that the detection apparatus inherently possesses imperfections, which do not compromise security but can diminish the generation rate of the final secret key, optical amplifiers are deployed to enhance the signal and compensate for these inherent imperfections. This deployment results in an increased

transmission distance. The same conclusion was found for the CV-MDI QCC [486]. The continuous variable measurement-device-independent quantum secret sharing and quantum conference based on a four-mode cluster state with different structures were conducted by Wang et al. [487].

Ottaviani et al. introduced an MDI-modular network in their work [488], presenting a modular design for continuous-variable networks. In this architecture, each module functions as a MDI star network. Within each module, users transmit modulated coherent states to an untrusted relay, thereby establishing multipartite secret correlations through a generalized Bell detection mechanism. Their investigation revealed that under ideal conditions, up to 50 users can achieve private communication exceeding 0.1 bit per use within a radius of 40 m, comparable to the size of a large building. Fletcher et al. [489] utilized the same generalized Bell detection technique to establish multipartite correlations between user variables. Their study demonstrates that postselection procedures based on performing reconciliation on the signs of prepared quadratures of coherent states can be effectively used to broaden the protocol's operational range.

6.2.6. Experiments in measurement device independent QKD

MDI-QKD was an important advance in that it reduces vulnerability to detector attacks, while being feasible with current technology. Not long after the concept was introduced, several proof-of-principle realizations were achieved. Ref. [490] reported a demonstration of MDI-QKD over more than 80 km of spooled fiber as well as in inter-city fiber links. A demonstration using polarization qubits over two optical fiber links of 8.5 km each employed a full-polarization control system to stabilize and control the polarization drift in the fibers [491]. Moreover, the feasibility of MDI-QKD with polarization encoding was demonstrated in 10 km of telecom fiber using standard off-of-shelf devices [492]. Other sophisticated implementations using decoy-state MDI-QKD have been realized over tens and even hundreds of km of optical fibers [122,123,127]. MDI-QKD Progress has advanced quite rapidly, a summary MDI-QKD in terms of bit rate/distance is shown in Fig. 4(a).

Regarding the actual establishment of metropolitan communication networks based on the security of the MDI-QKD protocol, many advances have already been made, including the construction of a star-type quantum network in a metropolitan area of 200-square-km, which in addition to providing a high transmission bit rate, also proven to be safe against detection attacks [493]. MDI-QKD has been implemented in quantum channels that coexist in the same fiber with classical data channels [494,495].

6.3. Detector-device-independent quantum key distribution

As discussed in the previous section, implementing the MDI-QKD protocol requires the interference of photons from two separate lasers, making its implementation more challenging than conventional QKD schemes. Another issue lies in the finite-key analysis, which demands a relatively large post-processing data block to achieve optimal performance.

To address these challenges, an alternative approach called detector-device-independent QKD (DDI-QKD) has been proposed [496–498]. While DDI-QKD shares a similar conceptual framework with MDI-QKD, it differs in its use of a 'black box' model. In this method, Alice and Bob ensure that their measurement systems do not leak any unwanted information to external sources. This is accomplished, in principle, by replacing the measurement apparatus in Bob's laboratory with a device built by them but not necessarily characterized. Additionally, DDI-QKD replaces the two-photon Bell state measurement (BSM) with a 2-qubit single-photon BSM, eliminating the need for two-photon interference from independent light sources.

An example of such a protocol works as follows: Alice encodes BB84 polarization states in single photons, which she sends to Bob. Bob encodes his information into the spatial degree of freedom of the incoming photons (two modes). This is achieved using a 50:50 beam splitter along with a phase modulator that applies a random phase to each incoming signal. Bob then performs a BSM on the two qubits (polarization, spatial modes) to project each input photon into a Bell state. The remaining steps of the protocol are identical to MDI-QKD.

Despite the anticipated strong performance and partial security proofs, Sajeed et al. [499] demonstrated that the security of DDI-QKD cannot rely on the same principles as MDI-QKD. They demonstrated two key security vulnerabilities. First, DDI-QKD's security is not based on postselected entanglement, and a blinding attack renders its security. Second, Sajeed et al. [499] revealed that DDI-QKD is vulnerable to detector side-channel attacks, as well as other side-channel attacks that exploit imperfections in Bob's receiver. The source of these vulnerabilities seems to stem from Bob's preparation process, which, unlike MDI-QKD, can be influenced by Eve through the signals she sends to Bob.

6.4. Receiver-device-independent QKD

Ioannou et al. introduced another prepare-and-measure SDI-QKD protocol [500], where the sender's device is partially trusted, while the receiver's device is treated as a black box. They called these protocols "receiver-device-independent quantum key distribution (RDI-QKD)". The main assumption in RDI protocols is to bound the pairwise (possibly complex) overlaps between the various states prepared by Alice, denoted as $\gamma_{ij} = \langle \psi_i | \psi_j \rangle$. The states $|\psi_x\rangle$ represent the quantum systems prepared by Alice's devices or, more generally, the states of all systems outside Alice's lab, conditioned on her applying the preparation sequence labeled by x. If Alice's states are mixed, their purifications must also satisfy the overlap bounds. These bounds prevent any side-channel from leaking additional information about x to Eve. No characterization of the receiver's (Bob's) device is required, and no fair-sampling assumption is made. As a result, these protocols are resilient to attacks where Eve controls Bob's device.

Simplest protocol. In the simplest protocol, given a key bit k, Alice prepares one of two possible states by setting $x = k$. using a coherent state $|\alpha\rangle$ with two possible polarization states $|\phi_x\rangle = \cos\frac{\theta}{2}|H\rangle + e^{i\pi x}\sin\frac{\theta}{2}|V\rangle$, she prepares one of the following states $(x = 0, 1)$

$$|\psi_x\rangle = |\alpha\cos\frac{\theta}{2}\rangle_H|\alpha\sin\left(\frac{\theta}{2}\right)e^{i\pi x}\rangle_V. \tag{199}$$

The overlap between two preparation is given by $\langle\psi_1|\psi_0\rangle = e^{-2|\alpha|^2\sin^2\theta}$ and the main assumption is then written as

$$\gamma = \langle\psi_1|\psi_0\rangle \geq C, \tag{200}$$

where C is a parameter chosen by the user.

Bob, then, performs a measurement of the polarization states. For $y = 0$ ($y = 1$), he projects the incoming signal to $|\phi_0^\perp\rangle$ ($|\phi_1^\perp\rangle$). If he gets a click, then the round is conclusive and he outputs $b = 0$, otherwise, the round is inconclusive and he outputs $b = 1$ and the round will be discarded during sifting. In the case of an ideal channel without noise and loss, the following statistics will be observed by Alice and Bob

$$p(b = 0|x, y) = 1 - e^{-|\alpha|^2\sin(\theta)^2\sin(\frac{\pi(x-y)}{2})^2}, \tag{201}$$

which is nonzero only when $x \neq y$. Therefore, the raw key can be constructed after removing the inconclusive rounds, by Bob flipping all his bits.

General case of $n > 2$ different preparations [121]. Consider a given ensemble of states $|\psi_x\rangle_{x=0}^{n-1}$ that Alice can prepare, and that Bob can perform binary measurements $\{B_{0|y}, B_{1|y}\}_{y=0}^{n-1}$ corresponds to projections onto the polarization states orthogonal to the states that Alice prepares. Alice randomly chooses a pair of integers $\mathbf{r} = (r_0, r_1)$ where $0 \leq r_0 \leq r_1 \leq n-1$ and a bit k and sends the state $|\psi\rangle_{x=r_k}$ to Bob, who randomly chooses an integer y ($0 \leq y \leq n-1$) and performs the binary measurement $\{B_{0|y}, B_{1|y}\}$. If the outcome is $b = 1$, the round will be discarded, otherwise $b = 0$. Bob then asks Alice to reveal $\mathbf{r}$. If $y = r_0$ or $y = r_1$ Bob informs Alice that the round is conclusive otherwise it is aborted. The main assumption concerns the complex pairwise overlaps between preparation states, which is encompassed in the Gram matrix G, whose entries are given by $G_{ij} = \langle\psi_i|\psi_j\rangle$.

6.4.1. Security analysis

Eve's information about the secret bit k is bounded by assuming that the Gram matrix G of the set of encoding states is fully characterized and that the probabilities $p(b|x, y)$ are perfectly estimated by Alice and Bob. There is no other restriction on the protocol, no bound on the dimension, and neither any characterization on the prepared states, transmission channel, or measurement device. To attack the protocol, Eve can correlate herself to the state Alice sent and design Bob's measurement. Moreover, Eve can benefit from having a quantum memory. By denoting p_{succ} as the probability that a round is not discarded, the asymptotic key rate is lower bounded by using the Devetak–Winter key rate formula and gives

$$r^{\text{RDI}} \geq [H(k|\text{Eve, succ}) - H(k|\text{Bob, succ})]p(\text{succ}) \geq [-\log_2(p_g(e = k|\text{succ})) - h(Q)]p(\text{succ}).$$

Here the second inequality comes from the fact that Bob's entropy can be upper-bounded as $H(k|\text{Bob, succ}) \leq h(Q)$ and Eve's conditional entropy can be lower-bounded by conditional min-entropy $H_{\min}(k|\text{Eve, succ}) = -\log_2(p_g(e = k|\text{succ}))$. $p_g(e = k|\text{succ})$ is the maximal probability that Eve guess the bit k correctly, and is the only quantity that needs to be upper bounded to give a lower bound on r^{RDI}, since the QBER Q and $p(\text{succ})$ can be extracted from the observed statistics $p(b|x, y)$. The guessing probability $p_g(e = k|\text{succ}) = \frac{p(e=k,\text{succ})}{p(\text{succ})}$ then can be upper bound by an upper bound on $p(e = k, \text{succ})$. In [121], it is shown that by using SDP an upper bound on $p(e = x, \text{succ})$ can be obtained.

SDP method for upper bounding $p(e = x, \text{succ})$. Let us define the set $\{S_i\}_{i=0}^{s-1}$ where its elements are monomials of the operators $B_{b|y}$ and $E_{e|\mu}$ (Eve's measurements). The ns×ns moment matrix Γ then can be defined as

$$\Gamma = \sum_{i,j=0}^{n-1}\Gamma_{xx'} \otimes |e_x\rangle\langle e_x| \tag{202}$$

with the sub-blocks $\Gamma_{xx'}$ defined as $\Gamma_{xx'} = \sum_{i,j=0}^{s-1}\otimes|\hat{e}_j\rangle\langle\hat{e}_j|$ where $\{|e_x\rangle\}_{x=0}^{n-1}$ ($\{|\hat{e}_i\rangle\}_{i=0}^{s-1}$) is an orthonormal basis on $\mathbb{R}^n$ ($\mathbb{R}^s$). If we define $\Gamma_{xx'}^{ST} := \langle\psi_x|S^\dagger T|\psi_{x'}'\rangle$ ($S, T \in \mathbb{S}$), then the SDP upper bounding $p(e = x, \text{succ})$ is given by

$$\max_\Gamma \frac{1}{(n-1)n^2} \sum_{r=0}^{\binom{n}{2}} \sum_{k=0}^{1} \sum_{y=0}^{n-1} \Gamma_{r_k r_k}^{B_{0|y}E_{r_k|r}}(\delta_{y,r_0} + \delta_{y,r_1}),$$

such that

$$\Gamma_{xx'}^{\mathbb{I}\mathbb{I}} = \langle\psi_x|\psi_{x'}\rangle = \gamma_{xx'} \forall x, x', \tag{203}$$

$$\Gamma_{xx}^{\mathbb{I}B_{b|y}} = p(b|x, y), \forall b, x, y$$
$$\mathrm{tr}(\Gamma_{xx'}F_k) = f_k, k = 0, \ldots,$$
$$\Gamma \geq 0$$

The first condition is the overlap constraint between the sets of states. The second equation ensures that the moment matrix Γ is compatible with the observed correlation $p(b|x, y)$. The matrices F_k and the coefficients f_k are Hermitian and complex, respectively, and are defined to satisfy the constraints on the measurement operators for Bob and Eve. These constraints include positivity, completeness, commutativity $[M_{b|y}, E_{e|y}] = 0$, and the requirement that both $M_{b|y}$ and $E_{e|y}$ are projectors.

Case study: Ideal qubit protocol. As an example [121], consider the case where Alice prepares states from a set of n single-qubit states $\{|\psi_x\rangle\}_{x=0}^{n-1}$, where

$$|\psi_x\rangle = \cos\left(\frac{\theta}{2}\right)|0\rangle + e^{i\frac{\pi x}{n}}\sin\left(\frac{\theta}{2}\right)|1\rangle,$$

for a given θ. In the presence of loss and noise, the Gram matrix and the probability distribution for this set of states are given by:

$$G_{ij} = \cos^2\left(\frac{\theta}{2}\right) + e^{i\frac{2\pi(i-j)}{n}}\sin^2\left(\frac{\theta}{2}\right),$$

and

$$p(b = 0|x, y) = \zeta\left(\frac{\lambda}{2} + (1 - \lambda)\sin^2(\theta)\sin^2\left(\frac{\pi(x - y)}{n}\right)\right),$$

where $\lambda \in [0, 1]$ is the noise parameter, modeled as a depolarizing channel, and $\zeta \in (0, 1]$ represents the loss, modeled by a binary erasure channel with erasure probability $1 - \zeta$.

By optimizing over θ, for different QBERs (Q) and values of n, the raw key rate as a function of the transmission ζ can be derived. In their calculations, Ioannou et al. [121] demonstrated that the lower bound of the key rate asymptotically approaches zero as $\zeta \to \frac{1}{n}$. This is considered optimal because at $\zeta \to \frac{1}{n}$, Eve can compromise security by intercepting the states sent by Alice and manipulating Bob's detector based on her outcome and Bob's input. Therefore, for any prepare-and-measure protocol, the key rate becomes zero for $\zeta \leq \frac{1}{n}$. Furthermore, the proposed protocol surpasses the B92 protocol (a specific case of the proposed protocol with $n = 2$ and fixed $\theta = \frac{\pi}{4}$) in terms of both transmission efficiency and noise tolerance. Similarly, BB84 is also outperformed by a qubit-based RDI protocol using three states.

6.5. One-sided device-independent quantum key distribution

6.5.1. Standard 1SDI-QKD

Another approach to relaxing technical requirements of DI-QKD systems is to consider an asymmetric scenario, known as one-sided DI-QKD (1SDI-QKD), in which one party trusts their device and the other does not. Note that this situation might describe QKD between a user who is technologically sophisticated enough characterize and trust their equipment (such as a bank or government agency), with a client with untrusted devices.

The protocol first introduced by Branciard et al. [119] is as follows: Alice and Bob each receive part of an entangled photon pair. Alice has two binary measurement settings A_1 and A_2. Since she does not trust her measurement apparatus, it is treated as as a block box with a single bit input to choose between settings. On the other side, Bob has two fully trustful projective measurements B_1 and B_2 in some qubit subspaces. Alice and Bob might not always detect their photons due to channel losses or inefficient detectors. Alice and Bob will to try to extract a secret key from the outcomes of A_1 and B_1 and can estimate the information of a possible Adversary (Eve) using the results of A_2 and B_2. Since Bob fully trusts his measurement device, he can safely discard the events where he does not detect a photon, since Eve cannot gain any information from these. Alice, on the other hand, cannot, and must include no-click events in her analysis. For the security proof and key rate in this protocol, let us denote by $\boldsymbol{A_i} = (\boldsymbol{A_i^{\mathrm{ps}}}, \boldsymbol{A_i^{\mathrm{dis}}})$ and $\boldsymbol{B_i} = (\boldsymbol{B_i^{\mathrm{ps}}}, \boldsymbol{B_i^{\mathrm{dis}}})$ the strings of classical bits of Alice and Bob get from the recording of their measurements results. Here $\boldsymbol{A_i^{\mathrm{ps}}}$ and $\boldsymbol{B_i^{\mathrm{ps}}}$ applied for actual detection (ps for post selection) and $\boldsymbol{A_i^{\mathrm{dis}}}$ and $\boldsymbol{B_i^{\mathrm{dis}}}$ are for no detection and they will be discarded for the key extraction. Then from n-bit strings of $\boldsymbol{A_1^{\mathrm{ps}}}$ and $\boldsymbol{B_1^{\mathrm{ps}}}$ on which Eve can have some information, Alice and Bob can extract a secret key of length l [501] where

$$l \approx H_{\min}^\epsilon(\boldsymbol{B_1}|E) - nh(Q_1^{\mathrm{ps}}), \tag{204}$$

here Q_1^{ps} is the bit error rate between $\boldsymbol{A_1^{\mathrm{ps}}}$ and $\boldsymbol{B_1^{\mathrm{ps}}}$. By bounding $H_{\min}^\epsilon(\boldsymbol{B_1}|E)$ using the chain rule and the data-processing inequality for smooth min-entropy, the following bound on the secret key rate can be obtained

$$r \geq \eta_A[1 - h(Q_1^{\mathrm{ps}})] - h(Q_2) - (1 - q), \tag{205}$$

where q is a measure of how distinct Bob's two measurements are. Q_2 is the bit error rate between A_2 and B_2.

In analogy to the connection between DI-QKD and the violation of Bell inequalities, here the security of this one-sided DI-QKD is related to the demonstration of quantum steering. That is, $\eta_A[1-h(Q_1^{\text{ps}})]-h(Q_2)-(1-q) \leq 0$ can be understood as an EPR-steering inequality [502–504]. Because closing the detection loophole in a steering experiment is easier than in a Bell test, 1SDI-QKD is more feasible to realize experimentally. For example, consider a typical experimental setup, where a source sends maximally entangled two-qubit states to Alice and Bob through a depolarizing channel with visibility v, with measurement settings $A_1 = B_1 = \sigma_z$ and $A_2 = B_2 = \sigma_x$. Then, for perfect visibility $v = 1$, a positive secret key can be obtained when Alice's detection efficiency $\eta_A > 65.9\%$, which is much lower compared to those in DI-QKD. As a comparison, for the cases where Alice and Bob have the same detection efficiency, to close the detection loophole in DI-QKD requires $\eta > 94.6\%$ are needed ($\eta > 91.1\%$ for post-selected data).

As is the case for most conventional proofs, the security for the above 1SDI-QKD protocol provided for the asymptotic limit of infinitely long keys. In practical implementations, the number of signals used for establishing a secure key is finite. For the case of 1SDI-QKD, finite key analysis was addressed by Wang et al. [505] based on the asymptotic of 1SDI-QKD presented above. They present the secure key rate of 1SDI-QKD with finite resources by employing the smooth min-entropy and smooth max-entropy [239,506]:

$$l \approx H_{\min}^{\epsilon'}(Y_1^{\text{ps}}|E) - H_{\max}^{\epsilon'}(Y_1^{\text{ps}}|X_1^{\text{ps}}). \tag{206}$$

Using the uncertainty relation for smooth entropies [507] and the upper bound for smooth-max entropy [508], the following bound for the key rate will be obtained

$$r \geq \eta_A P_Z^2[1 - h(Q_1^{\text{ps}})] - P_Z^2[1 - q + h(Q_2 + \mu)] - \frac{1}{N} \log_2 \frac{2}{\epsilon_{\text{cor}}}, \tag{207}$$

where P_Z is the probability that Alice (and also Bob) chooses the measurement in Z basis and $\mu = \sqrt{\frac{n+k}{nk} \cdot \frac{k+1}{k} \cdot \ln \frac{2}{\epsilon_{\text{sec}}}}$, with n and k being the length of the raw key and the length of the bit string used for parameter estimation respectively. ϵ_{cor} is the security parameter bounding the possibility that Alice and Bob have different outputs.

For comparison purposes the simulation results were done in [505] and show that the sifted key rate is consistently lower than that predicted by the asymptotic case, particularly when considering finite-key analysis. Furthermore, the outcomes reveal that the relative difference between the asymptotic and non-asymptotic cases ($\delta = \frac{r_\infty - r_N}{r_\infty}$) gradually diminishes as the detection efficiency η_A increases. Notably, the investigation also pinpoints the minimum number of exchanged quantum signals required for achieving efficient detection efficiencies. The results illustrate the potential for a non-zero final secret key rate, approaching 9×10^6, specifically when η_A reaches 0.67. This underscores the viability of attaining substantial secret key rates even in scenarios involving moderate detection efficiency.

The protocols mentioned above are the QKD schemes that encode a discrete variable (DV) key in a two-dimensional space, typically encoded into a pair of entangled photons. Considerable attention has also been devoted to schemes that instead utilize the quadratures of the optical field, in which one has access to deterministic, high-efficiency broadband source and detectors. In this case, the secret key is now a continuous variable (CV) that is encoded in states living in an infinite-dimensional Hilbert space. This kind of protocol has some advantages over the discrete variable counterpart. The very important ones are that in the CV case, detection-loophole-free tests have been experimentally feasible for over 30 years [215] and very strong violations of steering inequalities have been demonstrated. These benefits provide enough motivation for studying the possible one-sided device-independent CV QKD (1SDI-CV-QKD). This was done by Walk et al. [509] where they studied Gaussian CV-QKD protocols from the perspective of 1SDI-QKD against collective attacks, and showed that 1SDI-CV-QKD is possible even with coherent states. The existence of non-zero key rates was connected to the steering parameters for Gaussian states. An experimental implementation achieved positive secret keys under a lossy channel for both entanglement based and coherent state protocols. A version of a 1SDI-CV-QKD protocol that generates a finite and composable key and is secured against coherent attacks was reported by Gehring et al. [126]. The experiment used two continuous wave optical light fields whose amplitude and phase quadrature amplitude modulations were mutually entangled, and CV equivalent of the BBM92 protocol for discrete variables was implemented. This scheme is secure against memory-free attacks performed on Bob's untrusted detector, that is, attacks that are independent of Bob's previous measurement, and secure against Trojan-horse attacks on the source that usually threaten electro-optical modulators commonly used in Gaussian-modulation QKD protocols. A hybrid scheme where Alice uses a Gaussian-modulated coherent state while Bob uses a two-mode squeezed state was studied in [510].

A 1SDI-QKD protocol using high-dimensional time–energy entanglement was proposed in Ref. [511]. The security of this scheme was established by applying the entropic uncertainty relation introduced in [512] against coherent attacks. Their numerical results demonstrate that the protocol achieves higher bit rates per two-photon coincidence count while requiring lower detection efficiencies compared to the original 1SDI-QKD protocol (achieving a key rate with $\eta_A = 50\%$). This improvement stems from the limitation imposed by photon information efficiency in the original 1SDI-QKD protocol, which restricted the key generation rate to no more than 1 bit per coincidence. Encoding information in high-dimensional photonic degrees of freedom proves to be an efficient approach for overcoming this limitation.

6.5.2. Generalized 1SDI-QKD and quantum secret sharing

In 2017, Kogias et al. [513] tackled the problem by considering the protocol as a generalized 1SDI-QKD problem for a continuous-variable version of QSS [305]. They started with the simplest case involving three parties, Alice, Bob, and Charlie. Alice is fully trusted and shares the secret using a three-mode continuous-variable entangled-state. She keeps one mode and sends the other modes to the untrusted players, Bob and Charlie, through individual unknown quantum channels. In this way, the protocol can be seen as a generalized 1SDI-QKD protocol from Alice (trusted part) to Bob and Charlie as untrusted players. Alice is assumed to perform two homodyne measurements of two canonically conjugate quadratures $\hat{x}$ and $\hat{p}$, and her goal is to establish a unique secret key, not with Bob's or Charlie's individual measurements (as in standard two-party QKD), but with a collective (nonlocal) degree of freedom for Bob and Charlie that strongly correlates with one of Alice's quadratures (X_A for example). Alice sends a sufficient number of states to the players and in each run, they randomly choose measurements and measure their parts, and collect the outcomes X_i and P_i. In the next step, all parties announce their measurements and keep the data originating from correlated measurements, using it for extracting a secret key.

The final bound on the asymptotic key rate to provide unconditional security against general attacks of an eavesdropper, and against arbitrary (individual) cheating methods of both Bob and Charlie, which include the announcement of faked measurements and general attacks of Bob on Charlie's system and of Charlie on Bob's system, can be written as

$$r \geq -\log(e\sqrt{V_{X_A|\bar{X}} \max\{V_{P_A|P_C}, V_{P_A|P_B}\}}), \tag{208}$$

where

$$V_{X_A|\bar{X}} = \int d\bar{X} p(\bar{X})(\langle X_A^2 \rangle_{\bar{X}} - \langle X_A \rangle_{\bar{X}}^2), \tag{209}$$

and $\bar{X}$ is Bob and Charlie's collective degree of freedom that strongly correlated with Alice's quadrature X_A.

While the resource behind the standard 1SDI-QKD is known to be (bipartite) steering, one could suspect a similar connection with the case of multi-player QSS, which is indeed the case for the case of Gaussian measurements [514]. For a generic Gaussian $(n + m)$-mode state ρ_{AB} of a bipartite system, composed of a subsystem A (for Alice) of n modes and a subsystem B (for Bob) of m modes, one can define a steering measure as [515]

$$\mathcal{G}^{A \to B}(\sigma_{AB}) = \max\left\{0, \frac{1}{2}\ln\frac{\det A}{\det \sigma_{AB}}\right\} = \max\{0, S(A) - S(\sigma_{AB})\}, \tag{210}$$

where $\sigma_{AB} = \begin{bmatrix} A & C \\ C^{\mathsf{T}} & B \end{bmatrix}$ is the covariance matrix of the state ρ_{AB}.[20] This measure has an operational meaning in 1SDI-QKD. For a two-mode entangled Gaussian state with covariance matrix σ_{AB}, the key rate can be readily expressed in terms of the $B \to A$ Gaussian steerability of σ_{AB} [509], yielding

$$r \geq \max\{0, \mathcal{G}^{B \to A} + \ln 2 - 1\}. \tag{211}$$

The Gaussian steering measure $\mathcal{G}$ is monogamous and then satisfies a Coffman–Kundu–Wootters type monogamy inequality [514], in direct analogy with entanglement [516]. For an m-mode Gaussian state with covariance matrix $\sigma_{A_1,\dots,A_m}$, the following inequalities hold for each party A_j composed of a single mode ($n_j = 1$, $1 \leq j \leq m$):

$$\begin{aligned}
\mathcal{G}^{(A_1,\dots,A_{k-1},A_{k+1},\dots,A_m) \to A_k}(\sigma_{A_1,\dots,A_m}) &\quad -\sum_{j \neq k} \mathcal{G}^{A_j \to A_k}(\sigma_{A_1,\dots,A_m}) \geq 0, \\
\mathcal{G}^{A_k \to (A_1,\dots,A_{k-1},A_{k+1},\dots,A_m)}(\sigma_{A_1,\dots,A_m}) &\quad -\sum_{j \neq k} \mathcal{G}^{A_k \to A_j}(\sigma_{A_1,\dots,A_m}) \geq 0.
\end{aligned} \tag{212}$$

For the tripartite case, this becomes

$$\begin{aligned}
\mathcal{G}^{(AB) \to C}(\sigma_{ABC}) - \mathcal{G}^{A \to C}(\sigma_{ABC}) - \mathcal{G}^{B \to C}(\sigma_{ABC}) &\geq 0, \\
\mathcal{G}^{C \to (AB)}(\sigma_{ABC}) - \mathcal{G}^{C \to A}(\sigma_{ABC}) - \mathcal{G}^{C \to B}(\sigma_{ABC}) &\geq 0.
\end{aligned} \tag{213}$$

In analogy with the case of entanglement, residual Gaussian steering (RGS) can be defined by calculating the residuals from (213) and minimization over all mode permutations. Therefore, in the case of a pure three-mode Gaussian state, the RGS can be defined as

$$\mathcal{G}^{A:B:C}(\sigma_{ABC}^{\text{pure}}) = \min_{\langle i,j,k \rangle}\{\mathcal{G}^{(jk) \to i} - \mathcal{G}^{j \to i} - \mathcal{G}^{k \to i}\}. \tag{214}$$

This quantity is a monotone under Gaussian local operations and classical communication, such that a nonzero value of the RGS certifies genuine tripartite steering [517]. Therefore, it can be regarded as a meaningful quantitative indicator

---

[20] Any Gaussian state ρ_{AB} is fully specified, up to local displacements, by its covariance matrix σ_{AB} with the elements $\sigma_{ij} = \text{Tr}[\{\hat{R}_i, \hat{R}_j\}\rho_{AB}]$ and $\hat{R} = (\hat{x}_1^A, \hat{p}_1^A, \dots, \hat{x}_n^A, \hat{p}_n^A, \hat{x}_1^B, \hat{p}_1^B, \dots, \hat{x}_m^B, \hat{p}_m^B)^{\mathsf{T}}$

of genuine tripartite steering for pure three-mode Gaussian states under Gaussian measurements. Returning to the key rate of the QSS protocol (208), the mode-invariant QSS key rate bound $K_{\text{full}}^{A:B:C}$ that takes into account eavesdropping and potential dishonesty of the players can be obtained by minimizing the right-hand side of (208) over permutations of A, B, and C. It was found that it admits the exact linear upper and lower bounds as a function of the RGS (214):

$$\frac{\mathcal{G}^{A:B:C}(\sigma_{ABC}^{\text{pure}})}{2} - \ln\frac{e}{2} \leq K_{\text{full}}^{A:B:C}(\sigma_{ABC}^{\text{pure}}) \leq \mathcal{G}^{A:B:C}(\sigma_{ABC}^{\text{pure}}) - \ln\frac{e}{2}. \tag{215}$$

Thus, partial DI QSS yields a direct operational interpretation for the RGS in terms of the guaranteed key rate of the protocol.

EPR steering is a necessary requirement for non-zero key rates in all of the protocols mentioned above. Therefore, it is essential to have a procedure for generating EPR steering between two or more distant parties. Xiang et al. [518] designed a protocol that allows the distribution of one-way Gaussian steering. This can be subsequently employed for 1SDI-QKD and also for three-user scenarios to distribute richer steerability properties, including one-to-multimode steering and collective steering, which can be utilized for 1SDI quantum secret sharing. Since all of their protocols can be implemented with squeezed states, beam splitters, and displacements, they can be readily realized experimentally. A related experiment was done by Wang et al. [519] which experimentally demonstrate the deterministic distribution of Gaussian entanglement and steering with separable ancillary states both in two-user and multi-user scenarios by preparing independent squeezed states and applying classical displacements on them, which makes initial states fully separable. In a later development in 2023, Lv et al. [520] demonstrated that a 2-qubit entangled state can consistently produce steering through sequential and independent pairs of observers, given that the initial pair shares either a pure entangled state or a specific category of mixed entangled states.

6.5.3. Experiments: One-sided device independent QKD

1SDI-QKD is rigorously based upon the loophole-free observation of EPR-steering (also known as quantum steering) [502,503]. As EPR-steering is below Bell nonlocality in the hierarchy of correlations, 1SDI-QKD provides a security paradigm that is less robust than that of full-DI QKD. However, it is much easier to close the detection loophole for EPR-steering than in Bell non-locality. As such 1SDI-QKD can be realized with much lower detection efficiencies. In fact, EPR-steering can be observed for arbitrarily large losses in the DV context, provided that a sufficiently large number of measurements can be realized on a bipartite state with sufficient entanglement [220,521]. 1SDI-QKD has also been implemented in continuous variable systems, with the advantage that Gaussian states and measurements can be used [522,523].

7. Towards future a DI-QKD network: requirements, challenges and solutions

DI-QKD has the appeal that it can help resolve security risks associated to implementation issues, as it aims to provide information theoretic security with minimum physical assumptions and uncharacterized hardware, thus reducing or eliminating many of the side-channels and security concerns in real-world deployment. However, DI-QKD requires satisfactory demonstration of Bell non-locality over long distances, and as such introduces demanding technical requirements, in particular related to the distance limitations (signal loss requires advanced quantum technology such as quantum repeaters) and high efficiency (high-quality detectors, sources, devices) required to achieve reasonable key rates.

In this section we discuss the current outlook towards real-world implementation of DI-QKD, presenting the first set of DI-QKD experiments and additional promising experimental platforms, the current technical challenges, and possible solutions. In Section 7.5, we discuss the efforts towards real-world deployment of QKD in general, including efforts towards standardization, interoperability, and integration into cybersecurity and network architecture, since future implementation of DI-QKD will most likely benefit from most of this groundwork. When possible, we mention MDI-QKD benchmarks, and highlight specific or unique challenges that DI-QKD will likely encounter on the road to real-world deployment.

7.1. The first DI-QKD experiments

In July 2022, three independent research groups (one based in the UK [54], one in Germany [56], and one in China [55]) successfully implemented DI-QKD in three different platforms. The first successful photonic-based experiment [55] demonstrated DI-QKD (against collective attack) over fiber lengths of $d = 20{,}100$ and 220 m and verified that the measured correlations between the entangled photons were strong enough to guarantee a positive secret key rate. Optimized high-efficiency entangled photon source and single-photon detectors resulted in a single photon heralding efficiency slightly greater than 87%. To address the locality loophole, the experiment employs a shielding assumption that prohibits unnecessary communications between untrusted devices and a potential adversary. Essentially, it ensures that the information about the input choices and output results of one party remains unknown to the other party and Eve.

Proof-of-principle memory-based experiments reported in Oxford [54] and Munich [56] used entangled strontium ions and entangled rubidium atoms, respectively. Each system has its advantages and disadvantages. However, when

compared to all-photonic implementations, these experiments have the advantage that they can be "event-ready", so that link efficiencies can be partially mitigated. The Oxford-based experiment was the only one of the three to complete the entire DI-QKD protocol, with a generated secret key of 95 kbits between Alice and Bob achieved over about 8 h and with a distance of $d = 2$ m between the two quantum memories. The Munich-based experiment created heralded entanglement between atoms separated by a line of sight distance of $d = 400$ m (700 m of optical fiber). An asymptotic security analysis was performed, and a secret key rate of 0.07 bits per entanglement generation event was obtained from results accumulated over 75 h.

These three landmark experiments demonstrate that experimental DI-QKD is feasible. In addition, they highlight the technical challenges to be face in achieving real-world utility. In the next two sections we discuss some of the fundamental requirements and technical challenges to be faced for the next generation of DI-QKD experiments, and present some of the techniques and proposals meant to address them.

7.2. Bell loopholes in the DI-QKD scenario

Section 2 discussed several of the loopholes in conclusive Bell tests. Most of these loopholes are also present in DI-QKD, with several caveats. The locality loophole, that is, having space-like separation between measurement processes, as discussed in Section 2.4.2, is necessary to rule out LHV theories. However, to guarantee security in DI-QKD we must ensure that the users stations do not leak any information to an adversary Eve, even at sub-luminal velocity. From Eve's point of view it is most likely much easier to install a backdoor that sends information from a user's devices to her station, rather than make them communicate with each other to fake a Bell inequality violation.

Thus, DI-QKD calls for complete isolation of the measurement stations, involving shielding, electromagnetic or otherwise, to avoid broadcasting of any type of signal related to measurement basis choices and outcomes. In addition, whether the quantum systems are photonic or stationary, the users stations are connected by a photonic channel, which in principle opens a backdoor for side-channel attacks using external light sources, as has been exploited for fake Bell violations [168], in QKD [10–15] and QRNGs [524,525]. To isolate the users stations, a switch or shutter mechanism should be used to block the optical channel after the relevant optical signal has passed, and before the measurements are performed. In a recent DI-QKD implementation with trapped ions, this was achieved by shifting the ions out of the focal point of the collection lens, thus decoupling them from the optical link, and also scrambling the quantum state after measurement, so that the state after measurement (and thus the measurement result) could not be determined by a third party probing the ions [54].

Another difference between Bell and DI-QKD scenario lies in the memory loophole (see Section 3.15.). The ability of the devices to remember the inputs and outcomes of the previous rounds to be used in the future has been proved to be of very little consequence for Bell inequalities already in Ref. [526]. For DI-QKD, on the other hand, memory attacks pose a very serious threat [78,240]. While some countermeasures against them are possible, there is no known method of full protection.

The experimental loophole which is of crucial importance for both Bell and DI-QKD scenarios is the detection efficiency loophole, which currently is the main problem in experimental realizations and implementations, as we address in the next section.

7.3. Detection efficiency and channel losses

The issues of detection efficiency and channel losses are intimately related in determining the performance characteristics of a DI-QKD link. In both all-photonic setups and those with stationary qubits, the efficiency in which photons can be detected at a distant measurement station is a critical metric in determining the overall performance characteristics of the system.

The overall detection efficiency of a photon can be expressed as $\eta = \eta_c \eta_\ell \eta_m \eta_d$, where η_c is the coupling efficiency from the source to the optical link (ex: optical fiber), η_ℓ is the transmission efficiency of the optical link, η_m is the efficiency of the measurement device, and η_d is the quantum efficiency of the detector.

The efficiencies η_c, η_m and η_d depend upon specific characteristics of the source, the optical components of the measurement device and detectors. For example, coupling or "collection" losses can range from near zero to several tens of dB in the case of coupling from an optical source into an optical fiber.[21] While bulk optical components such as (polarizing or non-polarizing) beam splitters can present very low losses $\leq$0.5% ($\sim$0.02 dB), fiber-based components can have losses up to a few dB. State-of-the-art commercial superconducting single-photon detectors typically have $\eta_d \leq 0.85$, but efficiencies reaching over 0.95 have been reported [527,528]. These efficiencies do not typically depend upon the propagation distance within the optical channel.

The link efficiency η_ℓ, on the other hand, does depend upon the propagation distance, decaying exponentially with the length ℓ of the channel [429,529,530]. In particular, $\eta_\ell = 10^{-\gamma\ell/10}$, where γ is the attenuation coefficient in dB/distance. Losses in an optical fiber link include contributions from attenuation (typically value $\sim$0.2 dB/km in the telecom band) that accumulate over distance, as well as from fiber splices connecting different sections of fiber. Mechanical splices

---

[21] Here we give efficiency in terms of probability, and losses in terms of dB. For loss L, one has $\eta = 10^{-L/10}$.

Table 8
Summary of relevant DI-QKD parameters and technical characteristics affecting them for both point-to-point photonic setups with SPDC sources, and event-ready setups using stationary qubits. Here η is the overall photonic detection efficiency, ε is the decoherence of photonic quantum systems in the optical link, T_2 is the decoherence time of stationary node qubits, and B is the overall "brightness" (entangled pairs created/sec) of the source.

Setup type	CHSH value	QBER	Raw bit rate	Distance
point-to-point SPDC	η, ε	ε	η, B	η
Event ready	T_2, ε	T_2, ε	η, B	T_2

using barrel connectors typically have losses greater than 0.5 dB/connection, while fusion splicing can give losses less than 0.01 dB/splice in standard single-mode fiber, showing the necessity of dedicated high-quality optical fiber links for DI-QKD. Moreover, networking hardware, such as optical switches, can also present losses of several dB.

Achieving the critical detection efficiency required for DI-QKD (typically $\eta > 80\%$, see Section 3) in an all-photonic setup (such as a single SPDC source) presents significant technical challenges. Even considering $\eta_c = \eta_m = \eta_d = 1$ and that all link loss is due to attenuation, $\eta_\ell = 0.8$ (or about 1 dB loss) corresponds to ~4.85 km of propagation in an optical fiber. Fortunately, "event ready" setups can be used to overcome the probabilistic nature of most sources of entangled particles, as well as low collection efficiency and losses between source and the detection stations. These are schemes in which the presence of the entangled state at the respective detection sites is heralded by a separate detection event [190–192]. While there have been proposals and experiments involving all-photonic event-ready setups, a considerable advantage arises when employing stationary quantum systems such as ions, atoms, quantum dots and NV centers, since these can be measured with efficiency close to unity, making event-ready setups involving entangled stationary qubits one of the most promising path towards useful implementation of DI-QKD. We discuss event-ready sections in further detail in Section 7.4.2. In addition, we note here that there has been theoretical progress in reducing the CDE for DI-QKD, by including pre- and post-processing, as discussed in Section 3.

7.4. High-quality entanglement sources

High-quality sources of entangled quantum systems are a necessary resource for DI-QKD. Quality refers not only to robust violation of detection loophole-free Bell-inequalities, but also a high brightness B (or repetition rate R), as these two characteristics have a direct effect on the key rates obtainable. In addition to the overall detection efficiency discussed in Section 7.3, decoherence in the channel (such as depolarization, dephasing, etc.) will also degrade the quality of entanglement. In the next two subsections, we describe the two principle entanglement sources used for DI-QKD. A summary of the merits of these sources for DI-QKD in terms of the relevant experimental parameters is given in Table 8.

7.4.1. Spontaneous parametric down-conversion sources

A major step in experimental Bell tests was the development of spontaneous parametric down-conversion sources (SPDC) as a source of entangled photon pairs in the 1990's [531,532], which offered much higher count rates than the first generation of experiments based on atomic cascade [198,533]. The most efficient SPDC sources today are based on periodically poled nonlinear crystals in Sagnac interferometers, as shown in Fig. 21. An adequate choice of crystal length and optics produces highly pure entangled polarization states, reaching state fidelities over 99.5%, where the transverse spatial mode of the photons is optimized for coupling into single-mode fibers [55,534,535]. Coupling efficiencies over 95% have been achieved [55]. SPDC is a probabilistic source of photon pairs, and the state fidelities refer to the post-selected state obtained when two photons are registered. The full SPDC output is described by the two-mode squeezed vacuum state

$$|TMSV\rangle = \sum_{n=0}^{\infty} \frac{\bar{n}^{n/2}}{(1+\bar{n})^{(n+1)/2}} |n\rangle_1 \otimes |n\rangle_2, \tag{216}$$

where $\bar{n}$ is mean photon number in each mode 1,2. The ratio of multiple pair events to single pair events is $\bar{n}$, and the probability of a multi-pair event is $P_{n>1} = \bar{n}^2/(\bar{n}+1)^2$. Thus, there is a trade-off between the brightness achievable and the fidelity, since multiple-pair events become non-negligible at high pump beam intensity. Since photons from different pairs are uncorrelated, multiple pair events limit the quality of the two-photon state, especially for pulsed sources [536]. Indeed, it has been shown that the absence of post-selection results in a limited violation of Bell inequalities [537]. The full photon statistics of state (216) have been considered in key rate analysis for DI-QKD [243], where it was shown that unity key rate is impossible, even with perfect detection efficiency. In addition, the authors showed that, by adding artificial noise, the critical detection efficiency can be lowered to 83.2%, even with the multi-photon events of SPDC sources.

SPDC sources have been used for point-to-point DI-QKD [55], and can also be incorporated into event-ready setups using absorptive quantum memories (see next section). The main parameters affecting performance of SPDC sources for point-to-point DI-QKD are the detection efficiency η, the overall brightness B (pairs emitted/time) and the quality of the entangled states reaching the measurement devices, which for simplicity we will describe in terms of a general
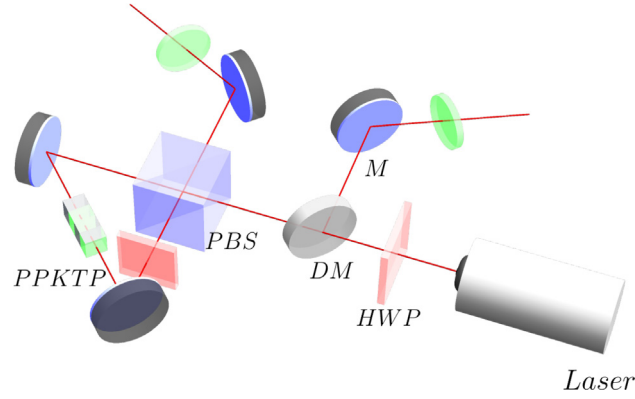
Fig. 21. Sagnac source of entangled photons: A pump laser is directed through a half-wave plate (HWP) to control polarization, followed by a dichroic mirror (DM), which separates the pump beam by reflecting one wavelength while transmitting the other. The beam enters a polarizing beam splitter (PBS), splitting it into orthogonal polarization propagating paths. These paths pass through a periodically poled nonlinear crystal (PPKTP) inside the interferometer loop, generating photon pairs via spontaneous parametric down-conversion (SPDC). Mirrors (M) guide the beams, which recombine at the PBS. A HWP is placed in the reflecting path to adjust de polarization. The entangled photon pairs are separated using dichroic mirrors and sent to high pass filters (green) to be detected at single-photon detectors.
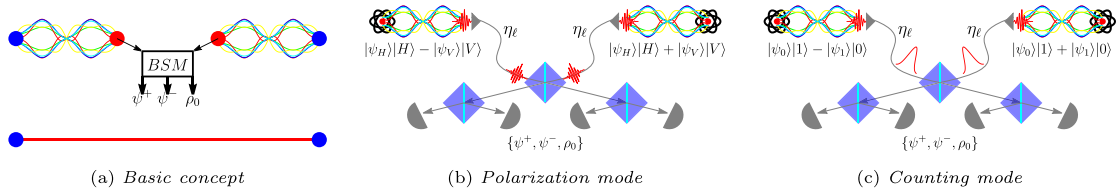
Fig. 22. Event-ready setups — (a) Remote subsystems A and D of two entangled pairs are entangled via a Bell state measurement on their entangled partners (B and C). 22(b) Event ready scheme with stationary qubits and two photon heralds. Stationary qubits are each entangled with the polarization state of a photon, which are are sent to a central station for the two-photon Bell-state measurement (BSM). Joint detection events at pairs of detectors signal preparation of an entangled state $\psi^\pm = |\psi_H\rangle_A|\psi_H\rangle_B \pm |\psi_V\rangle_A|\psi_V\rangle_B$. 22(c) Stationary qubits each emit a photon with probability p. The optical modes are coupled, so that detection of one and only one photon results in an entangled state of the stationary qubits. Here, $\psi^\pm = |\psi_0\rangle_A|\psi_1\rangle_B \pm |\psi_1\rangle_A|\psi_0\rangle_B$.

decoherence channel $\mathcal{E}$, which may incorporate imperfections in the source as well as noise in the optical channel. The detection efficiency η affects the obtainable bit rate of these sources, since not only do both photons need to be detected to establish a key bit, but also through the obtainable loophole-free CHSH violation (see Section 3). Decoherence $\mathcal{E}$ can affect both the QBER as well as the CHSH violation. In some cases, decoherence is due to random unitaries operations (such as phase fluctuations or polarization rotations), which can be monitored and corrected. The source brightness B affects only the raw bit rate in principle, aside from multi-pair events that will result in uncorrelated events, increasing the QBER and lowering the CHSH value.

7.4.2. Heralded or event ready setups

Two recent DI-QKD experiments used entanglement sources that are "event-ready" [54,56]. These sources use entanglement swapping to herald the creation of a remote entangled pair [190–192], as illustrated in Fig. 22(a). While entanglement swapping can be used to create all-photonic event-ready entanglement sources [538–542], the near-unity detection efficiencies achievable with stationary quantum systems such as ions, atoms, quantum dots or NV centers, and the possibility to use them as quantum memory, make these systems most attractive for DI-QKD and quantum networks as a whole. For generality, let us refer to these stationary systems as "nodes". Through the application of external fields, the node qubit can be entangled with a flying qubit, in the form of emission of an optical pulse that can be coupled into an optical channel (fibers). When the pulses emitted from two nodes are combined at a beam splitter, a Bell state measurement (BSM) can be realized resulting in an entangled state of the two nodes A and B. A BSM with 50% efficiency can be realized with linear optics (see Section 6.2.1 and Fig. 20), where classical communication from the BSM station to A, B is required for heralding. Optical decoherence $\mathcal{E}$ in the link, such as phase or polarization fluctuations, can prohibit the creation of high-quality entanglement. If these two nodes are already the end points of the quantum channel, they can be measured after successful node-photon entanglement, and the final results post-selected upon a successful BSM [543]. However, the critical advantage to the node systems is in storing entanglement in quantum memories to be used in repeater protocols [544]. Once created, the entangled state begins to deteriorate due to a number of possible decoherence

processes. The quality of the memory can be quantified by the coherence time T_2, which is the time during which phase coherence of the quantum state can be maintained. When the goal is heralding an entangled pair of nodes, T_2 also determines the maximum separation distance L, since the coherence must be maintained long enough for the BSM station to communicate to the nodes, and subsequent measurements at A and B to occur. That is, $L \ll vT_2$, where v is the velocity of light in the optical link. A coherence time of 10 ms has been recently observed for Rubidium atoms, allowing for a link distance over 100 km [545].

Thus, developing good quantum memories, resulting in increased T_2, is crucial for increasing separation distance between nodes, while maintaining the high CHSH violation and QBER required for DI-QKD. Entangled quantum memories will also play a crucial role in quantum repeaters, required for quantum networking and establishing long-distance entanglement (see Ref. [544] for a comparison of decoherence times of candidate platforms and Ref. [546] for a review of quantum networks with neutral atoms).

Event-ready setups can be divided into two main categories: those that use two photons as heralds and those with a single-photon herald. A double-herald setup requires one photon from each node A and B to arrive at the BSM station (see Fig. 22(b)). The BSM relies on two-photon interference, which is inherently robust to phase instability [547] (low optical decoherence), but is less efficient, as it requires the emission, arrival and detection of two photons. Thus, if the overall efficiency to detect a single photon at the BSM is η, the double-herald setup has efficiency $\sim \eta^2$. Event-ready entangled states have been generated over tens of km of optical fibers with atomic ensembles [548] and single atoms [549].

To improve efficiency, single-photon event-ready setups can be employed. These again require entanglement between the node system and a photonic system, however in this case the state is of the form $|\psi_0\rangle|1\rangle \pm |\psi_1\rangle|0\rangle$, where $|\psi_j\rangle$ are states of the node system, and $|n\rangle$ are n-photon Fock states. This scheme has the advantage in that the relevant events are those where only one of the nodes emits a photon. When the two optical channels are combined at a beam splitter, so that one cannot determine which node emitted the photon, a detection in either output results in an entangled state at A and B (see Fig. 22(c)). Using single-photon events increases the event rate (efficiency $\sim \eta$), but requires optical phase stability to attain high-quality entanglement [550–554].

Event-ready schemes are probabilistic, and for heralding and storing entanglement, the generation attempts can only be retried after a time interval that permits two-way communication between the devices and the BSM setup, creating a balance between distance, node decoherence and generation rate. If the distance is too large, then decoherence sets in at the node qubits before successful heralding can be confirmed. Several important figures of merit can be considered. In addition to the fidelity of the state produced, there is the entanglement generation rate, given by $r_{ent} = p_{ent} \times R$, where p_{ent} is the probability that entanglement attempt is successful, and R is the attempt (repetition) rate of the protocol. The probability p_{ent} is determined by the emission probability of the emitter(s), optical transmission and collection losses, and losses due to the probabilistic nature of the BSM. The ratio between r_{ent} and the decoherence rate r_{dec} is known as the "link efficiency" $\eta_{link} = r_{ent}/r_{dec}$ [551]. When η_{link} is on the order of unity or better, then entanglement can be created faster than it is destroyed, which can be used to create entangled nodes deterministically. This was achieved in Ref. [551] by delivering a separable state in the cases when entanglement generation fails. More specifically, entanglement creation was attempted repeatedly, and when entanglement was heralded successfully, it was stored for use at the end of the time window. If all attempts failed, then a separable state was delivered at the end of the time window. This results in a state of the form $\rho_{det} = p_{success}\rho_{success} + p_{fail}\rho_{fail}$. If ρ_{det} has a fidelity greater than 1/2 with a maximally entangled state (for 2×2 systems), then the system delivers entanglement deterministically at the given time intervals.

Event-ready schemes can be used to eliminate the importance of the optical link inefficiency in DI-QKD, but the entanglement generation rate diminishes exponentially with distance due to the attenuation during light propagation to the BSM. Moreover, most quantum memories emit photons in the visible or near-IR regime, where attenuation can be 1–2 orders of magnitude larger than the telecom bands. A solution to this problem is through quantum frequency conversion to the telecom window using difference-frequency conversion with an intense pump pulse [555,556], which has been used to establish entanglement across distances of tens of kilometers for spin systems [543] and atomic ensembles [548,549,557].

Nodes consisting of absorptive quantum memories [558,559], can be entangled in a similar scheme using entangled photons from SPDC. Here each node consists of a memory that is coupled to an SPDC source, so that a single photon can be absorbed, while the other photon is sent to the BSM station. Similar to the single-photon event-ready schemes, if one cannot determine which node produced the photon detected at the BSM, the result is a pair of entangled nodes. In comparison to single-qubit nodes discussed above, here the non-degenerate frequencies of the SPDC photons can be tuned such that one photon is produced at the required frequency for level transition in the memory, and the other at telecom wavelengths for optimal transmission in the optical link to the BSM.

Finally, we note that several direct entanglement generation schemes of stationary nodes have been demonstrated. In Ref. [557], entanglement between two Rb atomic memories separated by 12.5 km was generated by sending a single photon emitted from one memory to be absorbed by the other. Here, atom–photon entanglement was generated in the first memory node between an atom and a photon at 795 nm, which was frequency converted to 1342 nm for transmission in the optical fibers. It was sent to the second node, where it was converted back to 795 nm using sum-frequency generation, and stored in the second memory. A second experiment [560] produced entangled photons from SPDC, stored the state of one of them in a single-ion quantum memory, while the other was sent to a remote detection station via a 14 km deployed urban fiber link.

An all-optical approach for an event-ready setup is through qubit amplifiers, several of which have been proposed [561–564], and are based on a previous proposal for probabilistic noiseless amplification for quantum optical signals [565].

Based on quantum teleportation, these qubit amplifiers can not only act as a herald of an incoming signal but also introduce an optical gain on the desired optical mode. This can reduce or eliminate the effects of transmission losses, but also increases technical demands due to the need for ancilla photons or photon pairs on demand, which must be coupled and detected efficiently with the linear optical measurement device. A recent finite-key analysis analysis shows that detection efficiencies greater than 96.5% are required [566] to achieve a positive key rate with 39 dB of overall transmission loss (about 195 km distance if only fiber attenuation is considered).

Many types of encoding and protocols can be used to produce photon-mediated entanglement for quantum networking (for details see a recent tutorial [567]). To realize long-distance DI-QKD, it will be crucial to realize quantum protocols through quantum networks of different physical types. In this direction, a quantum network stack has been defined [568] and realized [569], in analogy with classical networking models such the Open Systems Interconnection (OSI).

Despite impressive progress in "event-ready" entanglement generation using solid-state and atomic qubits, and the realization of proof-of-principle DI-QKD with these setups [54,56], there still remains a substantial gap between the current state of the art of these systems and the realization of a practical (even short-haul) DI-QKD system. To date, the entanglement generation rates prohibit realization of DI-QKD over larger distances, where the losses in optical fiber become critical. Moreover, there is a tradeoff between state fidelity and entanglement generation rate [567]. Multi-photon events can be produced during the production of the node qubit/photonic qubit entanglement. This requires lower excitation strength or filtering mechanisms [56], which reduces p_{ent}. The photonic interference in the BSM requires spatial, spectral and temporal mode matching, which also requires filtering and leads to losses, lowering p_{ent}. Recent experiments have reported $p_{ent} \sim 10^{-4}-10^{-6}$ [54,56,543,567]. Thus, a repetition rate R of a few MHz would lead to a few hundred events per second in the best case scenario. Thus, considerable technical improvements are still necessary for DI-QKD to reach reasonable key rates over useful distances. One approach to improve these numbers might be through multiplexing of event-ready sources.

7.4.3. Link relays

The transmission losses in optical fibers is a limiting factor for all quantum networking protocols, and limits point-to-point links to a few hundred kilometers in length. As is well known, the no-cloning theorem prevents quantum information from being copied deterministically, so classical optical amplification techniques cannot be used in the quantum regime. Several solutions exist to overcome this limitation.

Current fiber-based QKD systems over several hundred kilometers use trusted classical relays to extend transmission length [570]. Conceptually, these trusted relays consist of hardware security modules where the keys from the two neighboring links are stored confidentially. These keys (at all connecting relay points) are then post-processed,[22] resulting in a shared key between the two endpoints. However, DI-QKD is not possible in a trusted relay infrastructure, since entanglement cannot be shared between the two end points.

To overcome the need for trusted classical hardware devices, quantum relays consisting of quantum repeaters [544,571] are required. Many of the same event ready setups described above can be used to build quantum repeaters, which employ multiple stages of entanglement swapping between intermediate nodes to construct a long-distance entangled state between edge nodes. Since efficient entanglement preparation and swapping are typically probabilistic processes, quantum memory devices are needed to store quantum information from one link while swapping is performed on others. The development of robust quantum memory is one of the principle challenges in creating large-scale quantum networks for DI-QKD and other applications. For a review of recent progress on quantum memories and repeaters, see Refs. [544,546].

7.5. Integration of QKD into cybersecurity infrastructure

Significant advancements have been made worldwide in the proof-of-concept implementation of QKD networks in real-world scenarios, and their integration into cybersecurity infrastructure. Of critical importance was to demonstrate how QKD, which establishes a shared key between users in a point-to-point configuration, can be employed within the network architectures used in modern communications. As early as 2002–2006 the DARPA network demonstrated a multi-node QKD network with optical switching, connecting fiber and free-space links using weak coherent pulses and also entangled photons [572]. The issues of routing, trusted relays, key management and integration into communication protocols such as IPSec were also addressed for the first time. The SECOQC network operated from 2004–2008 in and around Vienna, Austria [573], and included weak coherent pulse, entanglement-based, and continuous variable QKD systems developed by several different groups and institutions. The SECOQC network demonstrated compatibility and interoperability of these different systems, and employed a "hop-by-hop" relay scheme, in which a cypher key (to be used for classical encryption) is sent along the chain of trusted nodes using one-time pad encryption between each connected pair of nodes. Routing and key consumption were also addressed. From 2009 to 2011, the three-node SwissQuantum network was deployed in Geneva, Switzerland [574]. The keys generated were tested for various applications, including high-speed commercial OS layer 2 encryptors (10 Gb/s Ethernet), research platforms for encryption and authentication, and IPSec encryptors. In 2010, high-speed QKD systems running at GHz clock rates were developed and deployed in Tokyo, enabling encrypted

---

[22] A bitwise XOR, publication of result and correction at one side, is a simple example.

video conferencing over 45 km using a one-time pad (OTP) [575]. In addition, a key management layer was included to control and coordinate key consumption. To date, China has constructed the largest QKD network, spanning over 2000 km and linking cities from Beijing to Shanghai using trusted relays [570]. Furthermore, in 2016 the Micius quantum science satellite was launched. Micius has facilitated quantum key distribution between various locations in China [570] and Europe and enabled real-time encrypted video calls between Beijing and Vienna [576]. The Cambridge quantum network achieved ∼2Mbps key rates coexistent with 100Gbps data traffic over metropolitan distances, and used link redundancy to mitigate denial of service risk. Another key advancement is the realization of a quantum network consisting of stationary nodes of solid-state spin qubits coupled by photons, and subsequent demonstration of post-selection free protocols in a scaleable architecture [552], also leading to definition of a quantum network stack [568,569]. A thorough overview of QKD networks implemented to date can be found in Ref. [132].

In terms of DI approaches, MDI-QKD has been field tested in a metropolitan network, where three users in a star configuration could communicate with each other through a central untrusted relay [493]. MDI-QKD systems have been realized in fiber optical links together with classical IP network signals [494,495]. Recently, free-space satellite links and fiber optic channels have been integrated for MDI-QKD [577], showing improvement to background noise when compared with BB84, and which could greatly increase transmission distances. There has also been considerable progress in CV MDI-QKD [578].

Though these field-tested QKD networks and other important advances have propelled QKD towards real-world use, there are still many challenges to be faced before QKD (of any type) can be fully integrated into the existing cybersecurity infrastructure. Despite the progress mentioned above, many national security organizations and regulatory agencies worldwide still do not classify QKD as a viable replacement for key distribution based on public-key cryptosystems. To protect against the threat of quantum computation, post-quantum cryptography is currently seen as a more cost effective and robust solution to key agreement [579–581]. In one form or another, the critical issues most often cited are:

1. Implementation security — specialty hardware and implementation particularities (laser pulses are not single photons, detectors can be vulnerable to side-channel attacks) can introduce additional vulnerabilities that may not be considered into theoretical security proofs.
2. Authentication — Unlike public key cryptosystems, QKD does not provide a method for authentication protocols, which are widely used for handshaking, signatures, etc. Moreover, the security of QKD relies on an authenticated classical channel for post-processing.
3. Trusted Relays — without quantum repeaters, extending QKD to large distances requires intermediate trusted relays, where security depends upon a classical hardware device.
4. Denial of service risk — If a private key cannot be established, the QKD protocol aborts, opening the door to denial-of-service attacks in which the communication channel is shut down.
5. Cost - special-purpose equipment is required for QKD. These devices, such as single-photon detectors, are typically expensive, raising costs of installation, operation and maintenance.
6. Compatibility — QKD needs to coexist and integrate with classical encryption systems and networks, which is complex due to the different operational frameworks of quantum and classical cryptography.

Here we provide a brief description of how these issues are currently being tackled by QKD community.

Implementation security. Quantum cryptographic protocols can be shown to be information-theoretic secure in principle. However, practical implementations can open the door to a wide range of vulnerabilities that might not be considered in security proofs [36,582]. Thus, implementation security is of paramount importance in taking QKD into the real world. Of course QKD is not special in this regard, the same is true for all encryption techniques, which are based on security claims or assumptions that might not be valid upon implementation. It is essential that all components of any cybersecurity system be extensively vetted and routinely tested.

The effort to achieve implementation security in QKD has been two-fold. On the one hand is the effort to remedy the practical issues with specific solutions, either by including additional techniques to QKD protocols (as in the case of decoy-state QKD, for example) and/or characterization of the devices, or by adapting security proofs to include these practical details. In addition, there has been effort to develop certification procedures for QKD equipment that can be carried out by third parties [583], as is done for conventional IT and security equipment.

On the other hand, the development of device independent protocols can provide a more broad solution with its goal to achieve information-theoretic security with as few assumptions as possible. DI-QKD, MDI-QKD and SDI-QKD can solve many of the most important implementation issues. While DI techniques allow for the main concepts behind security to be rooted to fundamental laws of physics, practical implementation will inevitably introduce new issues that may not have been considered. These need to be identified and scrutinized in order for QKD (DI or otherwise) to have widespread use. This is one of the objectives of the ongoing standardization process of QKD systems (see next section).

Authentication. To prevent man-in-the-middle attacks, QKD requires two-way authentication of the classical channel between users for the classical post-processing stage of the QKD protocol (basis sifting, error correction, privacy amplification). In small networks, pre-shared keys can be used. However, this severely limits the network, as not only do the keys need to be stored securely, but new users should be able to join without having previously established a key.

In classical communications, the public-key infrastructure (PKI) provides methods for authentication, which will soon include post-quantum cryptography (PQC). Though it is not information-theoretic secure, PQC and crypto-agility is the current next step to be adopted in protecting public-key cryptosystems from quantum computing [584]. PQC has already been used to authenticate classical communications in QKD sessions in several network topologies [585,586]. Importantly, since PQC is used only for authentication (key exchange for data encoding is realized with QKD), only short-term security is required. That is, if the PQC method used is broken in the future, the encoded data is still safe. Thus, PQC+QKD can offer a more robust security paradigm.

Trusted relays. As discussed above, currently trusted relays are required to construct QKD links over several hundred kilometers. As the development of quantum repeaters evolves [544], these classical relays can be exchanged for quantum relays, which will solve this issue. In a quantum network architecture, distributing several keys over multiple paths incorporating different sets of nodes will improve security, should one or more trusted nodes become compromised. Post-processing of the keys by the end users can reduce any leaked information. In addition, MDI-QKD can be used to transform some of the trusted relay stations into untrusted ones. For DI-QKD at large-scale distances, however, quantum repeaters are indeed a requirement.

Denial of service. Since QKD involves sending a single quantum state over a channel, any interruption in transmission, such as simply cutting the optical fiber, or introducing high amounts of noise, will prevent key exchange. This risk, known as denial of service, has been reduced in several proof-of-concept implementations by using quantum link redundancy, which takes advantage of the quantum network architecture to distribute keys over multiple paths [587]. In addition, hybrid approaches using QKD and PQC can also mitigate denial of service [588,589].

Cost. When evaluating the cost of cybersecurity, it should be compared to the cost of cybercrime, which worldwide is the equivalent third largest economy in the world ($\sim$9.5 trillion USD in 2023 and growing) [590]. In this regard, massive investment in cybersecurity is warranted, as exemplified by the US governments migration to post-quantum encryption, which is estimated to be 7.1 billion USD over ten years [591]. Second, the last century has shown that the evolution of technology typically leads to cheaper and better devices, as is the case of the microchip, for example. In this regard, integrated photonics will inevitably bring not only miniaturization and improvement but also the cost-reduction of quantum photonic devices, as it has done for classical equipment (see Ref. [592] for a recent review). It should also be noted that research and investment in quantum technology in general will accelerate development in quantum communications, since quantum photonic devices are widely used in most applications. In regards to QKD, manufacture of on-chip transmitters and receivers should facilitate the standardization and deployment of QKD systems. While chip integration of sources and optical circuits is quite advanced, the current technological roadblock is the integration of on-chip single-photon detectors, which are currently at a proof-of-principle or development stage [592].

Much progress has been made in integrating QKD into existing telecommunications infrastructure (see below), which will help decrease costs and requirement of special purpose equipment. In addition, QKD network architecture can be designed for cost reduction. For example, Hub and spoke [493] or multi-user [593] architectures with MDI-QKD or standard QKD [594], incorporating a central detection station, reduce the need for multiple detectors, which should minimize infrastructure costs. Finally, we note that that quantum communication systems might also find use as dual-purpose devices. For example, as large-scale quantum sensors capable of vibrational sensing [595], which could also motivate investment, development and deployment.

Compatibility. For over thirty years, the data capacity of fiber-optical communications has increased by a factor of ten every four years. The demand for increased capacity has not subsided, leading to even more optical intensity within the fibers as channel density increases. Though many of the QKD links demonstrated in field-deployed systems employed dark fiber (no copropagating classical data channels) [575,596,597], QKD will most likely need to coexist with classical data transmission in the same telecommunications network infrastructure. Moreover, to avoid loss of capacity, a QKD channel should not occupy much more bandwidth than a classical one. Multiplexing quantum and classical communication channels together is a considerable challenge, since noise from Raman scattering of light from the classical data channel, in which photons in the optical fiber are scattered inelastically, can easily contaminate a quantum signal. We note that Raman noise is not such an issue for CV-QKD, since the local oscillator used in homodyne detection acts as a mode filter, thus eliminating a large part of the Raman background [598,599]. Several methods have been proposed to mitigate this problem for DV-QKD. One method to minimize Raman noise, demonstrated as early as 1997 [600], is to employ a quantum signal with shorter wavelength, such as the telecommunications O-band ($\sim$1260−1360 nm), with the classical channels in the C-band ($\sim$1530−1565 nm) or L-band ($\sim$1565−1625 nm). In this way, the Raman noise is less prevalent. This approach has allowed QKD with keyrates of 4.5 kbps and 5.1 kbps for O-band quantum signals co-propagating and counter-propagating with 3.6 Tbps C-band classical signal ($\sim$21 dBm), over a 66 km commercial backbone network [601]. An MDI-QKD session was realized in a deployed link of about 25 km, resulting in a positive key rate with up to about 45 dB of link loss, when the quantum signal (@1310 nm) was multiplexed with classical telecommunications signals at 10 Gb/s (@ 1550 nm) and 10Mb/s ($\sim$1510 nm) [495]. Recently, a quantum link sending one O-band photon of an entangled pair through 47 km of fiber with 18 dBm of classical signal (C-band) was demonstrated [602], also showing improved performance for wavelengths less than 1300 nm. A similar setup was recently used for quantum teleportation coexistent with classical communications [603]. Despite the difficulties due to Raman noise, wavelength-division multiplexing (WDM) has been

used to implement QKD in C-band channels coexisting with 100Gb/s the encrypted classical channel (C-band) in a metropolitan network [587]. A possible way to minimize Raman noise is to use hollow-core fiber, which also reduces noise arising from nonlinear effects. Noise reduction of roughly 35 dBm compared to standard SMF28 fiber has been observed in QKD trials [604].

Another route for coexistence of classical and quantum signals is space division multiplexing (SDM), where multiple spatial modes are used as communication channels. SDM, involving new types of optical fiber, is currently seen as a necessary step to solve the current capacity crunch in optical fiber communications [605]. Multi-core optical fibers contain several single-mode cores within the same cladding material, and can be used to transmit independent classical and quantum signals [606–608]. Other types of specialty fibers, such as few-mode fibers and ring-core fibers, can support multiple transverse modes, which can each function as an independent channel. Propagation of quantum and classical signals in these fibers is currently being investigated for future communications infrastructure [132,609].

Concerning DI-QKD specifically, Raman noise presents a considerable obstacle for deployment in commercial fibers along with classical data channels. Quantum process tomography of the effect of Raman noise on DV QKD protocols has shown that it can be accurately described by a depolarizing channel for both co-propagating and counter-propagating signals [610], where the degree of depolarization is a function of fiber link length. Since depolarization reduces and can destroy entanglement, it is most likely that DI-QKD will require a dedicated standard fiber, or one of the more advanced noise-reduction solutions involving specialty fiber mentioned above.

The second observation that is typically made about the compatibility concerns integration and interoperability with existing cybersecurity hardware and protocols. In this regard, QKD has already been integrated with various cybersecurity protocols, including IPSec, TLS, Kerberos, AES, etc, as briefly discussed above. We will further discuss interoperability in the next section.

7.5.1. Standardization and interoperability

In addition to the scientific and technical challenges of realizing QKD in real-world conditions, there is also a need for coordinated effort towards standardization and interoperability to enable the integration of QKD into practical security services [611]. As QKD is an evolving technology, there are additional challenges ranging from immediate concerns, such as ensuring the security and interoperability of trusted relay-based QKD networks to medium- and long-term considerations like the large-scale integration of quantum and classical telecommunications networks, expanding the applications of QKD, and scaling up the network using quantum repeaters. Moreover, the global deployment of QKD may employ multiple types of links (fiber, free space) depending on the type of network and application [612].

Cryptographic hardware and software in use today has been developed under a set of industry standards that help maintain a consistent and high level of security across different systems and networks. This involves defining industry-wide guidelines, best practices, compliance and regulatory criteria, as well as interoperability parameters. In the US, standards for IT equipment are produced by National Institute of Standards and Technology (NIST) as Federal Information Processing Standards (FIPS) and approved by the Secretary of Commerce. In Europe, the International Organization for Standardization (ISO) developed the Common Criteria standard (ISO/EN 15408) (http://www.commoncriteriaportal.org/index.cfm). These standards provide a mechanism for certification of IT and security devices.

QKD equipment, protocols and methods need to be standardized, so that they can be certified for use by government agencies and/or third parties. Standardization should be realized with QKD protocols and security proofs that closely match the real-world conditions of the QKD implementation. While almost all QKD systems in operation today implement some form of device-dependent prepare and measure QKD, these efforts are equally important to the future deployment of DI-QKD in that they will accelerate its adoption as the relevant technology comes to maturity, since many of the technical issues related to integration, interoperability and standardization will have already been solved at least partially. Government security agencies have noted the need for standardization of QKD before the technology can considered for adoption on a broad scale [579–581]. This includes developing protocols for connectivity and interoperability, so that QKD systems can be linked with cryptographic key management systems and the application layer. These standards not only ensure quality and security, but ensure that equipment from different future vendors can interoperate together, and are important to establish an industry supply chain by defining interfaces and technical specifications for components and modules in various systems or distributed networks.

The successful deployment of QKD testbeds and proof-of-concept integration with cybersecurity hardware demonstrated that QKD technology and networking was sufficiently advanced for the standardization process to begin. In 2008, the European Telecommunications Standards Institute (ETSI) created the industry specification group for QKD (ISG-QKD) [613], which has produced recommendations regarding QKD architecture, use cases, certification, security proofs and assurances, integration into standard optical networks, interoperability and interfacing, among other topics [614]. Notably, in 2023 a Common Criteria Protection Profile for QKD was recently published (GS QKD 016), which "will help manufacturers to submit pairs of 'prepare and measure' QKD modules for evaluation under a security certification process. Such modules can be used by telecom operators and enterprises in securing their networks with the knowledge that certified products have been subjected to the scrutiny of a formal security evaluation process" [615]. The International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) have developed the ISO/IEC 23837 series, which specifies security requirements, testing procedures, and evaluation methods for quantum key distribution (QKD) modules [616,617]. This series is structured under the framework of the ISO/IEC 15408 series,
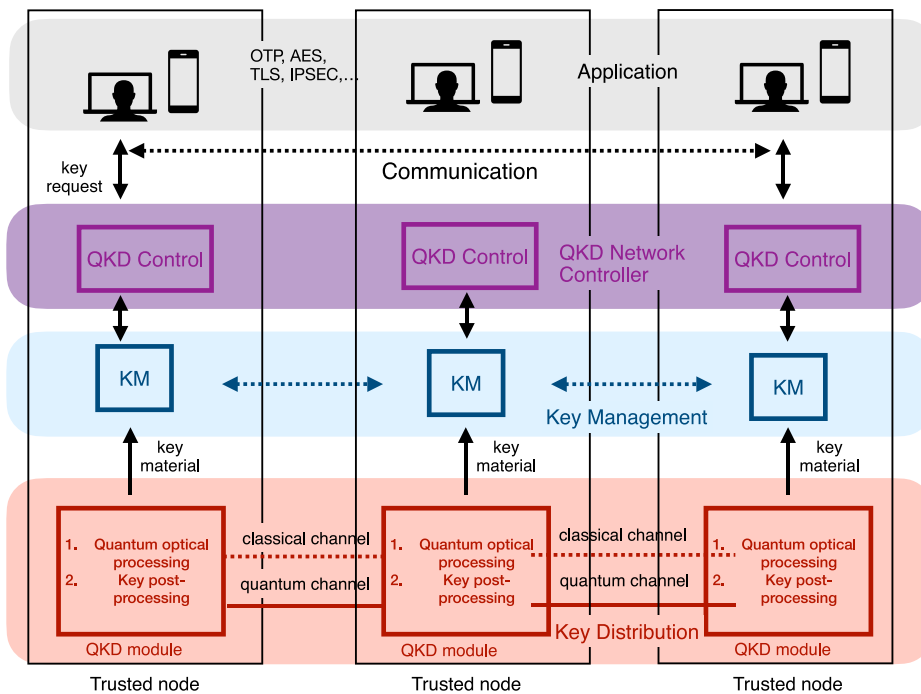
Fig. 23. Illustration of integrated QKD network.

commonly referred to as the Common Criteria for Information Technology Security Evaluation. By establishing rigorous standards and assessment methods, the objectives of the ISO/IEC 23837 series are the security and reliability of QKD technologies for practical and secure implementations. These standards were developed under subcommittee 27 of joint technical committee (JTC) 1 (Information security, cybersecurity and privacy protection) [618]. In 2024, a ISO/IEC JTC on quantum technologies was established [619]. The International Telecommunications Union (ITU) have also published documents containing definitions and recommendations in the ITU-T Y.3800 series (quantum communication) and ITU-T X.1700 series (QKD networks). An overview of standardization processes and documents can be found in Ref. [132], and on the organization websites [614,618–620]. The certification of MDI-QKD devices has been studied in Ref. [621], in which it is noted that similarities between these findings and ETSI GS QKD 016 suggest that a generic framework could be created to permit certification of various implementations and protocols, including MDI-QKD.

7.5.2. Quantum key distribution network architecture

Part of the challenge of implementing real-world QKD is determining how this new quantum layer will integrate into the existing cybersecurity infrastructure. The field tests realized over the last two decades have been important in accelerating this integration. A number of authors have discussed network layer architectures for QKD systems [131,132, 575,622–624], and similar models have appeared in technical recommendations by international agencies, such as the ITU (documents Y.3800–Y.3805) [620].

Fig. 23 shows a simplified illustration of a QKD network architecture containing only three users, similar to the model put forth in Recommendation ITU-T Y.3800 [625]. The network consists of a QKD layer, a key management layer, a QKD control layer and the application layer. The users reside in the application layer, which contains all hardware devices and software that will consume cryptographic keys, for use in protocols such as TLS for secure connection to web servers, IPSec for VPN connections, AES for data encryption, etc.

In this simplified example, each node is responsible for generating and managing keys between users in their local network and users in the local networks of other nodes. Depending on the network architecture, each node could serve as an end point as well as a trusted node used for linking other end points. The raw key material is generated by the QKD modules residing in two connected nodes, which are linked by quantum and classical channels used for point-to-point QKD sessions. In the case of DI-QKD, the quantum channel would consist of entangled states shared across the link, and the trusted node would employ a repeater station to connect the two neighboring links. In the near term, the trusted nodes are the classical trusted relay nodes described above. We note that this architecture permits the key distribution layer to be constructed from different types of QKD systems or protocols, or to employ parallel QKD links between nodes
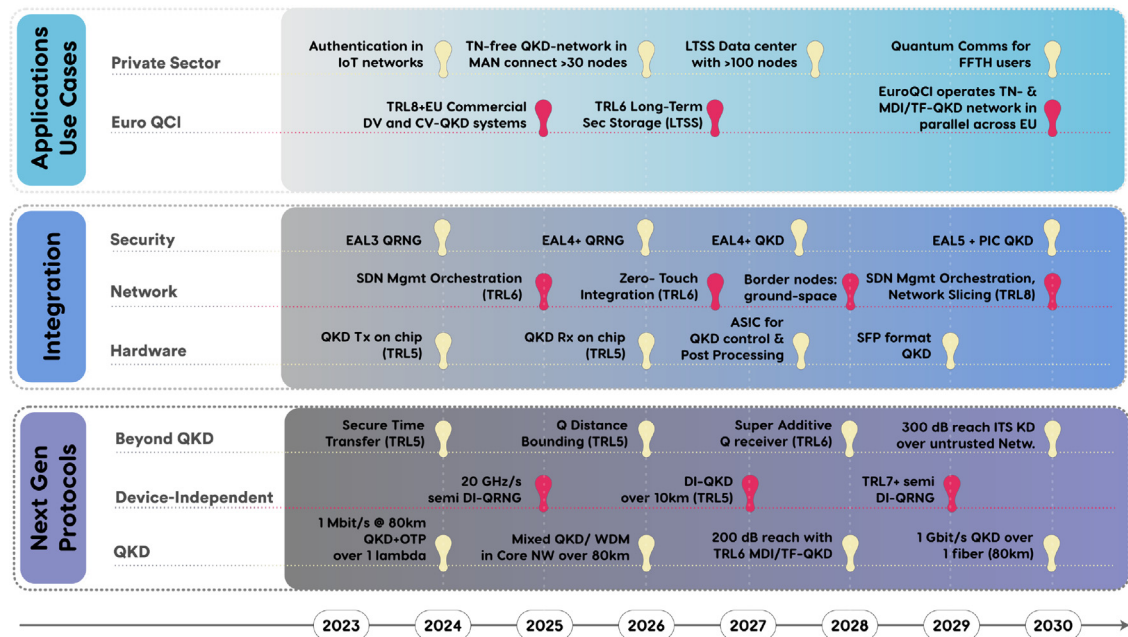
Fig. 24. European roadmap for the QKD architecture deployment (from https://qsnp.eu/).

to increase the key rate and reduce denial of service risk. In addition, in a network architecture, two users might be linked through different sets of intermediary nodes to the same effect.

Through the QKD protocol(s) used, cryptographic key material in the form of shared random bit strings is produced between linked QKD modules and uploaded to the key managers, which store it for future use. When end users need to be connected, the key managers at the intermediate trusted nodes perform the necessary post processing to produce shared keys between the users. Upon request, the key managers at the endpoints can format the keys and deliver them to the security application that will use them. Key managers at different trusted nodes must communicate to synchronize the key request and delivery, to assure that two end users can communicate with the same key.

The QKD control layer manages the end-to-end connectivity from one user to the another through the required trusted nodes, so that the middle nodes perform the appropriate processing to enable the link between end users. The QKD controllers are responsible for routing control for key relays, management of QKD and KM links, session control for QKD services, authentication and authorization, as well as ensuring quality of service. The QKD control layer might also employ a centralized architecture. In addition to the layers shown in Fig. 23, management layers (not shown) monitor the entire stack and ensure quality of service and that the required functionality is met.

As technology progresses, the QKD layer can be upgraded from device-dependent QKD to semi-DI and eventually full-DI. A roadmap for development of QKD architecture and rollout in the EU is shown in Fig. 24, where we note that device independence is included as a key benchmark. As quantum repeaters come on line, quantum connectivity between end users would be managed by the QKD control layer, which would allow for the realization of full DI-QKD in principle. Conceivably, the network could employ several types of QKD protocols, depending on the security profile of each user group, and the types of available hardware in each section of the network.

Conclusion

DI-QKD represents a transformative advancement in QKD, addressing fundamental security challenges by using nonlocal correlations rather than relying on the trustworthiness of quantum devices. In this review, we have highlighted both the fundamental theoretical aspects and the progress in implementing experimental setups. Moreover, the growing exploration of semi-device-independent protocols such as MDI-QKD, RDI-QKD, and 1SDI-QKD have been presented.

DI-QKD achieves its robust security through the violation of Bell inequalities, ensuring that any eavesdropping attempts disturb the nonlocal correlations, thereby making such third parties detectable. While the first successful implementations of DI-QKD marked a milestone by addressing all Bell test loopholes, practical challenges related to scalability and technology readiness persist. Current experimental realizations have achieved limited distances of a few hundred meters with low key rates, far short of the scales required for widespread commercial deployment.

Despite the remaining challenges in practical deployment, DI-QKD is poised to redefine the future of cryptographic security. The ongoing researches on DI-QKD protocols together with relaxed versions of semi-device-independent

frameworks are paving the way for this groundbreaking technology to transition from the laboratory to real-world applications, ensuring unconditional security for the next generation of quantum communication networks. A view as to how the rollout of DI technique might unfold is provided in the European roadmap shown in Fig. 24.

CRediT authorship contribution statement

Seyed Arash Ghoreishi: Writing – review & editing, Writing – original draft, Project administration, Investigation, Conceptualization. **Giovanni Scala:** Writing – review & editing, Writing – original draft, Methodology, Investigation, Conceptualization. **Renato Renner:** Writing – review & editing, Writing – original draft, Supervision, Conceptualization. **Letícia Lira Tacca:** Writing – review & editing, Writing – original draft, Methodology, Investigation. **Jan Bouda:** Writing – review & editing, Writing – original draft, Supervision, Conceptualization. **Stephen Patrick Walborn:** Writing – review & editing, Writing – original draft, Conceptualization. **Marcin Pawłowski:** Writing – review & editing, Writing – original draft, Supervision, Investigation, Conceptualization.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgments

References

[1] N. Gisin, G. Ribordy, W. Tittel, H. Zbinden, Rev. Modern Phys. 74 (2002) 145.
[2] S. Pirandola, U.L. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani, J.L. Pereira, M. Razavi, J. Shamsul Shaari, M. Tomamichel, V.C. Usenko, G. Vallone, P. Villoresi, P. Wallden, Adv. Opt. Photonics 12 (2020) 1012.
[3] V. Zapatero, T. van Leent, R. Arnon-Friedman, W.-Z. Liu, Q. Zhang, H. Weinfurter, M. Curty, Npj Quantum Inf. 9 (2023) http://dx.doi.org/10.1038/s41534-023-00684-x.
[4] M. Bozzio, C. Crépeau, P. Wallden, P. Walther, 2024, http://dx.doi.org/10.48550/arXiv.2411.08877, arXiv preprint.
[5] W. Diffie, M. Hellman, IEEE Trans. Inform. Theory 22 (1976) 644.
[6] R.L. Rivest, A. Shamir, L. Adleman, Commun. ACM 21 (1978) 120.
[7] C.H. Bennett, G. Brassard, Theoret. Comput. Sci. 560 (2014) 7.
[8] C. Gidney, M. Ekerʾa, Quantum 5 (2021) 433.
[9] F.A.P. Petitcolas, Kerckhoffs' principle, in: Encyclopedia of Cryptography and Security, Springer US, 2011, 675–675.
[10] B. Qi, C.-H.F. Fung, H.-K. Lo, X. Ma, Quantum Inf. Comput. 7 (2005) 73.
[11] A. Lamas-Linares, C. Kurtsiefer, Opt. Express 15 (2007) 9388.
[12] Y. Zhao, C.-H.F. Fung, B. Qi, C. Chen, H.-K. Lo, Phys. Rev. A 78 (2008) 042333.
[13] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, V. Makarov, Nat. Photonics 4 (2010) 686.
[14] C. Wiechers, L. Lydersen, C. Wittmann, D. Elser, J. Skaar, C. Marquardt, V. Makarov, G. Leuchs, New J. Phys. 13 (2011) 013043.
[15] H. Qin, R. Kumar, V. Makarov, R. Alléaume, Phys. Rev. A 98 (2018) 012312.
[16] I.W. Primaatmaja, K.T. Goh, E.Y.-Z. Tan, J.T.-F. Khoo, S. Ghorai, C.C.-W. Lim, Quantum 7 (2023) 932.
[17] S.-K. Liao, W.-Q. Cai, W.-Y. Liu, L. Zhang, Y. Li, J.-G. Ren, J. Yin, Q. Shen, Y. Cao, Z.-P. Li, F.-Z. Li, X.-W. Chen, L.-H. Sun, J.-J. Jia, J.-C. Wu, X.-J. Jiang, J.-F. Wang, Y.-M. Huang, Q. Wang, Y.-L. Zhou, L. Deng, T. Xi, L. Ma, T. Hu, Q. Zhang, Y.-A. Chen, N.-L. Liu, X.-B. Wang, Z.-C. Zhu, C.-Y. Lu, R. Shu, C.-Z. Peng, J.-Y. Wang, J.-W. Pan, Nature 549 (2017) 43.
[18] Y. Li, W.-Q. Cai, J.-G. Ren, C.-Z. Wang, M. Yang, L. Zhang, H.-Y. Wu, L. Chang, J.-C. Wu, B. Jin, H.-J. Xue, X.-J. Li, H. Liu, G.-W. Yu, X.-Y. Tao, T. Chen, C.-F. Liu, W.-B. Luo, J. Zhou, H.-L. Yong, Y.-H. Li, F.-Z. Li, C. Jiang, H.-Z. Chen, C. Wu, X.-H. Tong, S.-J. Xie, F. Zhou, W.-Y. Liu, Y. Ismail, F. Petruccione, N.-L. Liu, L. Li, F. Xu, Y. Cao, J. Yin, R. Shu, X.-B. Wang, Q. Zhang, J.-Y. Wang, S.-K. Liao, C.-Z. Peng, J.-W. Pan, Nature 640 (2025) 47.
[19] S. Singh, The Code Book, Knopf Doubleday Publishing Group, Westminster, 2011, description based on publisher supplied metadata and other sources.
[20] G. Scala, Public GitHub folder, 2024, https://github.com/giovanniscala/DI-QKD-review.git.
[21] J. Daemen, Aes proposal: Rijndael, 1999.
[22] D.J. Bernstein, T. Lange, Nature 549 (2017) 188.
[23] L.K. Grover, Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing, STOC '96, Association for Computing Machinery, New York, NY, USA, 1996, pp. 212–219.
[24] E. Rescorla, T. Dierks, The transport layer security (TLS) protocol version 1.2, 2008, RFC 5246.
[25] E. Rescorla, The transport layer security (TLS) protocol version 1.3, 2018, RFC 8446.
[26] P.W. Shor, SIAM J. Comput. 26 (1997) 1484.
[27] D. Bruss, G. Erdélyi, T. Meyer, T. Riege, J. Rothe, ACM Comput. Surv. 39 (2007) 6.

[28] S. Wiesner, ACM SIGACT News 15 (1983) 78.
[29] T. Metger, O. Fawzi, D. Sutter, R. Renner, Comm. Math. Phys. 405 (2024) http://dx.doi.org/10.1007/s00220-024-05121-4.
[30] W.K. Wootters, W.H. Zurek, Nature 299 (1982) 802.
[31] S.M. Barnett, B. Huttner, S.J. Phoenix, J. Modern Opt. 40 (1993) 2501.
[32] B.A. Nguyen, Phys. Lett. A 328 (2004) 6.
[33] H. Ez-zahraouy, A. Benyoussef, Internat. J. Modern Phys. B 23 (2009) 4755.
[34] A. Acín, N. Gisin, L. Masanes, Phys. Rev. Lett. 97 (2006) 120405.
[35] F. Magniez, D. Mayers, M. Mosca, H. Ollivier, International Colloquium on Automata, Languages, and Programming, Springer, 2006, pp. 72–83.
[36] V. Scarani, C. Kurtsiefer, Theoret. Comput. Sci. 560 (2014) 27, theoretical Aspects of Quantum Cryptography – celebrating 30 years of BB84.
[37] R. Okuła, P. Mironowicz, arXiv preprint http://dx.doi.org/10.48550/arXiv.2404.19445 2404.19445.
[38] B. Huttner, N. Imoto, N. Gisin, T. Mor, Phys. Rev. A 51 (1995) 1863.
[39] N. Lütkenhaus, M. Jahma, New J. Phys. 4 (2002) 44.
[40] X.-B. Wang, Phys. Rev. Lett. 94 (2005) 230503.
[41] F.-X. Standaert, Secure integrated circuits and systems, 2010, p. 27.
[42] S.L. Braunstein, S. Pirandola, Phys. Rev. Lett. 108 (2012) 130502.
[43] A. Baliuka, M. Stöcker, M. Auer, P. Freiwang, H. Weinfurter, L. Knips, Phys. Rev. Appl. 20 (2023) 054040.
[44] C. Zhang, X.-L. Hu, C. Jiang, J.-P. Chen, Y. Liu, W. Zhang, Z.-W. Yu, H. Li, L. You, Z. Wang, X.-B. Wang, Q. Zhang, J.-W. Pan, Phys. Rev. Lett. 128 (2022) 190503.
[45] N. Gisin, S. Fasel, B. Kraus, H. Zbinden, G. Ribordy, Phys. Rev. A 73 (2006) 022320.
[46] N. Jain, E. Anisimova, I. Khan, V. Makarov, C. Marquardt, G. Leuchs, New J. Phys. 16 (2014) 123030.
[47] C.-H.F. Fung, B. Qi, K. Tamaki, H.-K. Lo, Phys. Rev. A 75 (2007) 032314.
[48] F. Xu, B. Qi, H.-K. Lo, New J. Phys. 12 (2010) 113026.
[49] P. Jouguet, S. Kunz-Jacques, E. Diamanti, Phys. Rev. A 87 (2013) 062313.
[50] Y. Mao, Y. Wang, W. Huang, H. Qin, D. Huang, Y. Guo, Phys. Rev. A 101 (2020) 062320.
[51] C. Emde, F. Pinto, T. Lukasiewicz, P.H.S. Torr, A. Bibi, Towards certification of uncertainty calibration under adversarial attacks, 2024.
[52] R.W.S. Giulio Chiribella, in: Springer (Ed.), Quantum Theory: Informational Foundations and Foils, Springer Netherlands, 2016.
[53] A.K. Ekert, Phys. Rev. Lett. 67 (1991) 661.
[54] D.P. Nadlinger, P. Drmota, B.C. Nichol, G. Araneda, D. Main, R. Srinivas, D.M. Lucas, C.J. Ballance, K. Ivanov, E.Y.-Z. Tan, P. Sekatski, R.L. Urbanke, R. Renner, N. Sangouard, J.-D. Bancal, Nature 607 (2022) 682.
[55] W.-Z. Liu, Y.-Z. Zhang, Y.-Z. Zhen, M.-H. Li, Y. Liu, J. Fan, F. Xu, Q. Zhang, J.-W. Pan, Phys. Rev. Lett. 129 (2022) 050502.
[56] W. Zhang, T. van Leent, K. Redeker, R. Garthoff, R. Schwonnek, F. Fertig, S. Eppelt, W. Rosenfeld, V. Scarani, C.C.-W. Lim, H. Weinfurter, Nature 607 (2022) 687.
[57] M. Héder, Innov. J. 22 (2017) 1.
[58] D. Mayers, A. Yao, Quantum Inf. Comput. 4 (2004) http://dx.doi.org/10.48550/arXiv.quant-ph/0307205.
[59] W. Yan, X. Zheng, W. Wen, L. Lu, Y. Du, Y.-Q. Lu, S. Zhu, X.-S. Ma, Npj Quantum Inf. 11 (2025) 97.
[60] S.-F. Shao, L. Zhou, J. Lin, M. Minder, C. Ge, Y.-M. Xie, A. Shen, Z. Yan, H.-L. Yin, Z. Yuan, Phys. Rev. X 15 (2025) 021066.
[61] W. Li, L. Zhang, Y. Lu, Z.-P. Li, C. Jiang, Y. Liu, J. Huang, H. Li, Z. Wang, X.-B. Wang, et al., Phys. Rev. Lett. 130 (2023) 250802.
[62] L. Zhou, J. Lin, Y.-M. Xie, Y.-S. Lu, Y. Jing, H.-L. Yin, Z. Yuan, Phys. Rev. Lett. 130 (2023) 250801.
[63] Y. Liu, W.-J. Zhang, C. Jiang, J.-P. Chen, D. Ma, C. Zhang, W.-X. Pan, H. Dong, J.-M. Xiong, C.-J. Zhang, et al., Quantum Front. 2 (2023) 16.
[64] X.-H. Zhan, Z.-Q. Zhong, J.-Y. Ma, S. Wang, Z.-Q. Yin, W. Chen, G.-C. Guo, Z.-F. Han, Npj Quantum Inf. 11 (2025) 1.
[65] L. Zhang, W. Li, J. Pan, Y. Lu, W. Li, Z.-P. Li, Y. Huang, X. Ma, F. Xu, J.-W. Pan, Phys. Rev. X 15 (2025) 021037.
[66] A.A.E. Hajomer, U.L. Andersen, T. Gehring, Quantum Sci. Technol. 10 (2025) 025032.
[67] J. Liu, X. Zhou, H. Ding, J. Xu, C. Zhang, J. Li, Q. Wang, 2025, arXiv preprint arXiv:2503.05095.
[68] M. Pittaluga, Y.S. Lo, A. Brzosko, R.I. Woodward, D. Scalcon, M.S. Winnel, T. Roger, J.F. Dynes, K.A. Owen, S. Juárez, et al., Nature 640 (2025) 911.
[69] A. Acin, S. Massar, S. Pironio, New J. Phys. 8 (2006) 126.
[70] A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, V. Scarani, Phys. Rev. Lett. 98 (2007) 230501.
[71] J. Barrett, L. Hardy, A. Kent, Phys. Rev. Lett. 95 (2005) 010503.
[72] V. Scarani, N. Gisin, N. Brunner, L. Masanes, S. Pino, A. Acín, Phys. Rev. A 74 (2006) 042339.
[73] S. Pironio, A. Acín, N. Brunner, N. Gisin, S. Massar, V. Scarani, New J. Phys. 11 (2009) 045021, 0903.4460.
[74] R. Gallego, N. Brunner, C. Hadley, A. Acín, Phys. Rev. Lett. 105 (2010) 230501.
[75] S. Pironio, A. Acín, S. Massar, A.B. de La Giroday, D.N. Matsukevich, P. Maunz, S. Olmschenk, D. Hayes, L. Luo, T.A. Manning, et al., Nature 464 (2010) 1021.
[76] E. Hänggi, R. Renner, 2010, http://dx.doi.org/10.48550/arXiv.1009.1833, arXiv preprint arXiv:1009.1833.
[77] L. Masanes, S. Pironio, A. Acín, Nat. Commun. 2 (2011) 238.
[78] J. Barrett, R. Colbeck, A. Kent, Phys. Rev. Lett. 110 (2013) 010503.
[79] C.C.W. Lim, C. Portmann, M. Tomamichel, R. Renner, N. Gisin, Phys. Rev. X 3 (2013) 031006.
[80] J.A. Slater, C. Branciard, N. Brunner, W. Tittel, New J. Phys. 16 (2014) 043002.
[81] U. Vazirani, T. Vidick, Phys. Rev. Lett. 113 (2014) 140501.
[82] U. Vazirani, T. Vidick, Commun. ACM 62 (2019) 133.
[83] E. Kaur, M.M. Wilde, A. Winter, New J. Phys. 22 (2020) 023039.
[84] E.Y.-Z. Tan, C.C.-W. Lim, R. Renner, Phys. Rev. Lett. 124 (2020) 020502.
[85] P. Brown, H. Fawzi, O. Fawzi, Nat. Commun. 12 (2021) http://dx.doi.org/10.1038/s41467-020-20018-1.
[86] P. Sekatski, J.-D. Bancal, X. Valcarce, E.Y.-Z. Tan, R. Renner, N. Sangouard, Quantum 5 (2021) 444.
[87] E. Woodhead, A. Acín, S. Pironio, Quantum 5 (2021) 443.
[88] R. Schwonnek, K.T. Goh, I.W. Primaatmaja, E.Y.-Z. Tan, R. Wolf, V. Scarani, C.C.-W. Lim, Nat. Commun. 12 (2021) 2880.
[89] F. Xu, Y.-Z. Zhang, Q. Zhang, J.-W. Pan, Phys. Rev. Lett. 128 (2022) 110506.
[90] M. Farkas, M. Balanzó-Juandó, K. Łukanowski, J. Kołodyński, A. Acín, Phys. Rev. Lett. 127 (2021) 050503.
[91] Y.-Z. Zhen, Y. Mao, Y.-Z. Zhang, F. Xu, B.C. Sanders, Phys. Rev. Lett. 131 (2023) 080801.
[92] A. Chaturvedi, G. Viola, M. Pawłowski, Npj Quantum Inf. 10 (2024) 7.
[93] E.P. Lobo, J. Pauwels, S. Pironio, Quantum 8 (2024) 1332.
[94] E.Y.-Z. Tan, R. Wolf, Phys. Rev. Lett. 133 (2024) 120803.
[95] T. Le Roy-Deloison, E.P. Lobo, J. Pauwels, S. Pironio, PRX Quantum 6 (2025) 020311.
[96] P. Sekatski, J. Pauwels, E.P. Lobo, S. Pironio, N. Brunner, Certification of quantum correlations and diqkd at arbitrary distances through routed bell tests, 2025.

[97]   A. Chaturvedi, M. Pawłowski, M. Farkas, Extending quantum correlations to arbitrary distances via parallel repetition of routed bell tests,
       2025.
[98]   M. Farkas, Phys. Rev. Lett. 132 (2024) 210803.
[99]   M. Giustina, A. Mech, S. Ramelow, B. Wittmann, J. Kofler, J. Beyer, A. Lita, B. Calkins, T. Gerrits, S.W. Nam, R. Ursin, A. Zeilinger, Nature 497
       (2013) 227.
[100] B. Hensen, H. Bernien, A.E. Dréau, A. Reiserer, N. Kalb, M.S. Blok, J. Ruitenberg, R.F.L. Vermeulen, R.N. Schouten, C. Abellán, W. Amaya, V.
       Pruneri, M.W. Mitchell, M. Markham, D.J. Twitchen, D. Elkouss, S. Wehner, T.H. Taminiau, R. Hanson, Nature 526 (2015) 682.
[101] M. Lucamarini, Z.L. Yuan, J.F. Dynes, A.J. Shields, Nature 557 (2018) 400.
[102] J. Yin, Y.-H. Li, S.-K. Liao, M. Yang, Y. Cao, L. Zhang, J.-G. Ren, W.-Q. Cai, W.-Y. Liu, S.-L. Li, R. Shu, Y.-M. Huang, L. Deng, L. Li, Q. Zhang, N.-L.
       Liu, Y.-A. Chen, C.-Y. Lu, X.-B. Wang, F. Xu, J.-Y. Wang, C.-Z. Peng, A.K. Ekert, J.-W. Pan, Nature 582 (2020) 501.
[103] T. Holz, H. Kampermann, D. Bruß, Phys. Rev. Res. 2 (2020) 023251.
[104] X. Valcarce, P. Sekatski, E. Gouzien, A. Melnikov, N. Sangouard, Phys. Rev. A 107 (2023) 062607.
[105] E.Y.-Z. Tan, P. Sekatski, J.-D. Bancal, R. Schwonnek, R. Renner, N. Sangouard, C.C.-W. Lim, Quantum 6 (2022) 880.
[106] A.A. Melnikov, P. Sekatski, N. Sangouard, Phys. Rev. Lett. 125 (2020) 160401.
[107] J. Kołodyński, A. Máttar, P. Skrzypczyk, E. Woodhead, D. Cavalcanti, K. Banaszek, A. Acín, Quantum 4 (2020) 260.
[108] F. Dupuis, O. Fawzi, R. Renner, Comm. Math. Phys. 379 (2020) 867.
[109] R. Arnon-Friedman, F. Dupuis, O. Fawzi, R. Vidick, Nat. Commun. 9 (2018).
[110] F. Grasselli, G. Murta, H. Kampermann, D. Bruß, PRX Quantum 2 (2021) 010308.
[111] T. Metger, O. Fawzi, D. Sutter, R. Renner, 2022, http://dx.doi.org/10.48550/arXiv.2203.04989, arXiv:2203.04989.
[112] R. Colbeck, R. Renner, Nat. Phys. 8 (2012) 450.
[113] A. Acín, L. Masanes, Nature 540 (2016) 213.
[114] C.-L. Li, K.-Y. Zhang, X. Zhang, K.-X. Yang, Y. Han, S.-Y. Cheng, H. Cui, W.-Z. Liu, M.-H. Li, Y. Liu, B. Bai, H.-H. Dong, J. Zhang, X. Ma, Y. Yu, J.
       Fan, Q. Zhang, J.-W. Pan, Proc. Natl. Acad. Sci. 120 (2023) http://dx.doi.org/10.1073/pnas.2205463120.
[115] Z. Cao, H. Zhou, X. Yuan, X. Ma, Phys. Rev. X 6 (2016) 011020.
[116] D.G. Marangon, G. Vallone, P. Villoresi, Phys. Rev. Lett. 118 (2017) 060503.
[117] M. Avesani, D.G. Marangon, G. Vallone, P. Villoresi, Nat. Commun. 9 (2018) http://dx.doi.org/10.1038/s41467-018-07585-0.
[118] M. Pawłowski, N. Brunner, Phys. Rev. A 84 (2011) 010302.
[119] C. Branciard, E.G. Cavalcanti, S.P. Walborn, V. Scarani, H.M. Wiseman, Phys. Rev. A 85 (2012) 010301.
[120] H.-K. Lo, M. Curty, B. Qi, Phys. Rev. Lett. 108 (2012) 130503.
[121] M. Ioannou, P. Sekatski, A.A. Abbott, D. Rosset, J.-D. Bancal, N. Brunner, New J. Phys. 24 (2022) 063006.
[122] Y. Liu, T.-Y. Chen, L.-J. Wang, H. Liang, G.-L. Shentu, J. Wang, K. Cui, H.-L. Yin, N.-L. Liu, L. Li, X. Ma, J.S. Pelc, M.M. Fejer, C.-Z. Peng, Q. Zhang,
       J.-W. Pan, Phys. Rev. Lett. 111 (2013) 130502.
[123] Y.-L. Tang, H.-L. Yin, S.-J. Chen, Y. Liu, W.-J. Zhang, X. Jiang, L. Zhang, J. Wang, L.-X. You, J.-Y. Guan, D.-X. Yang, Z. Wang, H. Liang, Z. Zhang,
       N. Zhou, X. Ma, T.-Y. Chen, Q. Zhang, J.-W. Pan, Phys. Rev. Lett. 113 (2014) 190501.
[124] C. Panayi, M. Razavi, X. Ma, N. Lütkenhaus, New J. Phys. 16 (2014) 043005.
[125] S. Pirandola, C. Ottaviani, G. Spedalieri, C. Weedbrook, S.L. Braunstein, S. Lloyd, T. Gehring, C.S. Jacobsen, U.L. Andersen, Nat. Photonics 9 (2015)
       397.
[126] T. Gehring, V. Händchen, J. Duhme, F. Furrer, T. Franz, C. Pacher, R.F. Werner, R. Schnabel, Nat. Commun. 6 (2015) 8795.
[127] H.-L. Yin, T.-Y. Chen, Z.-W. Yu, H. Liu, L.-X. You, Y.-H. Zhou, S.-J. Chen, Y. Mao, M.-Q. Huang, W.-J. Zhang, H. Chen, M.J. Li, D. Nolan, F. Zhou,
       X. Jiang, Z. Wang, Q. Zhang, X.-B. Wang, J.-W. Pan, Phys. Rev. Lett. 117 (2016) 190501.
[128] R. Alléaume, C. Branciard, J. Bouda, T. Debuisschert, M. Dianati, N. Gisin, M. Godfrey, P. Grangier, T. Länger, N. Lütkenhaus, C. Monyk, P.
       Painchault, M. Peev, A. Poppe, T. Pornin, J. Rarity, R. Renner, G. Ribordy, M. Riguidel, L. Salvail, A. Shields, H. Weinfurter, A. Zeilinger, Theoret.
       Comput. Sci. 560 (2014) 62.
[129] V. Scarani, H. Bechmann-Pasquinucci, N.J. Cerf, M. Dušek, N. Lütkenhaus, M. Peev, Rev. Modern Phys. 81 (2009) 1301.
[130] F. Xu, X. Ma, Q. Zhang, H.-K. Lo, J.-W. Pan, Rev. Modern Phys. 92 (2020) 025002.
[131] M. Mehic, M. Niemiec, S. Rass, J. Ma, M. Peev, A. Aguado, V. Martin, S. Schauer, A. Poppe, C. Pacher, M. Voznak, ACM Comput. Surv. 53 (2020)
       http://dx.doi.org/10.1145/3402192.
[132] Y. Cao, Y. Zhao, Q. Wang, J. Zhang, S. Ng, L. Hanzo, IEEE Commun. Surv. & Tutorials 24 (2022) 839.
[133] N. Brunner, D. Cavalcanti, S. Pironio, V. Scarani, S. Wehner, Rev. Modern Phys. 86 (2014) 419.
[134] V. Scarani, Bell Nonlocality, Oxford University Press, 2019.
[135] E.Y.-Z. Tan, 2021, http://dx.doi.org/10.48550/arXiv.2111.11769, arXiv preprint.
[136] R.F. Werner, Phys. Rev. A 40 (1989) 4277.
[137] G. Boole, Philos. Trans. R. Soc. Lond. (1862) 225.
[138] J. Pearl, Causality: Models, Reasoning, and Inference, Cambridge University Press, 2009.
[139] J.S. Bell, Phys. Phys. Fiz. 1 (1964) 195.
[140] P. Spirtes, C. Glymour, R. Scheines, Causation, Prediction, and Search, Springer New York, 1993.
[141] R. Spekkens, Causal inference lecture - 230320, 2023, pIRSA:23030073 see https://pirsa.org.
[142] N. Gigena, G. Scala, A. Mandarino, Int. J. Quantum Inf. (2022) http://dx.doi.org/10.1142/s0219749923400051.
[143] C.M. Lee, R.W. Spekkens, J. Causal Inference 5 (2017) http://dx.doi.org/10.1515/jci-2016-0013.
[144] S. Ali Ahmad, T.D. Galley, P.A. Höhn, M.P. Lock, A.R. Smith, Phys. Rev. Lett. 128 (2022) http://dx.doi.org/10.1103/physrevlett.128.170401.
[145] T. Zhang, O. Dahlsten, V. Vedral, arXiv preprint http://dx.doi.org/10.48550/arXiv.2002.10448, 2002.10448.
[146] A. Khrennikov, J. Math. Phys. 48 (2007) http://dx.doi.org/10.1063/1.2401673.
[147] M. Pawłowski, T. Paterek, D. Kaszlikowski, V. Scarani, A. Winter, M. Zukowski, Nature 461 (2009) 1101.
[148] N. Miklin, M. Pawłowski, Phys. Rev. Lett. 126 (2021) http://dx.doi.org/10.1103/physrevlett.126.220403.
[149] T.P. Le, C. Meroni, B. Sturmfels, R.F. Werner, T. Ziegler, Quantum 7 (2023) 947.
[150] P. Cieśliński, L. Knips, M. Kowalczyk, W. Laskowski, T. Paterek, T. Vértesi, H. Weinfurter, Proc. Natl. Acad. Sci. 121 (2024) http://dx.doi.org/10.
       1073/pnas.2404455121.
[151] M. Navascues, S. Pironio, A. Acin, Phys. Rev. Lett. 98 (2007) 010401.
[152] M. Navascués, S. Pironio, A. Acín, New J. Phys. 10 (2008) 073013.
[153] S. Pironio, M. Navascués, A. Acín, SIAM J. Optim. 20 (2010) 2157.
[154] M. Navascués, G. de la Torre, T. Vértesi, Phys. Rev. X 4 (2014) http://dx.doi.org/10.1103/physrevx.4.011011.
[155] T. Vértesi, W. Laskowski, K.F. Pál, Phys. Rev. A 89 (2014) http://dx.doi.org/10.1103/physreva.89.012115.
[156] M. Navascués, T. Vértesi, Phys. Rev. Lett. 115 (2015) http://dx.doi.org/10.1103/physrevlett.115.020501.
[157] P. Mironowicz, J. Phys. A 57 (2024) 163002.

[158] D. Mayers, A. Yao, Proceedings 39th Annual Symposium on Foundations of Computer Science (Cat. No. 98CB36280), in: SFCS-98, IEEE Comput. Soc.
[159] A. Acín, S. Massar, S. Pironio, Phys. Rev. Lett. 108 (2012) 100402.
[160] C. Bamps, S. Pironio, Phys. Rev. A 91 (2015) 052111.
[161] I. Šupić, J. Bowles, Quantum 4 (2020) 337.
[162] J.-D. Bancal, M. Navascués, V. Scarani, T. Vértesi, T.H. Yang, Phys. Rev. A 91 (2015) 022115.
[163] T.H. Yang, T. Vértesi, J.-D. Bancal, V. Scarani, M. Navascués, Phys. Rev. Lett. 113 (2014) 040401.
[164] N. Gigena, E. Panwar, G. Scala, M. Araújo, M. Farkas, A. Chaturvedi, Npj Quantum Inf. 11 (2025) http://dx.doi.org/10.1038/s41534-025-01029-6.
[165] K.T. Goh, J. Kaniewski, E. Wolfe, T. Vértesi, X. Wu, Y. Cai, Y.-C. Liang, V. Scarani, Phys. Rev. A 97 (2018) 022104.
[166] D.I. Kaiser, The Oxford Handbook of the History of Quantum Interpretations, Oxford University Press, 2022, https://academic.oup.com/book/0/chapter/364215131/chapter-ag-pdf/45613665/book_43513_section_364215131.ag.pdf.
[167] J. Larsson, J. Phys. A 47 (2014) 424003.
[168] I. Gerhardt, Q. Liu, A. Lamas-Linares, J. Skaar, V. Scarani, V. Makarov, C. Kurtsiefer, Phys. Rev. Lett. 107 (2011) 170404.
[169] P.H. Eberhard, P. Rosselet, Found. Phys. 25 (1995) 91.
[170] C. Branciard, Phys. Rev. A 83 (2011) 032123.
[171] N.S. Jones, L. Masanes, Phys. Rev. A 72 (2005) 052312.
[172] J. Barrett, S. Pironio, Phys. Rev. Lett. 95 (2005) 140401.
[173] J. Barrett, N. Linden, S. Massar, S. Pironio, S. Popescu, D. Roberts, Phys. Rev. A 71 (2005) 022101.
[174] J. Wilms, Y. Disser, G. Alber, I.C. Percival, Phys. Rev. A 78 (2008) 032116.
[175] M. Czechlewski, M. Pawłowski, Phys. Rev. A 97 (2018) 062123.
[176] A. Sauer, G. Alber, Cryptography 4 (2020) http://dx.doi.org/10.3390/cryptography4010002.
[177] P.M. Pearle, Phys. Rev. D 2 (1970) 1418.
[178] D.S. Tasca, S.P. Walborn, F. Toscano, P.H. Souto Ribeiro, Phys. Rev. A 80 (2009) 030101.
[179] P.H. Eberhard, Phys. Rev. A 47 (1993) R747.
[180] A. Garg, N.D. Mermin, Phys. Rev. D 35 (1987) 3831.
[181] S. Massar, Phys. Rev. A 65 (2002) 032121.
[182] T. Vértesi, S. Pironio, N. Brunner, Phys. Rev. Lett. 104 (2010) 060401.
[183] D. Collins, N. Gisin, J. Phys. A: Math. Gen. 37 (2004) 1775.
[184] S. Massar, S. Pironio, Phys. Rev. A 68 (2003) 062109.
[185] S. Massar, S. Pironio, J. Roland, B. Gisin, Phys. Rev. A 66 (2002) 052112.
[186] K.F. Pál, T. Vértesi, Phys. Rev. A 92 (2015) 052104.
[187] I. Márton, E. Bene, T. Vértesi, Phys. Rev. A 107 (2023) 022205.
[188] N. Miklin, A. Chaturvedi, M. Bourennane, M. Pawłowski, A. Cabello, Phys. Rev. Lett. 129 (2022) 230403.
[189] X.-M. Hu, C. Zhang, B.-H. Liu, Y. Guo, W.-B. Xing, C.-X. Huang, Y.-F. Huang, C.-F. Li, G.-C. Guo, Phys. Rev. Lett. 129 (2022) 060402.
[190] J. Bell, Comments At. Mol. Phys. 9 (1980) 121.
[191] M. Żukowski, A. Zeilinger, M.A. Horne, A.K. Ekert, Phys. Rev. Lett. 71 (1993) 4287.
[192] C. Simon, W.T.M. Irvine, Phys. Rev. Lett. 91 (2003) 110405.
[193] F. Marsili, V.B. Verma, J.A. Stern, S. Harrington, A.E. Lita, T. Gerrits, I. Vayshenker, B. Baek, M.D. Shaw, R.P. Mirin, S.W. Nam, Nat. Photonics 7 (2013) 210.
[194] L.K. Shalm, E. Meyer-Scott, B.G. Christensen, P. Bierhorst, M.A. Wayne, M.J. Stevens, T. Gerrits, S. Glancy, D.R. Hamel, M.S. Allman, K.J. Coakley, S.D. Dyer, C. Hodge, A.E. Lita, V.B. Verma, C. Lambrocco, E. Tortorici, A.L. Migdall, Y. Zhang, D.R. Kumor, W.H. Farr, F. Marsili, M.D. Shaw, J.A. Stern, C. Abellán, W. Amaya, V. Pruneri, T. Jennewein, M.W. Mitchell, P.G. Kwiat, J.C. Bienfang, R.P. Mirin, E. Knill, S.W. Nam, Phys. Rev. Lett. 115 (2015) 250402.
[195] M. Giustina, M.A.M. Versteegh, S. Wengerowsky, J. Handsteiner, A. Hochrainer, K. Phelan, F. Steinlechner, J. Kofler, J. Larsson, C. Abellan, W. Amaya, V. Pruneri, M.W. Mitchell, J. Beyer, T. Gerrits, A.E. Lita, L.K. Shalm, S.W. Nam, T. Scheidl, R. Ursin, B. Wittmann, A. Zeilinger, Phys. Rev. Lett. 115 (2015) 250401.
[196] G. Weihs, T. Jennewein, C. Simon, H. Weinfurter, A. Zeilinger, Phys. Rev. Lett. 81 (1998) 5039.
[197] M.A. Rowe, D. Kielpinski, V. Meyer, C.A. Sackett, W.M. Itano, C. Monroe, D.J. Wineland, Nature 409 (2001) 791.
[198] A. Aspect, J. Dalibard, G. Roger, Phys. Rev. Lett. 49 (1982) 1804.
[199] W. Tittel, J. Brendel, H. Zbinden, N. Gisin, Phys. Rev. Lett. 81 (1998) 3563.
[200] I. Marcikic, H. de Riedmatten, W. Tittel, H. Zbinden, M. Legré, N. Gisin, Phys. Rev. Lett. 93 (2004) 180502.
[201] J. Gallicchio, A.S. Friedman, D.I. Kaiser, Phys. Rev. Lett. 112 (2014) http://dx.doi.org/10.1103/physrevlett.112.110405.
[202] J. Handsteiner, A.S. Friedman, D. Rauch, J. Gallicchio, B. Liu, H. Hosp, J. Kofler, D. Bricher, M. Fink, C. Leung, A. Mark, H.T. Nguyen, I. Sanders, F. Steinlechner, R. Ursin, S. Wengerowsky, A.H. Guth, D.I. Kaiser, T. Scheidl, A. Zeilinger, Phys. Rev. Lett. 118 (2017) http://dx.doi.org/10.1103/physrevlett.118.060401.
[203] W. Tittel, J. Brendel, B. Gisin, T. Herzog, H. Zbinden, N. Gisin, Phys. Rev. A 57 (1998) 3229.
[204] N. Sangouard, C. Simon, H. de Riedmatten, N. Gisin, Rev. Modern Phys. 83 (2011) 33.
[205] J.R. Hance, S. Hossenfelder, Nat. Phys. 18 (2022) 1382.
[206] C.H. Brans, Internat. J. Theoret. Phys. 27 (1988) 219.
[207] W. Rosenfeld, D. Burchardt, R. Garthoff, K. Redeker, N. Ortegel, M. Rau, H. Weinfurter, Phys. Rev. Lett. 119 (2017) 010402.
[208] M.-H. Li, C. Wu, Y. Zhang, W.-Z. Liu, B. Bai, Y. Liu, W. Zhang, Q. Zhao, H. Li, Z. Wang, L. You, W.J. Munro, J. Yin, J. Zhang, C.-Z. Peng, X. Ma, Q. Zhang, J. Fan, J.-W. Pan, Phys. Rev. Lett. 121 (2018) 080404.
[209] P.J. Cavalcanti, J.H. Selby, A.B. Sainz, Phys. Rev. A 109 (2024) 042211.
[210] G. Chiribella, G.M. D'Ariano, P. Perinotti, Phys. Rev. A 84 (2011) 012311.
[211] P.J. Cavalcanti, J.H. Selby, J. Sikora, T.D. Galley, A.B. Sainz, Npj Quantum Inf. 8 (2022) http://dx.doi.org/10.1038/s41534-022-00574-8.
[212] D. Cavalcanti, P. Skrzypczyk, G.H. Aguilar, R.V. Nery, P.S. Ribeiro, S.P. Walborn, Nat. Commun. 6 (2015) 7941.
[213] A. Máttar, P. Skrzypczyk, G.H. Aguilar, R.V. Nery, P.H.S. Ribeiro, S.P. Walborn, D. Cavalcanti, Quantum Sci. Technol. 2 (2017) 015011.
[214] M. Revzen, P.A. Mello, A. Mann, L.M. Johansen, Phys. Rev. A 71 (2005) 022103.
[215] Z. Ou, S. Pereira, H. Kimble, Appl. Phys. B 55 (1992) 265.
[216] V. Händchen, T. Eberle, S. Steinlechner, A. Samblowski, T. Franz, R.F. Werner, R. Schnabel, Nat. Photonics 6 (2012) 596.
[217] S.P. Walborn, A. Salles, R.M. Gomes, F. Toscano, P.H. Souto Ribeiro, Phys. Rev. Lett. 106 (2011) 130402.
[218] D.H. Smith, G. Gillett, M.P. de Almeida, C. Branciard, A. Fedrizzi, T.J. Weinhold, A. Lita, B. Calkins, T. Gerrits, H.M. Wiseman, S.W. Nam, A.G. White, Nat. Commun. 3 (2012) 625.
[219] B. Wittmann, S. Ramelow, F. Steinlechner, N.K. Langford, N. Brunner, H.M. Wiseman, R. Ursin, A. Zeilinger, New J. Phys. 14 (2012) 053030.
[220] A.J. Bennet, D.A. Evans, D.J. Saunders, C. Branciard, E.G. Cavalcanti, H.M. Wiseman, G.J. Pryde, Phys. Rev. X 2 (2012) 031003.

[221] D. Cavalcanti, P. Skrzypczyk, Rep. Progr. Phys. 80 (2016) 024001.
[222] R. Uola, A.C.S. Costa, H.C. Nguyen, O. Gühne, Rev. Modern Phys. 92 (2020) 015001.
[223] A. Peres, Phys. Lett. A 151 (1990) 107.
[224] N.D. Mermin, Phys. Rev. Lett. 65 (1990) 3373.
[225] K. Horodecki, M. Horodecki, P. Horodecki, R. Horodecki, M. Pawlowski, M. Bourennane, Contextuality offers device-independent security, 2010.
[226] M.F. Pusey, Phys. Rev. Lett. 113 (2014) http://dx.doi.org/10.1103/physrevlett.113.200401.
[227] L. Catani, M. Leifer, G. Scala, D. Schmid, R.W. Spekkens, Phys. Rev. Lett. 129 (2022) http://dx.doi.org/10.1103/physrevlett.129.240401.
[228] L. Catani, M. Leifer, G. Scala, D. Schmid, R.W. Spekkens, Phys. Rev. A 108 (2023) http://dx.doi.org/10.1103/physreva.108.022207.
[229] R. Wagner, R.S. Barbosa, E.F. Galvão, Phys. Rev. A 109 (2024) http://dx.doi.org/10.1103/physreva.109.032220.
[230] G. Scala, S.A. Ghoreishi, M. Pawłowski, Phys. Rev. A 109 (2024) http://dx.doi.org/10.1103/physreva.109.022230.
[231] D.R. Arvidsson-Shukur, W.F. Braasch Jr., S. De Bievre, J. Dressel, A.N. Jordan, C. Langrenez, M. Lostaglio, J.S. Lundeen, N.Y. Halpern, arXiv preprint http://dx.doi.org/10.48550/arXiv.2403.18899 2403.18899.
[232] P. Janotta, H. Hinrichsen, J. Phys. A 47 (2014) 323001.
[233] M.D. Mazurek, M.F. Pusey, K.J. Resch, R.W. Spekkens, PRX Quantum 2 (2021) http://dx.doi.org/10.1103/prxquantum.2.020302.
[234] R. Canetti, J. Cryptology 13 (2000) 143.
[235] R. Canetti, Proceedings 42nd IEEE Symposium on Foundations of Computer Science, IEEE, 2001, pp. 136–145.
[236] M. Ben-Or, D. Mayers, General security definition and composability for quantum & amp; classical protocols, 2004.
[237] M. Ben-Or, M. Horodecki, D.W. Leung, D. Mayers, J. Oppenheim, The universal composable security of quantum key distribution, in: Theory of Cryptography, Springer Berlin Heidelberg, 2005, pp. 386–406.
[238] R. Renner, R. König, Universally composable privacy amplification against quantum adversaries, in: Theory of Cryptography, Springer Berlin Heidelberg, 2005, pp. 407–425.
[239] R. Renner, Int. J. Quantum Inf. 6 (2008) 1.
[240] L. Masanes, R. Renner, M. Christandl, A. Winter, J. Barrett, IEEE Trans. Inform. Theory 60 (2014) 4973.
[241] K. Marshall, C. Weedbrook, Phys. Rev. A 90 (2014) 042311.
[242] L. Masanes, Phys. Rev. Lett. 102 (2009) http://dx.doi.org/10.1103/physrevlett.102.140501.
[243] M. Ho, P. Sekatski, E.-Z. Tan, R. Renner, J.-D. Bancal, N. Sangouard, Phys. Rev. Lett. 124 (2020) 230502.
[244] S.L. Braunstein, C.M. Caves, Ann. Physics 202 (1990) 22.
[245] A. Kent, Phys. Rev. A 72 (2005) 012108.
[246] J. Barrett, A. Kent, S. Pironio, Phys. Rev. Lett. 97 (2006) 170409.
[247] A. Valentini, Phys. Lett. A 297 (2002) 273.
[248] S. Popescu, D. Rohrlich, Found. Phys. 24 (1994) 379.
[249] B.S. Tsirelson, Hadronic J. Suppl. 8 (1993) 329.
[250] N.J. Cerf, N. Gisin, S. Massar, S. Popescu, Phys. Rev. Lett. 94 (2005) http://dx.doi.org/10.1103/physrevlett.94.220403.
[251] L. Wooltorton, P. Brown, R. Colbeck, Phys. Rev. Lett. 132 (2024) 210802.
[252] H.F. Chau, Phys. Rev. A 66 (2002) 060302.
[253] D. Gottesman, H.-K. Lo, Inf. Theory IEEE Trans. 49 (2003) 457.
[254] X. Ma, 2008, arXiv:0808.1385 [quant-ph].
[255] U.M. Maurer, S. Wolf, IEEE Trans. Inform. Theory 45 (1999) 499.
[256] H. Tyagi, IEEE Trans. Inform. Theory 59 (2013) 5627.
[257] L. Mišta, R. Tatham, Phys. Rev. A 91 (2015) 062313.
[258] A.B. Khesin, A. Tung, K. Vedula, New properties of intrinsic information and their relation to bound secrecy, 2023.
[259] L. Masanes, A. Acin, N. Gisin, Phys. Rev. A 73 (2006) 012112.
[260] J. Jogenfors, J. Larsson, Phys. Rev. A 96 (2017) 022102.
[261] J.D. Franson, Phys. Rev. Lett. 62 (1989) 2205.
[262] S. Aerts, P. Kwiat, J. Larsson, M. Zukowski, Phys. Rev. Lett. 83 (1999) 2872.
[263] J. Jogenfors, J. Larsson, J. Phys. A 47 (2014) 424032.
[264] J. Jogenfors, A.M. Elhassan, J. Ahrens, M. Bourennane, J. Larsson, Sci. Adv. 1 (2015) http://dx.doi.org/10.1126/sciadv.1500793.
[265] M. Tomasin, E. Mantoan, J. Jogenfors, G. Vallone, J. Larsson, P. Villoresi, Phys. Rev. A 95 (2017) 032107.
[266] B. Kraus, N. Gisin, R. Renner, Phys. Rev. Lett. 95 (2005) 080501.
[267] J. Kofler, T. Paterek, C. Brukner, Phys. Rev. A 73 (2006) http://dx.doi.org/10.1103/physreva.73.022104.
[268] X. Ma, N. Lutkenhaus, Quantum Inf. Process. 12 (2012) 203.
[269] M. McKague, New J. Phys. 11 (2009) 103037.
[270] M. Paternostro, H. Jeong, T.C. Ralph, Phys. Rev. A 79 (2009) 012101.
[271] D. Gottesman, A. Kitaev, J. Preskill, Phys. Rev. A 64 (2001) 012310.
[272] T. Vértesi, K.F. Pál, Phys. Rev. A 79 (2009) http://dx.doi.org/10.1103/physreva.79.042106.
[273] J. Briët, H. Buhrman, B. Toner, arXiv preprint 0901.2009.
[274] N. Brunner, S. Pironio, A. Acin, N. Gisin, A.A. Méthot, V. Scarani, Phys. Rev. Lett. 100 (2008) http://dx.doi.org/10.1103/physrevlett.100.210503.
[275] R. Jain, C.A. Miller, Y. Shi, IEEE Trans. Inform. Theory 66 (2020) 5567.
[276] R. Horodecki, P. Horodecki, M. Horodecki, Phys. Lett. A 200 (1995) 340.
[277] P. Brown, H. Fawzi, O. Fawzi, Quantum 8 (2024) 1445.
[278] M. Sandfuchs, R. Wolf, 2023, arXiv:2306.07364 [quant-ph].
[279] A. Cabello, Phys. Rev. Lett. 87 (2001) 010403.
[280] N. Gisin, A.A. Méthot, V. Scarani, Int. J. Quantum Inf. 05 (2007) 525.
[281] E. Cervero-Martín, M. Tomamichel, Quantum 9 (2025) 1652.
[282] M.F. Pusey, J. Opt. Soc. Am. B 32 (2015) A56.
[283] J.R. Gonzales-Ureta, A. Predojević, A. Cabello, Phys. Rev. A 103 (2021) 052436.
[284] N. Brunner, N. Gisin, Phys. Lett. A 372 (2008) 3162.
[285] A. Acin, V. Scarani, M.M. Wolf, Phys. Rev. A 66 (2002) 042323.
[286] D. Collins, N. Gisin, N. Linden, S. Massar, S. Popescu, Phys. Rev. Lett. 88 (2002) 040404.
[287] M. Żukowski, Č. Brukner, Phys. Rev. Lett. 88 (2002) 210401.
[288] M. Karczewski, G. Scala, A. Mandarino, A.B. Sainz, M. Żukowski, J. Phys. A 55 (2022) 384011.
[289] J. Ho, G. Moreno, S. Brito, F. Graffitti, C.L. Morrison, R. Nery, A. Pickston, M. Proietti, R. Rabelo, A. Fedrizzi, et al., Npj Quantum Inf. 8 (2022) 13.
[290] R. Jain, S. Kundu, 2021 IEEE 62nd Annual Symposium on Foundations of Computer Science (FOCS), IEEE, 2022, pp. 1285–1295.
[291] https://apps.dtic.mil/sti/tr/pdf/ADB811200.pdf.

[292] A. Fine, Phys. Rev. Lett. 48 (1982) 291.
[293] R. Colbeck, 2009, http://dx.doi.org/10.48550/arXiv.0911.3814, arXiv preprint arXiv:0911.3814.
[294] R. Colbeck, A. Kent, J. Phys. A 44 (2011) 095305.
[295] C.A. Miller, Y. Shi, J. ACM 63 (2016) 1.
[296] Y. Liu, Q. Zhao, M.-H. Li, J.-Y. Guan, Y. Zhang, B. Bai, W. Zhang, W.-Z. Liu, C. Wu, X. Yuan, H. Li, W.J. Munro, Z. Wang, L. You, J. Zhang, X. Ma, J. Fan, Q. Zhang, J.-W. Pan, Nat. 562 (2018) 548.
[297] P. Bierhorst, E. Knill, S. Glancy, Y. Zhang, A. Mink, S. Jordan, A. Rommal, Y.-K. Liu, B. Christensen, S.W. Nam, M.J. Stevens, L.K. Shalm, Nat. 556 (2018) 223.
[298] M.-H. Li, X. Zhang, W.-Z. Liu, S.-R. Zhao, B. Bai, Y. Liu, Q. Zhao, Y. Peng, J. Zhang, Y. Zhang, W. Munro, X. Ma, Q. Zhang, J. Fan, J.-W. Pan, Phys. Rev. Lett. 126 (2021) 050503.
[299] W.-Z. Liu, M.-H. Li, S. Ragy, S.-R. Zhao, B. Bai, Y. Liu, P.J. Brown, J. Zhang, R. Colbeck, J. Fan, Q. Zhang, J.-W. Pan, Nat. Phys. 17 (2021) 448.
[300] L.K. Shalm, Y. Zhang, J.C. Bienfang, C. Schlager, M.J. Stevens, M.D. Mazurek, C. Abellán, W. Amaya, M.W. Mitchell, M.A. Alhejji, H. Fu, J. Ornstein, R.P. Mirin, S.W. Nam, E. Knill, Nat. Phys. 17 (2021) 452.
[301] S. Storz, J. Schär, A. Kulikov, P. Magnard, P. Kurpiers, J. Lütolf, T. Walter, A. Copetudo, K. Reuer, A. Akin, J.-C. Besse, M. Gabureac, G.J. Norris, A. Rosario, F. Martin, J. Martinez, W. Amaya, M.W. Mitchell, C. Abellan, J.-D. Bancal, N. Sangouard, B. Royer, A. Blais, A. Wallraff, Nat. 617 (2023) 265.
[302] V. Mongia, A. Kumar, S. Prabhakar, A. Banerji, R. Singh, Phys. Lett. A 526 (2024) 129954.
[303] M. Liu, R. Shaydulin, P. Niroula, M. DeCross, S.-H. Hung, W.Y. Kon, E. Cervero-Martín, K. Chakraborty, O. Amer, S. Aaronson, A. Acharya, Y. Alexeev, K.J. Berg, S. Chakrabarti, F.J. Curchod, J.M. Dreiling, N. Erickson, C. Foltz, M. Foss-Feig, D. Hayes, T.S. Humble, N. Kumar, J. Larson, D. Lykov, M. Mills, S.A. Moses, B. Neyenhuis, S. Eloul, P. Siegfried, J. Walker, C. Lim, M. Pistoia, Nat. 640 (2025) 343.
[304] O. Amer, S. Chakrabarti, K. Chakraborty, S. Eloul, N. Kumar, C. Lim, M. Liu, P. Niroula, Y. Satsangi, R. Shaydulin, M. Pistoia, Nat. Rev. Phys. (2025) http://dx.doi.org/10.1038/s42254-025-00845-1.
[305] M. Hillery, V. Buž, A. Berthiaume, Phys. Rev. A 59 (1999) 1829.
[306] S. Roy, S. Mukhopadhyay, Phys. Rev. A 100 (2019) 012319.
[307] M.G.M. Moreno, S. Brito, R.V. Nery, R. Chaves, Phys. Rev. A 101 (2020) 052339.
[308] G. Svetlichny, Phys. Rev. D 35 (1987) 3066.
[309] Q. Zhang, W. Zhong, M.-M. Du, S.-T. Shen, X.-Y. Li, A.-L. Zhang, L. Zhou, Y.-B. Sheng, Phys. Rev. A 110 (2024) 042403.
[310] Q. Zhang, J.-W. Ying, Z.-J. Wang, W. Zhong, M.-M. Du, S.-T. Shen, X.-Y. Li, A.-L. Zhang, S.-P. Gu, X.-F. Wang, L. Zhou, Y.-B. Sheng, Phys. Rev. A 111 (2025) 012603.
[311] G.L. Long, X.S. Liu, Phys. Rev. A 65 (2002) 032302.
[312] L. Zhou, Y.-B. Sheng, G.-L. Long, Sci. Bull. 65 (2020) 12.
[313] L. Zhou, Y.-B. Sheng, Sci. China Phys. Mech. Astron. 65 (2022) http://dx.doi.org/10.1007/s11433-021-1863-9.
[314] L. Zhou, B.-W. Xu, W. Zhong, Y.-B. Sheng, Phys. Rev. Appl. 19 (2023) 014036.
[315] H. Zeng, M.-M. Du, W. Zhong, L. Zhou, Y.-B. Sheng, Fundam. Res. 4 (2024) 851.
[316] P. Roy, S. Bera, S. Gupta, A.S. Majumdar, Quantum Inf. Process. 23 (2024) http://dx.doi.org/10.1007/s11128-024-04397-8.
[317] F. Dupuis, O. Fawzi, IEEE Trans. Inform. Theory 65 (2019) 7596.
[318] R. Bhavsar, S. Ragy, R. Colbeck, New J. Phys. 25 (2023) 093035.
[319] T. Metger, R. Renner, Nat. Commun. 14 (2023) http://dx.doi.org/10.1038/s41467-023-40920-8.
[320] T. Metger, O. Fawzi, D. Sutter, R. Renner, 2022 IEEE 63rd Annual Symposium on Foundations of Computer Science (FOCS), IEEE, 2022.
[321] R. Arnon-Friedman, R. Renner, T. Vidick, SIAM J. Comput. 48 (2019) 181.
[322] M. Tomamichel, R. Colbeck, R. Renner, IEEE Trans. Inform. Theory 55 (2009) 5840.
[323] A. De, C. Portmann, T. Vidick, R. Renner, SIAM J. Comput. 41 (2012) 915.
[324] Y. Zhang, E. Knill, P. Bierhorst, Phys. Rev. A 98 (2018) 040304.
[325] Y. Zhang, H. Fu, E. Knill, Phys. Rev. Res. 2 (2020) 013016.
[326] X. Zhang, P. Zeng, T. Ye, H.-K. Lo, X. Ma, Phys. Rev. Lett. 131 (2023) 140801.
[327] H.-K. Lo, H.F. Chau, Sci. 283 (1999) 2050.
[328] P.W. Shor, J. Preskill, Phys. Rev. Lett. 85 (2000) 441.
[329] M. Koashi, New J. Phys. 11 (2009) 045018.
[330] T. Vidick, Parallel diqkd from parallel repetition, 2017.
[331] M. Masini, S. Pironio, E. Woodhead, Quantum 6 (2022) 843.
[332] M. Berta, M. Christandl, R. Colbeck, J.M. Renes, R. Renner, Nat. Phys. 6 (2010) 659.
[333] E. Woodhead, Phys. Rev. A 90 (2014) 022306.
[334] T.A. Hahn, A. Philip, E.Y.Z. Tan, P. Brown, Analytic rényi entropy bounds for device-independent cryptography, 2025.
[335] J. Ribeiro, G. Murta, S. Wehner, Phys. Rev. A 97 (2018) 022307.
[336] F. Grasselli, G. Murta, H. Kampermann, D. Bruß, PRX Quantum 2 (2021) 010308.
[337] N.D. Mermin, Phys. Rev. Lett. 65 (1990) 1838.
[338] M. Ardehali, Phys. Rev. A 46 (1992) 5375.
[339] A.V. Belinskiĭ, D.N. Klyshko, Phys.-Usp. 36 (1993) 653.
[340] F. Grasselli, G. Murta, H. Kampermann, D. Bruß, Quantum 7 (2023) 980.
[341] P.J. Coles, E.M. Metodiev, N. Lütkenhaus, Nat. Commun. 7 (2016) 11712.
[342] A. Winick, N. Lütkenhaus, P.J. Coles, Quantum 2 (2018) 77.
[343] M. Navascués, T. Vértesi, Phys. Rev. Lett. 115 (2015) 020501.
[344] OpenQKD Security, Open quantum key distribution security, 2025, https://openqkdsecurity.wordpress.com. (Accessed 24 January 2025).
[345] J.-D. Bancal, L. Sheridan, V. Scarani, New J. Phys. 16 (2014) 033011.
[346] O. Nieto-Silleras, S. Pironio, J. Silman, New J. Phys. 16 (2014) 013035.
[347] E.Y.-Z. Tan, R. Schwonnek, K.T. Goh, I.W. Primaatmaja, C.C.-W. Lim, Npj Quantum Inf. 7 (2021) http://dx.doi.org/10.1038/s41534-021-00494-z.
[348] M. Müller-Lennert, F. Dupuis, O. Szehr, S. Fehr, M. Tomamichel, J. Math. Phys. 54 (2013) http://dx.doi.org/10.1063/1.4838856.
[349] M. Araújo, M. Huber, M. Navascués, M. Pivoluska, A. Tavakoli, Quantum 7 (2023) 1019.
[350] R. Arnon-Friedman, F. Leditzky, IEEE Trans. Inform. Theory 67 (2021) 6606.
[351] M. Winczewski, T. Das, K. Horodecki, Phys. Rev. A 106 (2022) 052612.
[352] M. Christandl, R. Ferrara, K. Horodecki, Phys. Rev. Lett. 126 (2021) 160501.
[353] E. Kaur, K. Horodecki, S. Das, Phys. Rev. Appl. 18 (2022) 054033.
[354] V. Vedral, M.B. Plenio, M.A. Rippin, P.L. Knight, Phys. Rev. Lett. 78 (1997) 2275.
[355] U. Maurer, S. Wolf, Proceedings of the IEEE International Symposium on Information Theory (ISIT), IEEE, Ulm, Germany, 1997, p. 88.
[356] K. Łukanowski, M. Balanzó-Juandó, M. Farkas, A. Acín, J. Kołodyński, Quantum 7 (2023) 1199.

[357] Y.-Z. Zhang, Y.-Z. Zhen, F. Xu, New J. Phys. 24 (2022) 113045.
[358] T. Lunghi, J.B. Brask, C.C.W. Lim, Q. Lavigne, J. Bowles, A. Martin, H. Zbinden, N. Brunner, Phys. Rev. Lett. 114 (2015) 150501.
[359] Z. Cao, H. Zhou, X. Ma, New J. Phys. 17 (2015) 125011.
[360] C.H. Bennett, S.J. Wiesner, Phys. Rev. Lett. 69 (1992) 2881.
[361] V. Scarani, A. Acin, G. Ribordy, N. Gisin, Phys. Rev. Lett. 92 (2004) 057901.
[362] A. Chaturvedi, M. Ray, R. Veynar, M. Pawłowski, Quantum Inf. Process. 17 (2018) http://dx.doi.org/10.1007/s11128-018-1892-z.
[363] H.-W. Li, P. Mironowicz, M. Pawłowski, Z.-Q. Yin, Y.-C. Wu, S. Wang, W. Chen, H.-G. Hu, G.-C. Guo, Z.-F. Han, Phys. Rev. A 87 (2013) 020302.
[364] E. Woodhead, S. Pironio, Phys. Rev. Lett. 115 (2015) 150501.
[365] T.V. Himbeeck, E. Woodhead, N.J. Cerf, R. García-Patrón, S. Pironio, Quantum 1 (2017) 33.
[366] S. Das, S. Bäuml, M. Winczewski, K. Horodecki, Phys. Rev. X 11 (2021) 041016.
[367] F.-Y. Lu, P. Ye, Z.-H. Wang, S. Wang, Z.-Q. Yin, R. Wang, X.-J. Huang, W. Chen, D.-Y. He, G.-J. Fan-Yuan, G.-C. Guo, Z.-F. Han, Optica 10 (2023) 520.
[368] K. Tamaki, H.-K. Lo, C.-H.F. Fung, B. Qi, Phys. Rev. A 85 (2012) 042307.
[369] I.W. Primaatmaja, E. Lavie, K.T. Goh, C. Wang, C.C.W. Lim, Phys. Rev. A 99 (2019) 062332.
[370] Y. Zhu, C.-M. Zhang, Opt. Express 29 (2021) 30168.
[371] J.E. Bourassa, A. Gnanapandithan, L. Qian, H.-K. Lo, Phys. Rev. A 106 (2022) 062618.
[372] X. Ma, M. Razavi, Phys. Rev. A 86 (2012) 062319.
[373] F. Xu, M. Curty, B. Qi, H.-K. Lo, New J. Phys. 15 (2013) 113007.
[374] Q. Wang, X.-B. Wang, Sci. Rep. 4 (2014) http://dx.doi.org/10.1038/srep04612.
[375] W. Li, S. Zhao, Phys. Rev. A 106 (2022) 042445.
[376] X. Ma, C.-H.F. Fung, M. Razavi, Phys. Rev. A 86 (2012) 052305.
[377] F.-Y. Lu, Z.-H. Wang, Z.-Q. Yin, S. Wang, R. Wang, G.-J. Fan-Yuan, X.-J. Huang, D.-Y. He, W. Chen, Z. Zhou, G.-C. Guo, Z.-F. Han, Optica 9 (2022) 886.
[378] Z.-Q. Yin, C.-H.F. Fung, X. Ma, C.-M. Zhang, H.-W. Li, W. Chen, S. Wang, G.-C. Guo, Z.-F. Han, Phys. Rev. A 88 (2013) 062322.
[379] Z.-Q. Yin, C.-H.F. Fung, X. Ma, C.-M. Zhang, H.-W. Li, W. Chen, S. Wang, G.-C. Guo, Z.-F. Han, Phys. Rev. A 90 (2014) 052319.
[380] W.-Y. Hwang, H.-Y. Su, J. Bae, Phys. Rev. A 95 (2017) 062313.
[381] X. Zhou, C. Zhang, G. Guo, Q. Wang, IEEE Photonics J. 11 (2019) 1.
[382] G.-D. Kang, Q.-P. Zhou, M.-F. Fang, Quantum Inf. Process. 19 (2019) http://dx.doi.org/10.1007/s11128-019-2494-0.
[383] G. Kang, X. Wang, J. Wen, C. Zeng, G. Zhou, J. Phys.: Conf. Ser. 1646 (2020) 012010.
[384] H.-W. Li, Z.-Q. Yin, W. Chen, S. Wang, G.-C. Guo, Z.-F. Han, Phys. Rev. A 89 (2014) 032302.
[385] C.-M. Zhang, M. Li, H.-W. Li, Z.-Q. Yin, D. Wang, J.-Z. Huang, Y.-G. Han, M.-L. Xu, W. Chen, S. Wang, P. Treeviriyanupab, G.-C. Guo, Z.-F. Han, Phys. Rev. A 90 (2014) 034302.
[386] T.-T. Song, Q.-Y. Wen, F.-Z. Guo, X.-Q. Tan, Phys. Rev. A 86 (2012) 022332.
[387] M. Curty, F. Xu, W. Cui, C.C.W. Lim, K. Tamaki, H.-K. Lo, Nat. Commun. 5 (2014) 3732.
[388] G. Brassard, N. Lütkenhaus, T. Mor, B.C. Sanders, Phys. Rev. Lett. 85 (2000) 1330.
[389] W.-Y. Hwang, Phys. Rev. Lett. 91 (2003) 057901.
[390] H.-K. Lo, X. Ma, K. Chen, Phys. Rev. Lett. 94 (2005) 230504.
[391] X.-B. Wang, Phys. Rev. A 87 (2013) 012320.
[392] S.-H. Sun, M. Gao, C.-Y. Li, L.-M. Liang, Phys. Rev. A 87 (2013) 052329.
[393] M. Li, C.-M. Zhang, Z.-Q. Yin, W. Chen, S. Wang, G.-C. Guo, Z.-F. Han, Opt. Lett. 39 (2014) 880.
[394] J.-R. Zhu, F. Zhu, X.-Y. Zhou, Q. Wang, Quantum Inf. Process. 15 (2016) 3799.
[395] H.-J. Ding, C.-C. Mao, C.-M. Zhang, Q. Wang, Quantum Inf. Process. 17 (2018) http://dx.doi.org/10.1007/s11128-018-2026-3.
[396] C.-C. Mao, C.-H. Zhang, C.-M. Zhang, Q. Wang, Quantum Inf. Process. 18 (2019) http://dx.doi.org/10.1007/s11128-019-2404-5.
[397] Z.-W. Yu, Y.-H. Zhou, X.-B. Wang, Phys. Rev. A 88 (2013) 062339.
[398] Q. Wang, X.-B. Wang, Phys. Rev. A 88 (2013) 052332.
[399] C.-H. Zhang, C.-M. Zhang, G.-C. Guo, Q. Wang, Opt. Express 26 (2018) 4219.
[400] C. Zhou, W.-S. Bao, W. Chen, H.-W. Li, Z.-Q. Yin, Y. Wang, Z.-F. Han, Phys. Rev. A 88 (2013) 052333.
[401] X.-H. Zhan, Z.-Q. Zhong, S. Wang, Z.-Q. Yin, W. Chen, D.-Y. He, G.-C. Guo, Z.-F. Han, Phys. Rev. Appl. 20 (2023) 034069.
[402] F. Xu, H. Xu, H.-K. Lo, Phys. Rev. A 89 (2014) 052333.
[403] Z.-W. Yu, Y.-H. Zhou, X.-B. Wang, Phys. Rev. A 91 (2015) 032318.
[404] C. Jiang, Z.-W. Yu, X.-L. Hu, X.-B. Wang, Phys. Rev. A 103 (2021) 012402.
[405] Y.-M. Xie, Y.-S. Lu, C.-X. Weng, X.-Y. Cao, Z.-Y. Jia, Y. Bao, Y. Wang, Y. Fu, H.-L. Yin, Z.-B. Chen, PRX Quantum 3 (2022) 020315.
[406] S. Abruzzo, H. Kampermann, D. Bruß, Phys. Rev. A 89 (2014) 012301.
[407] P. Zeng, H. Zhou, W. Wu, X. Ma, Nat. Commun. 13 (2022).
[408] X. Liu, D. Luo, Z. Zhang, K. Wei, Phys. Rev. A 107 (2023) 062613.
[409] Z.-H. Wang, R. Wang, Z.-Q. Yin, S. Wang, F.-Y. Lu, W. Chen, D.-Y. He, G.-C. Guo, Z.-F. Han, Commun. Phys. 6 (2023).
[410] Z. Lu, G. Wang, C. Li, Z. Cao, Phys. Rev. A 109 (2024) 012401.
[411] Z. Li, T. Dou, Y. Xie, W. Kong, N. Chen, Q. Zhao, W. Gao, P. Han, Y. Hao, H. Ma, Y. Liu, J. Tang, New J. Phys. 26 (2024) 093011.
[412] X.-Y. Zhou, J.-R. Hu, C.-H. Zhang, Q. Wang, Quantum Inf. Process. 24 (2025).
[413] W. Wang, F. Xu, H.-K. Lo, Phys. Rev. X 9 (2019) 041012.
[414] Z.-Q. Yin, S. Wang, W. Chen, H.-W. Li, G.-C. Guo, Z.-F. Han, Quantum Inf. Process. 13 (2014) 1237.
[415] Y. Zhou, H.-J. Ding, J.-Y. Liu, C.-H. Zhang, X.-Y. Zhou, Q. Wang, Phys. Rev. Appl. 23 (2025) 024007.
[416] H. Chau, C. Wong, Q. Wang, T. Huang, 2016, http://dx.doi.org/10.48550/arXiv.1608.08329, arXiv preprint arXiv:1608.08329.
[417] T. Sasaki, Y. Yamamoto, M. Koashi, Nature 509 (2014) 475.
[418] H. Chau, Phys. Rev. A 92 (2015) 062324.
[419] W.-Y. Hwang, H.-Y. Su, J. Bae, Sci. Rep. 6 (2016) 30036.
[420] Y. Jo, W. Son, Phys. Rev. A 94 (2016) 052316.
[421] H. Bechmann-Pasquinucci, W. Tittel, Phys. Rev. A 61 (2000) 062308.
[422] Y. Jo, K. Bae, W. Son, Sci. Rep. 9 (2019) 687.
[423] C. Sekga, M. Mafu, M. Senekane, Sci. Rep. 13 (2023).
[424] L. Dellantonio, A.S. Sørensen, D. Bacco, Phys. Rev. A 98 (2018) 062301.
[425] Z.-X. Cui, W. Zhong, L. Zhou, Y.-B. Sheng, Sci. China Phys. Mech. Astron. 62 (2019).
[426] Y.-F. Yan, L. Zhou, W. Zhong, Y.-B. Sheng, Front. Phys. 16 (2020).
[427] Y. Li, Z. Sun, P. Li, Z. Li, J. Wang, L. Zhou, H. Ma, Quantum Inf. Process. 22 (2023).
[428] Ö. Erkılıç, L. Conlon, B. Shajilal, S. Kish, S. Tserkis, Y.-S. Kim, P.K. Lam, S.M. Assad, Npj Quantum Inf. 9 (2023).

[429] S. Pirandola, R. Laurenza, C. Ottaviani, L. Banchi, Nat. Commun. 8 (2017).
[430] C. Lupo, C. Ottaviani, P. Papanastasiou, S. Pirandola, Phys. Rev. A 97 (2018) 052327.
[431] Z. Li, Y.-C. Zhang, F. Xu, X. Peng, H. Guo, Phys. Rev. A 89 (2014) 052301.
[432] X.-C. Ma, S.-H. Sun, M.-S. Jiang, M. Gui, L.-M. Liang, Phys. Rev. A 89 (2014) 042335.
[433] R. García-Patrón, N.J. Cerf, Phys. Rev. Lett. 97 (2006) 190503.
[434] Y.-C. Zhang, Z. Li, S. Yu, W. Gu, X. Peng, H. Guo, Phys. Rev. A 90 (2014) 052325.
[435] Z. Chen, Y. Zhang, G. Wang, Z. Li, H. Guo, Phys. Rev. A 98 (2018) 012314.
[436] H.-X. Ma, P. Huang, D.-Y. Bai, T. Wang, S.-Y. Wang, W.-S. Bao, G.-H. Zeng, Phys. Rev. A 99 (2019) 022322.
[437] W. Zhao, R. Shi, J. Shi, X. Ruan, Y. Guo, D. Huang, Phys. Rev. A 102 (2020) 022621.
[438] K.N. Wilkinson, P. Papanastasiou, C. Ottaviani, T. Gehring, S. Pirandola, Phys. Rev. Res. 2 (2020) 033424.
[439] W. Ye, H. Zhong, X. Wu, L. Hu, Y. Guo, Quantum Inf. Process. 19 (2020) 1.
[440] W. Ye, Y. Guo, H. Zhang, H. Zhong, Y. Mao, L. Hu, J. Phys. B: At. Mol. Opt. Phys. 54 (2021) 045501.
[441] L. Kong, W. Liu, F. Jing, Z.-K. Zhang, J. Qi, C. He, Chin. Phys. B 31 (2022) 090304.
[442] C. Ding, Y. Wang, W. Zhang, Z. Li, Z. Wu, H. Zhang, Internat. J. Theoret. Phys. 60 (2021) 1361.
[443] H.-X. Ma, P. Huang, T. Wang, S.-Y. Wang, W.-S. Bao, G.-H. Zeng, Phys. Lett. A 383 (2019) 126005.
[444] Q. Liao, Y. Wang, D. Huang, Y. Guo, Opt. Express 26 (2018) 19907.
[445] J. Zhou, Y. Feng, J. Shi, R. Shi, Ann. Phys., Lpz 535 (2023) 2200614.
[446] L. Huang, X. Wang, Z. Chen, Y. Sun, S. Yu, H. Guo, Phys. Rev. Appl. 19 (2023).
[447] Y. Zheng, H. Shi, W. Pan, Q. Wang, J. Mao, Entropy 24 (2022) 127.
[448] Z. Li, X. Wang, Z. Chen, T. Shen, S. Yu, H. Guo, Quantum Inf. Process. 22 (2023).
[449] Y. Wang, X. Wang, J. Li, D. Huang, L. Zhang, Y. Guo, Phys. Lett. A 382 (2018) 1149.
[450] H.-L. Yin, W. Zhu, Y. Fu, Sci. Rep. 9 (2019) 49.
[451] D. Bai, P. Huang, Y. Zhu, H. Ma, T. Xiao, T. Wang, G. Zeng, Quantum Inf. Process. 19 (2020) 1.
[452] M. Boyer, D. Kenigsberg, T. Mor, Phys. Rev. Lett. 99 (2007) 140501.
[453] Y.-H. Zhou, S.-F. Qin, W.-M. Shi, Y.-G. Yang, Quantum Inf. Process. 21 (2022).
[454] P. Papanastasiou, C. Ottaviani, S. Pirandola, Phys. Rev. A 96 (2017) 042332.
[455] X. Zhang, Y. Zhang, Y. Zhao, X. Wang, S. Yu, H. Guo, Phys. Rev. A 96 (2017) 042334.
[456] A. Leverrier, Phys. Rev. Lett. 118 (2017) 200501.
[457] C. Lupo, C. Ottaviani, P. Papanastasiou, S. Pirandola, Phys. Rev. Lett. 120 (2018) 220505.
[458] X. Wu, Y. Wang, S. Li, W. Zhang, D. Huang, Y. Guo, Quantum Inf. Process. 18 (2019) 1.
[459] X.-D. Wu, Y.-J. Wang, D. Huang, Y. Guo, Front. Phys. 15 (2020) 1.
[460] P. Huang, G. He, J. Fang, G. Zeng, Phys. Rev. A 87 (2013) 012317.
[461] Y. Guo, Q. Liao, Y. Wang, D. Huang, P. Huang, G. Zeng, Phys. Rev. A 95 (2017) 032304.
[462] Y. Zhao, Y. Zhang, B. Xu, S. Yu, H. Guo, Phys. Rev. A 97 (2018) 042328.
[463] H.-X. Ma, P. Huang, D.-Y. Bai, S.-Y. Wang, W.-S. Bao, G.-H. Zeng, Phys. Rev. A 97 (2018) 042329.
[464] C. Kumar, J. Singh, S. Bose, et al., Phys. Rev. A 100 (2019) 052329.
[465] C. Yu, Y. Li, J. Ding, Y. Mao, Y. Guo, Commun. Theor. Phys. (Beijing) 74 (2022) 035104.
[466] P. Papanastasiou, A.G. Mountogiannakis, S. Pirandola, Sci. Rep. 13 (2023).
[467] M. Ghalaii, S. Pirandola, Phys. Rev. A 108 (2023) 042621.
[468] Y. Fu, H.-L. Yin, T.-Y. Chen, Z.-B. Chen, Phys. Rev. Lett. 114 (2015) 090501.
[469] X. Hua, M. Hu, B. Guo, Entropy 24 (2022) 841.
[470] F. Gao, F.-Z. Guo, Q.-Y. Wen, F.-C. Zhu, Phys. Rev. Lett. 101 (2008) 208901.
[471] C.-L. Li, Y. Fu, W.-B. Liu, Y.-M. Xie, B.-H. Li, M.-G. Zhou, H.-L. Yin, Z.-B. Chen, Phys. Rev. Res. 5 (2023) 033077.
[472] X.-X. Ju, W. Zhong, Y.-B. Sheng, L. Zhou, Chin. Phys. B 31 (2022) 100302.
[473] T. Zhang, L. Zhou, W. Zhong, Y.-B. Sheng, Laser Phys. Lett. 20 (2023) 025203.
[474] C. Zhang, Q. Zhang, W. Zhong, M.-M. Du, S.-T. Shen, X.-Y. Li, A.-L. Zhang, L. Zhou, Y.-B. Sheng, Phys. Rev. A 111 (2025) 012602.
[475] R. Chen, W. Bao, C. Zhou, H. Li, Y. Wang, H. Bao, Opt. Express 24 (2016) 6594.
[476] R.-K. Chen, W.-S. Bao, H.-Z. Bao, C. Zhou, M.-S. Jiang, H.-W. Li, Chin. Phys. Lett. 34 (2017) 080301.
[477] C. Zhu, F. Xu, C. Pei, Sci. Rep. 5 (2015).
[478] C. Liu, C. Zhu, S. Ma, C. Pei, Internat. J. Theoret. Phys. 57 (2017) 726.
[479] X.-Q. Cai, Z.-F. Liu, C.-Y. Wei, T.-Y. Wang, Phys. A 607 (2022) 128226.
[480] Y.-G. Yang, R.-C. Huang, G.-B. Xu, Y.-H. Zhou, W.-M. Shi, D. Li, Quantum Inf. Process. 22 (2023).
[481] B.-X. Liu, R.-C. Huang, Y.-G. Yang, G.-B. Xu, Front. Quantum Sci. Technol. 2 (2023).
[482] Y. Wu, J. Zhou, X. Gong, Y. Guo, Z.-M. Zhang, G. He, Phys. Rev. A 93 (2016) 022325.
[483] P. van Loock, A. Furusawa, Phys. Rev. A 67 (2003) 052315.
[484] J. Zhou, Y. Guo, J. Phys. Soc. Japan 86 (2017) 024003.
[485] Y. Guo, W. Zhao, F. Li, D. Huang, Q. Liao, C.-L. Xie, Commun. Theor. Phys. (Beijing) 68 (2017) 191.
[486] F. Li, W. Zhao, Y. Guo, Internat. J. Theoret. Phys. 57 (2017) 112.
[487] Y. Wang, C. Tian, Q. Su, M. Wang, X. Su, Sci. China Inf. Sci. 62 (2019).
[488] C. Ottaviani, C. Lupo, R. Laurenza, S. Pirandola, Commun. Phys. 2 (2019).
[489] A.I. Fletcher, S. Pirandola, Sci. Rep. 12 (2022).
[490] A. Rubenok, J.A. Slater, P. Chan, I. Lucio-Martinez, W. Tittel, Phys. Rev. Lett. 111 (2013) 130501.
[491] T. Ferreira da Silva, D. Vitoreti, G.B. Xavier, G.C. do Amaral, G.P. Temporão, J.P. von der Weid, Phys. Rev. A 88 (2013) 052303.
[492] Z. Tang, Z. Liao, F. Xu, B. Qi, L. Qian, H.-K. Lo, Phys. Rev. Lett. 112 (2014) 190503.
[493] Y.-L. Tang, H.-L. Yin, Q. Zhao, H. Liu, X.-X. Sun, M.-Q. Huang, W.-J. Zhang, S.-J. Chen, L. Zhang, L.-X. You, Z. Wang, Y. Liu, C.-Y. Lu, X. Jiang, X. Ma, Q. Zhang, T.-Y. Chen, J.-W. Pan, Phys. Rev. X 6 (2016) 011024.
[494] R. Valivarthi, P. Umesh, C. John, K.A. Owen, V.B. Verma, S.W. Nam, D. Oblak, Q. Zhou, W. Tittel, Quantum Sci. Technol. 4 (2019) 045002.
[495] R.C. Berrevoets, T. Middelburg, R.F.L. Vermeulen, L.D. Chiesa, F. Broggi, S. Piciaccia, R. Pluis, P. Umesh, J.F. Marques, W. Tittel, J.A. Slater, Commun. Phys. 5 (2022) 186.
[496] C.C.W. Lim, B. Korzh, A. Martin, F. Bussières, R. Thew, H. Zbinden, Appl. Phys. Lett. 105 (2014).
[497] P. González, L. Rebón, T. Ferreira da Silva, M. Figueroa, C. Saavedra, M. Curty, G. Lima, G.B. Xavier, W.A.T. Nogueira, Phys. Rev. A 92 (2015) 022337.
[498] W.-Y. Liang, M. Li, Z.-Q. Yin, W. Chen, S. Wang, X.-B. An, G.-C. Guo, Z.-F. Han, Phys. Rev. A 92 (2015) 012319.
[499] S. Sajeed, A. Huang, S. Sun, F. Xu, V. Makarov, M. Curty, Phys. Rev. Lett. 117 (2016) 250505.

[500] M. Ioannou, M.A. Pereira, D. Rusca, F. Grünenfelder, A. Boaron, M. Perrenoud, A.A. Abbott, P. Sekatski, J.-D. Bancal, N. Maring, et al., Quantum 6 (2022) 718.
[501] J.M. Renes, R. Renner, IEEE Trans. Inform. Theory 58 (2012) 1985.
[502] H.M. Wiseman, S.J. Jones, A.C. Doherty, Phys. Rev. Lett. 98 (2007) 140402.
[503] S.J. Jones, H.M. Wiseman, A.C. Doherty, Phys. Rev. A 76 (2007) 052116.
[504] J. Schneeloch, C.J. Broadbent, S.P. Walborn, E.G. Cavalcanti, J.C. Howell, Phys. Rev. A 87 (2013) 062103.
[505] Y. Wang, W.-s. Bao, H.-w. Li, C. Zhou, Y. Li, Phys. Rev. A 88 (2013) 052322.
[506] V. Scarani, R. Renner, Phys. Rev. Lett. 100 (2008) 200501.
[507] M. Tomamichel, R. Renner, Phys. Rev. Lett. 106 (2011) 110506.
[508] M. Tomamichel, C.C.W. Lim, N. Gisin, R. Renner, Nat. Commun. 3 (2012) 634.
[509] N. Walk, S. Hosseini, J. Geng, O. Thearle, J.Y. Haw, S. Armstrong, S.M. Assad, J. Janousek, T.C. Ralph, T. Symul, et al., Optica 3 (2016) 634.
[510] J. Xin, X.-M. Lu, X. Li, G. Li, Opt. Express 28 (2020) 11439.
[511] H.-Z. Bao, W.-S. Bao, Y. Wang, R.-K. Chen, H.-X. Ma, C. Zhou, H.-W. Li, Chin. Phys. B 26 (2017) 050302.
[512] M.Y. Niu, F. Xu, J.H. Shapiro, F. Furrer, Phys. Rev. A 94 (2016) 052323.
[513] I. Kogias, Y. Xiang, Q. He, G. Adesso, Phys. Rev. A 95 (2017) 012315.
[514] Y. Xiang, I. Kogias, G. Adesso, Q. He, Phys. Rev. A 95 (2017) 010101.
[515] I. Kogias, A.R. Lee, S. Ragy, G. Adesso, Phys. Rev. Lett. 114 (2015) 060403.
[516] V. Coffman, J. Kundu, W.K. Wootters, Phys. Rev. A 61 (2000) 052306.
[517] Q.Y. He, M.D. Reid, Phys. Rev. Lett. 111 (2013) 250403.
[518] Y. Xiang, X. Su, L. Mišta Jr., G. Adesso, Q. He, Phys. Rev. A 99 (2019) 010104.
[519] M. Wang, Y. Xiang, H. Kang, D. Han, Y. Liu, Q. He, Q. Gong, X. Su, K. Peng, Phys. Rev. Lett. 125 (2020) 260506.
[520] Q.-Q. Lv, J.-M. Liang, Z.-X. Wang, S.-M. Fei, J. Phys. A 56 (2023) 325301.
[521] D.A. Evans, E.G. Cavalcanti, H.M. Wiseman, Phys. Rev. A 88 (2013) 022106.
[522] T. Gehring, V. Hähen, J. Duhme, F. Furrer, T. Franz, C. Pacher, R.F. Werner, R. Schnabel, Nat. Commun. 6 (2015) 8795.
[523] N. Walk, S. Hosseini, J. Geng, O. Thearle, J.Y. Haw, S. Armstrong, S.M. Assad, J. Janousek, T.C. Ralph, T. Symul, H.M. Wiseman, P.K. Lam, Optica 3 (2016) 634.
[524] J. Garcia-Escartin, S. Sajeed, V. Makarov, PLoS One 15 (8) (2020) e0236630.
[525] P. Smith, D. Marangon, M. Lucamarini, Z. Yuan, A. Shields, Phys. Rev. Appl. 15 (2021) 044044.
[526] R.D. Gill, Lect. Not. Monogr. Ser. 42 (2003) 133.
[527] D. Reddy, R. Nerem, A. Lita, S. Nam, R. Mirin, V. Verma, (2019) p. FF1A.3.
[528] J. Chang, J.W.N. Los, J.O. Tenorio-Pearl, N. Noordzij, R. Gourgues, A. Guardiani, J.R. Zichi, S.F. Pereira, H.P. Urbach, V. Zwiller, S.N. Dorenbos, I. Esmaeil Zadeh, APL Photonics 6 (2021) 036114, https://pubs.aip.org/aip/app/article-pdf/doi/10.1063/5.0039772/14572142/036114_1_online.pdf.
[529] Optical fiber loss and attenuation, 2022, https://www.fiberoptics4sale.com/blogs/archive-posts/95048006-optical-fiber-loss-and-attenuation.
[530] M. Takeoka, S. Guha, M.M. Wilde, Nat. Commun. 5 (2014).
[531] P.G. Kwiat, K. Mattle, H. Weinfurter, A. Zeilinger, A.V. Sergienko, Y. Shih, Phys. Rev. Lett. 75 (1995) 4337.
[532] P.G. Kwiat, E. Waks, A.G. White, I. Appelbaum, P.H. Eberhard, Phys. Rev. A 60 (1999) R773.
[533] S. Freedman, J. Clauser, Phys. Rev. Lett. 28 (1972) 938.
[534] S. Gómez, A. Mattar, I. Machuca, E.S. Gómez, D. Cavalcanti, O.J. Farías, A. Acín, G. Lima, Phys. Rev. A 99 (2019) 032108.
[535] S. Meraner, R.J. Chapman, S. Frick, R. Keil, M. Prilmüller, G. Weihs, SciPost Phys. 10 (2021) 017.
[536] O. Cosme, S. Pádua, F.A. Bovino, A. Mazzei, F. Sciarrino, F. De Martini, Phys. Rev. A 77 (2008) 053822.
[537] Y. Tsujimoto, K. Wakui, M. Fujiwara, K. Hayasaka, S. Miki, H. Terai, M. Sasaki, M. Takeoka, Phys. Rev. A 98 (2018) 063842.
[538] J.-W. Pan, D. Bouwmeester, H. Weinfurter, A. Zeilinger, Phys. Rev. Lett. 80 (1998) 3891.
[539] H. Takesue, B. Miquel, Opt. Express 17 (2009) 10748.
[540] J. Jin, M. Grimau Puigibert, L. Giner, J.A. Slater, M.R.E. Lamont, V.B. Verma, M.D. Shaw, F. Marsili, S.W. Nam, D. Oblak, W. Tittel, Phys. Rev. A 92 (2015) 012329.
[541] Q.-C. Sun, Y.-F. Jiang, Y.-L. Mao, L.-X. You, W. Zhang, W.-J. Zhang, X. Jiang, T.-Y. Chen, H. Li, Y.-D. Huang, X.-F. Chen, Z. Wang, J. Fan, Q. Zhang, J.-W. Pan, Optica 4 (2017) 1214.
[542] F. Samara, N. Maring, A. Martin, A.S. Raja, T.J. Kippenberg, H. Zbinden, R. Thew, Quantum Sci. Technol. 6 (2021) 045024.
[543] A.J. Stolk, K.L. van der Enden, M. Slater, I. te Raa-Derckx, P. Botma, J. van Rantwijk, J.J.B. Biemond, R.A.J. Hagen, R.W. Herfst, W.D. Koek, A.J.H. Meskers, R. Vollmer, E.J. van Zwet, M. Markham, A.M. Edmonds, J.F. Geus, F. Elsen, B. Jungbluth, C. Haefner, C. Tresp, J. Stuhler, S. Ritter, R. Hanson, Sci. Adv. 10 (2024) eadp6442, open Access.
[544] K. Azuma, S.E. Economou, D. Elkouss, P. Hilaire, L. Jiang, H.-K. Lo, I. Tzitrin, Rev. Modern Phys. 95 (2023) 045006.
[545] Y. Zhou, P. Malik, F. Fertig, M. Bock, T. Bauer, T. van Leent, W. Zhang, C. Becher, H. Weinfurter, PRX Quantum 5 (2024) 020307.
[546] J.P. Covey, H. Weinfurter, H. Bernien, Npj Quantum Inf. 9 (2023) 90.
[547] K. Mattle, H. Weinfurter, P. Kwiat, A. Zeilinger, Phys. Rev. Lett. 76 (1996) 4656.
[548] Y. Yu, F. Ma, X.-Y. Luo, B. Jing, P.-F. Sun, R.-Z. Fang, C.-W. Yang, H. Liu, M.-Y. Zheng, X.-P. Xie, W.-J. Zhang, L.-X. You, Z. Wang, T.-Y. Chen, Q. Zhang, X.-H. Bao, J.-W. Pan, Nature 578 (2020) 240.
[549] T. van Leent, M. Bock, F. Fertig, R. Garthoff, S. Eppelt, Y. Zhou, P. Malik, M. Seubert, T. Bauer, W. Rosenfeld, W. Zhang, C. Becher, H. Weinfurter, Nature 607 (2022) 69.
[550] R. Stockill, M.J. Stanley, L. Huthmacher, E. Clarke, M. Hugues, A.J. Miller, C. Matthiesen, C. Le Gall, M. Atatüre, Phys. Rev. Lett. 119 (2017) 010503.
[551] P.C. Humphreys, N. Kalb, J.P.J. Morits, R.N. Schouten, R.F.L. Vermeulen, D.J. Twitchen, M. Markham, R. Hanson, Nature 558 (2018) 268.
[552] M. Pompili, S.L.N. Hermans, S. Baier, H.K.C. Beukers, P.C. Humphreys, R.N. Schouten, R.F.L. Vermeulen, M.J. Tiggelman, L. dos Santos Martins, B. Dirkse, S. Wehner, R. Hanson, Science 372 (2021) 259, https://www.science.org/doi/pdf/10.1126/science.abg1919.
[553] S.L.N. Hermans, M. Pompili, L.D.S. Martins, A.R.-P. Montblanch, H.K.C. Beukers, S. Baier, J. Borregaard, R. Hanson, New J. Phys. 25 (2023) 013011.
[554] A.J. Stolk, J.J.B. Biemond, K.L. van der Enden, L. van Dooren, E.J. van Zwet, R. Hanson, Extendable optical phase synchronization of remote and independent quantum network nodes over deployed fibers, 2024, arXiv:2408.12464 [quant-ph].
[555] F. Mann, H.M. Chrzanowski, F. Gewers, M. Placke, S. Ramelow, Phys. Rev. Appl. 20 (2023) 054010.
[556] J.F. Geus, F. Elsen, S. Nyga, A.J. Stolk, K.L. van der Enden, E.J. van Zwet, C. Haefner, R. Hanson, B. Jungbluth, Opt. Quantum 2 (2024) 189.
[557] X.-Y. Luo, Y. Yu, J.-L. Liu, M.-Y. Zheng, C.-Y. Wang, B. Wang, J. Li, X. Jiang, X.-P. Xie, Q. Zhang, X.-H. Bao, J.-W. Pan, Phys. Rev. Lett. 129 (2022) 050503.
[558] D. Lago-Rivera, S. Grandi, J.V. Rakonjac, A. Seri, H. de Riedmatten, Nature 594 (2021) 37.
[559] X. Liu, J. Hu, Z.-F. Li, X. Li, P.-Y. Li, P.-J. Liang, Z.-Q. Zhou, C.-F. Li, G.-C. Guo, Nature 594 (2021) 41.

[560] S. Kucera, C. Haen, E. Arenskötter, T. Bauer, J. Meiers, M. Schäfer, R. Boland, M. Yahyapour, M. Lessing, R. Holzwarth, C. Becher, J. Eschner, Npj Quantum Inf. 10 (2024) 88.
[561] N. Gisin, S. Pironio, N. Sangouard, Phys. Rev. Lett. 105 (2010) 070501.
[562] M. Curty, T. Moroder, Phys. Rev. A 84 (2011) 010304.
[563] D. Pitkanen, X. Ma, R. Wickert, P. van Loock, N. Lütkenhaus, Phys. Rev. A 84 (2011) 022325.
[564] E. Meyer-Scott, M. Bula, K. Bartkiewicz, A. Černoch, J. Soubusta, T. Jennewein, K. Lemr, Phys. Rev. A 88 (2013) 012327.
[565] T.C. Ralph, A.P. Lund, AIP Conf. Proc. 1110 (2009) 155, https://pubs.aip.org/aip/acp/article-pdf/1110/1/155/11396998/155_1_online.pdf.
[566] V. Zapatero, M. Curty, Sci. Rep. 9 (2019) 17749.
[567] H.K. Beukers, M. Pasini, H. Choi, D. Englund, R. Hanson, J. Borregaard, PRX Quantum 5 (2024) 010202.
[568] A. Dahlberg, M. Skrzypczyk, T. Coopmans, L. Wubben, F. Rozpundefineddek, M. Pompili, A. Stolk, P. Pawełczak, R. Knegjens, J. de Oliveira Filho, R. Hanson, S. Wehner, Proceedings of the ACM Special Interest Group on Data Communication, SIGCOMM '19, Association for Computing Machinery, New York, NY, USA, 2019, pp. 159–173.
[569] M. Pompili, C. Delle Donne, I. te Raa, B. van der Vecht, M. Skrzypczyk, G. Ferreira, L. de Kluijver, A.J. Stolk, S.L.N. Hermans, P. Pawełczak, W. Kozlowski, R. Hanson, S. Wehner, Npj Quantum Inf. 8 (2022) 121.
[570] Y.-A. Chen, Q. Zhang, T.-Y. Chen, W.-Q. Cai, S.-K. Liao, J. Zhang, K. Chen, J. Yin, J.-G. Ren, Z. Chen, S.-L. Han, Q. Yu, K. Liang, F. Zhou, X. Yuan, M.-S. Zhao, T.-Y. Wang, X. Jiang, L. Zhang, W.-Y. Liu, Y. Li, Q. Shen, Y. Cao, C.-Y. Lu, R. Shu, J.-Y. Wang, L. Li, N.-L. Liu, F. Xu, X.-B. Wang, C.-Z. Peng, J.-W. Pan, Nature 589 (2021) 214.
[571] H.-J. Briegel, W. Dür, J.I. Cirac, P. Zoller, Phys. Rev. Lett. 81 (1998) 5932.
[572] C. Elliott, H. Yeh, Technical Report, BBN Technologies Cambridge, New York, New York, 2007, p. 164.
[573] M. Peev, C. Pacher, R. Alléaume, C. Barreiro, J. Bouda, W. Boxleitner, T. Debuisschert, E. Diamanti, M. Dianati, J.F. Dynes, S. Fasel, S. Fossier, M. Fürst, J.-D. Gautier, O. Gay, N. Gisin, P. Grangier, A. Happe, Y. Hasani, M. Hentschel, H. Hübel, G. Humer, T. Länger, M. Legré, R. Lieger, J. Lodewyck, T. Lorünser, N. Lütkenhaus, A. Marhold, T. Matyus, O. Maurhart, L. Monat, S. Nauerth, J.-B. Page, A. Poppe, E. Querasser, G. Ribordy, S. Robyr, L. Salvail, A.W. Sharpe, A.J. Shields, D. Stucki, M. Suda, C. Tamas, T. Themel, R.T. Thew, Y. Thoma, A. Treiber, P. Trinkler, R. Tualle-Brouri, F. Vannel, N. Walenta, H. Weier, H. Weinfurter, I. Wimberger, Z.L. Yuan, H. Zbinden, A. Zeilinger, New J. Phys. 11 (2009) 075001.
[574] D. Stucki, M. Legré, F. Buntschu, B. Clausen, N. Felber, N. Gisin, L. Henzen, P. Junod, G. Litzistorf, P. Monbaron, L. Monat, J.-B. Page, D. Perroud, G. Ribordy, A. Rochas, S. Robyr, J. Tavares, R. Thew, P. Trinkler, S. Ventura, R. Voirol, N. Walenta, H. Zbinden, New J. Phys. 13 (2011) 123001.
[575] M. Sasaki, M. Fujiwara, H. Ishizuka, W. Klaus, K. Wakui, M. Takeoka, S. Miki, T. Yamashita, Z. Wang, A. Tanaka, K. Yoshino, Y. Nambu, S. Takahashi, A. Tajima, A. Tomita, T. Domeki, T. Hasegawa, Y. Sakai, H. Kobayashi, T. Asai, K. Shimizu, T. Tokura, T. Tsurumaru, M. Matsui, T. Honjo, K. Tamaki, H. Takesue, Y. Tokura, J.F. Dynes, A.R. Dixon, A.W. Sharpe, Z.L. Yuan, A.J. Shields, S. Uchikoga, M. Legré, S. Robyr, P. Trinkler, L. Monat, J.-B. Page, G. Ribordy, A. Poppe, A. Allacher, O. Maurhart, T. Länger, M. Peev, A. Zeilinger, Opt. Express 19 (2011) 10387.
[576] C.-Y. Lu, Y. Cao, C.-Z. Peng, J.-W. Pan, Rev. Modern Phys. 94 (2022) 035001.
[577] Y.-H. Li, S.-L. Li, X.-L. Hu, C. Jiang, Z.-W. Yu, W. Li, W.-Y. Liu, S.-K. Liao, J.-G. Ren, H. Li, L. You, Z. Wang, J. Yin, F. Xu, Q. Zhang, X.-B. Wang, Y. Cao, C.-Z. Peng, J.-W. Pan, Phys. Rev. Lett. 131 (2023) 100802.
[578] A. Hajomer, H. Nguyen, U. Andersen, T. Gehring, Optical Fiber Communication Conference, Optica Publishing Group, 2023, pp. M2I–2.
[579] N.S.A.S. Service, Quantum key distribution (qkd) and quantum cryptography (qc), 2024, (Accessed 03 October 2024).
[580] F.C.A. (ANSSI), The uses and limits of quantum key distribution, 2024, (Accessed 03 October 2024).
[581] U.N.C.S. Centre, Quantum security technologies, 2024, (Accessed 03 October 2024).
[582] M. Lucamarini, et al., Implementation Security of Quantum Cryptography, ETSI White Paper No. 27, 2018.
[583] V. Makarov, A. Abrikosov, P. Chaiwongkhot, A.K. Fedorov, A. Huang, E. Kiktenko, M. Petrov, A. Ponosova, D. Ruzhitskaya, A. Tayduganov, D. Trefilov, K. Zaitsev, Phys. Rev. Appl. 22 (2024) 044076.
[584] National Institute of Standards and Technology (NIST), Crypto agility: Considerations for migrating to post-quantum cryptographic algorithms, 2025, (Accessed 23 January 2025).
[585] L.-J. Wang, K.-Y. Zhang, J.-Y. Wang, J. Cheng, Y.-H. Yang, S.-B. Tang, D. Yan, Y.-L. Tang, Z. Liu, Y. Yu, Q. Zhang, J.-W. Pan, Npj Quantum Inf. 7 (2021) 67.
[586] Y.-H. Yang, P.-Y. Li, S.-Z. Ma, X.-C. Qian, K.-Y. Zhang, L.-J. Wang, W.-L. Zhang, F. Zhou, S.-B. Tang, J.-Y. Wang, Y. Yu, Q. Zhang, J.-W. Pan, Opt. Express 29 (2021) 25859.
[587] J.F. Dynes, A. Wonfor, W.W.S. Tam, A.W. Sharpe, R. Takahashi, M. Lucamarini, A. Plews, Z.L. Yuan, A.R. Dixon, J. Cho, Y. Tanizawa, J.P. Elbers, H. Greißer, I.H. White, R.V. Penty, A.J. Shields, Npj Quantum Inf. 5 (2019) 101.
[588] S. Gupta, I. Agarwal, V. Mogiligidda, R. Kumar Krishnan, S. Chennuri, D. Aggarwal, A. Hoodati, S. Cooper, Ranjan, M. Bilal Sheik, K.M. Bhavya, M. Hegde, M.N. Krishna, A.K. Chauhan, M. Korrapati, S. Singh, J.B. Singh, S. Sud, S. Gupta, S. Pant, Sankar, N. Agrawal, A. Ranjan, P. Mohapatra, T. Roopak, A. Ahmad, M. Nanjunda, D. Singh, Sci. Rep. 14 (2024) 16752.
[589] P. Zeng, D. Bandyopadhyay, J.A.M. Méndez, N. Bitner, A. Kolar, M.T. Solomon, F. Rozpedek, T. Zhong, F.J. Heremans, D.D. Awschalom, et al., 2024, arXiv preprint arXiv:2411.01086.
[590] The world's third-largest economy has bad intentions — and it's only getting bigger, 2024, https://sponsored.bloomberg.com/quicksight/check-point/the-worlds-third-largest-economy-has-bad-intentions-and-its-only-getting-bigger.
[591] Report on post-quantum cryptography, 2024, https://www.whitehouse.gov/wp-content/uploads/2024/07/REF_PQC-Report_FINAL_Send.pdf?utm_source=substack&utm_medium=email.
[592] E. Pelucchi, G. Fagas, I. Aharonovich, D. Englund, E. Figueroa, Q. Gong, H. Hannes, J. Liu, C.-Y. Lu, N. Matsuda, J.-W. Pan, F. Schreck, F. Sciarrino, C. Silberhorn, J. Wang, K.D. Jöns, Nat. Rev. Phys. 4 (2022) 194.
[593] X. Zhong, W. Wang, R. Mandil, H.-K. Lo, L. Qian, Phys. Rev. Appl. 17 (2022) 014025.
[594] B. Fröhlich, J.F. Dynes, M. Lucamarini, A.W. Sharpe, Z. Yuan, A.J. Shields, Nature 501 (2013) 69.
[595] J.-P. Chen, C. Zhang, Y. Liu, C. Jiang, D.-F. Zhao, W.-J. Zhang, F.-X. Chen, H. Li, L.-X. You, Z. Wang, Y. Chen, X.-B. Wang, Q. Zhang, J.-W. Pan, Phys. Rev. Lett. 128 (2022) 180502.
[596] C. Elliott, A. Colvin, D. Pearson, O. Pikalo, J. Schlafer, H. Yeh, Proceedings of SPIE - the international society for optical engineering, 2005.
[597] S. Wang, W. Chen, Z.-Q. Yin, H.-W. Li, D.-Y. He, Y.-H. Li, Z. Zhou, X.-T. Song, F.-Y. Li, D. Wang, H. Chen, Y.-G. Han, J.-Z. Huang, J.-F. Guo, P.-L. Hao, M. Li, C.-M. Zhang, D. Liu, W.-Y. Liang, C.-H. Miao, P. Wu, G.-C. Guo, Z.-F. Han, Opt. Express 22 (2014) 21739.
[598] R. Kumar, H. Qin, R. Alléaume, New J. Phys. 17 (2015) 043027.
[599] T.A. Eriksson, T. Hirano, B.J. Puttnam, G. Rademacher, R.S. Luís, M. Fujiwara, R. Namiki, Y. Awaji, M. Takeoka, N. Wada, M. Sasaki, Commun. Phys. 2 (2019) 9.
[600] P.D. Townsend, Electron. Lett. 33 (1997) 188.
[601] Y. Mao, B.-X. Wang, C. Zhao, G. Wang, R. Wang, H. Wang, F. Zhou, J. Nie, Q. Chen, Y. Zhao, Q. Zhang, J. Zhang, T.-Y. Chen, J.-W. Pan, Opt. Express 26 (2018) 6010.
[602] Opt. Express 31 (2023) 43035.
[603] J.M. Thomas, F.I. Yeh, J.H. Chen, J.J. Mambretti, S.J. Kohlert, G.S. Kanter, P. Kumar, Optica 11 (2024) 1700.

[604] F. Honz, F. Prawits, O. Alia, H. Sakr, T. Bradley, C. Zhang, R. Slavík, F. Poletti, G. Kanellos, R. Nejabati, P. Walther, D. Simeonidou, H. Hübel, B. Schrenk, J. Lightwave Technol. 41 (2023) 3587.
[605] D.J. Richardson, J.M. Fini, L.E. Nelson, Nat. Photonics 7 (2013) 354.
[606] J.F. Dynes, S.J. Kindness, S.W.-B. Tam, A. Plews, A.W. Sharpe, M. Lucamarini, B. Fröhlich, Z.L. Yuan, R.V. Penty, A.J. Shields, Opt. Express 24 (2016) 8081.
[607] C. Cai, Y. Sun, Y. Zhang, P. Zhang, J. Niu, Y. Ji, Opt. Express 27 (2019) 5125.
[608] G.B. Xavier, G. Lima, Commun. Phys. 3 (2020) 9.
[609] B.-X. Wang, Y. Mao, L. Shen, L. Zhang, X.-B. Lan, D. Ge, Y. Gao, J. Li, Y.-L. Tang, S.-B. Tang, J. Zhang, T.-Y. Chen, J.-W. Pan, Opt. Express 28 (2020) 12558.
[610] J.C. Chapman, J.M. Lukens, M. Alshowkan, N. Rao, B.T. Kirby, N.A. Peters, Phys. Rev. Appl. 19 (2023) 044026.
[611] O. van Deventer, N. Spethmann, M. Loeffler, M. Amoretti, R. van den Brink, N. Bruno, P. Comi, N. Farrugia, M. Gramegna, A. Jenet, B. Kassenberg, W. Kozlowski, T. Länger, T. Lindstrom, V. Martin, N. Neumann, H. Papadopoulos, S. Pascazio, M. Peev, R. Pitwon, M.A. Rol, P. Traina, P. Venderbosch, F.K. Wilhelm-Mauch, EPJ Quantum Technol. 9 (2022) 33.
[612] J. Wang, B.A. Huberman, in: K. Arai (Ed.), Advances in Information and Communication, Springer International Publishing, Cham, 2022, pp. 571–586.
[613] T. Länger, G. Lenhart, New J. Phys. 11 (2009) 055051.
[614] European Telecommunications Standards Institute (ETSI), Quantum key distribution (QKD), 2024, (Accessed 10 December 2024).
[615] European Telecommunications Standards Institute (ETSI), Industry specification group (ISG) on quantum key distribution for users (QKD) activity report 2023, 2023, (Accessed 28 December 2024).
[616] International Organization for Standardization (ISO), ISO/IEC 23837: Security requirements, test and evaluation methods for QKD modules. Part 1: Requirements, 2025, (Accessed 19 December 2025).
[617] International Organization for Standardization (ISO), ISO/IEC 23838: Information security — Security requirements, test and evaluation methods for quantum key distribution. Part 2: Evaluation and testing methods, 2025, (Accessed 19 December 2025).
[618] International Organization for Standardization (ISO), ISO/IEC JTC 1/SC 27: Information security, cybersecurity and privacy protection, 2025, (Accessed 05 January 2025).
[619] International Organization for Standardization (ISO), IEC/ISO JTC 3 quantum technologies, 2025, (Accessed 05 January 2025).
[620] International Telecommunication Union, ITU-T recommendations, 2024, (Accessed 17 December 2024).
[621] A.-R. Gârban, Certification of MDI-QKD Devices under the ISO 15408 Common Criteria Framework (Master's thesis), Eindhoven University of Technology, 2023, (Accessed 15 October 2024).
[622] M. Sasaki, Quantum Sci. Technol. 2 (2017) 020501.
[623] P.K. Tysowski, X. Ling, N. Lütkenhaus, M. Mosca, Quantum Sci. Technol. 3 (2018) 024001.
[624] R. Broberg, L. Bassett, J. Smith, Quantum 2.0 Conference and Exhibition, Optica Publishing Group, 2022, QTu2A.29.
[625] International Telecommunication Union, Recommendation ITU-T Y.3800: Overview on Networks Supporting Quantum Key Distribution, Tech. Rep. Y.3800, ITU-T, 2019, (accessed 17 December 2024).