Miloslav Dušek

Kvantová kryptografie

Pokroky matematiky, fyziky a astronomie, Vol. 41 (1996), No. 3, 113--123

Persistent URL: http://dml.cz/dmlcz/137764

Kvantová kryptografie

Miloslav Dušek, Olomouc

Kvantová kryptografie je nová metoda pro bezpečný přenos informací, využívající fundamentálních zákonů kvantové fyziky.

Úvod

Bezpečný (utajený) přenos dat je požadován v nejrůznějších oblastech. Klasicky ve vojenství a diplomacii. S rozvojem počítačových sítí, jejichž prostřednictvím jsou prováděny bankovní i různé další finanční operace a přenášeny obchodní a jiné důvěrné informace, se však tento požadavek stále více objevuje i v každodenním životě. Metodami utajování přenášených informací se zabývá *kryptografie* (ta je součástí širšího oboru — *kryptologie* — zahrnujícího navíc ještě tzv. *kryptoanalýzu*, která se naopak snaží utajené zprávy rozluštit).

Nejjednodušší způsob ochrany přenášených dat je přímá fyzická ochrana komunikačního kanálu. Ta je však prakticky těžko realizovatelná. Proto většina užívaných metod spoléhá spíše na šifrování přenášených zpráv. Jde o to, aby informace byla srozumitelná pouze tomu, komu je určena. K zašifrování zprávy se používá speciálních matematických algoritmů a tzv. klíče. Jak odesilatel, tak příjemce musejí mít samozřejmě stejný klíč. Tyto algoritmy obvykle využívají různých postupů generujících pseudonáhodné posloupnosti znaků nebo bitů. Odesilatel a příjemce se musí pouze dohodnout na některém z obecně dostupných algoritmů a na určitých „počátečních podmínkách" představujících klíč, jejž je třeba udržet v tajnosti. Blokové algoritmy provádějí operace s celými bloky dat; každý bit výstupní šifry pak závisí na všech vstupních bitech (z bloku dat) a na klíči. Moderní kryptografie také využívá tzv. „public key distribution". Pomocí „veřejného" klíče může každý zprávu zašifrovat; správně ji pak přečíst lze ovšem již jen pomocí „privátního", tajného klíče. Zprávy zašifrované těmito a podobnými způsoby mohou být ovšem, aspoň v principu, rozšifrovány. Jejich bezpečnost spočívá v matematické náročnosti procesů s tím spojených. V případě „public key distribution" se například využívá toho, že není snadné faktorizovat velká čísla. Výpočtová složitost (tj. počet jednoduchých operací, které je nutno provést) roste exponenciálně s délkou zprávy. I se současnými superpočítači je tedy téměř nemožné rozluštit takto utajené zprávy v rozumném čase. Nicméně případný nečekaný pokrok v technologii nebo v matematických algoritmech[1]) může situaci výrazně změnit. Zvláštní „ohrožení" by mohly představovat tzv. kvantové počítače [1].

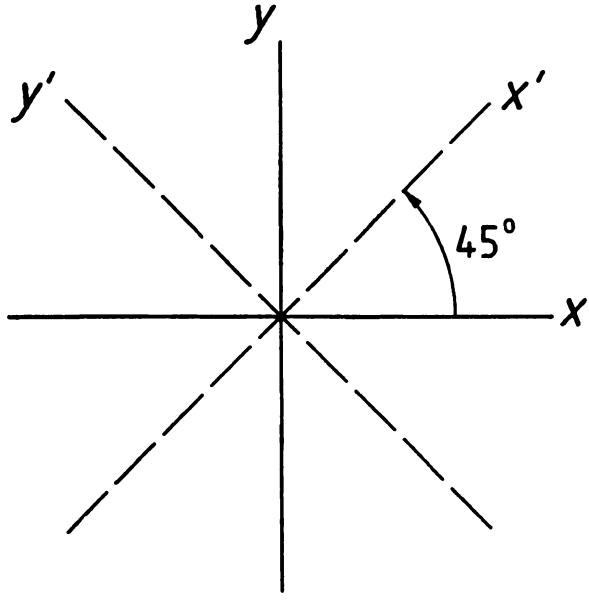
[1]) Není např. stále dokázáno, že k rozkrytí zprávy v případě „public key distribution" je nutné provádět faktorizaci ani že faktorizace je nutně exponenciálně složitá.

Dr. RNDr. Miloslav Dušek (1964), katedra optiky, Univerzita Palackého, 17. listopadu 50, 772 07 Olomouc.

Jedinou „dokonalou“ šifrovací metodou[2]) je použití skutečně náhodného tajného klíče, tedy nekorelované posloupnosti zcela náhodně vybraných znaků zvolené abecedy [2]. Po „přičtení“[3]) takového klíče (který může být pochopitelně použit pouze jednou) nabude zpráva charakteru náhodného signálu. „Neodečte-li“ se stejný klíč, je zpráva zcela nečitelná. Bezpečnost přenosu je tedy zcela závislá na utajení klíče. Jak ovšem dosáhnout toho, aby odesilatel i příjemce měli stejný klíč, a mít přitom jistotu, že jej nezískal nikdo třetí? Odpověď na tuto otázku nabízí právě kvantová kryptografie [3]. Klíč není přenášen klasickým způsobem. Jako abecedy je totiž použito kvantových stavů jedné částice (např. fotonu). Jakýkoli pokus o odposlech nevyhnutelně podstatně ovlivní stav částice, a může být proto odhalen. Při zjištění odposlechu se přenášený klíč prostě nepoužije; k žádnému úniku informace pochopitelně nedojde.

Kvantová měření

Všechny metody využívané v kvantové kryptografii vycházejí tak či onak z faktu, že kvantově mechanické měření jedné proměnné změní obecně stav systému a zavede neurčitost hodnot ostatních proměnných.



Obr. 1. Dva souřadnicové systémy pro lineárně polarizovaný foton.

Máme-li, například, klasické světlo lineárně polarizované ve směru x (viz obr. 1) a pokusíme-li se zjistit, kolik světla projde polarizačním filtrem pootočeným vzhledem

[2]) Bezpečnost této metody zvané „one-time pad“ je matematicky snadno dokazatelná.

[3]) Rozumí se sčítání modulo N, kde N je počet znaků používané abecedy.

k ose x o 45° (propouštějícím tedy pouze vlny polarizované ve směru x'), zjistíme, že za filtrem má světlo polovinu původní intenzity. Klasické světlo můžeme chápat jako složené z obrovského množství fotonů. Situace se ovšem podstatně změní, máme-li co do činění pouze s jediným fotonem. Zde se zřetelně projeví kvantový charakter zákonů přírody. Některé fyzikální veličiny mohou nabývat jen diskrétních hodnot[4]). Uplatňuje se také tzv. Heisenbergův princip neurčitosti. Nemůžeme například změřit průmět vektoru polarizace *zároveň* do obecně různých směrů.

Předpokládejme, že na počátku máme foton lineárně polarizovaný ve směru x. Postavíme-li mu do cesty polarizační filtr pootočený opět o 45° vůči ose x, foton se nemůže rozpůlit, a proto buď projde, nebo neprojde. S pravděpodobností 50 % (v tomto speciálním případě) projde a se stejnou pravděpodobností neprojde. Jakmile projde, změní se jeho polarizační stav[5]) a nadále je polarizován ve směru osy x'. Výsledek následného měření polarizace ve směru x nebo y bude pak zcela neurčitý. Této neurčitosti se nelze žádným způsobem vyhnout.

Zajímavé a velmi neklasické důsledky má kvantově mechanické měření v soustavách se dvěma nebo více korelovanými částicemi. Lze například připravit takový pár fotonů, že stav polarizace každého z nich je neurčitý, vzájemně jsou však jejich polarizace silně korelovány. Formálně zapíšeme stav takové soustavy ve tvaru[6])

$$|\psi\rangle = |x_1\rangle|x_2\rangle + |y_1\rangle|y_2\rangle, \tag{1}$$

kde $|x_1\rangle$ reprezentuje stav, v němž je první foton polarizován podél osy x, atd. (index 2 odpovídá druhému fotonu a y značí polarizaci ve směru y). Lze ukázat, že když provedeme měření s polarizačním filtrem na prvním fotonu, pak zaregistrujeme-li foton polarizovaný např. ve směru x', bude nadále i druhý foton nutně polarizován ve směru x'. Stav soustavy se totiž po měření změní na

$$|\psi'\rangle = |x_1'\rangle|x_2'\rangle. \tag{2}$$

Tedy měření na prvním fotonu ovlivní i stav druhého fotonu (bez ohledu na to, jak jsou od sebe vzdáleny). Tento jev úzce souvisí s tzv. Einstein-Podolsky-Rosenovým paradoxem [4]. John Bell ukázal, že jakýkoli pokus popsat tento typ korelace klasicky (pomocí tzv. lokálních[7]) teorií se skrytými parametry) nutně vede k určitým matematickým nerovnostem, které kvantová mechanika obecně porušuje [5]. Porušení těchto nerovností bylo potvrzeno experimentálně. Jak uvidíme dále, také tento jev může být přímo využit v kvantové kryptografii.

---

[4]) Například průmět spinu fotonu do směru šíření může nabývat pouze hodnot $\pm\hbar$. Spin je vlastní moment hybnosti. Stavy s ostrou hodnotou průmětu spinu do směru šíření odpovídají kruhově polarizovaným fotonům.

[5]) Dojde k tzv. „kolapsu" vlnové funkce.

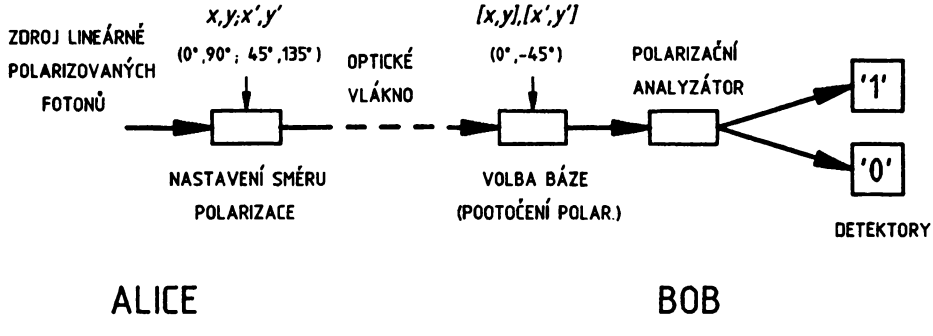
[6]) Pro jednoduchost neuvádíme normovací faktory.

[7]) „Lokální" v podstatě znamená, že informace se nemůže dostat z místa na místo okamžitě.

Princip kvantové kryptografie

Předpokládejme, že odesilatel — obvykle označovaný jako *Alice* — a příjemce — *Bob* — si chtějí vyměnit tajný klíč prostřednictvím přenosového kanálu, který je v principu přístupný odposlechu třetí osobou („eavesdropper"), označovanou jako *Eva*.

Funkci kvantového kryptografického systému ukážeme na jednoduchém modelovém uspořádání využívajícím lineárně polarizovaných fotonů. Schéma takového uspořádání je na obr. 2[8]). Předpokládejme napřed, že Alice a Bob použijí pouze fotony polarizované ve směrech x a y. Předem se domluví, že polarizace ve směru x bude představovat „1" a polarizace ve směru y bude představovat „0". Alice bude vysílat náhodnou sekvenci jedniček a nul. Protože Bob používá stejnou polarizační bázi (neboli souřadnicovou soustavu) $[x, y]$, je chování fotonů na polarizačním analyzátoru (např. polarizační hranol) zcela deterministické a všechny fotony polarizované ve směru x jsou odkloněny na jeden detektor a všechny fotony polarizované ve směru y na druhý. Bob je tedy schopen tuto sekvenci bitů bezchybně (v ideálním případě) přijmout.



Obr. 2. Schéma kvantově kryptografického systému využívajícího lineárně polarizovaných fotonů.

Co se stane, bude-li přenosový kanál odposloucháván? Pasivní odposlech nepřichází v úvahu, protože pro přenos každého bitu je použit právě jeden foton, a ten se — jak již bylo řečeno — nemůže rozdělit. Jestliže Eva foton absorbuje, Bob pochopitelně pozná, že mu nepřichází žádný signál. S principiálními potížemi by se setkal i pokus vyrobit „kopii" kvantového stavu a na ní provádět měření[9]). Jediná rozumná strategie pro odposlech je tedy použít podobného zařízení, jaké má Bob, provést měření a každý bit pak znovu poslat Bobovi podobným zařízením, jaké má Alice. Eva však neví, jakou polarizační bázi Alice a Bob používají. Zvolí-li jinou souřadnou soustavu, vnese

[8]) Vedle „kvantového" kanálu používají Alice a Bob ještě klasický „otevřený" (veřejný) kanál, který na obrázku zakreslen není.

[9]) Vybrané ortogonální stavy sice v principu kopírovat (neboli klonovat) lze. Vytváření kopií libovolných obecných stavů však brání linearita kvantové mechaniky [6]. Dále popsaná metoda střídání dvou různých polarizačních bází je proto odolná i proti případnému „klonování".

každým měřením do systému s určitou pravděpodobností chybu, jak jsme popsali v předchozí kapitole. Porovnají-li Alice a Bob část přenášené sekvence (kterou už potom nepoužijí), mohou odposlech odhalit.

Eva se však může nějakým způsobem dovědět, jakou polarizační bázi Alice a Bob používají, nebo má prostě štěstí a trefí se do ní. Pak samozřejmě zůstane neodhalena. Tomu lze předejít tak, že jak Alice, tak Bob náhodně (nezávisle) střídají polarizační báze $[x, y]$ a $[x', y']$. Tj. Alice vysílá fotony náhodně polarizované ve směrech x, y, x', y' a Bob pro každý přicházející foton náhodně mění natočení polarizačního analyzátoru (střídá 0° a −45°). Po přenosu si otevřeným kanálem vzájemně vymění informaci, v jakých bázích (souřadných soustavách) kdy pracovali, a ponechají pouze ty bity, pro které používali stejné báze (buď $[x, y]$ nebo $[x', y']$). Poznamenejme, že neporovnávají vlastní data („1" a „0") — tedy to, jestli byl foton polarizován ve směrech x, resp. x' nebo y, resp. y' — ale pouze informaci o tom, zda byla použita čárkovaná nebo nečárkovaná báze. Tento postup sice snižuje přenosovou rychlost přibližně na polovinu, zajišťuje však bezpečnost přenosu. Eva teď neví, jakou bázi vybrat, a ať zvolí jakoukoli strategii, bude se vždy zhruba v polovině případů mýlit. Předpokládejme na chvíli, že Alice a Bob mají právě nastavenou nečárkovanou bázi $[x, y]$ a že Eva chybně použije čárkovanou bázi $[x', y']$. Výsledky měření Evy i Boba jsou pak zcela neurčité. Za těchto okolností by Alice a Bob dosáhli shody výsledků asi v polovině případů. Celkově vnese odposlech pravděpodobnost chyby 25 % na jeden bit. Je-li odposlech nepřetržitý a není-li v systému jiný zdroj chyb, pak srovnáním dostatečného počtu bitů (u kterých Alice a Bob předpokládají 100 % shodu) lze pravděpodobnost, že odposlech nebude odhalen, učinit libovolně malou. Porovnají-li Alice a Bob např. 100 bitů z přenesené náhodné sekvence, bude pravděpodobnost, že odposlech nebude odhalen (tj. pravděpodobnost, že obě posloupnosti budou přesně stejné), rovna $(0{,}75)^{100} \approx 3 \times 10^{-13}$. Celý průběh přenosu kryptografického klíče je zachycen v tab. 1.

Eva by v principu mohla přerušit i otevřený kanál, kterým si Alice a Bob předávají informaci o použitých polarizačních bázích, a tvářit se vůči Alici zcela jako Bob. Bobovi by přitom mohla odeslat jiný náhodný klíč. Tento případ lze ovšem vyloučit tzv. „autentizací" zpráv posílaných otevřeným kanálem [7].

Poznamenejme ještě, že existuje i „minimální" kvantově kryptografický přenosový protokol, který používá pouze dvou neortogonálních stavů [8]. Má určité praktické výhody, využije se při něm však jen čtvrtina všech přenášených bitů.

Metody kvantové kryptografie

Metoda využívající polarizačních stavů fotonu [9] byla vlastně již popsána v předchozí části.

První experimenty s kvantovou kryptografií, které prováděl Bennett se svými spolupracovníky, využívaly kruhově polarizovaných fotonů [7]. Přenosovým kanálem o délce pouze 32 cm byl volný prostor.

Mnohem výhodnější je ovšem využít optických vláken. Optická vlákna v současné době umožňují realizovat kvantově kryptografický přenos až na vzdálenost desítek kilo-

Tabulka 1. Přenos kryptografického klíče

1)	0	1	1	0	1	1	0	0	1	0	1	1	0	0	1
2)	×	+	×	+	+	+	+	+	×	×	+	×	×	×	+
3)	↘	↔	↗	↕	↔	↔	↕	↕	↗	↘	↔	↗	↘	↘	↔
4)	+	×	×	+	+	×	×	+	×	+	×	×	×	×	+
5)	1		1		1	0	0	0		1	1	1		0	1
6)	+		×		+	×	×	+		+	×	×		×	+
7)			OK		OK			OK				OK		OK	OK
8)			1		1			0				1		0	1
9)					1									0	
10)					OK									OK	
11)			1					0				1			1

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*

II. Veřejná diskuse

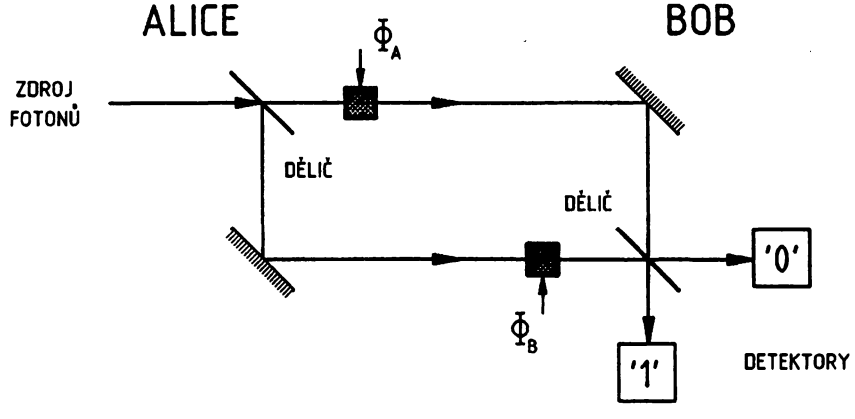
6) *Bob* oznamuje báze, ve kterých naměřil fotony
7) *Alice* oznamuje, které báze byly správně uhodnuty
8) informace, na kterou se *Alice* a *Bob* spoléhají (nenaslouchá-li *Eva*)

III. Obětování bitů

9) *Bob* obětuje některé náhodně vybrané bity k odhalení *Evy*
10) *Alice* potvrzuje tyto obětované bity
(*Eva* by způsobila odchylku přibližně v 1/4 případů)
11) zbylé tajné bity — klíč

metrů. Zdrojem optických pulsů je obvykle polovodičový laser. Každý puls je zeslaben atenuátorem tak, aby v průměru obsahoval asi 0,1 fotonu. Mnoho pulsů se tím sice ztratí, ale je to nezbytné, neboť jedině tak dosáhneme, že pravděpodobnost výskytu dvou nebo více fotonů v pulsu je mnohem menší než pravděpodobnost výskytu právě jednoho fotonu (pro Poissonovo rozdělení asi 1 : 20). Světlo projde též polarizátorem. Každý foton je tedy lineárně polarizován, řekněme ve směru x. Polarizace ve směrech y, x' a y' se dosahuje pootočením polarizační roviny např. dvěma Pockelsovými celami. Obě jsou řízeny náhodnými signály. První stáčí polarizační rovinu o 90° a tím přepíná mezi „1" a „0", druhá stáčí polarizaci o 45° a přepíná mezi nečárkovanou a čárkovanou bází. Optické vlákno, do kterého je signál zaveden, musí v tomto případě pochopitelně zachovávat polarizaci záření. Jakékoli případné změny polarizace během přenosu musejí být kompenzovány. Na přijímací straně, jak již bylo řečeno, je další Pockelsova cela řízená náhodným signálem, která přepíná mezi bází $[x, y]$ a $[x', y']$, pootočenou o 45°. Polarizační hranol rozděluje fotony navzájem kolmo polarizované a přivádí

je na dva oddělené detektory. Těmi bývají nejčastěji lavinové fotodiody s vysokou kvantovou účinností a nízkým šumem. Zaznamenávány jsou pouze ty případy, kdy přijde puls právě (a pouze) z jednoho z detektorů v koincidenci se spouštěcím pulsem laseru (vedeným samostatným kanálem). Tím se částečně vyloučí tzv. temné „county" detektorů[10]) a některé případy s více než jedním fotonem v pulsu. Případy, kdy se foton na trase ztratí, jsou tím také vyloučeny z úvahy. Dobře navržený systém sestavený z kvalitních komponent může pracovat s chybovostí výrazně menší než 1 %. Takovou chybovost lze snadno kompenzovat např. pomocí samoopravných kódů. Laserové pulsy jsou vysílány s frekvencemi řádu stovek kHz (což je dáno možnostmi řídící, detekční a koincidenční elektroniky). Skutečná přenosová rychlost je však o dva až tři řády menší, což je způsobeno především tím, že ne každý zeslabený puls laseru obsahuje foton, dále technikou náhodného střídání bází a v neposlední řadě ztrátami ve vlákně.

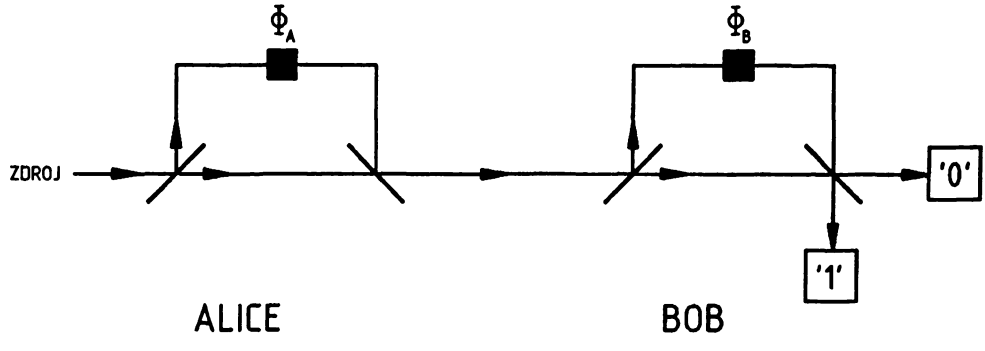


Obr. 3. Kvantově kryptografický systém založený na jednofotonové interferenci.

Jednofotonová interferenční metoda [8, 10]. Princip této metody lze ukázat na schématu na obr. 3. Úlohu směru polarizace z předchozí metody zde přebírá vzájemný fázový posuv svazků šířících se dvěma rameny Mach-Zehnderova interferometru. Obě ramena mají stejnou délku. Alice posílá do interferometru jednotlivé fotony a kontroluje fázi φ_A tak, že např. 0° odpovídá jedničce a 180° nule v jedné bázi a 90° odpovídá jedničce a 270° nule v bázi druhé. Vlastní klíč a posloupnost přepínání bází jsou opět zcela náhodné sekvence. Bob mění fázi φ_B: náhodně střídá hodnoty 0° a 90° odpovídající první, resp. druhé bázi. Mají-li Alice a Bob nastaveny stejné báze, dochází na druhém děliči svazku ke konstruktivní interferenci v jednom a destruktivní interferenci v druhém směru nebo naopak podle toho, vysílá-li Alice jedničku nebo nulu. Chování fotonu je tedy deterministické. Je-li ovšem rozdíl fází jiný než násobek 180° — např. v důsledku odposlechu — existují nenulové pravděpodobnosti zachytit foton jak v jednom, tak v druhém detektoru. To opět vnáší do přenosu chybu, umožňující odposlech odhalit.

[10]) Tj. případy, kdy detektor vyšle signál, aniž by na něj dopadl foton.

Z praktického hlediska je ovšem uspořádání podle obr. 3 nevhodné. Je totiž téměř nemožné udržet na delší vzdálenosti stejné fázové poměry svazků šířících se ve dvou různých vláknech (teplotní rozdíly, různé mechanické vlivy apod.). Proto se používá modifikované schéma podle obr. 4 se dvěma Mach-Zehnderovými interferometry v sérii. Dráhový rozdíl mezi kratším a delším ramenem je u obou interferometrů stejný a je větší než délka pulsu (koherenční délka). Díky těmto dráhovým rozdílům lze na výstupu časově rozlišit (pomocí koincidence s referenčním pulsem od zdroje) případy, kdy foton prošel v obou interferometrech kratším ramenem, kdy zvolil obě delší ramena a kdy šel jedním kratším a jedním delším ramenem[11]). První dva případy nás nezajímají, neboť chování fotonu na posledním děliči je při nich zcela náhodné. Ve třetím případě však nelze zjistit, zda foton napřed prošel kratším a potom delším ramenem nebo naopak. Dochází proto k interferenci a systém se chová přesně jako ten z obr. 3.



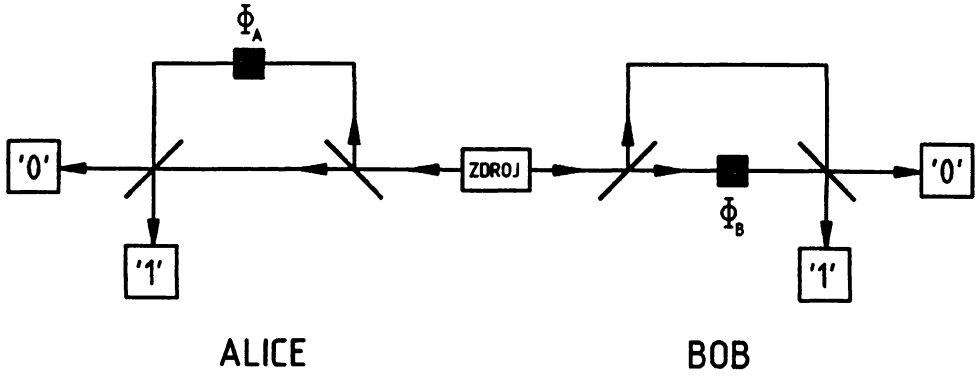
Obr. 4. „Praktická" realizace jednofotonové interferenční metody.

Jako zdroje se opět používá pulsního polovodičového laseru generujícího dostatečně krátké světelné pulsy, které jsou opět zeslabeny na průměrnou úroveň kolem 0,1 fotonu/puls. Interferometry jsou nejčastěji vláknové. Dráhový rozdíl jejich ramen bývá nanejvýš několik metrů a závisí na délce pulsu (max. jednotky ns) a časové rozlišovací schopnosti detektorů a koincidenční elektroniky (jednotky ns a méně). K řízení fáze se využívají elektrooptické fázové modulátory. Zařízení obvykle pracují na vlnové délce 1,3 μm, neboť v této oblasti mají používaná křemenná vlákna malý útlum. Chybovost přenosu se pohybuje kolem 1 %. Výhodou popsaného řešení je, že se vyhýbá potížím spojeným s požadavkem bezchybného přenosu různých polarizačních stavů optickým vláknem.

Jinou možností, jak realizovat jednofotonovou interferenční metodu s využitím pouze jediného vlákna, je odlišit dráhy polarizačně. V jednom rameni každého z interferometrů je polarizace fotonu pootočena kolmo k původní. Na posledním děliči dochází k interferenci pouze v původní polarizační rovině. Obě techniky, časové i polarizační rozlišení, lze případně spojit [11].

[11]) Zhruba polovina fotonů se ovšem do druhého interferometru vůbec nedostane, protože opustí první interferometr nevyužitým portem (výstupem) druhého děliče a nenávratně se ztratí.

Dvoufotonová interferenční metoda [12, 13] využívá zajímavých vlastností silně korelovaných fotonových párů („entangled states") produkovaných při sestupné parametrické frekvenční konverzi („down-conversion") [14]. Lze pracovat přímo se stavy popsanými rovnicí (1), které mají vzájemně korelované polarizace. Snazší je však připravit dvojici fotonů s korelovanými energiemi a impulsy. Interferenční měření na jednom z fotonů pak ovlivní interferenci druhého fotonu. Schéma zařízení pro dvoufotonovou interferometrii je na obr. 5. Jako zdroj párů fotonů slouží nelineární krystal (např. $LiIO_3$) čerpaný monochromatickým laserem (např. argonovým). Jeden čerpací foton se s jistou pravděpodobností přemění na dva sekundární subfrekvenční fotony. Celková energie a hybnost se při tom zachová[12]). Tyto fotony jsou navázány do vláken a každý z nich je veden do jednoho ze dvou Mach-Zehnderových interferometrů. Oba interferometry mají jedno rameno kratší a jedno delší. Dráhový rozdíl je ovšem u obou interferometrů stejný a je vybrán tak, aby byl výrazně delší, než je koherenční délka jednotlivých fotonů. V obou interferometrech jsou navíc umístěny fázové modulátory[13]), zavádějící fázové posuvy φ_A a φ_B.



Obr. 5. Zařízení využívající silně korelovaných fotonových párů.

Protože dráhový rozdíl mezi rameny je v každém interferometru větší než koherenční délka fotonu, nelze pozorovat jednofotonovou interferenci. Dá se však ukázat, že jsou-li oba fázové posuvy φ_A a φ_B stejné[14]), pak oba fotony budou v obou interferometrech detekovány vždy na stejných portech. Tj. Alice i Bob naměří oba buď „0", nebo oba „1". Liší-li se φ_A a φ_B o 180°, nastane situace opačná. Bob vždy zjistí opačný výsledek než Alice. Vlivem měření na jednom fotonu se totiž změní vlnová funkce popisující stav obou fotonů. Mezi okamžiky detekce obou fotonů existuje přesná časová koincidence. Samotný okamžik detekce je však zcela neurčitý. Pozorujeme-li

[12]) Díky anizotropii krystalu se přitom všechny tři fotony mohou šířit různými směry.

[13]) Fázové modulátory mohou být pochopitelně umístěny jak v kratším, tak v delším rameni každého interferometru, musí se pouze zvolit správné znaménko fázového posuvu.

[14]) Zároveň musí platit, že $2\Delta t\,\omega_0$ je celým násobkem 360°, přičemž Δt je rozdíl tranzitních časů v delším a kratším rameni interferometrů a ω_0 je čerpací frekvence.

tedy přesnou časovou shodu (v prostorově symetrickém uspořádání[15])), nejsme s to rozlišit, zda oba fotony prošly kratšími rameny interferometrů či zda oba prošly rameny delšími. Tato nerozlišitelnost drah je příčinou interference.

Postup při výměně kryptografického klíče je podobný jako u předchozích metod. Alice i Bob nezávisle náhodně střídají fázové posuvy 0° a 90° a provádějí koincidenční měření na svých interferometrech. Posléze si vymění informaci o fázových posuvech a ponechají pouze ta data, u kterých se shodli a nastavili φ_A a φ_B stejně. Pokus o odposlech naruší vzájemnou korelaci obou fotonů a — podobně jako v předchozích metodách — vnese do přenosu nevyhnutelně určitou chybu.

Střídání fázových posuvů odpovídá změně báze. Vlastní náhodná posloupnost nul a jedniček — klíč — je generována přímo fyzikálním procesem na základě samotné statistické podstaty kvantové mechaniky. Celý systém lze dokonce navrhnout tak, aby mohl být provozován zcela pasivně, tedy bez řízených fázových modulátorů [15].

Současný stav a perspektivy

Současné laboratorní systémy pro kvantový přenos kryptografického klíče pracují do vzdáleností nejvýš kolem 30 km a s přenosovými rychlostmi řádu kilobitů za sekundu (taktovací kmitočty však bývají až megahertzy). Omezení taktovací frekvence je dáno především možnostmi současných detektorů. Užitečná přenosová rychlost navíc klesá vlivem samotné metody, vlivem ztrát (zvláště ve vlákně), vlivem relativně malé účinnosti detektorů a vlivem zeslabení pulsu na velmi malou průměrnou hodnotu počtu fotonů v pulsu. Posledně zmíněný faktor by bylo možno zlepšit použitím neklasických (tzv. subpoissonovských) zdrojů světla, které by v každém pulsu generovaly s vysokou pravděpodobností právě jeden foton. Ztráty ve vlákně je možno omezit výběrem vhodné vlnové délky záření. Problém je, že pro vlnové délky, na nichž mají používaná vlákna nejmenší útlum, neexistují zatím vhodné detektory. Maximální vzdálenost, do níž lze kvantově kryptografický systém použít, klesá s rostoucími ztrátami a s rostoucím šumem detektorů. Střední počet temných „countů" za jednotku času je při dané hodinové frekvenci (a pevném časovém okně detektoru) konstantní. Počet bitů klíče přenesených za jednotku času však s rostoucí délkou vlákna vlivem ztrát klesá. Relativní chyba na jeden bit tedy roste, až je srovnatelná s chybou, kterou by vnesl potenciální odposlech. Zesilovače použít nelze, protože by ovlivňovaly kvantový stav částic podobným způsobem jako odposlech a znehodnocovaly tak přenos. Nastupující technologie (pro vlnovou délku 1,55 μm) umožní provoz až do vzdáleností kolem 50 km. Takový dosah již nabízí široké praktické uplatnění, např. pro počítačové sítě s bezpečnou komunikací mezi jednotlivými pracovišti bank či vládních úřadů v rámci velkých měst a podobně. Aby mohly kvantové kryptografické systémy zcela konkurovat současným konvenčním systémům, musí pochopitelně dospět do kompaktní komerční podoby — optimální bude asi forma karty do osobního počítače — a jejich cena musí

[15]) V praxi se samozřejmě zdroj umísťuje buď na stranu Alice nebo Boba a s časovým rozdílem způsobeným různými dobami šíření se počítá.

klesnout na srovnatelnou úroveň. To je ovšem jen otázkou času. Pak lze předpokládat, že nesporné výhody kvantové kryptografie — fyzikálními zákony garantovaná bezpečnost přenosu, ale také fakt, že klíč se generuje až v okamžiku, kdy je potřeba, čímž odpadají problémy s jeho „skladováním" — způsobí malou revoluci v oblasti bezpečného přenosu informací.

K urychlení nástupu kvantových kryptografických metod může výrazně přispět i rozvoj již zmíněných kvantových počítačů. Kvantové počítače pracují s kvantovou superpozicí všech možných stavů kvantového registru. V jediném kroku tedy mohou sledovat mnoho různých cest zároveň, přičemž se uplatňuje vliv interference. Byly navrženy sofistikované postupy využívající těchto neklasických vlastností k velmi efektivní faktorizaci velkých celých čísel. Výpočtová složitost takových postupů *není* exponenciální, ale pouze polynomiální. Praktická realizace kvantových počítačů by tedy silně otřásla pozicí konvenčních matematických kryptografických metod.

Kvantová kryptografie představuje první přímou praktickou aplikaci základů kvantové mechaniky. To nejen ukazuje na *praktickou* hodnotu základního výzkumu, ale vytváří i zajímavou zpětnou vazbu. Ověřování funkce a bezpečnosti kvantově kryptografických systémů s sebou může přinést nové experimentální testy kvantové mechaniky, které by snad mohly vést i k lepšímu porozumění jejím základům.

Výzkum v oblasti kvantové kryptografie, na němž se autor článku podílí, je částečně podporován GA ČR (projekt č. 202/95/0002).

Literatura

[1] A. Ekert: *Quantum Computation.* In Proc. ICAP 94, eds. C. Wieman and D. Wineland.
[2] G. S. Vernam: J. Am. Inst. El. Eng. *45* (1926), 109.
[3] J. D. Franson: Opt. & Photonics News, March 1995, 30.
[4] A. Einstein, B. Podolsky, N. Rosen: Phys. Rev. *47* (1935), 777.
[5] J. S. Bell: Physics *1* (1964), 195.
[6] W. K. Wootters, W. H. Zurek: Nature *299* (1982), 802.
[7] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, J. Smolin: J. Crypt. *5* (1992), 3.
[8] C. H. Bennett: Phys. Rev. Lett. *68* (1992), 3121.
[9] J. Breguet, A. Muller, N. Gisin: J. Mod. Opt. *41* (1994), 2405.
[10] P. D. Townsend, J. G. Rarity, P. R. Tapster: Electron. Lett. *29* (1993), 634.
[11] P. D. Townsend, I. Thompson: J. Mod. Opt. *41* (1994), 2425.
[12] A. K. Ekert, J. G. Rarity, P. R. Tapster, M. Palma: Phys. Rev. Lett. *69* (1992), 1293.
[13] A. K. Ekert, G. M. Palma: J. Mod. Opt. *41* (1994), 2413.
[14] J. Peřina, Z. Hradil, B. Jurčo: *Quantum Optics and Fundamentals of Physics.* Kluwer, Dordrecht 1994.
[15] J. G. Rarity, P. C. M. Owens, P. R. Tapster: J. Mod. Opt. *41* (1994), 2435.