Quark 2005/04

Svet kvantovej fyziky IV –
Kvantová kryptografia

Snaha človeka skrývať svoje tajomstvá je tu od nepamäti. Je jedno, či ide o zlato, šperky, zbrane, alebo o tajné recepty, technológie, vynálezy, či myšlienky. Kryptografia sa venuje problémom, s ktorými sa stretne každý, kto sa pokúsi svoje tajomstvá prenášať z jedného miesta na iné, prípadne sa chce s nimi s niekým podeliť. V tejto časti si priblížime ako sa zákony kvantovej fyziky dajú využiť k zlepšeniu bezpečnosti komunikácie.

Iba perfektné zvládnutie komunikácie medzi jednotlivými časťami kráľovstiev, impérií, alebo armád pomáhalo kráľom a cisárom udržať a riadiť svoje krajiny po celé stáročia, vyhrávať dôležité vojny, predchádzať domácim aj vonkajším útokom. Všetci si pritom uvedomovali potenciálne nebezpečenstvo, keby sa tajné príkazy, alebo depeše, dostali do tých nesprávnych rúk. Snaha o zabezpečenie citlivých informácií motivovala a stále motivuje vypracovávanie najrôznejších techník, vytváranie špecializovaných tímov, ktorých úlohov je zaistiť bezpečnosť komunikácie. Súčasne s tým však vznikala a rozvíjala sa aj potreba odhaľovania tajných správ, ktorej prínos je zrejmý: vedieť o zámeroch nepriateľa a byť o krok pred ním. Kdesi na pozadí celej histórie je skrytý súboj medzi tými, čo tajné šifry vytvárajú, a tými, čo tieto šifry lúštia. Boli obdobia keď mali navrch jedny, ale aj obdobia, keď mali navrch druhí. Tento súboj možno badať aj dnes a z tohoto pohľadu sa dá povedať, že internet je jedným veľkým bojiskom.

História kryptografie (t.j. umenia skrývania, utajovania a následného odhaľovania informácie) je nemenej zaujímavá ako história samotná. Bohužiaľ tu nemáme priestor, čo i len veľmi povrchne naznačiť, čo všetko bolo priamo, či nepriamo spojené s kryptografiou. Jej úlohou je premeniť ľubovoľný text na zmes symbolov, ktoré na prvý pohľad nič neznamenajú. Tento proces sa nazýva *zakódovanie*. Šifra je akýsi predpis (recept), ktorý nám umožňuje správu zakódovať. Rozlišujeme dva základné prístupy k šifrovaniu správ: *prehodenie písmen* (permutácia) a *nahradenie písmen* (substitúcia) inými písmenami, prípadne úplne novými symbolmi. Napríklad po zakódovaní jedného slova dostaneme RKUAQ (permutácia), alebo RVBSL (substitúcia). Viete uhádnuť pôvodné slovo? Nie je to zložité. Ide o slovo QUARK. V prvom prípade sme najprv slovo napísali odzadu a potom poprehadzovali dvojice písmen. V druhom prípade sme každé písmeno nahradili písmenom, ktoré stojí v abecede hneď za ním. Obidve tieto šifry je veľmi ľahké odhaliť. Typom šifry, ktorá nahrádza písmená novými znakmi, je napríklad *Morseova abeceda*. Namiesto písmen používa bodky a čiarky (krátke a dlhé signály). V tomto prípade však nie je cieľom správu utajiť, ale iba efektívne sprostredkovať, t.j. šifrovanie nie je vždy nutne motivované iba snahou informáciu utajiť.

Svätým grálom kryptografie sa stalo hladanie úplne bezpečnej šifry, t.j. takej, ktorú nikto a nikdy nebude vedieť rozlúštiť. Predtým ako si ju ukážeme, si povedzme niečo o tom, ako vlastne jednotlivé šifry odhaľovať, t.j. ako rozšifrovávať. Namiesto nahradenia písmenom, ktoré stojí v abecede posunuté o jedno miesto doprava, môžeme nahradiť písmenom, ktoré je posunuté o *N* miest. Takýto spôsob kódovania sa nazýva *Cézarova šifra* podľa rímskeho cisára, ktorý ju používal pri riadení svojich légií. Kľúčom k dešifrovaniu je nájsť, ktorý symbol, čo znamená, t.j. odhaliť, že B je namiesto A, C je namiesto B, atď. Ako však zistiť veľkosť posunutia? Môžeme skúsiť všetky možnosti posunutí, ktorých nie je až tak veľa. Ale, čo v prípade ak je abeceda usporiadaná nejakým neznámym spôsobom? Takýto prípad nemôžeme vylúčiť. Skúšať všetky možnosti v takomto prípade by už zabralo veľmi dlhý čas.

Existuje však aj iný spôsob. Pre slovenčinu (podobne aj pre iné jazyky) platí, že jednotlivé písmena sa v bežných textoch nevyskytujú rovnako často. Napríklad v tomto texte bolo písmeno A použité zhruba 1800 krát, kdežto písmeno G ani nie 10 krát. Vieme povedať, ktoré písmeno používame v ktorom jazyku najviac, a ktoré najmenej. Ak teda máme dostatočne dlhý zašifrovaný slovenský text, tak symbol, ktorý sa najviackrát opakuje, bude s veľkou pravdepodobnosťou nahradzovať písmeno A, alebo E. Takto môžeme odhadnúť niekoľko písmen a zvyšok poväčšine poľahky doplníme. Niekedy je potrebné si všímať aj dvojice, trojice, atď. Vieme napríklad, že písmená JG vedľa seba nebývajú. Využitie všetkých takýchto štatistických znalosti o používaní písmen v našom jazyku nám umožní nakoniec šifru pomerne veľmi rýchlo odhaliť. Cézarova šifra teda nie je úplne vhodná na posielanie utajených správ.

Vernamova šifra.

Úplne bezpečnú šifru dostaneme, ak iba trochu skomplikujeme šifru Cézarovu. Namiesto toho, aby sme posunutie zafixovali pre celú správu, prípadne pre nejaké bloky písmen zo správy, tak nadefinujeme iný (náhodný) posun pre každé jedno písmeno správy. Tieto posuny sú špecifikované tzv. *šifrovacím kľúčom*, ktorým správu akoby uzamkneme. Vďaka takémuto postupu dosiahneme to, že každý symbol sa nám v zašifrovanom texte vyskytuje zhruba rovnako často. Preto popísaný spôsob lúštenia šifry fungovať nebude. Výsledná správa je úplne náhodným zoskupením znakov, ktoré bez znalosti jednotlivých posunutí neobsahujú vôbec žiadnu informáciu (pozri obrázok 1). Tento spôsob šifrovania nazývame *Vernamova šifra*, ktorá je jedinou úplne bezpečnou šifrou. Jej drobnou nevýhodou je, že na používanie je trochu náročná. V prvom rade odosielateľ a aj adresát musia poznať dopredu hodnoty jednotlivých posunutí t.j. pred tým než začnú komunikovať, obidvaja poznajú šifrovací kľúč. Pri dekódovaní treba jednotlivé písmená podľa toho istého kľúča posúvať späť, t.j. tentokrát v abecede doľava. Aby sme dosiahli úplnú bezpečnosť, tak dĺžka šifrovacieho kľúča musí byť rovnako dlhá ako dĺžka celého zakódovaného textu. Naviac kľúč nemôžeme používať opakovane. Existujú totiž spôsoby ako v takomto prípade šifru odhaliť.

Proces bezpečnej komunikácie si môžeme predstaviť nasledovne. Šifrovanie nie je ničím iným ako ukladaním správ do pevnej krabice, ktorú zatvoríme a zámok uzamkneme kľúčom. Bezpečnosť znamená, že krabica, a aj zámok, sú neotvoriteľné nech použijeme akékoľvek prostriedky. Ani kladivom, ani pílkou sa do krabice nedostaneme. Jediným spôsobom ako zistiť obsah krabice, je použiť kľúč a zámku odomknúť. Bohužiaľ, žiadnu úplne odolnú krabicu nemáme a nepoznáme. V skutočnosti ju ani nepotrebujeme, pretože našim cieľom nie je ukryť niečo hmatateľné (papier), ale niečo viac abstraktné, t.j. informáciu zapísanú na papieri. Idea šifrovania je taká, že žiadna sila nám nepomôže dostať sa k obsahu. Práve naopak, použitie hrubej sily nie je vôbec potrebné. Zašifrovaná správa nemusí byť skrytá v krabici a každý si ju môže pozrieť. Avšak iba ten, kto má „kľúč“ môže skrytý obsah aj otvoriť a text odkódovať.

Pozrime sa teraz detailne na to ako Vernamova šifra funguje v prípade, že abeceda je zložená iba z dvoch „písmen“ 0,1. Hocijaký skutočný text vieme zapísať ako postupnosť núl a jednotiek. Nebudeme sa teraz zaujímať o nejakú konkrétnu správu a našou úlohou bude zašifrovať text 0011001100110011, nech už znamená čokoľvek. Na posunutia v takejto dvojprvkovej abecede nemáme veľa možností: alebo neposúvame písmená vôbec, alebo namiesto nuly píšeme jednotku a naopak. Suma sumárum máme k dispozícii dve rôzne Cézarove šifry: posunutie o N=0 a posunutie o N=1. Vernamova šifra (kľúč) je opäť iba postupnosťou núl a jednotiek, ktoré špecifikujú posunutie daného písmena v pôvodnej správe, napr. 0010111010111000. Výsledkom šifrovanie bude postupnosť 0001110110001011. Táto správa príde k adresátovi, ktorý použije ten istý kľúč na dešifrovanie, t.j. v prípade N=0 písmeno ponechá bez zmeny a v prípade N=1 písmeno nahradí jedným písmenom naľavo, t.j. nulu nahradí jednotkou a naopak. V tomto prípade je šifrovanie (posunutie doprava) a dešifrovanie (posunutie doľava) tou istou operáciou. Overte si, že ak použijete ten istý kľúč na zašifrovaný text, tak dostanete pôvodnú postupnosť núl a jednotiek.

Vernamova šifra z pohľadu fyzika

Na poslanie hodnoty bitu informácie z jedného miesta na druhé bezpochyby potrebujeme nejaký fyzikálny objekt, ktorý hrá úlohu kuriéra (nosiča) informácie. Informácia samotná je zakódovaná práve do stavu tohoto fyzikálneho objektu. Položme si otázku, či je nejaký rozdiel ak informácia je zapísaná na kuse papiera, uložená v elektronickom čipe, alebo zakódovaná do jediného elektrónu.

V prípade, že používame dvojprvkovú abecedu, tak kuriéra nazývame *klasickým bitom*. Ide o ľubovoľný fyzikálny systém, ktorý sa nachádza v dvoch rôznych stavoch, ktoré si pomenujeme ako stav 0 a stav 1. K uskutočneniu Vernamovej šifry potrebujeme aspoň dva klasické bity, ktoré pripadajú na prenos jedného bitu informácie, t.j. písmena 0, alebo 1. Prvým krokom Vernamovej šifry je *distribúcia kľúča*. V tomto kroku odosielateľ a aj adresát obdržia každý po K klasických bitoch, pričom x-tý bit oboch je vždy v rovnakom stave (pre každé x). Poslanie správy budeme vykonávať pomocou fyzikálnej transformácie uskutočnenej na klasických bitoch tvoriacich kľúč. Ak chceme poslať nulu, tak nevykonáme žiadnu operáciu a stav klasického bitu necháme nezmenený. Ak však posielame jednotku, tak stav klasického bitu zmeníme. Táto operácia spôsobuje, že hodnota klasického bitu sa zmení na opačnú (z nuly na jednotku a naopak), čo zodpovedá logickej operácii negácie. Hovoríme, že aplikujeme operáciu NOT. Po vykonaní príslušnej operácie pošleme klasický bit adresátovi. Dešifrovanie uskutočníme porovnaním stavov, resp. hodnôt, oboch klasických bitov. V prípade, ak sú stavy rovnaké, tak odosielateľ nevykonal žiadnu operáciu a posiela nám písmeno 0, kdežto ak sú rôzne, tak odosielateľ vykonal operáciu NOT, čím poslal písmeno 1. Treba si dobre rozmyslieť, že popísaný spôsob komunikácie je presne to isté ako Vernamova šifra popísaná v predošlom odstavci, t.j. správa je zašifrovaná tým istým spôsobom.

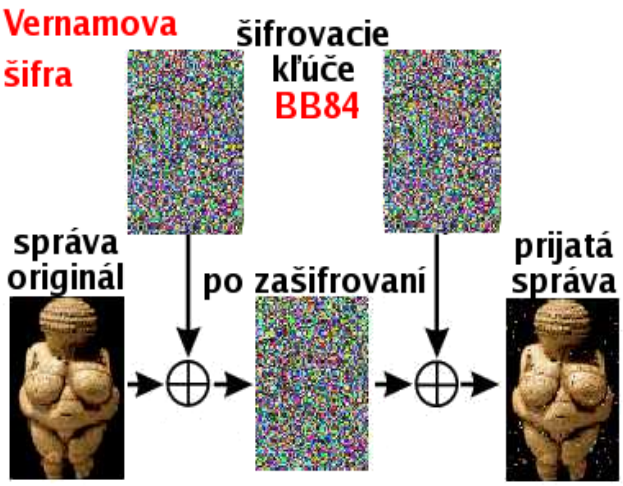
Aby sme zabezpečili bezpečnosť prenosu, tak distribuovaný kľúč musí byť úplne náhodný, t.j. nesmú sa v ňom opakovať nejaké reťazce núl a jednotiek. Napríklad kľúčom 00010001000100010001 nie je príliš bezpečné uzamykať. V podstate ide o opakované použitie tej istej Vernamovej šifry 0001 pre správy s dĺžkou 4 bity. V ideálnom prípade sa nuly a jednotky vyskytujú v šifrovacom kľúči rovnako často. Z pohľadu fyziky to znamená, že odosielateľ a adresát zdieľajú dva klasické bity, ktoré sa nachádzajú v tzv. *maximálne korelovanom stave*.

Superhusté kódovanie – dva v jednom

Pri prenesení jedného klasického bitu prenesieme jeden bit informácie. Je to však maximum, čo môžeme dosiahnuť? Všeobecne platí, že do jediného klasického bitu vieme zakódovať maximálne jeden bit informácie. Pri Vernamovej šifre však máme v hre spolu až dva klasické bity, ktoré potencionálne môžu obsahovať až dva bity informácie. Vieme ich plne využiť? Bohužiaľ nie, pretože na jednom klasickom bite nevieme vykonať viac ako dve rôzne operácie (nerobiť nič, alebo NOT), t.j. poslať vieme najviac dve hodnoty, ktoré predstavujú jeden bit informácie.

Predstavme si však situáciu, že namiesto klasických bitov používame bity kvantové. Z jedného kvantového bitu vieme takisto získať najviac jeden bit informácie. Z tohoto pohľadu sa klasické a kvantové bity vôbec nelíšia. V kvantovom prípade však odosielateľ môže vykonať oveľa viac operácii ako v prípade klasickom, kde máme transformácie iba dve. Inými slovami, v kvantovom prípade sa môžeme pokúsiť odoslať viac písmen a použiť tak viacpísmenovú abecedu. V prípade, ak odosielateľ a adresát zdieľajú *maximálne previazaný stav* (napr. stav s nulovým celkovým spinom), tak vieme vykonať štyri také operácie, že celkové stavy oboch kvantových bitov budú navzájom perfektne rozlíšiteľné. Jediným meraním potom vieme zistiť o ktorý z týchto štyroch stavov ide. Meranie je nám už známe Bellove meranie, ktoré bolo napríklad použité aj pri teleportácii (pozri Quark 2005/2). Adresát po prijatí kvantového bitu bude teda schopný jednoznačne určiť iba jediným meraním, ktorú zo štyroch operácií si odosielateľ zvolil, t.j. ktoré písmeno (jedno zo štyroch) poslal. Štyri písmená zodpovedajú dvom bitom prenesenej informácie. V kvantovom prípade teda dokážeme potenciál dvoch kvantových bitov využiť naplno a preniesť dva bity informácie pri poslaní jediného

kvantového bitu (dva v jednom). Samozrejme poslaný kvantový bit môže niesť najviac jeden bit informácie. Inak by sme si odporovali s tým, čo sme už povedali predtým. V tomto prípade ale paradoxne kuriér nenesie vôbec žiadny bit informácie. Hocikto, kto zachytí poslanú časticu nezíska žiadnu informáciu. Druhý kvantový bit slúži na odomknutie správy. Celá informácia je skrytá v počiatočných koreláciach medzi kvantovými (ak klasickými) bitmi. Ako však vieme korelácie (pozri Quark 2005/1,2) kvantových systémov sú silnejšie a divnejšie ako systémov klasických. Kvantový analóg Vernamovej šifry je príkladom tejto sily kvantových korelácií, ktoré zdvojnásobujú prenosovú kapacitu. Kvantovej verzii sa zvykne hovoriť *superhusté kódovanie*.



Obr. 1. *Na obrázku je znázornená ideaVernamovej šifry. Išlo o skutočný experiment, v ktorom bol pomocou kvantovej fyziky rozdistribuovaný šifrovací kľúč a následne bola prenesená fotografia sošky Venuše. Kľúč je definovaný farbou pixela, ktorá definuje „posunutie“ v abecede farieb. Ako vidno chybovosť prenosu bola veľmi malá.*

Kvantová distribúcia kľúča

Vernamova šifra je založená na existencii šifrovacieho kľúča, ktorý je známy iba odosielateľovi a adresátovi. Ako však zabezpečiť existenciu takéhoto kľúča? Kľúč nemôže byť jednoducho poslaný z jedného miesta na druhé. Každý by ho mohol prečítať. Na druhej strane zašifrovať ho nie je možné, lebo k zašifrovaniu potrebujeme kľúč, ktorý ešte nemáme. Distribúcia kľúča je najvážnejším problémom a nedostatkom Vernamovej šifry. Dokonca takým vážnym, že Vernamova šifra sa prakticky nepoužíva. Bezpečná distribúcia je klasicky neriešiteľný problém. Kvantová fyzika však ponúka riešenie aj v tejto oblasti. Bude nám stačiť posielať jediný kvantový bit a žiaden iný okrem tohoto nebudeme potrebovať.

V roku 1984 Charles Bennett a Gill Brassard navrhli kvantový protokol určený na distribúciu kľúča, ktorý dnes označujeme ako BB84. Pre lepšiu predstavu si tento protokol popíšeme na konkrétnom príklade. *Polarizácia fotónu* je (podobne ako spin 1/2) vhodným kandidátom na realizáciu kvantového bitu. Zhruba povedané, polarizácia predstavuje akýsi smer priradený každému fotónu, smer v ktorom kmitá „jeho“ elektrické pole. Perfektne rozlíšiť sa dá iba medzi tými dvoma smermi polarizácie, ktoré zvierajú pravý uhol, napríklad medzi *horizontálne* a *vertikálne* polarizovaným fotónom. K tomuto slúžia zariadenia zvané polarizátory, ktoré majú tú vlastnosť, že fotóny s istou polarizáciou neprepúšťajú vôbec. Naviac fotóny, ktorým sa podarí prejsť, sa vždy nachádzajú v smere kolmom na tento smer. Hovoríme, že svetlo (tvorené fotónmi) je po prechode polarizátorom polarizované v istom smere. Pre polarizáciu platí princíp neurčitosti, ktorý zaručuje bezpečnosť prenosu kľúča. O fotóne vieme zistiť hodnotu polarizácie iba v jedinom smere, t.j. nevieme súčasne presne zmerať veľkosť polarizácie v dvoch rôznych (nekolmých) smeroch.

BB84

Budeme potrebovať fotóny v štyroch rôznych stavoch: horizontálne polarizované $|H\rangle$ (t.j. pod uhlom 0 stupňov), vertikálne polarizované $|V\rangle$ (t.j. pod uhlom 90 stupňov), diagonálne polarizované pod uhlom 45 stupňov $|+\rangle$ a diagonálne polarizované pod uhlom 135 stupňov $|-\rangle$. Tieto stavy predstavujú dvojice navzájom kolmých polarizácií, t.j. dve bázy H/V a +/–. Odosielateľ určuje hodnotu bitu výberom stavu: hodnotu 1, ak vyberie $|H\rangle$, alebo $|+\rangle$, a hodnotu 0, ak vyberie stavy $|V\rangle$, alebo $|-\rangle$. Výbery stavov a aj báz robíme pre každý bit úplne náhodne. Úlohou adresáta je určiť, ktorý stav sme si vybrali. Kvôli princípu neurčitosti neexistuje meranie, ktorým by sme to vedeli určiť. Adresát preto strieda náhodne dve rôzne merania a zisťuje hodnoty polarizácie v dvoch rôznych bázach H/V, alebo +/–. Používa polarizátor v smere H, alebo polarizátor v smere +. Má dve možnosti: alebo tipne bázu správne, alebo nie. Správne tipnutie bázy znamená výber polarizátora H ak bol poslaný stav $|H\rangle$ (ako bit 1), alebo stav $|V\rangle$ (ako bit 0). Podobne pre výber polarizátora v smere +. Ak správne tipne adresát bázu, tak vie určiť ktorý bit bol poslaný. Ak fotón polarizátorom neprejde, tak poslaný bit má hodnotu 0, a ak fotón prejde, tak bol poslaný bit 1. V prípade, ak sa voľba polarizátora nezhoduje s výberom bázy odosielateľa, tak adresát nevie povedať o hodnote poslaného bitu informácie vôbec nič. V takomto prípade je šanca fotónu prejsť a nepresť polarizátorom jedna k jednej. Preto, ani keď fotón prejde a ani keď neprejde, nevieme povedať o fotón v akom stave išlo.

Zistili sme, že bit informácie sa nám podarí preniesť vždy, keď sa voľba polarizátora zhoduje s voľbou bázy. Bohužiaľ adresát nevie, či zvolil to správn nastavenie polarizátora, alebo nie. Riešenie je našťastie jednoduché. Odosielateľ zverejní, ktorú bázu kedy vybral a adresát zverejní, v ktorom smere polarizáciu meral. Napríklad si zatelefonujú a budú vedieť kedy sa zhodli a kedy nie. Vďaka tomu oddelia plevel od zrna a vyhodia tie výsledky, kedy sa nezhodli. Zvyšné hodnoty bitov sú potom presne také isté, t.j. majú k dispozícii ten istý kľúč, ktorý môžu použiť pri šifrovaní a dešifrovaní. Vôbec nevadí, že informácia o tom kedy sa zhodli je verejná a prístupná každému. Dôležité je, že nikto okrem nich

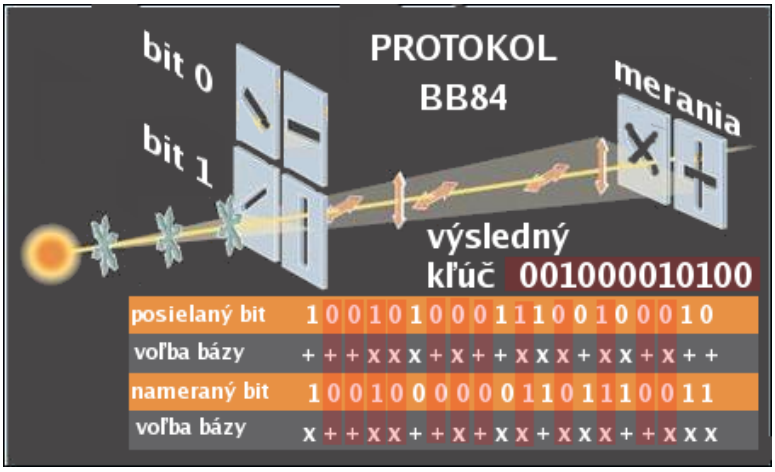
nepozná konkrétnu voľbu stavu (teraz už zo známej bázy) a ani výsledky meraní. A práve v nich je skrytý kľúč.

Distribúcia kľúča sa teda skladá z troch fáz. V pvej fáze odosielateľ, aj adresát ľubovoľne volia bázy a merania. Každý u seba zhromaždí postupnosť núl a jednotiek. V druhej fáze si oznámia voľby báz a meraní. To im umožní povyhadzovať zo získanej postupnosti tie nuly a jednotky, ktoré zodpovedajú prípadom keď sa nezhodli. Tieto dve fázy samozrejme nie možné zameniť. V priemere sa obidvaja zhodnú zhruba v polovici prípadov. Aby si boli istí, že majú skutočne rovnaký kľúč, tak zverejnia aj niektoré bity zo získaného kľúča. Ak pri porovnaní zistia nejaké chyby, tak vedia, že niekto sa snažil ich komunikáciu rušiť, nebodaj odpočúvať. Nepriateľ môže posielané kvantové bity zachytávať a posielať adresátovi úplne vymyslené stavy. Našťastie neexistuje spôsob ako by mohol zistiť, ktorý stav bol poslaný. Klonovanie kvantových stavov tiež nefunguje. Strategicky môže počkať na fázu, v ktorej sa zverejnia bázy, aby mohol uskutočniť merania. Jeho prítomnosť sa však nutne prejaví ako istá chybovosť výsledného reťazca bitov, t.j. kľúča. Adresátovi totižto nepriateľ podhadzoval vymyslené stavy, ktoré sú iba so štvrtinovou šancou správne. Aby sme ho skutočne odhalili, tak potrebujeme zverejniť zhruba polovicu svojich „správnych“ bitov. V tretej fáze teda overujeme bezpečnosť kľúča.

Kryptografia v praxi

Ako to už býva, v praxi sa stretávame s „drobnými“ problémami. Ako zabezpečiť prenos fotónu z jedného miesta na druhé spôsobom, aby ho neustále interakcie s prostredím, čo namenej zmenili, t.j. minimalizovať šum? Ako pripraviť jeden jediný fotón? Ako postaviť detektor, ktorý vždy detekuje prítomnosť, alebo neprítomnosť fotónu? Jednou z možností, ako vyriešiť tieto problémy, je jednoducho sa vykašlať na fotóny a skúsiť iné kvantové systémy. Fotóny sú však veľmi lákavé objekty, najmä vďaka svojej rýchlosti. Chceme predsa komunikovať čo najrýchlejšie. Na krátku vzdialenosť protokol BB84 nie je veľmi zložité zrealizovať priamo s polarizáciami fotónu. Dokonca by to išlo aj u Vás v škole. Postačí laserové ukazovátko, polarizačné okuliare, prípadne polarizačné filtre používané pri fotografovaní. Tento experiment nespĺňa síce všetky požiadavky bezpečnosti, ale to by Vás nemalo odradiť.

Druhou nevýhodou polarizácie je, že pri prenose na trochu dlhšie vzdialenosti je šum už príliš veľký. Ani pri prenose optickými vláknami, v ktorých je šum menší, zmenu polarizácie nevieme kontrolovať. Preto namiesto polarizačných stavov sa v reálnych experimentoch používajú iné kvantové stavy fotónu, ktoré sú na vplyvy prostredia menej citlivé. Svojimi experimentami v oblasti kvantovej kryptografie sa preslávila v Európe najmä skupina *prof. Nicolasa Gisina* v Ženeve. Okolo Ženevského jazera sa im podarilo preniesť šifrovací kľúč pomocou optických vlákien na vzdialenosť zhruba 67 km, čo bolo svojho času rekordom v tejto oblasti. Dokonca tam funguje malá firma s názvom *Id Optique*, ktorá predáva „plug and play“ zariadenie realizujúce protokol BB84.



Obr.2. *Na obrázku sú znázornené prvé dve fázy protokolu BB84, t.j. fáza vygenerovania núl a jednotiek na oboch stranách a spracovanie podľa následného zverejnenia báz, resp. nastavení polarizátora. Symbolom + označujeme bázu horizontánej a vertikálnej polarizácie. Diagonálna báza je označená ako x.*

V dnešnej dobe niektorí experimentátori prakticky po celom svete vedia preniesť šifrovací kľúč na vzdialenosti zhruba 100 km. Bohužiaľ, táto hranica je už na úrovni technologických možností dnešných optických káblov. Aj preto sa stále venuje pozornosť možnostiam prenosu fotónov vo vzduchu. Šum je v porovnaní s optickými vláknami síce oveľa väčší, ale ideou je prekonať iba asi 15km vzdialenosť smerom k najbližším sondám a potom pokračovať v prenose v tejto výške nad povrchom Zeme. V tejto výške je už atmosféra natoľko riedka (de facto už nie je), že aj šum pri prenose by bol oveľa menší a fotóny by neporušené mohli prekonať veľké vzdialenosti. Prvé experimenty tohoto typu sa uskutočňovali v Spojených štátoch americkým, ale aj napríklad v prostredí európskych Álp, kde nie sú rušivé vplyvy mestského prostredia. Pred zhruba dvoma rokmi experimentátori zo susednej Viedne uskutočnili prenos vzduchom ponad Dunaj. Nedávno bola kvantová kryptografia využitá aj na zabezpečenie prevodu peňazí medzi bankami. Zdá sa, že kvantová kryptografia si pomaly hľadá svoje uplatnenie aj v praktickom živote.

Protokol BB84 neslúži priamo na prenos informácie, ale rieši problém bezpečnej distribúcie šifrovacieho kľúča potrebného pre realizáciu Vernamovej šifry. Jediné, čo využívame je princíp superpozície (stavy $|+\rangle, |-\rangle$ sú superpozíciami stavov horizontálne a vertikálne polarizovaných fotónov) a princíp neurčitosti, ktorý zabraňuje nepriateľovi zakódovanú informáciu odhaliť. Poprvýkrát v histórii kryptografie je bezpečnosť zaručená fyzikálnymi zákonmi a princípmi. Všetky známe a používané šifry využívajú zložitosť tzv. jednosmerných matematických úloh. Príkladom takejto úlohy je rozklad na prvočísla. Každý ľahko určí výsledok násobenia dvoch prvočísiel 17x29, ale viete súčinom akých prvočísiel je 1643? Skúste obidve tieto úlohy vyriešiť a porovnajte si čas, ktorý ste na riešenie potrebovali. Jedným smerom (súčin) je úloha ľahká, kdežto pri opačnej úlohe už hovoríme o probléme. Práve na tomto princípe

je založené aj známa tzv. *RSA šifra*. Problém je tak zložitý, že ani použijúc tie najlepšie metódy, ktoré poznáme, nevyriešime faktorizáciu veľkých čísiel v rozumnom čase. Aj na tých najlepších počítačoch by sme potrebovali čas, ktorý presahuje vek vesmíru. Na druhej strane súčin aj pre takto veľké čísla je pomerne jednoduchou záležitosťou. Hlavne pre najnovšie počítače. Naša bezpečnosť v istom zmysle závisí na našej neschopnosti a nie je ani jasné, či táto neschopnosť je principiálna, alebo nie. Nech je to už akokoľvek, okrem toho, že kvantová teória ponúka vlastné riešenia pre kryptografiu, tak tzv. kvantový počítač by bol schpný súčasnú bezpečnosť do istej miery narušiť. Napríklad, by nám umožnil rozfaktorizovať zhruba rovnakou, alebo aspoň rádovo porovateľnou, rýchlosťou ako násobiť. O kvantovom počítači si povieme niečo nabudúce.

MÁRIO ZIMAN