Univerzita Karlova v Praze
Matematicko-fyzikální fakulta

BAKALÁŘSKÁ PRÁCE

Josef Stráský

Kvantová kryptografie

Katedra chemické fyziky a optiky

Prof. RNDr. Lubomír Skála, DrSc.

studijní program: fyzika studijní obor: obecná fyzika

2008

Na tomto místě bych rád poděkoval vedoucímu práce prof. Skálovi za výběr tématu, opatření studijní literatury a přínosné konzultace nad rozpracovaným textem.

Prohlašuji, že jsem svou bakalářskou práci napsal samostatně a výhradně s použitím citovaných pramenů. Souhlasím se zapůjčováním práce a jejím zveřejňováním.

V Praze dne 29. května 2008 Josef Stráský

Obsah

1 Úvod **6**

2 Základní teoretické koncepty **8**
2.1 Qubit 8
2.2 Neklonovací teorém 8
2.3 Zisk informace z neortogonálních stavů 9
2.4 Entanglement 10
2.5 Bellova nerovnost – důkaz lokality 10
2.6 Základní druhy propleteného stavu 11
2.6.1 Propletení spinu 11
2.6.2 Propletení polarizace 11
2.7 Vyvrácení Bellovy nerovnosti 12

3 Základní schéma kvantové kryptografie **14**
3.1 Klíčový je klíč 14
3.2 Základní schéma a dělení kvantové kryptografie 15

4 Kvantová distribuce klíče pomocí jednotlivých fotonů **16**
4.1 Kódování pomocí polarizace - BB84 16
4.2 Kódování pomocí fáze 17
4.3 Praktické problémy jednofotonové kryptografie 18
4.3.1 Zdroje chyb 18
4.3.2 Získání výsledného klíče 19
4.4 Jednofotonová kryptografie pomocí optických vláken 20
4.4.1 Uspořádání plug&play 20
4.4.2 Využití polarizace 21
4.5 Jednofotonová kryptografie volným prostorem 21

5 Kvantová distribuce klíče pomocí propletených stavů **23**
5.1 Základní schéma kvantové kryptografie pomocí entanglementu . . . 23
5.2 Výhody kryptografie propletených stavů . . . 24
5.3 Zdroje propletených stavů . . . 25
5.3.1 Time-bin entanglement . . . 25
5.3.2 Propletení hybnosti . . . 25
5.3.3 Propletení polarizace . . . 25
5.4 Experimenty využívající propletené stavy . . . 26
5.4.1 Ženeva . . . 26
5.4.2 Vídeň – optické vlákno . . . 26
5.4.3 Vídeň – volný prostor . . . 27
5.4.4 Boston – samonastavovací systémy . . . 27

6 Další kvantové koncepty **29**
6.1 Čištění propletenosti . . . 29
6.2 Výměna propletenosti . . . 30
6.3 Kvantový opakovač . . . 30
6.4 Kvantová síť . . . 31

7 Závěr **32**

Literatura **33**

Název práce: Kvantová kryptografie
Autor: Josef Stráský
Katedra (ústav): Katedra chemické fyziky a optiky
Vedoucí bakalářské práce: Prof. RNDr. Lubomír Skála, DrSc.
E-mail vedoucího: skala@karlov.mff.cuni.cz

Abstrakt: V této práci shrnuji nejdůležitější současné poznatky z rychle se rozvíjejícího oboru kvantové kryptografie. Po teoretickém úvodu, který je soustředěn na Bellovu nerovnici a důkaz nelokality, jsou podrobně vysvětleny základní principy kvantové kryptografie. Kvantovou kryptografii lze rozdělit na kryptografii jednofotonových pulsů a na kryptografii entanglovaných stavů. Pro oba tyto typy jsou popsány hlavní způsoby kódování (polarizační a fázové) a způsoby přípravy potřebných fotonových stavů. Pro různá kvantově kryptografická schémata jsou popsány reprezentativní realizované experimenty. Přes větší technickou náročnost se ukazují výhody entanglovaných stavů. Neintuitivní vlastnosti těchto stavů vedou k procesům, které v budoucnosti umožní vznik kvantových sítí, které budou sloužit k tajné komunikaci.

Klíčová slova: kvantová kryptografie, qubit, propletenost (entanglement)

Title: Quantum cryptography
Author: Josef Stráský
Department: Department of Chemical Physics and Optics
Supervisor: Prof. RNDr. Lubomír Skála, DrSc.
Supervisor's e-mail address: skala@karlov.mff.cuni.cz

Abstract: In this work I summarize the most important knowledge in fast-developing field of quantum cryptography. After theoretical introduction, that focuses on Bell's inequation and proof of nonlocality, basic principles of quantum cryptography are explained. Quantum cryptography can be divided into the cryptography of single-photon pulses and the cryptography of entangled states. Two main methods of coding (polarisation and phase) are described for both cryptography types as well as sources of desired photon states. Important experimental realizations are described for different quantum cryptographic schemes. Despite more technical complications, entangled states indicates more advantages. Counterintuitive properties of entangled states lead to processes that allow in future formation of quantum network that will serve for secret communication.

Keywords: quantum cryptography, qubit, entanglement

Kapitola 1

Úvod

Potřeba tajné komunikace vznikla se samým počátkem civilizace. Jednoduché šifry využívala již spartská armáda stejně jako Julius Caesar. Šifry byly používány především k vojenským účelům. Vrcholem takového užití byla německá Enigma a americký systém M-209. Spojovacím prvkem těchto šifer byla tajná šifrovací procedura. V dnešní době internetu je tajná komunikace každodenní nezbytností. Mnohé instituce v čele s bankami vydávají na bezpečnost komunikace nemalé prostředky. Šifrovací procedura je dnes zcela veřejná, ale kromě utajované zprávy do ní vstupuje ještě tzv. klíč. Šifrování funguje jako trezor, který má veřejný klíč k zamčení, ale tajný klíč k odemčení. Vyrobit tajný klíč z klíče veřejného je bezpochyby možné, je to ale obtížné. Dnešní systémy používají matematické operace, jejichž provedení je v jednom směru mnohem snazší než v opačném. Takovou operací je vynásobení dvou velkých prvočísel, které je (narozdíl od nalezení prvočíselného rozkladu) snadné. Předpokládá se (ačkoli to není precizně dokázáno), že čas, který potřebuje počítač k prvočíselnému rozkladu čísla o N číslicích, roste exponenciálně s N. Ve chvíli, kdy se znásobí síla výpočetní techniky anebo pokud dojde k převratnému vynálezu rychlejšího algoritmu, bude bezpečnost klasické kryptografie minulostí. Takový skok v rychlosti výpočetní techniky mohou způsobit kvantové počítače. Ukazuje se navíc, že kvantový počítač dokáže dělit nejen rychleji, ale i efektivněji než počítače klasické. Kvantový svět na jedné straně možná zničí bezpečnost klasické kryptografie, na druhé straně ale nabízí nepřeberné možnosti revoluční nové tajné komunikace. Tuto tajnou komunikaci, jejíž bezpečnost je zajištěna kvantovými principy, nazýváme kvantovou kryptografií.

Bezpečnost kvantové kryptografie nespočívá v utajení procedury ani ve výpočetní náročnosti. Základem bezpečnosti jsou fundamentální fyzikální vlastnosti. V první řadě jde o kolaps kvantového stavu. V mnoha experimentálních realizacích lze ukázat, že měření kvantového stavu může nabývat zcela náhodně dvou různých hodnot. Po takovém měření je hodnota již pevně dána (kolaps). Toto spolu s tzv. neklonovacím teorémem lze využít k odhalení odposlechu. Druhou vlastností, která může sloužit k tajné komunikaci, je vlastnost nelokality. Tato fundamentální kvantová vlastnost vyvrací Einsteinovu představu, že fyzikálně měřitelné veličiny musejí být

určeny prvkem fyzikální reality (částicí). Využití vlastnosti nelokality pro kvantovou kryptografii je přímočaré a elegantní. Využití jedné z těchto dvou popsaných fundamentálních fyzikálních vlastností vede k tajné komunikaci, jejíž bezpečnost je zajištěna přírodními zákony. Jakmile se podaří vytvořit dostatečně stabilní a spolehlivý systém, který správně využije tyto fyzikální vlastnosti, bude tajná komunikace jednou provždy vyřešeným problémem. Následující práce podává aktuální zprávu o tom, jak daleko je lidstvo na cestě za tímto cílem.

Kapitola 2

Základní teoretické koncepty

Při popisu teoretických základů jsem čerpal ze souborné knihy o kvantové fyzice informace [1].

2.1 Qubit

Základním prvkem informační vědy je bit, který nese dvě možné hodnoty „0“ a „1“. Kvantový analogon bitu – *qubit* tedy musí být dvoustavový systém, jehož dva stavy obvykle značíme $|0\rangle$ a $|1\rangle$. Základní vlastností kvantového stavu, který použijeme jako *qubit*, je možnost superpozice. Obecně takový stav můžeme zapsat:

$$|q\rangle = \alpha\,|0\rangle + \beta\,|1\rangle\,, \tag{2.1}$$

kde $|\alpha|^2 + |\beta|^2 = 1$. Qubit je v superpozici obou stavů a pokud ho změříme, zjistíme s pravděpodobností $|\alpha|^2$ hodnotu „0“ a s pravděpodobností $|\beta|^2$ hodnotu „1“. Důležité je, že se jedná o koherentní superpozici, a pro ni lze vždycky najít bázi, ve které je hodnota qubitu přesně určena.

Zobecněním qubitu je tzv. qutrit, qudit nebo qunit. Jedná se o kvantový systém, který je popsán superpozicí většího počtu stavů. V případě qutritu je to superpozice tří stavů. Qunit a qudit je různý název pro totéž – jsou tvořeny superpozicí n resp. d stavů. Stále předpokládáme, že pro tuto superpozici lze najít bázi, aby byla hodnota qu?itu přesně určena. Takový vícestavový systém může nést mnohonásobně víc informace.

2.2 Neklonovací teorém

Teoretickým základem tzv. jednofotonové kryptografie je použití neortogonálních stavů. Pro takové stavy platí neklonovací teorém (no-cloning theorem). *Neortogonální kvantové stavy (nebo jakýkoli neznámý kvantový stav) nelze naklonovat.* Uva-

žujme neortogonální stavy $|0\rangle$ a $|1\rangle$, tedy $\langle 0|1\rangle \neq 0$. Pro klonování je potřeba stroj $|s\rangle$, který bude fungovat takto:

$$|0\rangle\,|?\rangle\,|s\rangle \rightarrow |0\rangle\,|0\rangle\,|s_0\rangle\,, \tag{2.2}$$

$$|1\rangle\,|?\rangle\,|s\rangle \rightarrow |1\rangle\,|1\rangle\,|s_1\rangle\,, \tag{2.3}$$

kde $|?\rangle$ je jakýkoli vhodný původní stav částic, která se stane klonem, a $|s_0\rangle$, $|s_1\rangle$ jsou obecně různé koncové stavy stroje $|s\rangle$. Bez újmy na obecnosti můžeme předpokládat, že všechny stavy jsou normalizovány. Tato klonovací transformace musí být unitární, musí tedy zachovat skalární součin. Rovnice můžeme vynásobit a obdržíme:

$$\langle 0|1\rangle\,\langle ?|?\rangle\,\langle s|s\rangle = \langle 0|1\rangle\,\langle 0|1\rangle\,\langle s_0|s_1\rangle\,. \tag{2.4}$$

Vzhledem k normalizaci stavů platí $\langle ?|?\rangle = \langle s|s\rangle = 1$. Požadujeme tedy platnost vztahu:

$$\langle 0|1\rangle = \langle 0|1\rangle\,\langle 0|1\rangle\,\langle s_0|s_1\rangle\,. \tag{2.5}$$

Vzhledem k tomu, že stavy jsou normalizované, jsou členy $\langle 0|1\rangle$ a $\langle s_0|s_1\rangle$ nutně menší nebo rovné 1. Rovnice tak může být splněna pouze, když $\langle 0|1\rangle = 0$ (stavy jsou ortogonální) nebo $\langle 0|1\rangle = 1$ (dva stavy jsou nerozlišitelné, tudíž nemohou být použity pro zakódování dvou různých hodnot bitu). Pokud tedy nemáme informaci o tom, zda se jedná o stav $|0\rangle$ nebo $|1\rangle$, nelze tento stav věrně zkopírovat, aniž by byl změřen.

2.3 Zisk informace z neortogonálních stavů

V předchozí části jsme ukázali, že žádný ze dvou neznámých neortogonálních stavů nelze zkopírovat, aniž by byl změřen. Nyní ukažme, že vzájemně neortogonální stavy nelze změřit, aniž by byly poškozeny. Uvažujme, že měříme neortogonální stavy $|0\rangle$ a $|1\rangle$ přístrojem $|s\rangle$. Měření tedy lze zapsat:

$$|0\rangle\,|s\rangle \rightarrow |0\rangle\,|s_0\rangle\,, \tag{2.6}$$

$$|1\rangle\,|s\rangle \rightarrow |1\rangle\,|s_1\rangle\,. \tag{2.7}$$

Transformace musejí být opět unitární, tedy obdobně jako v minulé části musí platit vztah: $\langle 0|1\rangle\,\langle s|s\rangle = \langle 0|1\rangle\,\langle s_0|s_1\rangle$. Z toho (a z vlastnosti neortogonality stavů $|0\rangle$ a $|1\rangle$) plyne: $\langle s_0|s_1\rangle = 1$. Konečné dva stavy měřícího zařízení jsou nerozlišitelné. Nebyla tedy získána žádná informace o hodnotě qubitu.

Obecněji lze říci, že čím více informace se z qubitu získá (čím pravděpodobněji dojde k naměření qubitu), tím více se poškodí neortogonální stav (tím pravděpodobněji dojde ke kolapsu superpozice neortogonálních stavů).

2.4 Entanglement

Slovo entanglement se do češtiny obvykle překládá jako *propletenost* či *provázanost*. Jedná se o kvantový stav, ve kterém mají dvě (prostorově oddělené) částice korelované fyzikální vlastnosti. Tyto dvě částice lze popsat jedině společným dvoučásticovým superponovaným stavem. Pro dva qubity například:

$$|Q\rangle = \frac{1}{\sqrt{2}} \left(|0\rangle_1 |1\rangle_2 + |1\rangle_1 |0\rangle_2 \right). \tag{2.8}$$

Tento zápis vyjadřuje zcela propletený stav dvou qubitů, ve kterém ani jeden z qubitů nenese určitou hodnotu. Naměříme-li jeden z nich, dostaneme náhodně s poloviční pravděpodobností „0“ a s poloviční pravděpodobností „1“. V tu chvíli můžeme objevit, že druhý qubit má opačnou hodnotu. To svědčí o nelokálnosti kvantové teorie.

2.5 Bellova nerovnost – důkaz lokality

Teoreticky předpokládaná vlastnost nelokality kvantové teorie byla zpochybňována formulací tzv. EPR – paradoxu, kde Einstein, Podolski a Rosen tvrdili, že kvantová teorie je neúplná a že částice v propleteném stavu s sebou nesou nějaký skrytý parametr, který ve chvíli změření určí hodnotu měřené veličiny. Tím by byla lokalita zachráněna. V roce 1964 odvodil John Bell nerovnost, která při splnění zdánlivě triviálních předpokladů (speciálně například existence skrytých parametrů) musí být splněna. Nejnázorněji [2] ji můžeme uvést pokud budeme uvažovat, že objekty mají či nemají (¬) tři vlastnosti A,B,C, pak pro počty objektů jistě platí:

$$N(A, \neg B) + N(B, \neg C) \geq N(A, \neg C). \tag{2.9}$$

Důkaz je jednoduchý a jeho provedením se jasně ukáže základní vlastnost objektu v propleteném stavu. Uvažujme, že objekt má anebo nemá vlastnost, která v jednotlivých členech není specifikována. Celou nerovnici si pak můžeme rozepsat jako:

$$N(A, \neg B, C) + N(A, \neg B, \neg C) + N(A, B, \neg C) + N(\neg A, B, \neg C) \geq$$

$$N(A, B, \neg C) + N(A, \neg B, \neg C), \tag{2.10}$$

tedy máme:

$$N(A, \neg B, C) + N(\neg A, B, \neg C) \geq 0 \tag{2.11}$$

Vzhledem k tomu, že počty objektů můžou být jedině kladné, je nerovnost dokázána – pokud platí předpoklady. Je třeba podotknout, že jeden z předpokladů v důkazu je, že nespecifikovanou vlastnost částice buď má nebo nemá.

2.6 Základní druhy propleteného stavu

2.6.1 Propletení spinu

Jako vlastnosti A,B,C z předchozí podkapitoly můžeme uvažovat vlastnost: spin elektronu směřuje „nahoru“ při orientacích detektorů 0° (A), 45° (B) a 90° (C). Problémem je, že za účelem ověření Bellovy nerovnosti potřebujeme měřit dvě vlastnosti najednou. Při průchodu nejprve detektorem A a pak detektorem B naměříme něco zcela jiného než při měření v opačném pořadí. Měřící přístroje totiž obecně nekomutují. Použijeme tedy klíčový trik: vytvoříme dva elektrony ze substance, která měla na počátku nulový spin. Elektrony mají tedy nutně vzájemně ve všech směrech opačný spin. Očíslujeme-li elektrony, získáme Bellovu rovnici ve známém tvaru, byť úsporném zápisu:

$$N(A_1, B_2) + N(B_1, C_2) \geq N(A_1, C_2). \tag{2.12}$$

Pokud tato nerovnost neplatí, pak musí být narušený některý z předpokladů (specielně: skryté parametry neexistují). Obvykle je narušení Bellovy nerovnosti vnímáno jako důkaz nelokality. V důkazu je označen za špatný předpoklad, že částice má či nemá nespecifikovanou vlastnost, nelze to totiž vůbec určit. Vlastnost se projeví teprve změřením částice. Jiné důvody jsou poněkud odlišné povahy: logika nefunguje (opravdu se vyvíjí tzv. kvantová logika) nebo realita, která není pozorována neexistuje (svět je soustavou zrcadel) – tyto možnosti narušení Bellovy nerovnice nadále nebudu uvažovat.

2.6.2 Propletení polarizace

Jinou variantou je propletení polarizace fotonů. Experimentálním postupem, který bude vysvětlen později, lze získat dva fotony letící na opačné strany ve společném propleteném stavu:

$$|\Psi\rangle = \frac{1}{\sqrt{2}} \left(|V\rangle_1 |H\rangle_2 + e^{i\phi} |H\rangle_1 |V\rangle_2 \right), \tag{2.13}$$

kde V značí vertikální polarizaci, H polarizaci horizontální, oboje vůči nějaké zvolené bázi. ϕ značí fázi. Vhodnou manipulací lze fázi vynulovat, proto ji dále neuvažuji.

Pokud tedy oba fotony současně naměříme ve stejné bázi, pak jistě dostaneme právě opačné výsledky. Měření můžeme provést pro různé úhly detektorů. Pro libovolné úhlové natočení α, β, γ lze odvodit Bellovu nerovnost ve tvaru:

$$N(\updownarrow_\alpha, \updownarrow_\beta) \leq N(\updownarrow_\alpha, \updownarrow_\gamma) + N(\updownarrow_\beta, \leftrightarrow_\gamma), \tag{2.14}$$

kde $N(\updownarrow_\alpha, \updownarrow_\beta)$ značí počet fotonů naměřených s příslušným výsledkem. (Naměření $\leftrightarrow$ polarizace je stejné jako naměření $\updownarrow$ polarizace při detektoru pootočeném o 90°.)

Dodejme, že kvantová mechanika předpovídá:

$$N\left(\updownarrow_\alpha, \updownarrow_\beta\right) = \frac{N_0}{2}\cos^2\left(\alpha - \beta\right), \tag{2.15}$$

kde N_0 je počet vyzářených párů. Nyní vidíme, že pro volbu například $(\alpha - \beta) = (\beta - \gamma) = 30°$ je rovnice porušena. Kvantově mechanickou předpověď tedy vnímáme jako nelokální.

2.7 Vyvrácení Bellovy nerovnosti

Nejprve odvodíme nerovnici CHSH. Tuto nerovnici odvodili Clauser, Horne, Shimony a Holt v roce 1969 z Bellovy nerovnice. Odvození z Bellovy nerovnice nebudu provádět [3], ukážu spíše názorné odvození na příkladě spinu elektronů. Uvažujme dva elektrony (a a b), které vznikly ze systému o celkovém spinu 0. Spin budeme měřit ve dvou různých směrech x a y. Předpokládáme, že spin každé částice v každém směru má hodnotu buď +1 nebo −1 (to je předpoklad lokality). Zápis $a_x = 1$ značí, že spin prvního elektronu ve směru x je +1, pak nutně $b_x = -1$. Z toho plyne, že tzv. množství Q:

$$Q = a_x(b_x - b_y) + a_y(b_x + b_y) \tag{2.16}$$

nabývá dvou různých hodnot +2 nebo −2. Tedy průměrné Q při více měření:

$$-2 \leq \langle Q \rangle \leq 2. \tag{2.17}$$

Toto je nerovnice CHSH.

Pro případ propletení polarizace lze množství Q vyjádřit [3]:

$$Q = E\left(\phi_1^a, \phi_1^b\right) - E\left(\phi_1^a, \phi_2^b\right) + E\left(\phi_2^a, \phi_1^b\right) + E\left(\phi_2^a, \phi_2^b\right), \tag{2.18}$$

kde $\phi_1^a, \phi_2^a, \phi_1^b$ a ϕ_2^b jsou úhly, které vyjadřují natočení báze, ve které měříme levý či pravý foton. Index a vyjadřuje příslušnost k levému (resp. b k pravému) fotonu a index 1 či 2 vyjadřuje naši volbu natočení báze. Celkem se jedná o čtyři nezávislá měření, při kterých volíme jako úhly natočení báze kombinace čtyř „Bellových testovacích úhlů“ (0°; 22,5°; 45°; 67,5°), při kterých je Bellova nerovnice nejsilněji narušena. Naměření každého fotonu může dát dva výsledky: buď +1 (polarizace $\updownarrow$ vůči zvolené bázi) nebo −1 (polarizace $\leftrightarrow$ vůči zvolené bázi). Počet naměření určité kombinace označíme: $N_{\pm\pm}$. Čísla $E\left(\phi_i, \phi_j\right)$ vyjadřují kvantové korelace [4], tedy:

$$E = \frac{N_{++} + N_{--} - N_{+-} - N_{-+}}{N_{celkem}}. \tag{2.19}$$

Dle kvantových pravidel platí [1]:

$$E\left(\phi_i^a, \phi_j^b\right) = -cos\left[2\left(\phi_i^a - \phi_j^b\right)\right]. \tag{2.20}$$

Pak ale:

$$Q = -2\sqrt{2}. \tag{2.21}$$

Kvantová pravidla tedy vyvracejí nerovnost CHSH. Záhy po odvození byla nerovnost CHSH měřením veličiny E pro různá natočení báze experimentálně vyvrácena. Od té doby bylo provedeno mnoho experimentů nejen s fotony, ale i s elektrony, protony či ionizovanými atomy. Přesto se zdá, že nejsnáze a nejlépe proveditelné experimenty pro demonstrování nelokality jsou založeny na polarizaci fotonů [5], [6].

Kapitola 3

Základní schéma kvantové kryptografie

Nejdříve si představíme hlavní postavy v kryptografické hře. Jsou to (dle anglického značení) **Alice**, která chce poslat tajnou zprávu Bobovi, **Bob**, který chce přijmout zprávu od Alice, a **Eva** (eavesdropper) – slídilka, která je chce odposlouchávat. Alice a Bob v této hře ztělesňují „dobro“, které je třeba, aby zvítězilo nad seberafinovanějším „zlem“ – Evou. Při tvorbě kvantových sítí nebo při sdílení kvantového klíče více uživateli se přidávají postavy se jmény Charlie, Anna a Boris, Alex a Barbara, a obzvláště rafinovaná dvojice Ali – Baba.

3.1 Klíčový je klíč

Společným jmenovatelem dřívějších šifer byla tajnost šifrovacích a dešifrovacích **procedur**. S rozvojem počítačů se prosadily šifry, jejichž procedury není třeba utajovat. Kromě vlastní zprávy však šifrovací i dešifrovací algoritmus vyžaduje vložení **klíče**. Pro utajení zprávy je tedy nutné dobré utajení klíče. Typickým zástupcem takových šifer je *Vernamova šifra*. Jedná se o označení písmen abecedy a dalších nutných znaků postupně čísly (např. od 0 do 29). Ze zprávy tak obdržíme řadu čísel, k této řadě čísel přičteme (člen po členu) jinou, náhodnou řadu čísel od 0 do 29 (klíč). Získáme tak řadu čísel, která reprezentuje zašifrovanou zprávu. Pokud příjemce zprávy zná klíč, zprávu si snadno přečte. Lze dokázat, že pokud je klíč stejně dlouhý jako zpráva a není použit víckrát, pak je tato šifra zcela bezpečná. Zdá se, že je to krok „z bláta do louže“, místo zprávy určité délky je třeba tajně poslat stejně dlouhý klíč. V kvantové kryptografii se však jedná o opravdu *klíčový* rozdíl. Záhy se ukáže, že v kvantové kryptografii dokážeme rozlišit, zda byla či nebyla tajná komunikace odposlouchávána. Pokud jsme posílali klíč, nic se neděje – zahodíme ho a zkusíme poslat jiný. Pokud bychom si byli posílali přímo zprávu, byla by už prozrazená. V kvantové kryptografii se tedy zabýváme pouze procesem, jak si tajně poslat **klíč** a zabránit

odposlechu, nebo alespoň případný odposlech odhalit.

3.2 Základní schéma a dělení kvantové kryptografie

Kvantová distribuce klíče začíná přenosem jednoduchého či propleteného qubitu mezi Alicí a Bobem. Odposlouchávání je, z fyzikálního pohledu, měření provedené na přenášeném nosiči informace (qubitu). Dle principů kvantové mechaniky jakékoli měření obecně změní stav systému[1], což může být odhaleno Alicí a Bobem díky současné komunikaci veřejnou cestou. Základními složkami jsou tedy kvantová cesta, kterou si Alice a Bob posílají qubity, a dále veřejná cesta, o které předpokládáme, že ji může kdokoli odposlouchávat, ale nemůže měnit posílané informace (například telefon). Nyní přehledně uvedu základní kritéria, podle kterých lze dělit kvantovou kryptografii:

1. *Povaha posílaných částic*: Způsob posílání qubitu kvantovým kanálem se po informatickém vzoru jmenuje protokol. Protokoly rozdělujeme do dvou základních skupin. První skupinu reprezentuje vůbec první protokol, který navrhli v roce 1984 Charles H. Bennett and Gilles Brassard (protokol **BB84** viz podrobně dále). Využívá se v něm jednofotonových pulsů (**single–photon cryptography**).

   Naopak druhý typ protokolů využívá propletené stavy (**entanglement cryptography**). Tento postup poprvé navrhl v roce 1991 Artur Ekert. Jeho základem je využití vlastností nelokality. Výhody tohoto protokolu budou diskutovány.

2. *Kódování informace v qubitu*: Jako qubit se obvykle používá foton, proto pro kódování používáme základní vlastnosti světla. Buď se používá různá **polarizace**, nebo kódujeme informaci fázovým posunem (tj. pomocí **fáze**). V případě fáze měříme interferenci dvou pulsů, z nichž jeden je fázově posunutý. Pokud posíláme oba pulsy stejnou cestou těsně za sebou používáme označení *time-bin qubit* viz dále.

3. *Způsob přenosu qubitu*: V současných experimentech se použivají pro přenosy qubitu – fotonu buď **optická vlákna** anebo se fotony přenášejí **volným prostorem**. Výhody a nevýhody budou diskutovány. Záměrem obou přístupů je snadná aplikace kvantové kryptografie buď pomocí standardních optických vláken nebo běžně používanou satelitní komunikací.

[1] Měřený stav se nezmění pouze v případě, že je vlastním stavem přístroje.

Kapitola 4

Kvantová distribuce klíče pomocí jednotlivých fotonů

Název této kapitoly by v anglické literatuře zněl přibližně takto: Single–photon QKD, kde QKD znamená quantum key distribution. Nejprve vysvětlím první a nejnázornější protokol BB84, který byl navržen pro kódování pomocí polarizace. Pak popíšu kódování pomocí fáze. Při experimentu vzniká několik praktických problémů, které plynou z neideálních zdrojů, detektorů a přenosových soustav. Pokusím se vysvětlit, jak tyto praktické problémy vedou ke snížení bezpečnosti a ke zkrácení výsledného klíče. Na konci kapitoly popíšu několik důležitých experimentů. Některé využívají optická vlákna, v jiném byly kvantově spojeny volným prostorem dva alpské vrcholky. Popis praktických problémů kvantové kryptografie a údaje o provedených experimentech pocházejí ze sborníku o kvantově kryptografii [7].

4.1 Kódování pomocí polarizace - BB84

V tomto uspořádání Alice posílá Bobovi světelné pulsy, z nichž každý obsahuje právě jeden foton určité polarizace. Zatím předpokládejme, že polarizace je buď svislá ($|\updownarrow\rangle$) nebo vodorovná ($|\leftrightarrow\rangle$). Tyto dvě polarizace vyjadřují hodnoty „0“ nebo „1“ a foton tak tvoří qubit. Pokud tedy Alice posílá fotony pouze v polarizacích $|\updownarrow\rangle$ nebo $|\leftrightarrow\rangle$, můžeme říct, že je posílá v $\oplus$ bázi.[1] Bob použije polarizační dělič svazku (polarisation beam splitter – PBS) a každý foton naměří v jednom ze dvou detektorů, podle toho zda měl horizontální či vertikální polarizaci. Pak říkáme, že použije také bázi $\oplus$. Dosud systém vůbec není bezpečný. Eva si totiž může každý z fotonů naměřit a vyrobit foton se stejnou polarizací, který pošle Bobovi. Alice však může také použít bázi $\otimes$, kde diagonální polarizace $|\nearrow\rangle$ znamená „0“ a polarizace $|\nwarrow\rangle$ značí „1“. Bob může svoji měřící aparaturu také pootočit o 45° a měřit v bázi $\otimes$. Bezpečnost je

[1] To je báze, ve které lze přesně odlišit fotony, které jsou polarizovány vertikálně, od těch, co jsou polarizovány horizontálně.

zaručena tím, že pokud je foton připraven v bázi $\otimes$ ale změřen v bázi $\oplus$, pak bude zcela náhodně (bez ohledu na skutečnou polarizaci) se stejnou pravděpodobností zaregistrován v prvním či druhém detektoru. Alice tedy náhodně vybere bázi, ve které foton připraví, dále vybere jednu ze dvou polarizací (tedy hodnotu „0“ nebo „1“) a foton pošle. Pokud chce Eva foton změřit, musí si také vybrat nějakou bázi. Pokud naměří například polarizaci $|\updownarrow\rangle$, nemůže vědět, zda původní polarizace byla opravdu $|\updownarrow\rangle$, anebo $|\nearrow\rangle$ či $|\nwarrow\rangle$. V každém případě musí poslat Bobovi nějaký foton a často se splete. Důležitá je zde platnost neklonovacího teorému. Eva nemůže foton zkopírovat, ale je donucena ho změřit. To vede ke kolapsu superponovaného stavu. Bob s Alicí si **během** posílání telefonují a Bob Alici sděluje, zda zaregistroval foton, který Alice poslala. Takto vznikne tzv. surový klíč (raw key) – m odeslaných bitů. **Po** posílání si Alice s Bobem veřejně sdělí, u kterého fotonu použili kterou bázi, a záznamy o fotonech, u kterých použili různé báze, vyhodí – jsou bezcenné. Tím vznikne „prosetý klíč“ (sifted key), to je při použití dvou bází přibližně polovina bitů (n bitů). Z tohoto společného kódu si hodnoty některých naměřených fotonů řeknou a tím zjistí chybovost (informace o prozrazených fotonech už dále nepoužijí – tím se opět zkrátí klíč – na L bitů). V ideálním případě jakýkoli nesouhlas v prosetém klíči svědčí o odposlechu. V praxi je však chybovost způsobena neideálními přístroji a bude podrobně diskutována. Při nulové (nízké) chybovosti nyní sdílí Alice s Bobem L shodných a tajných bitů, které využijí jako klíč.

4.2 Kódování pomocí fáze

Místo tvorby qubitu pomocí polarizace můžeme vytvořit qubit pomocí fáze. Jde vlastně o měření konstruktivní či destruktivní interference, které lze rozlišit pomocí dvojice detektorů, čímž vzniká bitová informace. Tato metoda byla původně vymyšlena pro kvantovou kryptografii propletených stavů, nicméně ji lze využít i v kvantové kryptografii jednotlivých částic. Alice a Bob využívají *Machova-Zehnderova inteferometru* [8] a jsou mezi nimi natažena dvě optická vlákna. Bob i Alice mají také fázový modulátor. Alice vysílá dva pulsy a může se rozhodnout buď pro jeden z dvojice fázových posunů 0 či π (odpovídá bázi $\oplus$) anebo pro jeden z dvojice fázových posunů $\frac{\pi}{2}$ či $\frac{3\pi}{2}$ (odpovídá bázi $\otimes$). Bob si může na svém fázovém modulátoru nastavit fázový posun 0 (tím měří v bázi $\oplus$) a nebo $\frac{\pi}{2}$ (čímž měří v bázi $\otimes$). Analogie s předchozím polarizačním postupem je zřejmá. Praktický problém však tkví v tom, že je potřeba udržet fázový posun mezi dvěma pulsy ve dvou dlouhých vláknech natažených mezi Alicí a Bobem. Tento problém, lze však vyřešit tak, že na výstupu Aliciny částí Machova-Zehnderova interferometru jeden z pulsů necháme projít kratší drahou (S – short) a druhý delší drahou (L – long). A poté pošleme oba pulsy za sebou společným optickým vláknem. Pro časový odstup dvou pulsů v jednom vlákně se takto vytvořený qubit označuje jako *time-bin qubit*. Oba pulsy, které přiletí k Bobovi, rozdělíme

a necháme projít podobnými drahami S a L. V Bobově části interferometru se tedy objeví celkem čtyři pulsy, které lze zřejmě popsat jako: SS, SL, LS a LL. Pulsy SS a LL nejsou podstatné, neboť s ničím neinterferují. Pulsy SL a LS však prošly po stejné dráze a jejich dráhový rozdíl je dán pouze Aliciným fázovým modulátorem. Tyto pulsy tedy konstruktivně či destruktivně interferují a tím tvoří qubit. Toto uspořádání je mnohem stabilnější než uspořádání se dvěma optickými vlákny.

4.3 Praktické problémy jednofotonové kryptografie

Hlavním problémem kvantové kryptografie v praxi je, že jakmile dochází k nějakým chybám při posílání klíče, tak nelze rozlišit, zda jsou tyto chyby způsobeny nepřesností přístrojů anebo odposlechem. Chybovost (QBER - quantum bit error rate) tedy snižuje bezpečnost komunikace. Tento problém se řeší procesy, které opravují chyby (error correction) a zesilují bezpečnost (privacy amplification). Výsledkem těchto procedur je shodný společný zcela tajný klíč. Na tyto procesy je však třeba obětovat některé bity z prosetého klíče (zveřejnit výsledky některých měření). Při vysoké chybovosti se tedy neúnosně snižuje množství přenesených tajných bitů.

4.3.1 Zdroje chyb

Přístrojové řešení kvantové kryptografie je optickou soustavou, která se skládá ze zdroje (laser), přenosové soustavy (polarizátory, cirkulátory, destičky, děliče svazku, polarizační děliče svazku, Faradayova zrcadla a další) a detektorů (lavinové fotodiody).

1. Prvním problémem je zdroj. Dosud neexistuje vhodný zdroj, který by vysílal jednofotonové pulsy. Používané lasery vysílají pulsy v nichž je počet fotonů určen poissonovským rozdělením. Střední hodnota počtu fotonů je nastavena dostatečně pod jedničku, aby se minimalizoval počet pulsů obsahujících více než jeden foton. Důvodem je, že pokud puls obsahuje více než jeden foton, tak jsou všechny tyto fotony stejné (stejně polarizované, se stejnou fází apod.). Eva může jeden z fotonů z tohoto pulsu naměřit, tím získá přesnou informaci. Zbytek pulsu však doletí k Bobovi a odposlech není odhalen – princip kvantové kryptografie se tím ztrácí.

2. Druhým problémem jsou ztráty v přenosové soustavě. Cílem je používat takové prvky, které nesnižují intenzitu světla a nedochází tak (alespoň teoreticky) k občasným ztrátám fotonu. Při přenosu optickým vláknem však ke ztrátám nutně dochází. Pravděpodobnost ztráty navíc exponenciálně roste s délkou optického

vlákna. Délka je tedy hlavním limitujícím faktorem kryptografie pomocí optických vláken (současným provedeným maximem je vzdálenost přibližně 100 km).

3. Třetím problémem jsou nepřesnosti detektorů. U současných detektorů je hlavním problémem poměrně vysoká pravděpodobnost jejich sepnutí, aniž by přiletěl jakýkoli foton (dark count probability). Toto je hlavní limitující faktor současného kryptografického vývoje. Při posílání fotonů volným prostorem ještě vzniká problém pozadí, kdy na detektor dopadají kromě vyslaných fotonů také fotony pozadí. Dobré odfiltrování pozadí je důležitým experimentálním úkolem.

4.3.2 Získání výsledného klíče

Výsledný klíč získají Alice a Bob z klíče prosetého tím, že obětují některé bity pro opravu chyb a ověření bezpečnosti. Délku výsledného klíče můžeme vyjádřit vzorcem [7]:

$$L = n - (e_T + q + t + \nu) - (a + g_{pa}). \tag{4.1}$$

Člen n vyjadřuje délku prosetého klíče. Pokud předpokládáme poissonovský zdroj, lze délku prosetého klíče vyjádřit vzorcem [7]:

$$n = \frac{m}{2}\left[\psi_1(\eta\mu\alpha)(1 - r_d) + r_d\right], \tag{4.2}$$

kde m je počet odeslaných pulsů (bitů), η je účinnost Bobova detektoru (tedy pravděpodobnost, že detektor sepne pokud foton opravdu přiletěl), r_d je dark count probability (tedy pravděpodobnost, že detektor sepne, přestože vyslaný foton nepřiletěl) a konečně α je pravděpodobnost, že foton projde kvantovým kanálem. Výrazem ψ zapisujeme poissonovské rozdělení:

$$\psi_k(x) = \sum_{l=k}^{\infty} e^{-x}\frac{x^l}{l!}. \tag{4.3}$$

Takto získáme prosetý klíč v praxi.

Člen e_T vyjadřuje počet chyb v prosetém klíči. Tyto chyby lze opravit procedurou, při které je dle Shannonova kódovacího teorému nutné obětovat další bity z tajného kódu. Ty vyjadřuje člen q. Chyby mohly být způsobeny odposlechem. Množství informace, které uniklo Evě, vyjadřuje člen t, který lze vypočítat podle vzorce $t = Te_T$, kde T je koeficient, který složitým způsobem [7] závisí na chybových parametrech a také na uvažované pravděpodobnosti úspěšnosti Evina útoku na jednofotonový puls.

Člen ν vyjadřuje informaci, kterou získala Eva útokem na vícefotonové pulsy. Útoky na vícefotonové pulsy lze rozdělit na *přímé* (unambiguous state discrimination – USD) a *nepřímé* (photon number splitting – PNS). Při přímých útocích Eva okamžitě v nějaké náhodné bázi naměří část fotonů z pulsu a zbytek nechá

proletět k Bobovi. Při nepřímém útoku Eva část fotonů odebere a snaží se je přechovat, dokud si Alice a Bob nesdělí použité báze, Eva pak změří foton ve správné bázi. Volba vhodné strategie závisí na chybových charakteristikách kryptografického zařízení a také na technických možnostech, které přisuzujeme Evě.

Poslední dva členy jsou ve vzorci (4.1) odděleny, jelikož se jejich hodnota nezvyšuje s celkovým množstvím m posílaných bitů. Člen a vyjadřuje náklad na autentifikaci. Tyto bity potřebujeme, abychom ověřili, že informace posílané veřejným kanálem nejsou po cestě měněny (tzv. man in the middle). Poslední člen g_{pa} odpovídá efektivitě procesu zesílení bezpečnosti (privacy amplification). Jedním ze způsobů zesílení bezpečnosti je, že Alice pošle veřejně Bobovi binární matici K o rozměrech $(n - g_{pa}) \times n$, kterou oba vynásobí celý klíč. Evinu informaci o výsledném klíči lze takto snížit na libovolnou požadovanou hodnotu za cenu obětování určitého počtu bitů.

4.4 Jednofotonová kryptografie pomocí optických vláken

Skupina aplikované fyziky na Ženevské univerzitě provedla již řadu zajímavých realizací kvantové kryptografie. První experimenty používaly protokol BB84 a podařilo se přenášet fotony volným prostorem na vzdálenost nejprve 30 cm a později až 20 km. Větší pozornost je však věnována transportu fotonů optickými vlákny. Polarizace v tomto případě není vhodným způsobem kódování, neboť polarizace se v optických vláknech nezachovává. Proto se využívá kódování pomocí fáze, pro které byl navržen tzv. plug&play systém.

4.4.1 Uspořádání plug&play

Toto uspořádání využívá tzv. time-bin qubitů a nabízí velmi stabilní (a již komerčně produkovaný!) systém pro kvantovou komunikaci. Hlavní myšlenkou je posílání fotonu (qubitu) tam i zpět za účelem vzájemného odečtení všech změn fáze vzniklých na trase. Laserový puls tentokrát vysílá Bob. V Bobově aparatuře se puls pomocí děliče svazku rozdělí na dvě stejné poloviny (50/50 BS). Jedna polovina projde krátkým ramenem, kde dochází k pootočení polarizace o 90°. Druhá polovina prochází dlouhým ramenem, které puls zpozdí o 50 ns a navíc obsahuje fázový modulátor (PM_b). Oba ortogonálně polarizované pulsy pak společným optickým vláknem putují k Alici, kde fázový modulátor (PM_a) posune fázi druhého pulsu. Oba pulsy se odrazí na Faradayově zrcadle, které kompenzuje jakékoli změny polarizace v optickém vlákně, pokud jím puls posíláme tam i zpět. Oba ortogonální pulsy dorazí k Bobovi, kde jsou opět rozděleny pomocí polarizačního děliče svazku (PBS). Pulsy tentokrát putují opačnými rameny. Podle interference (která je daná fází) je foton

zachycen jedním ze dvou detektorů. Alice může ve svém modulátoru (PM_a) zvolit některý ze čtyř fázových posunů: 0 či π (odpovídá bázi $\oplus$) nebo $\frac{\pi}{2}$ či $\frac{3\pi}{2}$ (odpovídá bázi $\otimes$). Bob podle nastavení svého modulátoru (PM_b): 0 či π měří v bázi $\oplus$ nebo $\otimes$, čímž jsou splněna pravidla kvantové komunikace.

Za pozornost stojí, že počet ramen v Alicině a Bobově přístroji lze zvýšit. Při použití d ramen je místo qubitu posílán qudit. To může zmnohonásobit rychlost přenášení informace. Systém s větším počtem ramen se dokonce ukazuje stabilnějším.

Hlavní výhodou tohoto výzkumu je použití systému, který je díky posílání fotonů tam a zpět stabilní a nevyžaduje opakované nastavení (jedná se o tzv. autokompenzovaný interferometr). Další výhodou je použití běžných vlnových délek a díky tomu běžných optických vláken. To umožnilo komerční využití systému. Hlavní nevýhodou je velice omezená vzdálenost, na kterou lze komunikovat. Aktuální omezení vzdálenosti je přibližně 100 km. Mezikontinentální komunikace je touto technologií vyloučena.

4.4.2 Využití polarizace

Tým na Bostonské univerzitě navrhuje zajímavá uspořádání, která jsou odolná proti nepřesnostem v optické soustavě a především nevyžadují opakované nastavování. Mezi taková patří i právě popsané uspořádání plug&play díky autokompenzovanému interferometru. Bostonský tým ale navrhl i uspořádání, které využívá kódování pomocí polarizace. Jednofotonový puls opět vysílá Bob, který aktivně vybírá mezi vertikální nebo horizontální polarizací. Alice odráží foton Faradayovým zrcadlem a kromě toho posílá Bobovi ještě jeden nepolarizovaný foton. Hodnotu qubitu určuje Alice tím, že nepolarizovaný foton pošle buď před fotonem („0“) nebo za fotonem („1“), který odráží. Vzhledem k tomu, že Eva nezná původní polarizaci Bobova fotonu, nedokáže zjistit hodnotu Alicina bitu. Systém je odolný proti změnám polarizace v optickém vlákně díky Faradayově zrcadlu, které zajistí, že foton poslaný Bobem se k němu vrátí s přesně kolmou polarizací. Pokud tedy Bob pošle foton $|V\rangle$ a u prvního fotonu, který přiletí, naměří polarizaci $|H\rangle$, kdežto u druhého třeba $|V\rangle$, pak jde o bit s hodnotou „1“. Pokud Bob naměří dvě stejné polarizace (v polovině případů), pak je třeba výsledek měření zahodit.

4.5 Jednofotonová kryptografie volným prostorem

Výzkum vedený Mnichovskou univerzitou se zaměřuje na posílání fotonů volným prostorem. Hlavním cílem je dospět k tajné komunikaci prostřednictvím satelitů na oběžné dráze. Je tedy nutné vyrobit dostatečně miniaturizovaný a přitom spolehlivý vysílač a přijímač. Nejdůležitějším experimentem byla realizace kvantové komunikace

mezi alpskými vrcholy Zugspitze a Karwendelspitze na vzdálenost 23,4 km. Zvláštností experimentu je použití čtyř různých laserů pro čtyři různé polarizace místo polarizování světla jediného laseru. Průměrný počet fotonů v jednom pulsu byl 0,1. Vysílací zařízení vyžaduje sekvenci náhodných čísel, podle kterých se volí polarizace. Naopak v přijímacím zařízení přilétající foton náhodně vletí do první či druhé báze a je změřen. Aktivní náhodná volba báze proto není nutná. Větší nadmořská výška byla volena kvůli snížení rušivého vlivu vzdušných turbulencí. Největším zdrojem chyb bylo silné světelné pozadí způsobené sněhovou pokrývkou. Brzdou v rychlosti spojení byl veřejný kanál, který tvořila mobilní internetová linka. Výsledná rychlost byla několik set bitů bezpečného společného klíče za vteřinu. Teoreticky je dokázáno, že tajná kvantová komunikace s využitím satelitům je touto technologií realizovatelná. Případné experimenty jsou však velmi nákladné.

Kapitola 5

Kvantová distribuce klíče pomocí propletených stavů

V této kapitole nejprve vysvětlím základní princip kryptografie propletených (entanglovaných) stavů. Následně budu diskutovat hlavní výhody kryptografie propletených stavů oproti jednofotonové kryptografii. Po přehledu používaných zdrojů propletených stavů podrobně uvedu hlavní uskutečněné experimenty pomocí entanglementu.

5.1 Základní schéma kvantové kryptografie pomocí entanglementu

Základem této komunikace je propletený stav. Jedná se obvykle o pár (někdy i více) fotonů, jejichž některá vlastnost (např. polarizace) je vzájemně korelovaná. Fotony pak popisujeme jedním společným kvantovým stavem. Kvantové schéma vysvětlím pro případ propletené polarizace. Tento názorný protokol je mírným zjednodušením protokolu, který navrhnul Artur Ekert v roce 1991. Princip je podobný protokolu BB84, ačkoli Ekert tento starší protokol neznal.

Uvažujme zdroj propletených stavů (např. SPDC viz dále), který vytvoří pár fotonů, který má zcela korelovanou vzájemně ortogonální polarizaci. Takový stav páru fotonů můžeme společně zapsat:

$$|\Psi\rangle = \frac{1}{\sqrt{2}}\left(|\updownarrow\rangle|\leftrightarrow\rangle - |\leftrightarrow\rangle|\updownarrow\rangle\right). \tag{5.1}$$

Jeden z fotonů letí k Alici a druhý k Bobovi. Každý z nich provádí měření pomocí báze $\oplus$, kterou však otáčí kolem osy, podél které přilétají fotony. Alice například o úhly: $\phi_1^a = 0$, $\phi_2^a = \frac{1}{4}\pi$ a Bob: $\phi_1^b = \frac{1}{8}\pi$, $\phi_2^b = \frac{3}{8}\pi$ (jedná se o Bellovy testovací úhly). Každé měření má dva možné výsledky: „+1“ (pokud je foton v prvním polarizačním stavu vůči zvolené bázi) nebo „-1“ (foton je v druhém polarizačním stavu vůči zvolené bázi). Alice a Bob mění báze, ve kterých měří, nezávisle a náhodně. Pokud oba

zvolí stejnou bázi, vědí, že nutně naměřili opačné hodnoty. Poté, co naměří dostatečné množství fotonů, sdělí Alice a Bob veřejně, které rotace báze zvolili. U fotonů, pro které použili různé báze, si sdělí i výsledek měření. Z toho vypočtou hodnotu množství Q. Hodnota Q musí narušovat nerovnost CHSH a měla by být dle (2.21): $Q = -2\sqrt{2}$. Pokud tomu tak je, pak ty fotony, které byly naměřeny se stejnou rotací báze, tvoří společný tajný klíč. Pokud je hodnota $|Q|$ nižší, svědčí to o (částečném) odposlechu. Užitečná informace je nesena pouze vzájemnou korelací fotonů. Pokud chce Eva tuto informaci získat, pak tuto korelaci nutně zničí. Nerovnost CHSH pak ale nebude narušena. Jedna z výhod tohoto postupu je zřejmá. Nedochází ke ztrátě bitů z prosetého klíče pro odhalení odposlechu. Kvantová kryptografie pomocí propletených stavů však skýtá řadu důležitějších výhod.

5.2 Výhody kryptografie propletených stavů

1. První výhodu je, že při vytváření propleteného stavu dochází k nižším ztrátám fotonů než při kódování potřebné informace do jednofotonových pulsů. Zdroj propletených stavů navíc vůbec nemusí být součástí Alicina či Bobova přístroje. Může být obecně kdekoli na trase mezi nimi. Pokud je zdroj umístěn uprostřed mezi Alici a Boba, dochází vůbec k nejmenším ztrátám fotonů.

2. Druhou výhodou je, že pokud puls obsahuje více než jeden pár, pak každý pár je korelován zvlášť a dohromady netvoří qubit. Útoky na vícefotonové pulsy v tomto případě nefungují a neuniká jimi žádná informace. Při detekci vícefotonového pulsu však může dojít k neshodě mezi Aliciným a Bobovým přijímačem a tím k chybě. Celkově je možné zvýšit výkon poissonovského zdroje za účelem zvýšení rychlosti komunikace.

3. Třetí a velice důležitou výhodou je, že Alice i Bob mohou mít jen pasivní přijímače, tedy přijímače v nichž si přilétající foton sám zcela náhodně vybere bázi, ve které bude změřen. Není tedy potřeba žádné aktivní přepínání ani sekvence náhodných čísel.

4. Čtvrtou výhodou je, že porušení nerovnosti CHSH zajišťuje, že fotony tvořící pár jsou nerozlišitelné i ve všech ostatních stupních volnosti. Naproti tomu v jednofotonovém případě jsou jednotlivé stavy aktivně vytvářeny odlišným nastavením nějakého přístroje (např. polarizátoru). Mohou se tak lišit kromě např. polarizace ještě třeba vlnovou délku. Měřením vlnové délky by tak mohla Eva celý klíč rozšifrovat, aniž by narušila měřenou polarizaci. Podobně Eva nemůže zjistit klíč tím, že bude „odposlouchávat“ právě nastavování např. polarizátoru. Žádná takovou aktivní složku komunikace pomocí propletených stavů nevyžaduje.

5.3 Zdroje propletených stavů

K vytvoření propletených stavů se využívá efektů nelineární optiky. Základem je vždy laser, který vysílá fotony do krystalu vyrobeného z nelineárního materiálu. V krystalu vznikají dva fotony s propletenými vlastnostmi (down-conversion). Teoreticky správněji funguje laseru jako energetická pumpa, která dodává do krystalu energii. Pár fotonů vzniká spontánní emisí, přičemž je využita vždy veškerá energie přijatá z laseru a krystal je zachován přesně v původním stavu (parametric down-conversion). Celý proces obvykle zkracujeme písmeny SPDC (spontaneous parametric down-conversion).

5.3.1 Time-bin entanglement

Jednou z propletených vlastností může být čas. V rámci koherenční doby laseru je čas, kdy dvojice fotonů vznikne, zcela náhodný. Oba fotony však vznikají ve stejném čase, čili jsou časově propleteny (time-entanglement). Omezujícím faktorem je v tomto případě koherenční doba laseru. Pokud ale použijeme laser vysílající krátké pulsy a před nelineární krystal vložíme interferometr, který z laserem vyslaného fotonu vytvoří superponovaný stav (superpozice stavu odpovídajícího průchodu dlouhým resp. krátkým ramenem), tak v krystalu vznikají fotonové páry, jejichž časově propletené stavy lze využít v kvantové kryptografii. Jedná se o přímou analogii time-bin qubitů v jednofotonovém případě a propletený stav lze obecně zapsat ve tvaru:

$$|\psi\rangle = \alpha\,|0,0\rangle + e^{i\varphi}\beta\,|1,1\rangle\,, \tag{5.2}$$

kde $|0,0\rangle$ značí stav, při kterém jsou oba fotony v časové jámě (time-bin) 0, podobně pro stav $|1,1\rangle$.

5.3.2 Propletení hybnosti

Další možností je propletení hybnosti fotonů. Využívá se zde toho, že různé vlnové délky jsou nelineárním krystalem vysílány do různých směrů, přičemž celková energie se zachovává (parametric down-conversion). Dvě různé vlnové délky dvou fotonových párů jsou rekombinovány použitím děliče svazku. Výsledkem je stav propletených hybností. V současné době se tohoto propletení příliš nevyužívá. Je mu však přisuzována značná budoucnost v tzv. spojité kvantové kryptografii.

5.3.3 Propletení polarizace

Velmi používaným způsobem je propletení polarizací. Nelineární krystal vyzařuje páry fotonů, z nichž jeden je polarizován ordinárně a druhý extraordinárně. Při tzv. typu I jsou fotonové páry polarizovány souhlasně, při typu II (type-II parametric

down-conversion) jsou fotony v páru polarizovány ortogonálně. V nedávno objeveném zdroji jsou ortogonálně polarizované fotony vysílány ve směru dvou kuželů (nikoli souosých, ale protínajících se). Ve dvou průsečnicích máme tedy nepolarizované světlo, protože u konkrétního fotonu nedokážeme rozlišit, z kterého kužele pochází. (To není úplně pravda – dvojlomným krystalem lze ordinární a extraordinární fotony rozlišit.) Vložení vhodných identických ale vzájemně o 90° pootočených krystalů do každého z paprsků vymaže informaci o původu jednotlivých fotonů a dojde k dokonalému propletení polarizace (5.1).

5.4 Experimenty využívající propletené stavy

5.4.1 Ženeva

Ženevské skupině se podařilo využít hlavní výhody propletených stavů, a to je automatická náhodná volba měřicí báze přilétajícím fotonem. Alice a Bob tak mohou použít pouze pasivní optické prvky. Nejdůležitějším výsledkem je značný pokles ztrát v měřicích optických soustavách. K pokusu byl použit poissonovský pulsní laser a krystal vytvářející time-bin entanglement. Každý z časově propletených fotonů byl analyzován interferometrem, jehož rozdíl v délce ramen je shodný s interferometrem před krystalem. Bob a Alice tedy nezávisle na sobě zjišťovali stav fotonů vyslaných zdrojem, který byl umístěn přibližně v polovině cesty mezi jejich přijímači. Toto symetrické uspořádání je nejodolnější proti ztrátám v optickém vlákně. Při experimentu bylo opět použito standardní optické vlákno. Přenos byl úspěšně realizován optickým vláknem délky 50 km (namotaným na cívce).

5.4.2 Vídeň – optické vlákno

Vídeňská výzkumná skupina realizovala experiment v reálných podmínkách. Komunikace probíhala mezi jednou z vídeňských bank a vídeňskou radnicí pomocí optického vlákna dlouhého 1,45 km. Jako zdroj sloužil GaN laser pumpující fotony do nelineárního krystalu z β-barium borátu (BBO). Výsledkem byly zcela polarizačně propletené fotonové páry. Alicina část přístroje sestávala ze zdroje a ze čtyř pasivních detektorů napojených na elektronické zpracování dat a na synchronizační laser. Bobova část obsahovala podobné čtyři pasivní detektory pro detekci kvantových stavů a dále jeden detektor pro detekci paprsku synchronizačního laseru. Jako veřejný kanál byl použit standardní TCP-IP protokol. Elektronika na Alicině straně otevírala v detektorech časové okno 10 ns pro detekci příchozího fotonu. Zároveň byl odeslán synchronizační puls pro Bobovy detektory. Zpracování dat bylo opatřeno i odhadem chybovosti, opravou chyb, posílením bezpečnosti a autentifikací veřejné cesty. Hrubý naměřený klíč (raw key) vykazoval chybovost (QBER) nižší než 8%. Z toho 2,6% je způsobeno chybami v detekci a 1,2% špatnou viditelností propletených stavů. Rych-

lost přeneseného hrubého klíče byla přibližně 80 bitů/s. Experiment celkově ukázal, že kvantová kryptografie pomocí propletených stavů není omezena na laboratorní podmínky a její komerční využití není daleko.

5.4.3 Vídeň – volný prostor

Hlavní motivací pro kvantovou komunikaci volným prostorem je zvětšení možné vzdálenosti komunikujících subjektů. Cílem je umožnit komunikaci pomocí satelitů. Vzdálenost Alice a Boba tak bude neomezená. Zajímavé je, že vertikální průchod atmosférou vykazuje přibližně stejné rušivé vlivy jako pouhá vzdálenost 4 km při komunikaci podél zemského povrchu v běžné nadmořské výšce. První vídeňský experiment proběhl na vzdálenost 600 m mezi Alicí a Bobem při mírně asymetrickém umístění zdroje. Pro pokus byl opět využit zdroj polarizačně propletených stavů, obsahující nechlazený laser. K určitým ztrátám dochází v teleskopech, které směrují fotony od zdroje k přijímačům. Další ztráty jsou způsobeny dark count probability detektorů – to omezuje především rychlost spojení. Přesto výsledná QBER je 8,4%, což je dostatečně nízká míra pro uplatnění v satelitní kvantové komunikaci s teleskopy o průměru 20 cm na satelitu a o průměru 1 m na Zemi. Při pokusu byla také určena hodnota $Q = 2,41 \pm 0,10$, což bezpečně vyvrací nerovnost CHSH a svědčí o skutečném sdílení propletených stavů. Experiment pak byl neméně úspěšně zopakován pro vzdálenost 7,8 km. Časové sladění zajišťovaly atomové rubidiové hodiny synchronizované systémem GPS.

5.4.4 Boston – samonastavovací systémy

Stejně jako pro jednofotonové systémy i pro propletené stavy vymýšlí Bostonský tým stabilní a odolná uspořádání umožňující tajnou kvantovou komunikaci. Hlavní výhoda používání propletených stavů v těchto systémech spočívá v tom, že fotony nemusejí absolvovat cestu tam i zpět a nemusejí být odráženy Faradayovým zrcadlem. Jedná se buď o jednosměrná uspořádání (fotony letí od Alice k Bobovi), nebo o tzv. symetrická uspořádání (zdroj je mezi Alicí a Bobem a každému z nich vysílá propletené fotony).

Jednosměrné polarizačně kódované schéma

Alice posílá tři fotony s časovými odstupy τ, z toho dva v polarizačně propleteném stavu a jeden nepolarizovaný. Alice aktivně ovlivňuje pořadí fotonů. Propletené jsou tedy buď fotony 1 a 2 nebo 2 a 3 nebo 3 a 1. Bobův pasivní systém sestává z interferometru, jehož delší rameno vytváří časový odstup τ. Náhodně dva ze tří fotonů interferují (Bob ale třetí foton detekuje buď před nebo za těmito dvěma, čili dokáže rozlišit, které dva fotony interferují.) Interferující fotony spolu vstupují do polarizačního děliče svazku. Pokud jsou fotony propletené, pak jistě opustí dělič svazku

různými směry. Naopak pokud oba opustí polarizační interferometr stejnou cestou, pak jistě nebyly v propleteném stavu. V tomto úspěšném případě tedy Bob může vyloučit propletenost jedné ze tří možných kombinací. Před první popsaný interferometr je třeba ještě umístit interferometr se zpožděním 4τ, díky kterému na druhém interferometru může dojít i k interferenci prvního a třetího fotonu. Alice nyní vyhlásí, zda se jednalo o datové měření (propletenost po sobě jdoucích fotonů) nebo testovací měření (propletený stav byl mezi fotony 1 a 3). Pro případ datového měření Bob může díky této veřejné Alicině informaci v případě úspěšného měření již přesně určit hodnotu bitu. Testovací měření slouží k odhalení odposlechu.

Symetrické uspořádání využívající time-bin qubitů

Zdroj umístěný mezi Alicí a Bobem produkuje dva páry propletených fotonů ve stavu:

$$(|EE\rangle_{13} + |LL\rangle_{13})(|EE\rangle_{24} + |LL\rangle_{24}\,, \tag{5.3}$$

kde E znamená dřívější amplituda (early) a L značí pozdější amplitudu (late). Fotony 3 a 4 jsou přímo poslány Bobovi, kdežto fotony 1 a 2 projdou řadou tří přepínačů. První je dělič, který rozdělí fotony do dvou různých cest. Druhým je přepínač, který každou amplitudu každého fotonu ze dvou vstupů může buď odrazit nebo propustit do jednoho ze dvou výstupů. Důležité jsou případy, kdy E amplitudu fotonu 1 a L amplitudu fotonu 2 odrazí; zbylé dvě amplitudy propustí. Tím ve dvou výstupech dochází ke kombinaci amplitud fotonů 1 a 2 a vznikají stavy 5 a 6. Třetí spínač pak pošle oba fotony do jednoho optického vlákna. Pokud se ve stavu 5 a ve stavu 6 nachází po jednom fotonu, k čemuž s určitou pravděpodobností dochází, pak Alice a Bob měří výsledné stavy Mach-Zehnderovým interferometrem. Jiná měření zahodí. Procedurou se třemi přepínači se ze dvou propletených párů stávají čtyři vzájemně propletené fotony:

$$|ELLE\rangle_{5634} + |LEEL\rangle_{5634}\,. \tag{5.4}$$

Pokud dřívější amplituda projde delším ramenem interferometru, pak spolu obě amplitudy interferují a dojde k měření podobně jako v jednofotonovém time-bin případě. Stabilita systému je dána tím, že každým ramenem March-Zehnderova interferometru prochází jeden ze čtyř fotonů. Relativní fázový posun mezi rameny obou interferometrů tedy nemůže nijak ovlivnit měření, což je klíčové při praktické konstrukci interferometrů.

Kapitola 6

Další kvantové koncepty

V této kapitole popíšu některé postupy, kterými lze propletené stavy lépe stabilizovat a posílat na větší vzdálenost. Tyto procesy by mohly v budoucnosti umožnit vznik kvantových sítí, v rámci kterých by si mohli libovolní účastníci tajně sdělovat informace.

6.1 Čištění propletenosti

Tento proces v literatuře najdeme obvykle pod anglickým názvem *purification of entanglement*. Vzhledem k nevyhnutelné dekoherenci v kvantovém kanále dochází s délkou kanálu ke zhoršování kvality propleteného stavu. Cílem procesu je tedy po určité uražené délce v kvantovém kanále propletený stav vylepšit. Přesněji řečeno jde o zkvalitnění propletenosti dvou prostorově oddělených propletených částic. Hlavní roli zde hraje jeden ze základních prvků kvantového počítání tzv. CNOT gate viz např. [7]. V případě polarizačního propletení však roli CNOT gate může převzít polarizační dělič svazku (PBS), který propouští horizontálně polarizované světlo a odráží vertikálně polarizované (má dva vstupy a dva výstupy). Uvažujme, že Alice a Bob díky kvantovému kanálu sdílejí dohromady dva páry stejných smíšených propletených stavů: $\rho_{AB} = F.\left|\Phi^+\right\rangle\left\langle\Phi^+\right|_{AB} + (1-F)\left|\Psi^-\right\rangle\left\langle\Psi^-\right|_{AB}$, kde $\left|\Phi^+\right\rangle = (\left|HH\right\rangle + \left|VV\right\rangle)$ tvoří jeden ze čtyř zcela propletených Bellových stavů. F vyjadřuje čistotu propletenosti stavu ρ_{AB}, tedy procento poslaných stavů, které po průletu kvantovým kanálem stále vykazují propletenost. Nyní Alice a Bob dva své fotony ze dvou sdílených párů vpustí do dvou vstupů PBS (a_1, a_2 u Alice; b_1, b_2 u Boba). Pokud u obou dojde k tomu, že dva fotony využijí k opuštění PBS oba výstupy (a_3, a_4, b_3, b_4) (fotony tedy byly stejně polarizované), pak došlo ke zkombinování: $\left|\Phi^+\right\rangle_{a_1,a_2} \otimes \left|\Phi^+\right\rangle_{b_1,b_2}$ nebo $\left|\Psi^-\right\rangle_{a_1,a_2} \otimes \left|\Psi^-\right\rangle_{b_1,b_2}$. Pokud nedojde k opuštění fotonů všemi čtyřmi výstupy, je měření zahozeno. V tomto „čtyřvýstupovém“ případě nyní stavy vystoupivší z a_4, b_4 zprojektujeme na bázi $\left|\pm\right\rangle = \frac{1}{\sqrt{2}}(\left|H\right\rangle \pm \left|V\right\rangle)$, tím ve výstupech a_3, b_3 vznikne požadovaný stav $\left|\Phi^+\right\rangle_{a_3,b_3}$ s pravděpodobností $F' = \frac{F^2}{F^2+(1-F)^2}$. Čistota stavu F' se tedy zvýší

pokud původní čistota byla $F > \frac{1}{2}$.

Pokud tedy máme dva páry o čistotě propletení 75%, lze z nich (s určitou pravděpodobností) získat jeden pár s čistotou propletenosti 92%. Entanglement purification je tedy cesta, jak překonat problémy s chybovostí kvantového kanálu při kvantové komunikaci. Tento proces hraje také významnou roli při opravě chyb v kvantovém počítání. Ve vídeňském experimentu úspěšnost tohoto procesu přesáhla 98%, což v principu umožňuje vznik kvantových opakovačů, viz dále.

6.2 Výměna propletenosti

I tento proces, který v literatuře najdeme pod názvem *entanglement swapping*, lze využít pro kvantovou komunikaci na dlouhé vzdálenosti. Funguje na odlišném principu a využívá další zvláštní vlastnosti propletenosti.

Uvažujme, že máme dva prostorově oddělené zdroje propletených stavů, které vyzařují fotony 0,1 resp. 2,3. Uvažujme, že foton 0 je poslán Alici a foton 3 je poslán Bobovi. U fotonů 1 a 2 společně změříme Bellův stav, čímž se stanou fotony 1 a 2 propletenými. Fotony 1 a 2 jsou ale stále propleteny s fotony 0 resp. 3. Tím pádem jsou i fotony 0 a 3 propleteny, ačkoli nepocházejí ze stejného zdroje, ani se spolu nikdy v minulosti nestřetly! Řetěz takových výměn propletenosti by umožnil kvantovou komunikaci na libovolně velkou vzdálenost. Propletenost byla experimentálně prokázána vídeňskou i ženevskou skupinou. V jednom případě bylo použito nelineárního krystalu, který byl pumpován světlem ze dvou stran, čímž vznikaly vždy dva páry propletených fotonů. V druhém případě byly názorněji použity dva oddělené nelineární krystaly. V obou případech se podařilo u fotonů, které spolu nikdy přímo neinteragovali, prokázat propletenost, která porušovala Bellovu nerovnici.

6.3 Kvantový opakovač

Cílem ve vývoji kvantových opakovačů (*quantum repeater*) je, aby se jednalo o přístroje, které dokáží rozpoznat a opravit všechny druhy chyb, které mohou během přenosu na kvantovém stavu nastat (např. dekoherence). Takové přístroje umožní kvantovou komunikaci na libovolnou vzdálenost. Předpokládá se, že tyto přístroje budou kombinovat postupy entanglement purfication, entanglement swapping a další procesy.

Jedním z nejsilnějších zdrojů chyb při kvantové komunikaci je ztráta posílaného fotonu. Řešením tohoto problému se zabývá skupina v Jet Propulsion Laboratory. Základním trikem je speciální zakódování dvou logických bitů do čtyř fyzikálních qubitů (čtyř fotonů), které neumožňuje takové naměření hodnoty jednoho ze dvou logických bitů, které by vypadalo jako ztráta jednoho ze čtyř fotonů; ale zároveň naopak umožňuje ztrátu jednoho ze čtyř přenášených fotonů opravit. Schéma opravy

je poměrně složité. K rozpoznání ztrát se využívají nepřímá měření, která nevedou ke kolapsu kvantového stavu (QND - quantum nondemolition). A k doplnění ztracených fotonů jsou potřeba jednofotonové pulsy. Při kvantové komunikaci musejí být každé dva kvantové opakovače tak blízko u sebe, aby mezi nimi byla pravděpodobnost ztráty dvou a více fotonů zanedbatelně malá (ztrátu jednoho fotonu lze opravit). Zajímavé je, že stočení vláken mezi kvantovými opakovači do smyček vede k vytvoření kvantové paměti. Qubity běhají smyčkami stále dokola, ale jejich ztráty jsou pravidelně opravovány. Čas, po který lze qubit v kvantové paměti uchovat, se tak zmnohonásobí.

6.4 Kvantová síť

V případě, že se podaří vytvořit a realizovat dostatečně účinné procesy pro opravu chyb, pak už nebude nic bránit ve vybudování globální kvantové sítě, ve které si budou moci účastníci tajně posílat informace. Prototypem kvantové sítě se zabývá bostonská firma BBN technologies, jejíž síť městských rozměrů zatím nevyužívá procesy opravující chyby. V síti, která spojuje sídlo firmy s Bostonskou a Harvardskou univerzitou, se kombinuje komunikace prostřednictvím jednofotonových pulsů i propletených stavů, a to jak optickými vlákny, tak volným prostorem.

Sítě lze rozdělit na dva různé typy. Prvním typem je tzv. důvěrná síť (trusted network), ve které v každém bodě je přijatý stav změřen a znovu poslán. Ostatní účastníci sítě tedy musejí věřit, že z jednotlivých bodů sítě informace neuniká. Taková síť je využitelná například pro armádu, která dokáže jinými prostředky zajistit, aby jednotlivé body, kde dochází k měření informace, byly bezpečné. Taková síť je při dostatečné hustotě bezpečných bodů již realizovatelná současnou technologií. Představu sítě, do které bude mít přístup mnoho různých uživatelů (třeba bank) a budou si moci vzájemně tajně posílat informace, to však nesplňuje. Toto je cílem tzv. *nedůvěrné sítě* (untrusted network), ve které v každém bodu dochází pouze k přenosu kvantového stavu dále a nikoli k jeho změření. Taková síť splňuje bezpečnostní představy, ale při současné technologii je její rozměr omezen například na větší město. Rozšíření takové sítě je podmíněno právě vznikem například účinných kvantových opakovačů. V principu je možné oba typy sítě kombinovat, tedy některé body takové sítě by byly důvěrné (například satelity nebo některé instituce) a ostatní nedůvěrné. Globální kvantová síť pro svoji složitou technologickou realizaci těžko nahradí internet, ale pro subjekty, které potřebují tajně komunikovat, bude důležitým doplňkem. To je ale hudba budoucnosti.

Kapitola 7

Závěr

Přestože jsem se snažil čerpat z aktuálních zdrojů, tak již v této chvíli se vývoj na poli kvantové kryptografie posunul. Málokterá vědecká disciplína se může pochlubit tak úzkým svázáním fundamentálních teoretických výsledků, experimentálních realizací a okamžitého komerčního využití. Proto je vývoj tak neuvěřitelně rychlý. Vlastnosti, které ještě nedávno byly předmětem filosofických disputací, jsou dnes prokazatelně využívány.

První systémy, které využívají kolapsu kvantového stavu a jednofotonových pulsů, dnes již nalézají komerční využití. Tyto systémy se jistě ještě zjednoduší a potažmo zlevní a budou k dispozici široké řadě institucí a jednotlivců, kteří využijí výhody prokazatelně tajné komunikace. Předpokládám však, že postupem času převáží výhody entanglovaných stavů. Při této „propletené kryptografii“ se využívá velmi zajímavé vlastnosti nelokality. Tyto moderní systémy principielně umožňují vznik kvantových sítí, které vedou k možnosti celosvětové tajné komunikace. Není jistě náhodou, že výzkumy v této oblasti podporuje mimo jiné americká armáda. Přestože kvantová síť pravděpodobně nebude znamenat tak revoluční změnu jako internet, může se stát významným doplňkem moderní globální komunikace. To je výzva, které nyní čelí řada vědců a inženýrů celého světa.

Literatura

[1] Bouwmeester D., Ekert A., Zeilinger A. (editoři): *The Physics of Quantum Information*, Springer, 2000

[2] Thomas, Andrew: *What is reality?*,
http://www.ipod.org.uk/reality/

[3] Wikipedia, *CHSH inequality*

[4] Wikipedia, *Quantum correlation*

[5] Groeblacher, S. a kol.: *An experimental test of non-local realism*,
http://arxiv.org/PS_cache/arxiv/pdf/0704/0704.2529v2.pdf

[6] Harrison, D. M.: *Bell´s Theorem*,
http://www.upscale.utoronto.ca/GeneralInterest/Harrison/BellsTheorem/

[7] Sergienko, A. (editor): *Quantum Communications and Cryptography*, CRC Press, 2006

[8] Wikipedia, *Mach-Zehnder interferometer*