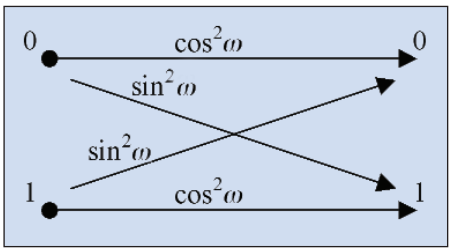
Kryptologie pro praxi – Agent Foton

Na první pohled by se mohlo zdát, že téma tohoto dílu patří stále spíše do vědeckofantastické literatury, avšak vězte, že v užším kruhu byly základní principy využití jevů kvantové fyziky v kryptografii formulovány již kolem roku 1970 [5], tedy zhruba šest let před veřejnou formulací fenoménu asymetrické kryptografie [3]. Patrně díky technologické základně však tehdy zůstalo jen u teoretických úvah, které byly posléze znovu objeveny v osmdesátých letech minulého století, kdy vznikl koncept takzvané kvantové kryptografie. Za jeden ze stěžejních příspěvků té doby lze považovat protokol označovaný jako BB84 [2], umožňující bezpečné ustanovení sdíleného symetrického klíče po kanálu, který není chráněn proti odposlechu. S ohledem na druh služby, který tento protokol poskytuje, jej můžeme považovat za analogii k dnes již klasickému asymetrickému protokolu dohody na klíči podle Diffieho-Hellmana, který popisujeme v ST 5/2004 [6].

Kromě protokolu BB84, na který se zde pro ilustraci zaměříme, nabízí současná kvantová kryptografie mnoho dalších zajímavých schémat, přičemž některá z nich mohou poskytovat analogické služby jako jisté protokoly asymetrické kryptografie. Rozdíl mezi těmito schématy tkví ve způsobu, jakým je garantována jejich bezpečnost. Víme, že v asymetrické kryptografii spoléháme na omezenou výpočetní sílu útočníka. Z praktického hlediska jsou tato omezení sice více než dostatečně naddimenzována, avšak kvalitativně se přece jen jedná o jiný druh podmínek, než na jakých je založena kvantová kryptografie. Ta sází na platnost zákonů takzvané kvantové mechaniky (viz například čtivá monografie [4]), jejichž neplatnost by znamenala naprosto zásadní převrat ve fyzikálním chápání světa. S mírnou dávkou cynismu a spekulací lze prohlásit, že pokud by došlo k prolomení principů kvantové kryptografie, pak by měl každý z nás nejspíš poněkud jiné starosti, než zdali mu někdo cizí čte důvěrné elektronické dopisy. Zákony kvantové mechaniky dále ukazují na existenci takzvaných kvantových počítačů ([4], [6]), které jsou schopny schůdným způsobem řešit matematické úlohy garantující bezpečnost řady asymetrických schémat včetně RSA (ST 3/2004), DSA (ST 4/2004) a již zmíněného protokolu D-H. To vše díky velmi specifickým výpočetním operacím, které u klasických počítačů nemají obdoby. Na druhou stranu jejich konstrukce je technologicky nesmírně náročná a je nesnadné odhadnout dobu, kdy bude možné kvantový počítač o odpovídající výpočetní síle, byť i za cenu obrovských investic, sestavit. Optimistické odhady se vesměs pohybují v řádu desítek let. V běžné kryptografii se proto zatím s hrozbou tohoto fenoménu nepočítá. Nicméně v teoretické rovině je to zřejmý argument podporující výše uvedenou kvalitativně vyšší třídu bezpečnosti kvantových protokolů.



Obr. 1 Informační model fotonového kanálu

Protokol BB84

V centru naší pozornosti budiž lineárně polarizovaný světelný svazek, tedy světlo, jehož vektor elektrického pole kmitá pouze v jedné konkrétní rovině. Úhlem polarizace či prostě jen polarizací zde budeme rozumět úhel, který tato rovina svírá s rovinou horizontální, měřený proti směru hodinových ručiček. Polarizované světlo lze poměrně snadno získat příslušnou fyzikální aparaturou sestávající z vhodného generátoru světelného svazku a nastavitelného filtru. V principu se jedná o spojitou fyzikální veličinu, kterou můžeme změřit pomocí detektoru a polarizačního filtru. Intenzita světla dopadajícího na detektor bude odpovídat tomu, nakolik souhlasí jeho polarizace s tzv. osou filtru. Otáčením filtru pak snadno zjistíme, jakou polarizaci světlo má. To vše ovšem pouze za předpokladu, že světelný svazek obsahuje dostatečné množství elementárních kvant světelné energie – fotonů. Přesnost měření polarizace se rapidně omezí, pokud světelný zdroj vyšle pouze jediný polarizovaný foton. Označme α úhel polarizace měřeného fotonu a β úhel filtru před detektorem. Potom bude měřený foton s pravděpodobností $\cos^2(\alpha-\beta)$ zaznamenán detektorem a s pravděpodobností $1-\cos^2(\alpha-\beta) = \sin^2(\alpha-\beta)$ pohlcen filtrem. Víc informace nám zákony kvantové mechaniky získat nedovolí. Pro ilustraci uveďme například, že nelze vytvořit identickou kopii neznámého kvantového stavu (to znamená náš foton několikrát zkopírovat a nezávisle změřit), a jakmile měřený foton projde filtrem, získá polarizaci odpovídající ose filtru, atp. Poslední zmíněný postulát souvisí se skutečností, že v kvantovém světě čtení nosičů informace zároveň nevratně ovlivňuje jejich stav. Je to jev, který není závislý na technické či technologické výbavě čtenáře a který nemá v našem makrosvětě obdoby.

Díky chování kvantového světa můžeme radikálně změnit pohled na to, co to znamená doručit bezpečně šifrovací klíč po kanálu s nechráněným odposlechem. V makrosvětě musíme počítat s tím, že veškerá takto vyměňovaná data může útočník bez újmy na kvalitě libovolně číst, kopírovat, přenášet a ukládat. Vhodným návrhem protokolu pak musíme zaručit, aby mu odposlechnuté údaje nebyly k užitku. V mikrosvětě částic však můžeme vsadit na úplně jinou strategii – klíč prostě poslat a následně detekovat případný odposlech. Pokud se odposlech vyskytl, klíč zahodíme a pošleme jiný. Při sestavování protokolu umožňujícího detekci odposlechu vyjdeme právě ze skutečnosti, že čtení zprávy ovlivňuje její obsah.

Předpokládejme, že zdroj bude vysílat jednotlivé bity klíče (binární hodnoty 0/1) kódované do polarizace jednotlivých fotonů následovně: Má-li bit hodnotu 1, vyšle foton s polarizací ϕ, má-li hodnotu 0, vyšle foton s polarizací $\phi+\pi/2$. Úhel ϕ zde nazveme úhlem polarizační báze. Pokud příjemce zná hodnotu ϕ, může přijatou zprávu snadno dekódovat správně nastaveným polarizačním filtrem (úhel filtru je roven úhlu báze) a detektorem. Nese-li foton hodnotu 1, potom bude s jistotou zaznamenán detektorem, v opačném případě bude s jistotou pohlcen filtrem. Lze použít i prvek zvaný polarizační dělič se dvěma detektory [4], které mimo jiné eliminují některé strategie odposlechu, což pro jednoduchost ponecháme stranou. Uvažujme však, co se stane, když příjemce úhel báze nezná. Podle kvantové mechaniky mu nezbývá, než na svém filtru nastavit odhadnutý úhel γ a dekódovat fotony s chybou, kterou ilustruje *obr. 1*. Na něm vidíme in-

Tabulka 1 Základní fáze protokolu BB84

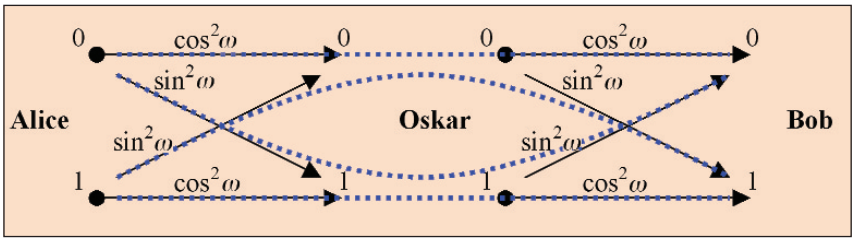
fáze I	vyslaný bit	1	0	1	1	0	1	0	0	1	0	0	0	1	...
	báze Alice	x	+	+	+	x	+	x	x	x	x	x	+	+	...
	polarizace	/	I	-	-	\	-	\	\	/	\	\	/	-	...
	báze Boba	+	+	x	x	x	x	x	x	x	+	x	+	+	...
	přijatý bit	0	0	1	0	0	0	0	0	1	-	0	0	1	...
fáze II	shoda báze	-	0	-	-	0	-	0	0	1	-	0	0	1	...
fáze III	výsledek	-	**0**	-	-	OK	-	**0**	OK	**1**	-	OK	**0**	**1**	...

formační model popsaného kanálu. V uzlech grafu jsou vyslané, respektive přijaté hodnoty nějakého bitu a na hranách jsou přechodové pravděpodobnosti popisující chybovost kanálu. Ta závisí na úhlu, který definujeme jako chybu v natočení filtru přijímače $\omega=\phi-\gamma$. Příslušné pravděpodobnosti lze snadno odvodit: vysílá-li zdroj hodnotu 0, má foton polarizaci $\phi+\pi/2$. Aby nedošlo k chybě na straně přijímače, musí být foton pohlcen filtrem. K tomu podle pravidel postulovaných výše dojde s pravděpodobností:

$p=\sin^2(\phi+\pi/2-\gamma) = \sin^2(\omega+\pi/2) = \cos^2\omega$.

S doplňkovou pravděpodobností $1-\cos^2\omega = \sin^2\omega$ přitom dojde k zaznamenání fotonu na detektoru, což v tomto případě znamená chybný příjem. Obdobně určíme i přechodové pravděpodobnosti pro případ, kdy je vysílána hodnota 1. Vidíme, že výsledkem je symetrický binární kanál, který se chová deterministicky, právě když $\omega = k.\pi/2$, kde $k\in\mathbf{Z}$. Jinak je výsledek zatížen náhodnou chybou, která v případech, kdy $\omega = (2.k+1).\pi/4$, kde $k\in\mathbf{Z}$, kanál zcela zaruší. Řečeno lapidárně: přijatý bit pak může být ve skutečnosti stejně tak dobře nulou jako jedničkou. Připomeňme, že toto platí bez ohledu na technologickou výbavu příjemce.

Protokol BB84 využívá uvedený model přenosového kanálu následujícím způsobem: pojmenujme vysílající stranu Alice, stranu příjemce Bob a útočníka Oskar. Průběh dohody na klíči mezi Alicí a Bobem znázorňuje *tabulka 1*. Hlavní myšlenka spočívá ve využití dvou polarizačních bází, které jsou vzájemně otočeny o $\pi/4$. První nazýváme rektilineární a značíme symbolem „+“, druhou pak nazýváme diagonální a značíme symbolem „×“. Jednotlivé polarizace fotonů pak značíme symboly uvedenými v *tabulce 2*, která zároveň předepisuje kódování vysílaných bitů v příslušných bázích. Z výše uvedeného rozboru víme, že pokud by příjemce zaměnil báze + a ×, získal by zcela nepoužitelný přenosový kanál. Této skutečnosti Alice využije tak, že pro každý zasílaný bit náhodného klíče volí náhodně i použitou polarizační bázi. Její volba je v tuto chvíli tajná i pro Boba, takže ten při příjmu volí bázi rovněž náhodně. Pokud se strefí (což bude zhruba v 50 % případů), přijme daný bit správně, v opačném případě získá náhodnou hodnotu. Takto Alice s Bobem postupují bit za bitem. Jakmile dojdou na konec posloupnosti, přijde na řadu druhá fáze, kdy si Alice s Bobem porovnají, v jakých bázích kdy komunikovali. Ponechají si pouze ty bity, kde se shodli. Dále je nutné ještě provést detekci odposlechu. Předpokládejme, že padouch Oskar bude během první fáze stejně jako Bob náhodně odhadovat zvolenou bázi, dekódovat v ní fotony od Alice a vysílat nové fotony k Bobovi. Podívejme se, jak se tato strategie projeví na bitech, které si Alice s Bobem nechali na konci druhé fáze. Pokud se i Oskar u takového bitu správně strefil do použité báze (pravděpodobnost je 1/2), bude mít Bob stejnou hodnotu tohoto bitu jako Alice. Pokud se Oskar zmýlil, bude výsledek přijatý Bobem náhodný, takže shoda s Alicí nastane s podmíněnou pravděpodobností 1/2. Dáno dohromady, Alice s Bobem mají u daného bitu z konce druhé fáze stejnou hodnotu s pravděpodobností 3/4. Ilustrace s využitím zavedeného modelu přenosového kanálu je na *obr. 2*, kde předpokládáme, že chybový úhel nabývá hodnot z množiny $\{-\pi/4, 0, \pi/4\}$, podle toho, v jaké bázi byl daný bit přenášen a zdali se Oskar do této volby trefil. Modře jsou vyznačeny cesty vedoucí ke shodě hodnot na straně Alice a Boba (tj. nedetekovaný odposlech). Nyní se dostáváme k třetí fázi, kterou můžeme nazvat obětováním bitů. Alice s Bobem si porovnají hodnoty pro n náhodně vybraných bitů z konce druhé fáze. Pokud se Oskar snažil nepřetržitě odposlouchávat, je pravděpodobnost, že budou všechna porovnání souhlasit $(3/4)^n$. Odposlech tak bude detekován s pravděpodobností $1-(3/4)^n$, což je vztah, podle kterého volíme n tak, abychom dosáhli požadované úrovně bezpečnosti.



Obr. 2 Odposlech na fotonovém kanálu

Tabulka 2 Kódování binárních hodnot

Hodnota/báze	1	0
+	-	|
	0	π/2
x	/	\
	π/4	3π/4

Pokud se vyskytne podezření na odposlech, startuje se celý protokol znovu od začátku. Výsledné sdílené tajemství je ve finále tvořeno zbylými bity na konci třetí fáze.

Co dál

V našem krátkém seznámení jsme se soustředili zejména na výklad způsobu uplatnění fyzikálních zákonů při návrhu kryptografických protokolů. Uvedený popis protokolu BB84 vyžaduje ještě další netriviální rozvedení, zejména je nutné doplnit autentizaci původu zpráv vyměňovaných mezi Alicí a Bobem, aby je Oskar nemohl padělat a tím maskovat svou přítomnost. Rozvést lze i zpracování dohodnutého tajemství s cílem minimalizovat užitečnost případných střípků částečné informace, kterou Oskar získal díky technologickým nedokonalostem konkrétní realizace. Zdroj například vyšle pro jeden bit víc fotonů, odposlech zanikne v rámci tolerovaného šumu, atp. – v podstatě se jedná o obdobu postranních kanálů, které dobře známe z klasické kryptografie. Zajímavý je rovněž způsob následného využití dohodnutého klíče jako takového. Všechny algoritmy, které zde použijeme, přitom nesmějí zavádět závislost bezpečnosti na výpočetní síle útočníka. Jinak bychom popřeli zásadní důvod, proč se vlastně kvantovou kryptografií zabýváme. Naštěstí existují schémata, která v tomto smyslu nepodmíněnou bezpečnost nabízejí. Za všechny zmiňme Vernamovu šifru, která by s příchodem kvantových šifrátorů mohla zažít doslova období renesance.

Závěr

Kvantová kryptografie se postupně dostala ze stadia myšlenkových experimentů do fáze existence a dostupnosti skutečných zařízení, která jsou schopna kvantové protokoly prakticky realizovat. Zatím se jedná zejména o dohodu na klíči, kde se používají různé varianty a nástupci představeného protokolu BB84. Raději zde nebudeme uvádět jména konkrétních dodavatelů, která není těžké najít na Internetu. Základní výhodou těchto protokolů je nezávislost na výpočetní síle útočníka, kterážto se s příchodem kvantových počítačů může stát pro řadu schémat asymetrické kryptografie osudnou.

Vlastimil Klíma, Tomáš Rosa,
v.klima@volny.cz, trosa@ebanka.cz

LITERATURA

[1] Bennett, C. H., Brassard, G., Breidbart, S., Wiesner, S.: Quantum cryptography, or unforgeable subway tokens, CRYPTO 82, pp. 267-275, 1982.

[2] Bennett, C. H., Brassard, G.: Quantum cryptography: public-key distribution and coin tossing, International Conference on Computers, Systems and Signal Processing, pp. 175-179, India, 1984.

[3] Diffie, W., Hellman, M. E.: New directions in cryptography, IEEE Transactions on Information Theory, Vol. 22, pp. 644-654, 1976.

[4] Dušek, M.: Koncepční otázky kvantové teorie, Univerzita Palackého v Olomouci, 2002.

[5] Wiesner, S.: Conjugate coding, rukopis z roku cca 1970, publikován v SIGACT NEWS, Vol. 15, No. 1, pp. 78-88, 1983.

[6] E-archivy http://cryptography.hyperlink.cz http://crypto.hyperlink.cz