Foton jako důvěryhodný kurýr

Co je to kvantová kryptografie

MILOSLAV DUŠEK
ONDŘEJ HADERKA
MARTIN HENDRYCH

Záhadný ornament, v němž věhlasný Sherlock Holmes rozpoznal jednoduchou šifru (zpráva zní: AM HERE ABE SLANEY). Každému písmenu abecedy je přiřazena jedna póza tančící postavičky (Sir Arthur Conan Doyle: *The Adventure of the Dancing Men*).

Nejen zamilovaní touží po důvěrné komunikaci, ale – snad odjakživa – také vojáci, diplomati, spiklenci, teroristé a mnozí další. S rozvojem počítačových sítí, v nichž putují z místa na místo nejrůznější důvěrné obchodní informace, osobní či zdravotní údaje lidí a s jejichž pomocí se provádějí rozmanité finanční transakce, se ovšem potřeba bezpečné komunikace stále bezprostředněji dotýká každého z nás. Kvantová kryptografie nabízí zajímavý způsob jak zabránit, aby se k přenášené informaci dostala neoprávněná osoba. Spoléhá se při tom na fundamentální kvantové zákonitosti našeho fyzikálního světa.

Proč vlastně kvantová kryptografie?

Když je řeč o kryptografii,[1] mnohé z nás snadno zavede vlastní fantazie k mysteriózním obrazům z prostředí tajných agentů a spěchajících generálských pobočníků. Od takové směsice romantiky a mrazení v zádech nás dnes ale každodenní realita přece jen rychle přivede zpět na pevnou zem. Tajnými hesly se denně připojujeme k počítačovým sítím, tajný PIN vyťukáváme na klávesnici bankomatu a v profesi i v soukromí často manipulujeme s informacemi, které bychom chtěli před zveřejněním chránit, ať už z důvodů obchodních, či osobních.

Taková potřeba samozřejmě není nikterak nová. Mezopotámští hrnčíři zaznamenávali složení svých vzácných glazur šifrou už kolem roku 1500 př. n. l. Sparťanští vojenští velitelé používali již ve čtvrtém století př. n. l. speciální šifrovací pomůcku: zužující se kolík, na nějž se navinul pásek kůže či pergamenu, na který se pak napsala tajná zpráva. Po rozvinutí byla písmena „zpřeházená“. Navinul-li se ale pásek znovu na kolík stejných rozměrů, zpráva byla opět čitelná. Julius Caesar šifroval své rozkazy do římských provincií a na bojiště tak, že je psal v abecedě posunuté o několik písmen (obvykle o tři). Od starověku až do současnosti se neustále zkvalitňovaly jak šifrovací metody, tak schopnosti luštitelů. Dnes existuje řada rafinovaných a matematicky propracovaných šifrovacích postupů.

Vždy jde samozřejmě o to, aby informace byla srozumitelná pouze tomu, komu je určena. Proto se odesílatel a příjemce musí předem domluvit na nějakém konkrétním algoritmu, s jehož pomocí budou zprávy šifrovat a dešifrovat (ten může být veřejně známý), a na klíči (heslu), který však oba musí uchovat v tajnosti. Klíč představuje spolu se zprávou vstup do algoritmu, na jehož výstupu obdržíme šifru.

Šifrovací algoritmy fungují např. tak, že generují (na základě zvoleného klíče) pseudonáhodnou posloupnost čísel a podle ní nějakým způsobem mění nebo přeskupují jednotlivé znaky zprávy.[2] Jiné algoritmy provádějí operace s celými bloky dat. „Zamíchají“ určitý kus zprávy tak, aby každý bit výstupní šifry závisel na všech vstupních bitech (z dané části zprávy) a na všech bitech klíče. Moderní kryptografie zná však ještě jiný velmi zajímavý postup – metodu veřejného klíče. Ta se objevila koncem sedmdesátých let a dnes je velmi rozšířená. Jde o to, že místo jednoho klíče se používají klíče dva. Jeden z nich zveřejníte, druhý ponecháte tajný. Každý pak může zprávu pomocí „veřejného“ klíče zašifrovat. Správně ji přečíst lze ovšem již jen s „privátním“ tajným klíčem (viz Vesmír *71*, 615, 1992/11).

Ve skutečnosti ale zprávy zašifrované těmito a podobnými způsoby mohou být, alespoň v principu, rozluštěny. Jejich bezpečnost spočívá v tom, že luštění bez znalosti klíče je matematicky velmi, velmi náročné. Některé matematické operace je totiž docela snadné provést v jednom směru, ale obtížné ve směru inverzním. Obtížné v tom smyslu, že počet elementárních operací, které je nutno vykonat, roste exponenciálně s délkou klíče. Třeba algoritmus RSA,[3] který je představitelem metody veřejného klíče, se spoléhá na to, že není snadné faktorizovat (rozložit na prvočinitele) velká čísla. Zdálo se, že ani se současnými superpočítači nelze takto utajené zprávy rozluštit v rozumném čase. Pokrok v technologii i v matematických algoritmech je však neuvěřitelně rychlý. V roce 1994 požádali Arjen Lenstra a Mark Manase uživatele internetu o možnost použít jejich výpočetní prostředky, a tak spojením mnoha počítačů a použitím efektivní metody kvadratického síta rozložili na součin dvou prvočísel za osm měsíců 129ciferné číslo ze souboru RSA (bylo při tom nutno provést 10^{17} elementárních početních operací).

1) Slovo *kryptografie* je řeckého původu a volně přeloženo znamená „psaní tajným písmem“. Kryptografie – věda o šifrování – je součástí širšího oboru – *kryptologie*. Obsahuje navíc ještě *kryptoanalýzu*, nauku nebo spíše umění luštit šifry bez znalosti klíče.

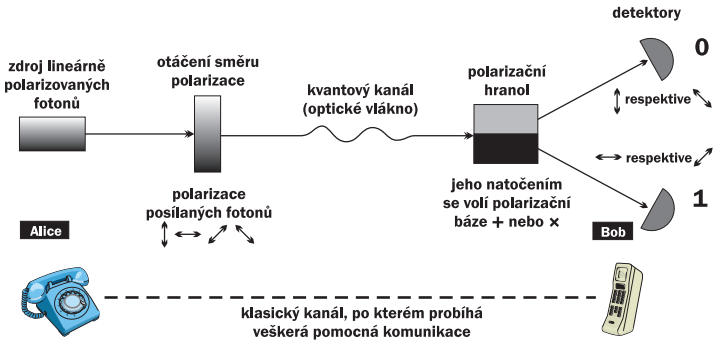
2) Nestačí, aby zpráva byla na první pohled nečitelná. Např. různá písmena se v přirozeném jazyku vyskytují různě často. Toho lze velmi dobře využít při luštění jednoduchých šifer. Proto i podobné „jemnosti“ musí být dobrou šifrovací metodou „zamlženy“.

3) Označení podle jmen autorů: Rivest, Shamir a Adleman.

RNDr. Miloslav Dušek, Dr., (*1964) vystudoval Matematicko-fyzikální fakultu UK. Na katedře optiky Přírodovědecké fakulty Univerzity Palackého v Olomouci se zabývá kvantovou a koherenční optikou, zvláště kvantovými korelacemi a kvantovou kryptografií.

Dr. Ondřej Haderka (*1968) vystudoval Přírodovědeckou fakultu Univerzity Palackého v Olomouci, doktorát získal na UK v Praze. Ve Společné laboratoři optiky UP a FzÚ AV ČR se zabývá nelineárními jevy spojenými s generací ultrakrátkých laserových pulzů, kvantovou statistikou nelineárních procesů a kvantovou kryptografií.

Mgr. Martin Hendrych (*1971) vystudoval Přírodovědeckou fakultu UP v Olomouci. Ve společné laboratoři optiky UP a FzÚ AV ČR se v rámci postgraduálního doktorandského studia věnuje experimentální práci na kvantové kryptografii.



1. Schéma kvantového kryptografu pracujícího s polarizovanými fotony

Ještě větší nebezpečí pro klasické matematické kryptografické metody ale představují kvantové počítače (Vesmír *76*, 250, 1997/5). Kvantové počítače pracují s kvantovou superpozicí všech možných stavů kvantového registru. V jediném kroku tedy mohou „sledovat" mnoho různých cest zároveň. Byly navrženy sofistikované postupy využívající tyto vlastnosti např. právě k velmi rychlé faktorizaci velkých celých čísel. Ačkoli mají kvantové počítače k praktické realizaci zřejmě zatím ještě dost daleko, intenzita, s jakou se na jejich stavebních prvcích pracuje, a zprávy o prvních laboratorních výsledcích jsou velmi povzbudivé.

Přece jen ale existuje jedna poměrně jednoduchá a přitom bezpečná šifrovací metoda. Poprvé ji popsal v roce 1918 Gilbert S. Vernam. Dnes je využívána např. na telefonní lince mezi Bílým domem a Kremlem. V roli klíče v ní vystupuje náhodná posloupnost stejné délky, jako je zpráva. Tato posloupnost (klíč) se ke zprávě „přičte" (viz rámeček na této straně). Jestliže se stejný klíč zas „neodečte", je zpráva zcela nečitelná. Bezpečnost přenosu je tedy zcela závislá na utajení klíče. Dovedeme bezpečně přenést zprávu,[4] ale jen tehdy, když se nám nejdřív podaří bezpečně přenést klíč.

Zdá se, že jsme narazili na kryptografickou „Hlavu XXII". Jak dosáhnout toho, aby odesílatel i příjemce měli stejný klíč, a zároveň mít jistotu, že jej nezískal nikdo třetí? Můžeme klíč poslat po důvěryhodném kurýrovi. Ale který kurýr je zaručeně důvěryhodný?

Vypadá to tak, že dokonalá bezpečnost je jenom snem. Právě zde však nabízí pomocnou ruku kvantová fyzika. Možná vás už napadla otázka, co by mělo být na kvantové kryptografii vlastně kvantového. Odpověď zní: klíč se nepřenáší klasickým způsobem jako „abeceda", do níž se informace pro přenos kóduje, používá se totiž kvantových stavů jedné částice (např. fotonu). Jakýkoli pokus o odposlech obecně ovlivní podstatně stav částice, a může být proto odhalen (viz rámeček na protější straně). Při zjištění odposlechu se přenášený klíč prostě nepoužije. K žádnému úniku informace pochopitelně nedojde (klíč je jen pomocná náhodná posloupnost). Proč tedy kvantová kryptografie? Protože řeší problém distribuce kryptografického klíče. Neumí sice odposlechu zabránit, ale umožňuje spolehlivě zjistit, zda k odposlechu došlo. A to v případě přenosu klíče úplně stačí.

Jak to tedy funguje?

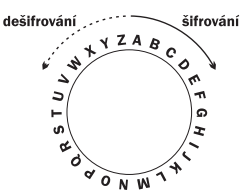
Předpokládejme, že odesílatel – obvykle označovaný jako *Alice* – a příjemce – *Bob* – si chtějí vyměnit tajný klíč prostřednictvím přenosového kanálu, který je v principu přístupný odposlechu třetí osobou označovanou jako *Eva* (podle anglického „eavesdropper" = ten, kdo tajně naslouchá). Klíč je reprezentován náhodnou posloupností nul a jedniček. Funkci kvantového kryptografického systému si vysvětlíme na jednoduchém modelovém uspořádání využívajícím lineárně polarizované fotony. Jeho schéma je na obr. 1. Binární znaky 0 a 1 budou kódovány do dvou stavů fotonu se vzájemně kolmými lineárními polarizacemi. *Alice* a *Bob* se samozřejmě musí domluvit, které konkrétní směry polarizace zvolí, tedy jaké použijí *polarizační báze* – viz obr. 2.

Uvažujme napřed, že *Alice* a *Bob* budou používat pouze fotony polarizované vodorovně („1") a svisle („0"). *Alice* bude vysílat náhodnou sekvenci jedniček a nul. Protože *Bob* používá stejnou polarizační bázi jako *Alice*, je chování fotonů na jeho polarizačním hranolu zcela jednoznačné: všechny fotony polarizované ve směru ↔ jsou odkloněny na jeden detektor a všechny fotony polarizované ve směru ↕ na

VERNAMOVA ŠIFRA

Je to asi jediná šifrovací metoda, jejíž bezpečnost je matematicky dokazatelná. Její princip spočívá v tom, že se zpráva zakóduje pomocí stejně dlouhé náhodné posloupnosti (klíče), čímž získá charakter zcela náhodného sledu znaků. Takový klíč může být pochopitelně použit pouze jednou (proto se této metodě v angličtině říká také *one time pad*) a musí být *skutečně* náhodný a nekorelovaný. Bez znalosti klíče nelze zprávu rozluštit. Jinými slovy, pravděpodobnosti všech možných výsledků jsou stejné. Neoprávněný luštitel má stejnou šanci dostat Shakespearovy sonety jako třeba daňové zákony. Opakované použití klíče nebo jeho části, či jakákoli pravidelnost v něm mohou dát luštitelům určitou šanci.

Jak šifrování a dešifrování probíhá, ukazuje následující jednoduchý příklad. Používáme-li např. abecedu o 26 znacích, potřebujeme jako klíč sekvenci náhodných čísel z intervalu 0 až 25 (odesílatel i příjemce musí mít pochopitelně stejný klíč). Při šifrování se prostě posuneme v abecedě o patřičný počet míst (daný odpovídající hodnotou klíče) vpřed, při dešifrování vzad (viz obrázek).



zpráva	V	E	R	N	A	M
klíč	7	23	11	5	0	16
šifra	C	B	C	S	A	C

V případě binárně kódované zprávy je situace ještě jednodušší. Klíč má podobu náhodné posloupnosti nul a jedniček (stejně dlouhé, jako je zpráva), kterou můžeme získat třeba házením mincí. Při šifrování i dešifrování se bity zprávy a klíče jednoduše sečtou modulo 2 (pro lid počítačový – jde o operaci XOR):

zpráva	1	1	1	1	0	0	0	0
klíč	1	0	1	0	0	1	1	0
šifra	0	1	0	1	0	1	1	0

šifrovací a dešifrovací předpis

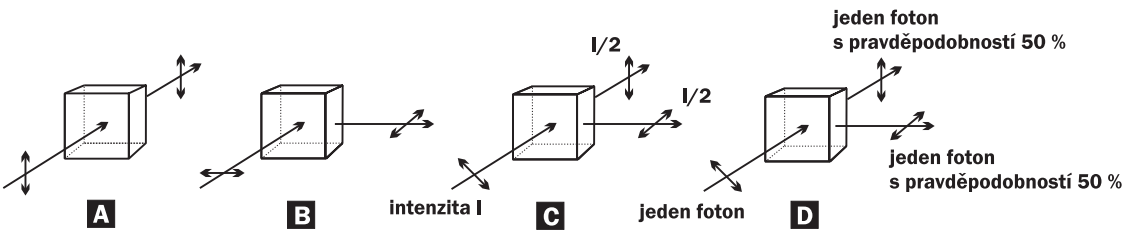
11 → 0
10 → 1
01 → 1
00 → 0

4) Tj. tak, aby nebyla prozrazena.

5) V principu jsou možné i způsoby měření polarizace, při nichž foton není pohlcen detektorem, ale pokračuje dál. Dá se však ukázat, že výsledný efekt (ovlivnění stavu fotonu měřením) je úplně stejný. Zákony kvantové mechaniky navíc zabraňují *Evě* i ve vytvoření dostatečně přesné kopie neznámého polarizačního stavu fotonu. Nemůže si tedy jen tak udělat duplikát přilétajícího fotonu a *nezměněný* originál poslat *Bobovi*. Jakákoli interakce bude mít na stav fotonu určitý vliv.

ROZDÍL MEZI KLASICKÝM A KVANTOVÝM MĚŘENÍM

Odposlouchávat znamená provádět „měření“ na fyzikální entitě nesoucí informaci. V klasické fyzice lze hodnotu kterékoli veličiny změřit víceméně libovolně přesně. Navíc vliv, který má měření na měřený objekt, lze teoreticky libovolně zmenšit. Úplně jinak je tomu ale v kvantové mechanice, která popisuje chování přímé zkušenosti vzdáleného mikrosvěta (viz Vesmír *77*, 189, 1998/4). Některé fyzikální veličiny se prostě na určitých stavech systému (třeba atomu či částice) přesně změřit nedají. Kdybychom opakovali měření na dokonalých kopiích systému, dostávali bychom nejrůznější výsledky, pouze některé častěji, jiné méně často. Krom toho kvantové měření stav systému obecně změní (to je ona podstatná vlastnost, ze které kvantová kryptografie těží). Přibližme si to na jednoduchém příkladu měření lineární polarizace světla. Z hlediska klasické fyziky je světlo elektromagnetické vlnění. Kmitá-li vektor elektrického pole pouze v jednom směru (kolmém ke směru šíření vlny), mluvíme o lineární polarizaci. Existují optické prvky (polarizační hranoly), které umožňují rozdělit dopadající svazek světla na dva svazky polarizované ve dvou pevně určených vzájemně kolmých směrech (řekněme svisle a vodorovně). Dopadne-li tedy na hranol svisle polarizované světlo, projde veškerá jeho intenzita na výstup odpovídající svislé polarizaci (obr. A). Podobně se všechno vodorovně polarizované světlo odrazí (odbočí vpravo – obr. B). Dopadá-li však na hranol světlo polarizované „šikmo“ (pod úhlem 45°), rozdělí se na složku se svislou a složku s vodorovnou polarizací, obě s poloviční intenzitou (obr. C). Dnes ale víme, že se světlo skládá z nedělitelných kvant energie – z fotonů. Co se stane, dopadne-li na polarizační hranol jediný foton? Je-li polarizován svisle jako na obr. A (i pro jediný foton má stále smysl mluvit o polarizaci), pak prostě projde. Je-li naopak polarizován vodorovně, vždy se odrazí (obr. B). Jestliže je ale polarizován „šikmo“, pak ho s pravděpodobností 50 % „spatříme“ projít rovně a od té chvíle bude polarizován *svisle*, s pravděpodobností 50 % *uvidíme*, že se odrazí doprava a změní svou polarizaci na *vodorovnou* (obr. D). Někdy tedy projde, jindy se odrazí a jeho výsledná polarizace bude pokaždé jiná!



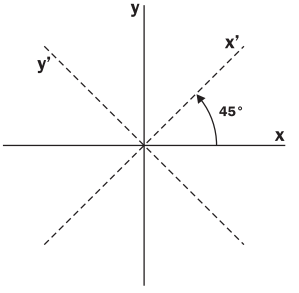
druhý (viz obr. A a B v rámečku o kvantovém měření). *Bob* je tedy schopen sekvenci bitů posílaných *Alicí* bezchybně přijmout (v ideálním případě).

Co se stane, bude-li přenosový kanál odposlouchávám? Především si musíme vyjasnit, *jak* může být odposlouchávám. Klasický pasivní odposlech, kdy se *Eva* (ta potvora zvědavá) prostě napojí na kanál, čímž odvede malou část signálu stranou a na ní pak provádí měření, nepřichází v úvahu. To proto, že pro přenos každého bitu je použit právě jeden foton, a ten se nemůže rozdělit. Udělá-li *Eva* na přenosovém kanálu „odbočku“, foton buď pokračuje k *Bobovi* a ona nemá nic, nebo odbočí k *Evě*, ale pak zase nedojde k *Bobovi* a příslušný bit nebude použit v klíči (s podobnými „výpadky“ se počítá, neboť některé fotony se pochopitelně mohou na trase ztratit i „přirozenou“ cestou – vlivem nejrůznějších „technologických“ ztrát). Jediná rozumná strategie pro odposlech je použít podobné zařízení, jaké má *Bob*, provést měření polarizace a každý bit pak znovu poslat *Bobovi* podobným zařízením, jaké má *Alice*.[5] *Eva* ale neví, jakou polarizační bázi *Alice* a *Bob* používají. Jestliže pro svá měření zvolí polarizační bázi odlišnou od jejich, vnese každým měřením do přenášené sekvence s určitou pravděpodobností chybu. Při „nesprávném“ natočení svého polarizačního hranolu totiž nebude schopna s jistotou určit, jaké bity vlastně *Alice* vysílá. Kromě toho, bude-li *Bobovi* posílat fotony polarizované např. ve směrech ⤢ a ⤡, stanou se i výsledky *Bobových* měření zcela nezávislé na tom, co odeslala (viz obr. D v rámečku o kvantovém měření). Porovnají-li tedy *Alice* a *Bob* část přenesené sekvence, mohou odposlech odhalit.

Eva se však může nějak dozvědět, jakou polarizační bázi *Alice* s *Bobem* používají. Nebo má prostě štěstí a trefí se do ní. Pak by samozřejmě zůstala neodhalena. Tomu lze předejít tím, že jak *Alice*, tak *Bob* náhodně (a nezávisle) střídají polarizační báze + a × (tj. *xy* a *x'y'* na obr. 2). *Alice* tedy vysílá fotony náhodně polarizované ve směrech ↔, ↕, ⤢, ⤡, a *Bob* pro každý přicházející foton náhodně mění natočení polarizačního analyzátoru (střídá 0° a 45°, což odpovídá + a ×) – viz obr. 1. Po přenosu si veřejným kanálem (třeba telefonem nebo počítačovou sítí) vzájemně vymění informaci, v jakých polarizačních bázích kdy pracovali, a ponechají pouze ty bity, pro které použili stejné báze (neboť jedině tyto bity mohl *Bob* detegovat správně).

Popsaný postup sice snižuje přenosovou rychlost přibližně na polovinu, ale zajišťuje bezpečnost metody. *Eva* teď neví, jakou bázi má vybrat, a ať zvolí jakoukoli strategii, bude se vždy zhruba v polovině případů mýlit. Předpokládejme na chvíli, že *Alice* a *Bob* právě komunikují v bázi +, a že *Eva* chybně použije bázi × (nebo naopak). Výsledky měření *Evy* i *Boba* jsou pak zcela neurčité. Za těchto okolností by se sekvence přijatá *Bobem* lišila od sekvence vyslané *Alicí* přibližně v polovině všech bitů. Celkově způsobí nepřetržitý odposlech asi 25 % chyb (někdy také *Eva* použije náhodou správnou bázi).

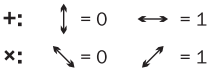
Srovnáním dostatečného počtu bitů (u kterých *Alice* a *Bob* předpokládají 100% shodu) lze odposlech odhalit. Není-li v systému jiný zdroj chyb, pak každá odchylka signalizuje přítomnost *Evy*. Porovnají-li *Alice* a *Bob* pouhých 100 náhodně vybraných bitů z přenesené sekvence, bude pravděpodobnost, že odposlech zůstane neodhalen, přibližně 10^{-13}. Celý



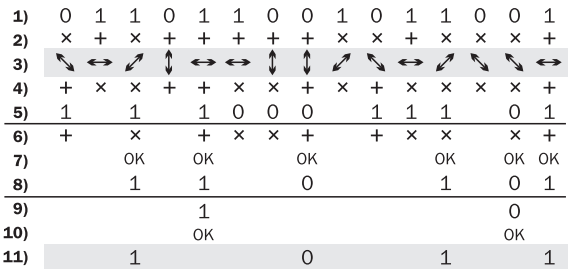
2. Dvě polarizační báze používané při kvantovém přenosu klíče. Každý posílaný foton je polarizován v jednom ze čtyř vyznačených směrů. „Jednička“ je kódována do polarizací *x* a *x'*, „nula“ do *y* a *y'*.

KVANTOVÝ PŘENOS KRYPTOGRAFICKÉHO KLÍČE (POLARIZAČNÍ KÓDOVÁNÍ)

***Alice* a *Bob* se především dohodnou na dvou polarizačních bázích otočených vzájemně o 45°, které budou používat, a na tom, která ze dvou vzájemně kolmých lineárních polarizací fotonu v každé bázi bude značit „0“ a která „1“. Např.**



***Alice* pak generuje náhodné bity, vybírá náhodně polarizační báze a pootáčí odpovídajícím způsobem polarizaci fotonů, které posílá *Bobovi*. *Bob* nezávisle na ní také náhodně volí polarizační báze a podle toho pro každý přicházející foton natáčí svůj polarizační hranol, na jehož dvou výstupech má umístěny detektory fotonů – jeden odpovídá „0“, druhý „1“. Nakonec si *Alice* a *Bob* veřejně sdělí, jaké báze použili, a ponechají jen tu část přenesených bitů, kde se v bázích shodli. (Sdělí si *pouze* báze, ne konkrétní polarizace fotonů!) Část přenesené bitové sekvence obětují (později už ji nemohou použít k jiným účelům). Zveřejní ji, aby ji mohli vzájemně porovnat a odhalit tak případné rozdíly prozrazující působení odposlouchávající *Evy*. Celé je to zachyceno v následujícím schématu:**



I. KVANTOVÝ PŘENOS:

1) náhodné bity vytvořené *Alicí*,

2) náhodně vybrané vysílací polarizační báze *Alice*,

3) polarizace fotonů posílaných *Alicí*,

4) náhodně vybrané přijímací polarizační báze *Boba*,

5) bity obdržené *Bobem* (prázdná místa znamenají, že se foton ztratil – nebyl detegován).

II. VEŘEJNÁ DISKUSE:

6) *Bob* oznamuje báze, ve kterých naměřil fotony,

7) *Alice* oznamuje, které báze byly zvoleny stejně,

8) přenesená náhodná sekvence bitů (nenaslouchala-li *Eva*, má *Bob* přesně to, co *Alice* poslala).

III. OBĚTOVÁNÍ BITŮ:

9) *Bob* obětuje některé náhodně vybrané bity k odhalení *Evy*,

10) *Alice* potvrzuje tyto obětované bity; *Eva* by způsobila odchylky),

11) zbylé tajné bity sdílené *Alicí* a *Bobem* – klíč.

Popsaný přenosový protokol se nazývá BB84 podle Bennetta a Brassarda, kteří jej v roce 1984 navrhli.

průběh přenosu kryptografického klíče je shrnut v rámečku na této straně.

Poznamenejme, že *Eva* by v zásadě mohla nějakým způsobem zasahovat i do komunikace po veřejném kanálu. Mohla by ho třeba přerušit a tvářit se vůči *Alici* zcela jako *Bob* a vůči *Bobovi* jako *Alice*. S každým z nich by si přitom vyměnila (obecně jiný) klíč. Pak by mohla bez problémů přečíst zprávu zašifrovanou kýmkoli z nich.

Informace posílané po veřejném kanálu je proto třeba *autentizovat*. Příjemce musí být schopen ověřit, že zpráva pochází od „správného“ odesílatele a že nebyla cestou pozměněna. K tomuto účelu musí *Alice* a *Bob* sdílet na začátku jisté malé množství tajné informace, které jim slouží jako počáteční heslo pro autentizaci.[6)]

Hlavní výhodou kvantové kryptografie je, že Eva je nakonec vždy odhalena (Antonio Rizzo, Eva, 2. polovina 15. století, mramor)

Protože v každém reálném zařízení existuje šum, který způsobuje chyby během přenosu, v praxi nezbývá než nějaké malé procento odchylek v *Alicině* a *Bobově* posloupnosti tolerovat. Nevadí, řeknete, existují přece způsoby jak chyby opravit. Ano, ale máme-li být důslední, musíme předpokládat, že chyby nezpůsobilo zařízení, nýbrž *Eva*, která tak něco málo zvěděla o klíči. Naštěstí se dá odhadnout, jakou informaci o klíči může *Eva* nanejvýš získat, tolerujeme-li chybovost např. do 1 %. S touto znalostí pak můžeme použít matematickou proceduru nazývanou *zesílení utajení*, která za cenu zkrácení klíče *Evinu* informaci minimalizuje.

Pro úplnost dodejme, že vedle metod kvantové kryptografie používajících stavy jednotlivých fotonů existují i takové, které pro přenos klíče využívají „podivné“ vlastnosti tzv. *propletených stavů* dvojic fotonů (Vesmír 77, 333 a 393, 1998/6 a 7). *Alice* a *Bob* mají v tomto případě každý k dispozici vždy jeden foton z propleteného páru a každý měří jeho polarizaci. Tentokráte oba pouze náhodně střídají dvě polarizační báze (tedy natočení svých polarizačních hranolů). O náhodnou volbu jednotlivých bitů se postará kvantová mechanika sama. Nakonec si *Alice* a *Bob* opět báze porovnají a ponechají jen ty bity, kde se v bázích shodli.

Retrospektiva a perspektivy

Myšlenka využít zákony kvantové mechaniky pro účely kryptografie se pravděpodobně poprvé objevila počátkem sedmdesátých let u Stephena Wiesnera. Publikována však byla až r. 1983. První prakticky použitelné schéma pro kvantovou distribuci klíče přišlo o rok později. Jeho autory byli Američan

6) Po každém přenosovém aktu je toto „heslo“ nahrazeno novým (pro příští použití), „dočerpaným“ z přeneseného klíče. Je-li klíč dost dlouhý, aby z něho potom ještě něco zbylo, lze postupně – opakováním kvantového přenosu takových dílčích „klíčů“ – vytvořit libovolně dlouhou tajnou náhodnou posloupnost, kterou bude *Alice* sdílet s *Bobem*.

7) Omezení vzdálenosti je podmíněno ztrátami ve vlákně a šumem detektorů (detektor občas pošle impulz, i když na něj nedopadne žádný foton). Jakmile počet fotonů přicházejících za jednotku času poklesne vlivem ztrát natolik, že je srovnatelný s počtem šumových impulzů detektoru, přestává být zařízení použitelné. Zesilovače použít nelze, protože by ovlivňovaly kvantový stav částic podobným způsobem jako odposlech.

8) Něco málo o tom, jak pracuje interferometr, se můžete dočíst např. ve Vesmíru 77, 129, 1998/3. Výklad různých metod kvantové kryptografie je stručně podán v článku M. Duška *Kvantová kryptografie*, Pokroky matematiky, fyziky a astronomie *41*, 113, 1996/3. Podrobnější údaje o zmiňovaném experimentálním zařízení lze nalézt v článku M. Duška, O. Haderky a M. Hendrycha *Application of quantum key distribution for mutual identification – experimental realization*, Acta Physica Slovaca *48*, 169, 1998/3.

9) Připravit *jediný* foton není vůbec snadné. Ve skutečnosti nezbývá, než se spokojit jen s určitým „přiblížením“. Pulz laseru se musí zeslabit tak, aby pravděpodobnost, že v něm bude více než jeden foton, byla zanedbatelně malá ve srovnání s pravděpodobností výskytu právě jednoho fotonu. Nepříjemné na tom je, že tak slabé světelné pulzy neobsahují velmi často žádný foton. To pochopitelně snižuje efektivní přenosovou rychlost zařízení.

3. Vlevo: Řídící elektronika olomouckého kvantového kryptografického aparátu. Vpravo: „Alicina“ část zařízení. Jde vlastně o vláknový Machův-Zehnderův interferometr.

Charles H. Bennett a Kanaďan Gilles Brassard. Ti také (s dalšími spolupracovníky) uskutečnili r. 1989 první experiment s přenosem klíče. Využili k tomu polarizační stavy fotonu. Přenosovým kanálem o délce pouhých 32 cm byl volný prostor. Od té doby prodělává kvantová kryptografie bouřlivý rozvoj. Vedle velkého množství teoretických prací studujících různé varianty přenosových protokolů, podrobně analyzujících vliv šumu na bezpečnost přenosu a budujících základy kvantové teorie informace, přibývá i zpráv o úspěšných experimentálních zkouškách nových zařízení. V Evropě na experimentální kvantové kryptografii pracují výzkumné týmy ve Velké Británii a Švýcarsku. Ve Spojených státech je patrně nejdál skupina z Los Alamos. Současné kryptografické systémy používají jako přenosové médium vesměs optická vlákna a jsou testovány až do vzdáleností několika desítek kilometrů. Přenosové rychlosti jsou ovšem při takových vzdálenostech velmi malé: jednotky, maximálně desítky bitů za sekundu. Asi nejvíce se podmínkám potenciálního praktického použití přiblížili vědci z Univerzity v Ženevě, kteří vyzkoušeli kvantový přenos klíče prostřednictvím běžného optického telekomunikačního kabelu (vedeného pod Ženevským jezerem), jenž spojuje Ženevu s Nyonem (vzdáleným 23 km). Nastupující technologická generace optických vláken, detektorů a zdrojů světla by měla umožnit provoz do vzdálenosti padesáti až sta kilometrů.[7] Takový dosah je plně postačující např. pro počítačové sítě s bezpečnou komunikací mezi jednotlivými pracovišti bank či vládních úřadů v rámci velkých měst.

Možná se v duchu ptáte: „Máme něco takového také u nás?“ Máme. Na společném pracovišti Univerzity Palackého a Fyzikálního ústavu Akademie věd v Olomouci se podařilo postavit laboratorní vzorek kvantového kryptografu (obr. 3), jehož parametry jsou srovnatelné se zařízeními zkonstruovanými v zahraničních laboratořích. Zařadili jsme se tím mezi několik málo zemí, kde je tato problematika, alespoň na laboratorní úrovni, zvládnuta. Zařízení v Olomouci (podobně jako většina zařízení, která se dnes zkoušejí) ovšem nevyužívá zmíněné kódování do polarizačních stavů fotonu, nýbrž kódování fázové. To je technicky poněkud schůdnější (pro výklad však méně názorné). Na principu metody se ale nic podstatného nemění. Namísto pootáčení polarizací fotonů mění *Alice* pro každý posílaný foton velmi jemně délku jednoho ramene interferometru.[8] I zde má k dispozici čtyři možnosti odpovídající „0“ a „1“ ve dvou „bázích“. Podobně *Bob* místo točení polarizačním hranolem nastavuje délku druhého ramene (používá dvě hodnoty, vzájemně se lišící o čtvrtinu vlnové délky použitého světla). Všechno ostatní probíhá přesně tak, jak bylo popsáno. Přenos kryptografického klíče byl s tímto zařízením testován na vzdálenost půl kilometru. Jako kvantový kanál sloužilo optické vlákno, po němž se posílaly zeslabené světelné pulzy generované polovodičovým laserem.[9] Chybovost přenosu byla menší než 0,4 %.

Mezi nesporné výhody kvantové kryptografie patří bezpečnost přenosu garantovaná fyzikálními zákony (u klasických metod šlo spíš o to, zda vynálezci šifer „přechytračí“ luštitele, či naopak), ale také fakt, že klíč se generuje až v okamžiku, kdy je potřeba, čímž odpadají problémy s jeho skladováním. Kvantová kryptografie umožňuje nejen bezpečný přenos zpráv, ale například také spolehlivou vzájemnou identifikaci. Přihlašujete-li se třeba do počítačové sítě, není v principu nemožné vaše heslo v síti zachytit a příště se přihlásit místo vás. Kvantový identifikační protokol takovou možnost vylučuje.

Širšímu praktickému využití kvantové kryptografie brání zatím poměrně vysoká cena zařízení (některé součásti jsou opravdu „na hraně“ současné technologie) a relativně velké rozměry zbudovaných laboratorních prototypů. Je však jen otázkou času, kdy se obojí dostane do přijatelných mezí. Pak lze očekávat rychlý nástup kvantověkryptografických aplikací a možná malou revoluci v oblasti bezpečného přenosu informací. □

Výzkum v oboru kvantové kryptografie, na němž se autoři článku podílejí, je finančně podporován Ministerstvem vnitra ČR (19951997007, 19982003012), Ministerstvem školství ČR (VS 96028) a Grantovou agenturou ČR (202/95/0002).

Kresba © Špína ‘98