Maturitní práce z informatiky

Kvantová kryptografie

Kyberbezpečnost v éře kvantových počítačů

Lea Petřivalská

Gymnázium Matyáše Lercha, Žižkova 55
2020/2021

Čestné prohlášení

Prohlašuji, že jsem svou maturitní práci nazvanou *Kvantová kryptografie* aneb *Kyberbezpečnost v éře kvantových počítačů* vypracovala samostatně a s použitím odborné literatury a dalších informačních zdrojů, jež jsou všechny citovány v práci a uvedeny v seznamu literatury na konci práce.

V Brně dne: _____

_____

Lea Petřivalská

Anotace

Tato maturitní práce zkoumá budoucnost zabezpečení dat v době, kdy budou v důsledku kvantové nadřazenosti překonány dosavadní metody šifrování. V práci jsou zkoumány možnosti aplikace kvantových jevů v kryptografii, zejména pak problematika přenosu kvantového klíče (QKD). Součástí práce je implementace komunikačního protokolu BB84 [1] za využití simulátoru kvantových jevů QuTiP [2]. Dotýkáme se také tématu postkvantové kryptografie, postavené na vlastnostech klasické termodynamiky, avšak odolné vůči výpočetní síle kvantových počítačů.

Klíčová slova

počítačová bezpečnost; kvantová kryptografie; quantum key distribution

Obsah

Úvod

Potřeba utajení písemné komunikace šla s vynálezem písma téměř ruku v ruce. Původní snahou antických civilizací bylo písemně zaznamenané zprávy fyzicky překrývat tak, aby nebyly nepříteli přímo na očích. Brzy si však začaly uvědomovat, že nežli text skrývat mechanicky, bylo by rozumnější přijít s takovým způsobem jeho záznamu, který by byl i v případě přečtení srozumitelný pouze zamýšlenému příjemci a který by v nepravých rukou nevyzradil okamžitě svůj smysl. Tak vznikla myšlenka *šifry*, o níž pojednává nauka nazvaná *kryptografie*.

Nebylo by však kryptografie, aby nebylo také lidí snažících se odkrýt obsah tajné zprávy, jež pro ně nebyla určena. Vědní disciplínu, která se zabývá prolamováním šifer bez znalosti informace potřebné ke standardnímu dekódování textu (tedy například tajného klíče), nazýváme *kryptoanalýza*. Tak byli kryptografové kryptoanalytiky neustále vyzýváni k tvorbě silnějších a důmyslnějších šifrovacích systémů a kryptografie prošla za stovky let své existence významnou evolucí.

Důležitý mezník v dějinách kryptografie představuje vznik elektronické výpočetní techniky. Nejenže počítače dramaticky usnadnily práci kryptoanalytikům a mnoho do té doby účinných šifer pozbylo své někdejší účinnosti, ale revoluce v přenosu informace se prakticky neobešla bez požadavku na kvalitní zabezpečení přenášených dat. V současnosti tak používáme šifry nabízející vysokou míru bezpečí a za užití žádných dnes dostupných technologií zpravidla nelze získat obsah takto šifrovaných informací v rozumném čase.

Co kdyby však do hry vstoupily stroje mnohonásobně výkonnější než současné elektronické počítače? Taková otázka je zcela namístě a odpovědí na ni by se již v dohledné době mohla stát kvantová výpočetní technika. Kvantové počítače, operující na principech kvantové fyziky, by totiž, jak naznačují výzkumy, mohly v budoucnu nabídnout výpočetní sílu, jež by náhle umožňovala řešit matematické problémy, které by klasickému počítači zabraly několik miliard let, v řádech několika sekund. A to mnohdy právě ty matematické problémy, na jejichž časovou náročnost současná kryptografie zcela spoléhá.

Dostupnost výpočetní síly takových rozměrů, by měla nutně za následek destrukci mnohých současných šifrovacích systémů. Stojíme tedy před novým problémem moderní kryptografie: nalezení způsobu, kterým by bylo možné účinně chránit informace v éře kvantové výpočetní techniky. Lze využít poznatků z kvantové mechaniky, jež na jedné straně mohou vést k ohrožení naší digitální bezpečnosti, také k obnovení této bezpečnosti ve formě nových *kvantových* kryptosystémů, jejichž bezpečnost by nebyla ohrožena výpočetní silou kvantových počítačů?

Tato maturitní práce si klade za cíl prozkoumat existující přístupy k řešení této otázky a postupně představuje nejprve soudobé metody šifrování a jejich potenciální slabiny v kontextu kvantové výpočetní techniky (kapitola 1), dále koncept *nepodmíněné bezpečnosti* a to, jakým způsobem souvisí s kvantovou kryptografií (kapitola 2), poté základy kvantové fyziky a teorie kvantového počítače (kapitola 3), a konečně způsoby zabezpečení dat v kyberprostoru využívající kvantové fyziky, souhrnně nazývané *kvantová kryptografie* (kapitola 4). Součástí práce je také implementace kvantového komunikačního protokolu *BB84* [1] v programovacím jazyce *Python* s využitím aplikačního rámce pro simulaci dynamiky otevřených kvantových systémů *QuTiP* [2].

Kapitola 1

Klasická kryptografie

Digitální data mnohdy obsahují citlivé informace, které z různých důvodů nechceme sdílet úplně s každým. Přirozeně se tak snažíme chránit své datové nosiče před ztrátou či zcizením. V praxi však nelze fyzicky ochránit veškerá digitální data a skutečně bezpečný systém musí počítat i s variantou, že se k nim cizí osoba nějakým způsobem dostane. Naší snahou je, abychom jí maximálně zkomplikovali zjištění skutečného významu těchto dat. Navíc kdykoli vyšleme jakoukoli informaci do kyberprostoru, zvláště užijeme-li k tomu veřejný komunikační kanál, jakým je Internet nebo bezdrátové formy komunikace, vystavujeme svá data riziku odposlechu a je proto třeba zaručit jejich ochranu také na digitální rovině. Právě k softwarové ochraně informací patří zcela neodmyslitelně ***kryptografie***. Kromě své hlavní funkce, jíž je skrytí dat třetím stranám, poskytuje kryptografie i další výhody, jako jsou:

- **integrita dat** – ověření, že informace nebyly neoprávněně či nestandardním způsobem pozměněny;
- **párová autentizace entit** – jedna entita ověřuje totožnost druhé entity pomocí *autentizačního protokolu*;
- **autentizace původu dat** – ověřuje, odkud data skutečně pocházejí;
- **neodmítnutelnost odpovědnosti** – ujištění, že autor zprávy nemůže zpětně popřít své autorství této zprávy.

1.1 Základní pojmy v kryptografii

Kryptografie je věda zabývající se tvorbou *šifrovacích systémů*. Ty nám umožňují převést tzv. *otevřený text*, tedy text v běžně čitelné podobě, na *text šifrovaný* neboli *kryptogram*. Tento proces se nazývá *šifrování* a proces zpětný naopak *dešifrování*. Šifrování i dešifrování textu zajišťuje *šifrovací* (též *kryptografický*) *algoritmus* a může k tomu použít různé *šifrovací klíče*. Klíčem se rozumí zpravidla tajná informace, kterou disponují strany účastnící se komunikace, a která ovlivňuje průběh šifrovacího algoritmu. V kryptografii budeme typicky hovořit o dvou komunikujících stranách tradičně označovaných písmeny *A* a *B* nebo jmény *Alice* a *Bob*.

1.2 Dělení moderní kryptografie

Nejtypičtějším dělením moderních šifer je dělení na šifry *symetrické* a *asymetrické*. Pokud mají obě strany vstupující do komunikace, tedy Alice i Bob, jeden společný klíč, který se používá pro šifrování i dešifrování textu, jde o šifru **symetrickou**. Pokud má každý z účastníků komunikace svůj vlastní *klíčový pár*, jde o šifru **asymetrickou**. Jeden klíč z páru, klíč *soukromý*, pak jeho vlastník uchovává v tajnosti a slouží mu k dešifrování obdržených zpráv. Druhý klíč z páru je *veřejný*, dostane se k němu kdokoliv a lze pomocí něj zašifrovat data odesílaná vlastníkovi soukromého klíče.

1.2.1 Symetrická kryptografie

Šifrovací systém je označován jako *symetrický* nebo také *konvenční*, pokud jsou **šifrovací a dešifrovací klíč totožné**, nebo pokud lze jeden z druhého snadno odvodit. Symetrické kryptografické systémy používají jeden ze dvou základních šifrovacích mechanismů, případně jejich kombinace. Jedná se o metodu *substituční* a metodu *transpoziční*.

Metoda substituční spočívá v nahrazování jednotlivých znaků či bloků textu za znaky jiné dle určitého pravidla. Co za který znak nahradit, určuje *substituční tabulka*, která bývá proměnlivá v závislosti na klíči. Speciálním druhem substitučních šifer jsou *šifry posunové*, u nichž jsou znaky nahrazovány znakem vzdáleným v abecedě o příslušný počet polí. Pokud je nutné znak posunout o více polí, než kolik má používaná abeceda znaků, pokračuje se opět od začátku abecedy. To v šifrovacích algoritmech zaručuje použití *modulární aritmetiky*. Nejstarší známá šifra fungující na tomto principu je *Caesarova šifra*, která posouvá všechny znaky otevřeného textu o stejný počet písmen. Klíčem k ní je tedy jediné číslo a označujeme ji za šifru *monoalfabetickou*. Komplexnější šifry pak používají delší klíče, posun jednotlivých písmen otevřeného textu se tak liší a jedná se o šifry *polyalfabetické*.

Metoda transpoziční (permutační) spočívá v přesouvání jednotlivých znaků či bloků textu na jiné místo v textu, dle určitého pravidla. Ovlivňuje tedy jejich pořadí. V moderních šifrách bývá s metodou substituční vhodně kombinována. Příklady takových šifer jsou například kryptografické systémy DES a AES, o nichž pojednává sekce 1.3.1.

Výhodou symetrické kryptografie je rychlost šifrovacího a dešifrovacího procesu. Při použití symetrické kryptografie k šifrování komunikace se však stává problematickou tvorba a výměna klíče, který budou znát právě a jen ony dvě komunikující strany. Další nevýhodou je velké množství klíčů, které musíme udržovat, chceme-li komunikovat s více stranami. Symetrická kryptografie nachází uplatnění také např. v šifrování zálohovaných dat.

1.2.2 Asymetrická kryptografie

Kryptografické metody řadíme mezi *asymetrické*, používají-li k šifrování a dešifrování obsahu odlišné klíče. Bývá proto někdy označována také jako *kryptografie s veřejným klíčem*. Asymetrické šifrování se využívá především k ochraně elektronické korespondence a umožňuje mimo jiné vytvářet *elektronický podpis*, který v kyberprostoru v podstatě simuluje podpis vlastnoruční a zajišťuje tak *neodmítnutelnost odpovědnosti*. Výhodou asymetrické šifry je, že spolu odesílatel a příjemce zprávy nesdílí žádné tajemství, neboť jejich *veřejné* klíče slouží pouze k šifrování zpráv a samy o sobě nestačí k rozšifrování skrytého obsahu. K tomu slouží klíče *soukromé* a ty má každý účastník komunikace uloženy na svém zařízení a s nikým je nesdílí.

Princip asymetrické kryptografie spočívá v řešení nějakého **výpočetně náročného problému**, který lze se znalostí tajného klíče vyřešit v podstatně kratším čase než bez ní. Zde ovšem narážíme zároveň na úskalí použití dnešních asymetrických šifer v budoucnu, jak je dále osvětleno v sekci 1.4. Matematickými problémy typicky užívanými v asymetrické kryptografii jsou:

- **faktorizace součinu velkých prvočísel** – př. RSA (1.3.2);
- **výpočet diskrétního logaritmu** – př. Diffieho-Hellmanova výměna klíčů (angl. *Diffie-Hellman Key Exchange*);
- **problematika eliptických křivek** – eliptické kryptosystémy.

Zvláštním použitím asymetrické kryptografie je ***elektronický podpis***. Funkce veřejného a soukromého klíče jsou v tomto případě prohozeny, což odesílateli umožní šifrovat zprávy pomocí svého soukromého klíče, takže budou čitelné komukoli, kdo má přístup k jeho veřejnému klíči. Zároveň platí, že jsme-li schopni přijatou zprávu rozluštit veřejným klíčem daného odesílatele, máme jistotu, že tuto zprávu mohl skutečně odeslat jedině on, neboť jedině on má přístup ke svému soukromému klíči. Databázi veřejných klíčů prokazatelně patřících příslušným entitám zpravidla spravuje *certifikační autorita*.

1.3 Moderní šifry

1.3.1 Šifra Advanced Encryption Standard

Standardizovaný kryptografický systém Rijndael, známý pod názvem AES, vznikl jako reakce na prolomení šifrovacího standardu DES (Data Encryption Standard). Jedná se o nejvyužívanější algoritmus ze skupiny *symetrických blokových* šifrovacích algoritmů. Blokovým algoritmem se rozumí, že je třeba data rozdělit a šifrovat po blocích, v tomto případě velikosti 128 bitů. Klíč pak může mít délku 128, 192 nebo 256 bitů. V závislosti na délce klíče se na každý blok aplikuje 10, 12 nebo 14 *rund*. Z hlavního klíče je následně pro každou rundu odvozen *rundový klíč*, který ovlivňuje její průběh. Každá runda je zahájena substituční operací, následně je blok uspořádán do matice a aplikují se dvě operace transpoziční a závěrem jsou data zkombinována s rundovým klíčem. AES se běžně používá například k šifrování bezdrátové komunikace či datových úložišť. Celý algoritmus kryptosystému je detailně popsán v publikaci FIPS 197 [7].

1.3.2 Šifra RSA (Rivest–Shamir–Adleman)

RSA [9] je asymetrický kryptografický systém pojmenovaný po svých tvůrcích, vhodný jak pro podepisování, tak pro šifrování. Patří k nejrozšířenějším formám zabezpečení datového přenosu. Jeho bezpečnost je založena na obtížnosti faktorizace (prvočíselného rozkladu) součinů velkých prvočísel. Tedy zatímco najít součin $n = pq$, kde p a q jsou velká prvočísla, je triviálním úkolem, zpětná faktorizace čísla n je s dosavadními technickými možnostmi a známými algoritmy v rozumném čase prakticky nemožná. Délka prvočísel se zde typicky pohybuje mezi 100–200 řády. Čím delší klíč je použit, tím je systém bezpečnější. Běžně se používají klíče dlouhé 1024 bitů, potažmo 2048 bitů v prostředích s vysokým utajením.

1.4 Nedostatky současné kryptografie

Bezpečnost dnešní kryptografických systémů dávno není závislá na znalosti mechanismu šifrování, jako tomu bylo v minulosti, a dobrý kryptosystém musí počítat i s tím, že může mít útočník k dispozici vícero zašifrovaných zpráv. Klíče proto musí být dostatečně dlouhé a komplexní a neměly by být snadno odvoditelné porovnáním několika obdržených kryptogramů. Jediné, na co si mohou moderní šifry dovolit sázet, jsou hranice možností dostupné výpočetní techniky. Ačkoli je tedy teoreticky možné například odvodit z veřejného klíče k asymetrické šifře klíč soukromý, algoritmy takového odvození buď nebyly dosud objeveny, nebo by jejich vyhodnocení trvalo nemyslitelně dlouho. Chce-li tak útočník zkusit výpočetně dešifrovat kryptogram, k němuž nezná klíč, je odkázán výhradně na ***útok hrubou silou***. Ten spočívá v tom, že útočník postupně zkouší dešifrovat kryptogram za pomoci všech možných kombinací, jež by mohly být klíčem k dešifrování, dokud nenatrefí na tu správnou, tedy nezíská smysluplný text.

To, kolik pokusů by k takovému útoku bylo v průměru zapotřebí, závisí zejména na délce použitého klíče. Například prolomení 128bitového klíče potřebného k rozluštění zprávy zašifrované pomocí symetrického kryptosystému AES (1.3.1), by i vysoce výkonnému současnému superpočítači zabralo řádově $1 \cdot 10^{18}$, tedy miliardy miliard let [10]. Lze tedy říci, že jde vzhledem k současným technickým možnostem o mimořádně bezpečný kryptosystém. Prolomit takový šifrovací systém by znamenalo přijít s nějakým dosud neobjeveným algoritmem, což však není příliš pravděpodobné, nebo zkonstruovat počítač mnohonásobně výkonnější, než všechny dosud existující počítače a superpočítače dohromady. Jak už je zřejmé, mohlo by se jednat právě o počítač kvantový. Až takový počítač vznikne, mohlo by se dešifrování většiny tajných informací rázem stát otázkou sekund. Proto je třeba zabývat se problematikou zabezpečení dat v době kvantových počítačů již nyní. Odpovědí na ni by mohly být kryptosystémy stavící na ještě komplexnějších matematických problémech než ty současné, nebo jejichž bezpečnost **nebude vůbec podmíněna** výkonností dostupné výpočetní techniky.

Kapitola 2

Nepodmíněná bezpečnost

Myšlenka *nepodmíněné bezpečnosti* spočívá v nalezení takového šifrovacího systému, jenž **nestojí na předpokladech** limitovaných schopností a technických možností útočníka – jeho bezpečnost tak není ohrožena technologickým pokrokem. To znamená, že tvůrce kryptosystému musí šifru navrhnout tak, jakoby útočníka omezovaly pouze fyzikální zákony, přestože v praxi takto ideálních podmínek nemusí útočník dosahovat. Důvodem, proč se kryptografie hledáním tohoto svatého grálu datové bezpečnosti zabývá, je skutečnost, že technické možnosti civilizace jdou stále vpřed, tudíž jakkoli dobře současné kryptosystémy slouží své době, je třeba počítat s realitou, ve které budou v důsledku vědeckého pokroku prolomeny. Jejich životnost je tedy omezená. Nepodmíněně bezpečné naproti tomu s časem neztrácejí na účinnosti, neboť jejich bezpečnost zaručují přírodní zákony.

Problém tvorby nepodmíněně bezpečného kryptosystému by se dal rozdělit do dvou částí. První z nich je nalezení samotného algoritmu pro zašifrování zprávy, kterou nebude možné naprosto nijak analyzovat a získat tak informaci, jež by mohla napomoci k jejímu rozluštění. Takový algoritmus již existuje, je jím *Vernamova šifra* (2.1) a její nerozluštitelnost lze matematicky dokázat. Druhá část problému se zabývá distribucí informace potřebné k rozluštění k zamýšlenému příjemci. Aby spolu totiž dvě strany mohly šifrovaně komunikovat, potřebují přirozeně sdílet nějaké tajemství (typicky

číselný klíč), které zaručí, že zprávy dokážou rozluštit právě a jen oni dva. Pokud si takové tajemství nejsou schopni předat absolutně bezpečnou cestou, není jim ani matematicky dokonale bezpečný šifrovací algoritmus co naplat. Pro distribuci tajného klíče bylo navrženo vícero přístupů využívajících fyzikálních jevů z oblasti klasické i kvantové fyziky.

2.1 Vernamova šifra

Vernamova nebo též *jednorázová tabulková šifra* (angl. *one-time pad*) je symetrická substituční šifra, využívající **jednorázový klíč** o stejné délce, jakou má otevřený text.

Vernamova šifra funguje na podobném principu jako starší substituční šifry (př. Vigenèrova). Každý znak textu je v šifrovací abecedě posunut o určitý počet míst, daný šifrovacím klíčem. Stěžejní ovšem je, aby byla délka použitého klíče rovna délce zprávy, kterou se s ním chystáme šifrovat. Každý znak klíče potom odpovídá jednomu znaku textu, což dává Vernamově šifře výhodu oproti jiným posunovým šifrám. Šifry, které používají kratší klíče, totiž typicky rozdělí text na kratší bloky a k zašifrování každého bloku používají opakovaně stejný klíč. To vytváří potenciální riziko, že bude útočník schopen zprávu analyzovat a najít v ní určitý vzor. Při použití Vernamovy šifry však dostáváme kryptogram o délce původní zprávy, jehož každý znak je posunut o **náhodný** počet míst. Útočník tedy z šifrovaného textu nemůže zjistit žádnou informaci o původní zprávě než to, jakou měla délku. Tato informace mu však sama o sobě k ničemu nepřispěje, neboť i kdyby zkoušel metodou *útoku hrubou silou* rozšifrovat zprávu délky n všemi možnými klíči délky n, dostane pouze všechny možné zprávy délky n, ale nebude mít šanci určit, která je ta správná.

Je však třeba mít na paměti, že používaný šifrovací klíč musí být skutečně **dokonale náhodný**, aby jej nebylo možné nijak předpovědět. K jeho vygenerování lze tedy použít například *hardwarový generátor náhodných čísel*, nebo kvantové jevy (viz sekce 3.2.5), nikoli však generátory pseudonáhodných

čísel. Dále je zcela zásadní, aby byl klíč skutečně použit pouze jednou, protože opakované použití klíče by znamenalo, že bude útočník schopen získat informace porovnáním vícero obdržených kryptogramů. Pro každou novou zprávu je tedy třeba vygenerovat nový klíč.

Obdobným způsobem, jakým lze Vernamovu šifru aplikovat na řetězce znaků klasické abecedy, lze šifrovat i řetězce bitů. V podstatě je potom používanou abecedou dvouprvková množina $\{0, 1\}$ a znaky otevřeného textu lze posunout o 0 nebo 1 místo. Klíčem k zašifrování binárního řetězce je tedy *náhodný* binární řetězec o stejné délce, který určuje, zda ten který bit ponechat (posunout o 0 míst) nebo převrátit (posunout o 1 místo). Tento proces je ekvivalentní s binární operací XOR (též *výlučné nebo*). Použití své šifry na binárních řetězcích s využitím XOR si nechal Gilbert Vernam patentovat v roce 1919 [11].

2.1.1 Zašifrování a rozšifrování binárního řetězce

Nechť je dána zpráva $Z = 110100$ délky 6 bitů. Nechť je dán klíč $K = 010110$, jenž je náhodnou posloupností bitů, délky zprávy Z.

Nyní lze získat zašifrovanou zprávu $S = Z \oplus K = 100010$, kde $\oplus$ je bitovou operací *výlučné nebo*.

Z šifrovaného textu S a klíče K lze opětovnou aplikací operace $\oplus$ získat původní zprávu $Z = S \oplus K = 110100$.

Na příkladu použití Vernamovy šifry pro šifrování bitového řetězce je také dobře patrná **důležitost jednorázového použití klíče**. Binární operace *výlučné nebo* má totiž následující vlastnost: $(A \oplus X) \oplus (B \oplus X) = A \oplus B$.

Nechť je dána zpráva $Z' = 001001$ délky 6 bitů, odlišná od zprávy Z.

Zašifrováním zprávy Z' za opakovaného použití klíče K získáváme šifrovaný text $S' = Z' \oplus K = 011111$.

Předpokládejme, že útočník zachytí oba kryptogramy S a S', zašifrované klíčem K. Aplikací operace $\oplus$ na tyto šifrované zprávy získá posloupnost $P = S \oplus S' = 111101 = Z \oplus Z'$.

Na takové posloupnosti P už potom útočník snadno provede kryptoanalýzu, neboť se z ní vytratila veškerá náhodnost, kterou zaručuje jednorázový klíč.

2.2 Problém bezpečné distribuce klíče

V dokonalé náhodnosti a neopakovatelnosti šifrovacího klíče tkví jak neprolomitelnost, tak úskalí praktické využitelnosti Vernamovy šifry. I tehdy, rozhodneme-li se důsledně dodržet nárok na jednorázové použití klíče a zajistíme-li si generátor dokonale náhodných posloupností, jak je pro správné fungování šifry nezbytné, stojí před námi stále problém transportu tohoto klíče k příjemci zprávy. Abychom tedy mohli bezpečně odeslat šifrovanou zprávu po nezabezpečeném kanále, k čemuž nám má dopomoci Vernamova šifra, jsme nuceni nejprve **bezpečně odeslat klíč o stejné délce**. Aby se předešlo tomuto paradoxu, používaly se v minulosti předem vytvořené jednorázové papírové tabulky s klíčem (odtud název *one-time pad*). Obě komunikující strany tak měly k dispozici svou kopii seřazené sady těchto tabulek a po použití daného klíče příslušný list papíru zničily.

Je zřejmé, proč je takový postup pro elektronickou komunikaci nevhodný. Jediným způsobem, jak tedy umožnit dvěma komunikujícím stranám, aby se dohodly na klíči, aniž by tak musely učinit předem, je zprostředkovat *bezpečný komunikační kanál*, na němž **nebude fyzikálně možné** provést odposlech, respektive na němž bude možné případný odposlech odhalit, neboť se promítne do přenášených dat. Mějme na paměti, že po tomto kanálu nebudeme transportovat samotnou zprávu, ale pouze se domlouvat na šifrovacím klíči. Postačí nám tudíž kanál, umožňující bezpečný transport **náhodných posloupností**. Lze k tomu využít například fyzikální částice (typicky fotony) vyznačující se určitou vlastností, kterou nelze předvídat a kterou lze interpretovat jako dva či více stavů (př. polarizace fotonů). Byl však navržen též

přístup operující na bázi termodynamiky, jemuž se věnuje sekce 2.2.2 (míra jeho bezpečnosti je však diskutabilní). Poté, co se přes tyto bezpečné kanály domluví komunikující strany na tajném klíči, může dojít k odeslání samotné zašifrované zprávy již po klasickém, nezabezpečeném komunikačním kanále.

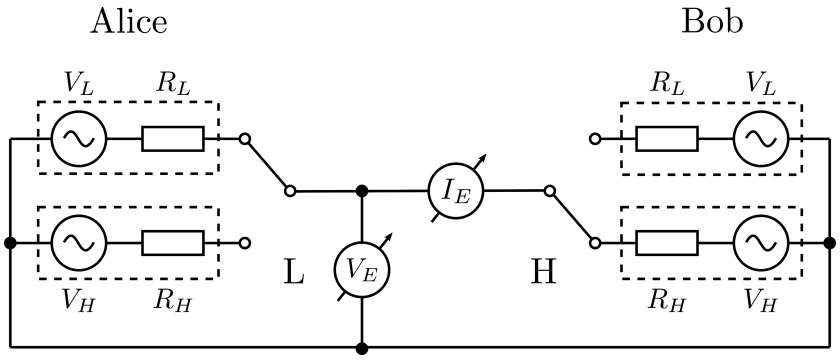
2.2.1 Využití kvantové fyziky k distribuci klíče

Kdykoli přenášíme informace jak po klasickém tak po kvantovém komunikační kanále, činíme tak s využitím **měřitelných fyzikálních veličin**. Ať už jde o *elektrické napětí* nebo *polarizaci fotonu*, jestliže příjemce zprávy může tyto veličiny měřit, není vyloučeno, že se je během přenosu podařilo změřit i útočníkovi přítomnému na komunikačním kanále. Specifikum kvantových jevů (jak je blíže osvětleno v kapitole 3) tkví však v tom, že jejich měřením zároveň dochází ke **změně jejich stavu**.

V protokolech *kvantové distribuce klíčů* (QKD) se tak využívá právě zákonů kvantové fyziky jako jsou *Heisenbergovy relace neurčitosti* (3.1.4) a *no-cloning theorem* (3.1.6) k tomu, aby bylo eliminováno **riziko odposlechu**. V kontextu nepodmíněné bezpečnosti budeme o kvantové distribuci klíče hovořit ve spojení s *Vernamovou šifrou*, teoreticky je však možné použít klíč k zašifrování zprávy i jinou symetrickou šifrou. Konkrétní přístupy navržené pro kvantovou distribuci klíče jsou dále představeny v kapitole 4.

2.2.2 Alternativa ke kvantové distribuci klíče

Metoda bezpečné výměny klíčů ***KLJN*** [12] (zkratka z angl. *Kirchhoff-law-Johnson-noise*), známá také jako *Kish key distribution*, slibuje podobně jako metody kvantové distribuce klíčů nepodmíněnou bezpečnost přenosu klíče. Rozdíl je však v tom, že staví čistě na zákonech **klasické fyziky**, konkrétně *Kirchhoffových zákonech* zachování náboje a energie v elektrických obvodech a *Johnsonově* (*tepelném*) *šumu*. Ačkoli je systém z pohledu teorie informace nepodmíněně bezpečný, pro neideálnost skutečných elektrických obvodů je reálná míra jeho bezpečnosti diskutabilní.



Obrázek 2.1: Schéma obvodu navrženého systémem KLJN. Podle [13].

Komunikace metodou KLJN probíhá s užitím jednoduchého elektrického obvodu, jehož schéma lze vidět na obrázku 2.1. Komunikující strany (Alice a Bob) mají na svých koncích komunikační linky každý svůj pár rezistorů. Jeden rezistor z páru (R_L) má vždy nižší odpor než druhý rezistor (R_H) a jejich hodnoty jsou veřejně známé. Nenulové napětí rezistorů zodpovědné za Johnsonův šum v obvodu je na obrázku 2.1 reprezentováno generátory střídavého napětí V_H a V_L. Rezistory na obrázku jsou zapojeny způsobem LH, tedy Alice zapojila rezistor s nižším odporem a Bob rezistor s vyšším odporem. Ve chvíli, kdy Alice přepojí na rezistor s vyšším odporem a Bob na rezistor s nižším odporem, ocitnou se ve schématu HL. Útočník, jehož měřící zařízení V_E a I_E jsou připojena na komunikačním kanále však stavy HL a LH nedokáže rozlišit, což lze matematicky dokázat. Alice a Bob se veřejně dohodnou na tom, který ze stavů LH a HL budou považovat za 1 a který za 0. Poté náhodně přepínají každý mezi svými dvěma rezistory a v pravidelných časových intervalech zaznamenávají aktuální stav systému. Analýzu měřeného signálu na vodiči v této fázi útočníkovi znemožňují výše zmíněné generátory šumu. Situace, kdy Alice i Bob zvolí stejný rezistor (tedy např. oba zapojili rezistor R_L) je však útočníkem stále detekovatelná, proto Alice s Bobem stavy LL a HH ze svých záznamů vyloučí. Vzniklá posloupnost stavů LH a HL je známá pouze Alici a Bobovi a slouží jako tajný binární klíč. Ten může být následně použit k zašifrování zprávy, již bude možné bezpečně sdílet po nezabezpečeném komunikačním kanále.

K realizaci systému KLJN stačí několik základních elektrotechnických součástek a vodič. Kdyby se tudíž nějaká verze tohoto systému ukázala v budoucnu v praxi efektivní, znamenalo by to nesrovnatelně levnější řešení problematiky bezpečného přenosu klíče ve srovnání s kvantovými přístupy. O reálné míře bezpečnosti současné podoby systému KLJN se však stále vedou spory. V minulosti bylo představeno několik úspěšných útoků na tento systém ([14], [15], [16]). Zda-li tak bude moci v budoucnu skutečně konkurovat kvantovým kryptografickým protokolům, zůstává otázkou.

2.3 Nepodmíněná bezpečnost v praxi

Třebaže výše zmíněné kryptografické metody zaručují v teorii matematicky dokazatelnou nepodmíněnou bezpečnost, jejich praktická implementace se neobejde bez jistých úskalí. Za předpokladu, že komunikující strany důsledně respektují přísné nároky na neopakovatelnost a dokonalou náhodnost klíče, o nepodmíněné bezpečnosti Vernamovy šifry není pochyb. Všechny dosud známé vydařené útoky na komunikaci šifrovanou tímto způsobem uspěly v důsledku nesprávného zacházení komunikujících stran s Vernamovou šifrou (jako v případech [17] a [18], kdy byl použit pouze pseudonáhodný klíč).

Pokud jde o problematiku distribuce klíče, je situace o něco komplikovanější. V případě kvantové distribuce klíčů, je-li systém korektně implementován, je prakticky nemožný, respektive rozpoznatelný, jakýkoliv odposlech na kvantovém komunikačním kanále, jak dále upřesňuje kapitola 4. Ani kvantové komunikační protokoly však nezaručují ochranu vůči útokům typu *man-in-the-middle*, kdy se útočník vydává za komunikující stranu. Aby se takovému útoku předešlo, musí Alice a Bob na počátku sdílet určité tajemství, popř. si takové tajemství vytvořit pomocí některé z navržených metod (př. [19], [20]). Díky tomuto tajemství si následně navzájem ověří své identity ještě před započetím samotné distribuce klíče. To lze provést za pomoci nepodmíněně bezpečného *autentizačního schématu* (př. [21]).

V neposlední řadě je pro všechny kryptosystémy usilující o nepodmíněnou bezpečnost zásadní, aby používaly vybavení od důvěryhodných výrobců. Přístroje z nedůvěryhodných zdrojů mohou totiž obsahovat tzv. *backdoor*, jenž by umožňoval nežádoucí únik informací, přestože na samotném komunikačním kanále k žádnému detekovatelnému odposlechu nedojde. Nutno však připomenout, že mluvíme-li o nepodmíněné bezpečnosti, pohybujeme se stále na rovině kryptografické. Žádný z výše uvedených přístupů nemůže zaručit odolnost vůči kybernetickým útokům, které se zaměřují na získání informace již při záznamu zprávy do počítače apod., neboť těmto nelze předejít šifrováním.

Nepodmíněné kryptografické systémy jsou tak nepodmíněné ve smyslu nezávislosti na schopnostech a výpočetních možnostech útočníka. Pro jejich správné fungování v praxi je i přesto potřeba stanovit několik předpokladů:

- generátor náhodných čísel je důvěryhodný a skutečně náhodný
- před započetím komunikace došlo k autentizaci komunikujících stran
- útočník nemá přístup k šifrovacím zařízením Alice a Boba

Kapitola 3

Kvantová fyzika a její aplikace v informatice

Abychom mohli hovořit o fyzikální podstatě kvantové kryptografie (resp. kvantové distribuce klíče) je třeba nejprve představit některé zákony kvantové fyziky, na nichž staví kvantová výpočetní technika a kryptografie. Protože kvantová fyzika je tématem nesmírně komplexním, pokusím se v této kapitole nastínit pouze vybrané, pro kvantovou kryptografii nezbytné pojmy. Pro detailnější studium této problematiky si pak dovoluji odkázat na sérii učebnic *Úvod do kvantové teorie I.* a *II.* [22] profesora Jiřího Formánka. Vedle fundamentálních konceptů kvantové mechaniky se v této kapitole budeme zabývat rolí kvantové fyziky v informatice a představíme si hlavní rozdíly mezi klasickou a kvantovou výpočetní technikou. Teorie kvantového počítače opět dalekosáhle přesahuje rozměry této práce, proto k jejímu dalšímu studiu doporučuji např. publikaci prof. Jozefa Grusky *Quantum Computing* [23].

3.1 Základní principy kvantové fyziky

Kvantová fyzika je jednou ze dvou fundamentálních fyzikálních teorií. Zrodila se v 1. polovině 20. století, aby objasnila fyzikální jevy odehrávající se na mikroskopické škále, které nebylo možné nijak objasnit pomocí fyziky klasické, tedy „nekvantové“. Kvantová fyzika v sobě zahrnuje *kvantovou mechaniku*, jež se zabývá mechanickým pohybem částic, a *kvantovou teorii pole*. Ačkoli byly principy klasické i kvantové fyziky experimentálně potvrzeny, není dosud známa teorie, jež by propojovala obě tyto teorie a nabízela tak jednotné pochopení vesmíru na všech škálách a úrovních uspořádání hmoty.

3.1.1 Stav a amplituda pravděpodobnosti

Dle *Kodaňské* (též *pravděpodobnostní*) *interpretace* kvantové mechaniky se fyzikální realita skládá ze dvou částí – *světa klasického* a *světa kvantového*. Svět klasický odpovídá tomu, jak fyzikální svět pozorujeme a jaký ho registrujeme. Svět kvantový nám není přímo přístupný, avšak jsme schopni z něj získat informace za pomoci *měření*. Celkovou reprezentaci fyzikální reality představuje ***kvantový stav***.

Klasický svět se chová deterministicky – na základě kompletní znalosti stavu systému se všemi silami, které na něj v daný okamžik působí, dokážeme (alespoň principiálně) předpovědět vývoj stavu tohoto systému v čase. Něco takového není u kvantového systému možné, neboť kvantový svět se deterministicky nechová. Pomocí kvantové mechaniky lze však určit, s jakou **pravděpodobností** dojde k určité události. Je-li kvantový systém izolován od okolí, lze jej matematicky popsat pomocí *vlnové funkce*, jejíž průběh popisuje *Schrödingerova rovnice*. Právě z vlnové funkce lze určit pravděpodobnost nalezení kvantového systému v daném okamžiku v příslušném stavu.
Pravděpodobnost p události je dána vztahem $p = |\alpha|^2$, kde α je komplexní číslo zvané ***amplituda pravděpodobnosti*** *dané události.* [23]

3.1.2 Superpozice a matematická notace stavu

Situaci, kdy se kvantový systém nachází ve dvou či více možných stavech zároveň, nazýváme ***superpozicí stavů***.
Na každý kvantový stav lze nahlížet jako na superpozici dvou a více stavů a naopak, jakékoli dva stavy mohou být superponovány dohromady za vzniku nového stavu. [25]

Princip superpozice stavů popsal ve své vědecké práci *Principy kvantové mechaniky* (1930) Paul Dirac a přišel zároveň se systémem zápisu vektorů, využívaných k matematické reprezentaci kvantových stavů, jenž vešel ve známost jako ***Diracova notace***. Standardní zápis vektoru ψ v *Hilbertově vektorovém prostoru* má následující podobu:

$$|\psi\rangle . \tag{3.1}$$

Symbol ψ v závorkách lze pak samozřejmě nahradit libovolnou jinou značkou, kterou zvolíme pro zápis daného stavu. Pro informatiku budou příznačné například stavy $|0\rangle$ a $|1\rangle$.

S využitím *Diracovy notace* tak nyní můžeme matematicky vyjádřit výše popsaný princip složení stavů A a B, reprezentovaných vektory $|A\rangle$ a $|B\rangle$ vztahem

$$c_1 |A\rangle + c_2 |B\rangle = |R\rangle , \tag{3.2}$$

kde komplexní čísla c_1 a c_2 určují, jakou měrou přispívají jednotlivé složky do výsledného vektoru $|R\rangle$, jenž je superpozicí stavů $|A\rangle$ a $|B\rangle$. Koeficienty c_1, c_2 musí navíc splňovat podmínku $|c_1|^2 + |c_2|^2 = 1$, která zaručuje, že k nim lze přistupovat jako k amplitudám pravděpodobnosti nalezení systému popsaného složeným stavem $|R\rangle$ v příslušném dílčím stavu $|A\rangle$ či $|B\rangle$. Celková pravděpodobnost kolapsu superponovaného stavu $|R\rangle$ do stavu jedné či druhé jeho ortogonální složky musí být totiž rovna 1.

3.1.3 Měření na kvantovém systému

Ať už o kvantové fyzice uvažujeme ve smyslu *Kodaňské interpretace* či např. *mnohosvětové interpretace* [26], rozeznáváme rozdílné účinky, které má naše **pozorování** či **měření** na klasický a kvantový svět. Zatímco v klasické fyzice představuje *měření* proces zjištění předem determinované informace o systému, ve fyzice kvantové nabývají veličiny konkrétní hodnoty až právě v okamžiku, kdy jsou měřeny. Jinými slovy: samotný akt *měření* přiřazuje hodnoty pozorovatelným veličinám, které byly do té doby neurčité. Výsledky měření na kvantovém systému navíc nezávisí pouze na stavu kvantového systému, ale také na *způsobu*, jakým veličinu měříme.

Vykonáním měření na kvantovém systému rovněž dochází k takzvanému ***kolapsu vlnové funkce***, jež popisovala stav tohoto systému před započetím měření. Informace o tomto výchozím stavu se tak ztrácí. Statistika rozložení hodnot získaných měřením příslušných veličin na několika identických izolovaných kvantových systémech pak odpovídá pravděpodobnostem určeným touto vlnovou funkcí (viz sekce 3.1.1).

3.1.4 Heisenbergovy relace neurčitosti

Heisenbergovy relace neurčitosti (též *princip neurčitosti*), jež popsal poprvé Werner Heisenberg v roce 1927 [27], patří k fundamentálním principům kvantové mechaniky. Ukazují další důležité specifikum měření na kvantovém systému, totiž že **přesnost, s jakou lze současně měřit určité páry fyzikálních veličin, je omezena**. Typickým příkladem takového páru veličin je *poloha* (x) a *hybnost* (p) elementární částice. Tedy pakliže budeme znát přesnou polohu elementární částice v určitém okamžiku, není možné přesně určit její hybnost v tomto okamžiku, a to bez ohledu na přesnost měřícího přístroje. Pro odchylky Δx, Δp měření kanonicky sdružených veličin x a p platí, že

$$\Delta x \Delta p \geqslant \frac{\hbar}{2}, \tag{3.3}$$

kde $\hbar$ značí *redukovanou Planckovu konstantu*.

Důvod, proč některé páry veličin podléhají relacím neurčitosti, se vědci snažili mnohokrát objasnit. Moderní vysvětlení ([28]) se opírá o myšlenku ***vlnově-korpuskulárního dualismu***. Ta říká, že fyzikální částice vykazují jak vlastnosti částic, tak vlastnosti vln, v závislosti na tom, jak jsou pozorovány. Měříme-li tak např. hybnost elementární částice, projevuje se její **vlnová povaha**, neboť hybnost p částice je svázána s její vlnovou délkou λ vztahem $p = h \cdot \lambda$, kde h značí Planckovu konstantu. Přesná poloha částice (určená bodem v prostoru) je naopak veličina typická pro její částicový charakter. Částice v experimentu může v daném čase demonstrovat buď svůj vlnový, nebo svůj částicový charakter, ne však oba současně. Proto není možné v jediný okamžik přesně změřit první i druhou veličinu z páru.

3.1.5 Kvantové provázání

Definice 3.1.1. Kvantově provázaný stav je *korelovaný stav* dvou a více kvantových systémů, o jejichž jednotlivých stavech nemá význam mluvit nezávisle na sobě.

Ve stavu provázanosti (angl. *entanglement*) se může vyskytovat například dvojice fotonů. Měření na jednom fotonu z páru způsobí *kolaps vlnové funkce* celého provázaného systému, a to bez ohledu na to, v jaké vzdálenosti od sebe se fotony v dané chvíli nacházejí. Mluvíme proto o *nelokalitě* kvantové mechaniky – účinky měření provedeného na jedné podčásti provázaného systému na ostatní podčásti tohoto systému jsou okamžité a nezávislé na lokaci jednotlivých podčástí. Provázaný systém vzniká například přeměnou jednoho fotonu s vysokou energií na dvojici fotonů s nižší energií, jež jsou v provázaném stavu v důsledku zákonů zachování energie a hybnosti. Na tomto principu funguje např. metoda získávání provázaných párů fotonů *SPDC* [29]. Způsobů jak vytvořit kvantově provázaný systém je však několik a stav provázanosti lze dokonce přenést na větší částice (př. atomy). Kvantové provázání má velký význam v kvantových počítačích, které pracují i s tisíci atomů v jednom provázaném systému [30], či kvantové kryptografii (viz kapitola 4). Interakcí s vnějším prostředím stav provázanosti zaniká.

3.1.6 No-cloning theorem

Teorém 3.1.1 (No-cloning theorem)**.** Není možné vytvářet nezávislé, identické kopie předem neznámého kvantového stavu.

Teorém o klonování neznámého kvantového stavu, známý pod anglickým názvem *no-cloning theorem*, dokázali jak William Wooters s Wojciechem Żurkem [32], tak Denis Dieks [33] v roce 1982. Spolu s *relacemi neurčitosti* patří k určujícím fyzikálním principům pro kvantovou kryptografii (viz kapitola 4). Co je však pro jedno odvětví výhodou, pro jiné představuje komplikace. V důsledku tohoto fyzikálního principu tak například nelze v kvantových počítačích využít mnohé *samoopravné kódy* (angl. *error correcting codes*), jež jsou užívány v klasických počítačích. S jeho pomocí byly také vyvráceny hypotézy o nadsvětelně rychlé komunikaci vycházející z *kvantové teorie pole*, jež byly v minulosti vysloveny [34].

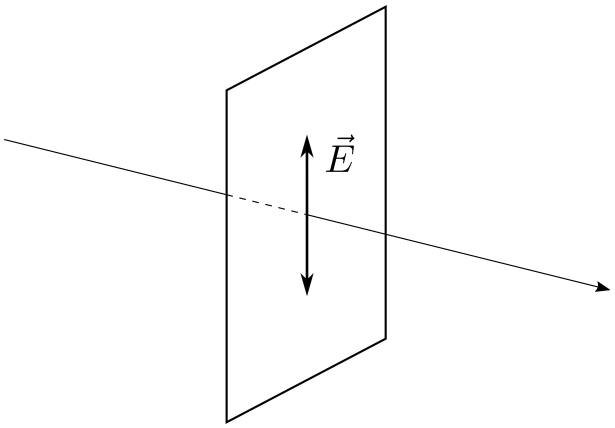
3.1.7 Polarizace světla

Výše popsané chování kvantových systémů lze demonstrovat na příkladu polarizace fotonu.

Fotony – kvanta elektromagnetického vlnění – mohou být *lineárně* či *kruhově* polarizovány. Lineární polarizace světla se liší od kruhové v závislosti na tom, jaká je **orientace kmitové roviny** vektoru *intenzity elektrického pole* elektromagnetického vlnění vůči směru šíření tohoto vlnění. V této sekci se konkrétně zaměříme na lineárně polarizované světlo.

Pro ***lineárně polarizované světlo*** platí, že povedeme-li svazkem světla rovinu, která je kolmá na směr jeho šíření, bude vektor intenzity elektrického pole $\vec{\boldsymbol{E}}$ kmitat stále v jedné přímce (viz obrázek 3.1).

Světlo vycházející z běžného zdroje (jakým je např. Slunce) je z principu *nepolarizované*. Vektor intenzity elektrického pole v něm tak kmitá zcela nahodile. Z *přirozeného* světla lze však získat světlo polarizované a to typicky užitím ***polarizačního filtru***, fungujícího na principu částečné absorpce. Vedle absorpce lze světlo polarizovat také odrazem či lomem.



Obrázek 3.1: Kmitající vektor intenzity elektrického pole $\vec{E}$ lineárně polarizovaného světla se pohybuje na pomyslné rovině, kolmé ke směru šíření světla, v přímce. Podle [35].

Lineární polarizační filtr umožňuje průchod takovým fotonům, které jsou ve chvíli dopadu na filtr v polarizaci **rovnoběžné** s polarizační rovinou filtru. Fotony nacházející se v polarizaci **kolmé** k polarizační rovině filtru jsou naopak filtrem absorbovány. Věnujme však pozornost situaci, kdy je rovina polarizace fotonu odkloněna od roviny polarizace filtru přesně o 45°. Na takový stav lze nahlížet jako na superpozici rovnoběžného a kolmého stavu, kdy oba stavy přispívají do tohoto superponovaného stavu stejnou měrou.

Vyjádřeme si tento stav matematicky pomocí výše zavedeného vztahu pro skládání kvantových stavů (rovnice 3.2). Stavy *vertikální polarizace* $|\uparrow\rangle$ a *horizontální polarizace* $|\rightarrow\rangle$ superponujeme za vzniku stavu *diagonální polarizace* $|\nearrow\rangle$, jehož polarizační rovina svírá s polarizačními rovinami stavů $|\uparrow\rangle$ a $|\rightarrow\rangle$ úhel $\theta = 45°$. Pro komplexní koeficienty c_1, c_2 ve vztahu 3.2 platí, že musí splňovat podmínku

$$|c_1|^2 + |c_2|^2 = 1. \tag{3.4}$$

V našem případě navíc skládáme dva stavy, jež budou do výsledné superpozice přispívat stejnou měrou, tudíž

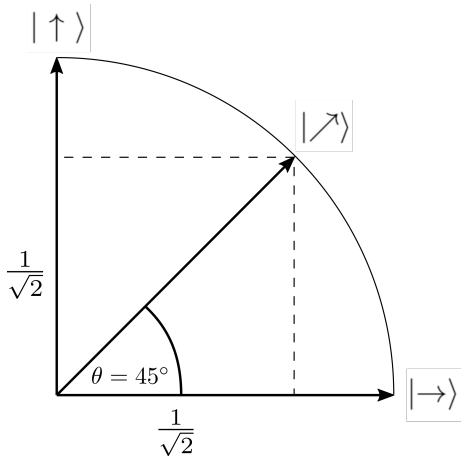
$$c_1 = c_2.$$

Nyní můžeme zvolit koeficient $c = c_1 = c_2 = \frac{1}{\sqrt{2}}$, který uspokojuje obě stanovené podmínky, neboť

$$\begin{aligned} |c|^2 + |c|^2 &= 1 \\ 2|c|^2 &= 1 \\ |c|^2 &= \frac{1}{2}. \end{aligned}$$

Se znalostí koeficientu c tak nyní dokážeme vyjádřit superponovaný stav diagonální polarizace dosazením do vztahu 3.2, jako

$$|\nearrow\rangle = \frac{1}{\sqrt{2}} |\uparrow\rangle + \frac{1}{\sqrt{2}} |\rightarrow\rangle . \tag{3.5}$$



Obrázek 3.2: Grafické znázornění vertikální, diagonální a horizontální polarizace fotonu. Polarizační rovina diagonální polarizace $|\nearrow\rangle$ svírá s polarizačními rovinami vertikální polarizace $|\uparrow\rangle$ a horizontální polarizace $|\rightarrow\rangle$ úhel $\theta = 45°$. Podle [36].

K čemu tedy dojde, dopadne-li na polarizační filtr foton, jehož polarizační rovina je od polarizační roviny filtru odkloněna právě o 45°? Zde je velmi dobře patrný **pravděpodobnostní charakter** kvantových jevů. Šance, že takový foton polarizačním filtrem projde, je totiž přesně 50 %. Lze tedy očekávat, že z množiny fotonů, polarizovaných diagonálně vůči polarizační

rovině filtru, jich po dopadu na filtr polovina projde a polovina bude absorbována.

Není však žádný způsob, jak předpovědět, který případ nastane pro konkrétní jednotlivé fotony.

Stejně tak nelze s jistotou předpovědět chování žádných fotonů, jejichž polarizační rovina je v okamžiku měření odkloněna od polarizační roviny filtru o jiný úhel z intervalu $(0°,\ 90°) \cup (90°,\ 180°)$. Čím více se bude úhel blížit kolmému či rovnoběžnému stavu, tím pravděpodobněji se do této pozice v okamžiku dopadu na filtr uchýlí, bude však vždy existovat určitá šance, že dojde k jevu opačnému.

Foton se při dopadu na filtr chová deterministicky pouze tehdy, je-li v polarizaci rovnoběžné, či kolmé na orientaci filtru.

Intenzitu výstupního paprsku světla po průchodu lineárně polarizovaného paprsku lineárním polarizačním filtrem svírajícím s polarizační rovinou fotonů úhel θ popisuje *Malusův zákon*.

Závislost *výstupní intenzity* světla I na vstupní intenzitě světla I_0 je dána vztahem

$$I = I_0 \cdot \cos^2(\theta). \tag{3.6}$$

Z tohoto vztahu lze odvodit pravděpodobnost p, že lineárně polarizovaný foton svírající úhel θ s polarizační rovinou filtru projde filtrem, jako

$$p = \frac{I}{I_0} = \cos^2(\theta). \tag{3.7}$$

Stejně tak lze odvodit pravděpodobnost p', že bude foton filtrem pohlcen,

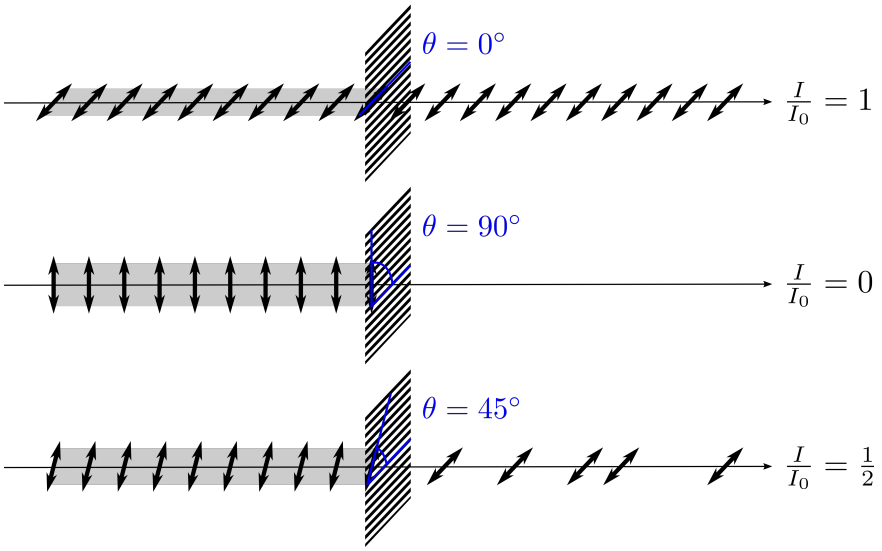
$$p' = 1 - \cos^2(\theta) = \sin^2(\theta). \tag{3.8}$$

S pomocí těchto vztahů lze mimo jiné ukázat, že se polarizace fotonu orientovaného rovnoběžně s filtrem, či kolmo na filtr chová deterministicky, avšak pro jiné úhly pravděpodobnostně.

$$p_1 = \cos^2(0°) \qquad p_2 = \cos^2(90°) \qquad p_3 = \cos^2(30°)$$
$$p_1 = 1 \qquad p_2 = 0 \qquad p_3 = \frac{3}{4}$$

$$p'_1 = \sin^2(0°) \qquad p'_2 = \sin^2(90°) \qquad p'_3 = \sin^2(30°)$$
$$p'_1 = 0 \qquad p'_2 = 1 \qquad p'_3 = \frac{1}{4}$$

Z výše uvedených vztahů lze navíc matematicky odvodit, že svítíme-li na libovolně orientovaný lineárně polarizační filtr přirozeným (tedy nepolarizovaným) světlem, bude intenzita výstupního paprsku poloviční, než paprsku vstupního, neboť průměrná hodnota funkce $\cos^2(\theta)$ pro všechny možné velikosti úhlu θ je $\frac{1}{2}$.



Obrázek 3.3: Ilustrace průchodu lineárně polarizovaného paprsku světla filtrem. Výstupní intenzita polarizovaného světla je závislá na orientaci polarizační roviny světla vůči filtru.

Polarizační filtry lze typicky použít dvěma způsoby:

Polarizátor slouží k získání fotonů o určité polarizaci.

Analyzátor slouží k získaní informace o polarizaci dopadajících fotonů.

V praxi může jít o identická zařízení, liší se pouze účelem, ke kterému je využíváme. Polarizovat lze jak nepolarizované světlo, tak světlo s již danou polarizací. Vždy je však třeba mít na paměti důležitý aspekt měření na kvantových systémech zmíněný v sekci 3.1.3, tedy že způsob, jakým veličinu měříme, ovlivňuje výstup tohoto měření. To, zda foton polarizačním filtrem projde nebo ne, není pouze otázkou kvantového stavu, ve kterém se foton v daný moment nachází, ale také pozice, do jaké polarizační filtr umístíme.

Necháme-li na analyzátor dopadnout foton, o kterém víme, že již byl lineárně polarizován, v závislosti na tom, zda filtrem projde nebo ne, zjistíme s jistotou pouze **1 bit informace**. Jestliže filtrem projde, víme, že *nebyl* v polarizaci kolmé na orientaci filtru. Pakliže je filtrem pohlcen, víme že *nebyl* v polarizaci rovnoběžné s orientací filtru.
Ve které z nekonečně mnoha možných polarizací se však foton před dopadem na filtr skutečně nacházel, nelze pouhým měřením bez konkrétnějších informací určit.
Množinu možných polarizaci nelze zúžit ani tak, že bychom provedli měření s různě orientovaným analyzátorem na několika kopiích fotonu, protože víme, že *no-cloning theorem* znemožňuje tvorbu takových kopií. Tato skutečnost hraje v kvantové kryptografii zásadní roli (viz kapitola 4).

Připomeňme si také, že při dopadu fotonu na filtr nastává *kolaps vlnové funkce* (viz sekce 3.1.3). Nejenže tedy pomocí polarizačního filtru o tomto stavu nelze zjistit více než jediný bit informace, ale z principu nemůže existovat metoda, která by zpětně dokázala určit stav polarizace, ve kterém se foton nacházel před průchodem filtrem.
V okamžiku kontaktu fotonu s filtrem původní stav jeho polarizace zcela zaniká a foton, je-li filtrem propuštěn, získává polarizaci určenou orientací filtru.

3.2 Kvantové zpracování informace

Vzhledem k odlišným povahám kvantových a klasických fyzikálních jevů se také simulace kvantových systémů ukázala být na *klasických počítačích* poměrně nešikovnou. Tak se zrodila myšlenka *kvantového počítače*, jenž by umožňoval simulovat kvantové systémy, a to i takové, které na klasickém počítači simulovat vůbec nelze [37]. Od 90. let 20. století tak vědci intenzivně pracují na modelech kvantových počítačů a algoritmech, které by umožnily nejen simulovat kvantové systémy, ale také řešit mnohé jiné matematické problémy lépe, než to umožňují počítače klasické. Kvantová teorie fyziky tak dala vznik zcela novému pojetí výpočetní techniky a teorie informace.

3.2.1 Kvantové bity a unitární operace

Elementární jednotkou *klasické* informace je jak známo *bit*. Bit nabývá jedné ze dvou hodnot, typicky označovaných *0* a *1*, jež jsou v klasickém počítači nejčastěji reprezentovány rozdílnými hladinami elektrického napětí. Na bitech lze provádět řadu *logických operací*, realizovaných v klasickém počítači pomocí *hradel*, majících jeden či více vstupů a zpravidla jediný výstup. Příklady takových operací jsou logický součin (AND), logický součet (OR) či logická negace (NOT).

Kvantový bit neboli *qubit* [39] je základní jednotka *kvantové informace*. Qubit se podobně jako klasický bit může nacházet v některém ze dvou základních stavů, navíc se ale může nacházet také v **superpozici** těchto stavů. Stav qubitu tedy reprezentujeme vektorově jako lineární kombinaci vzájemně kolmých jednotkových vektorů $|0\rangle$ a $|1\rangle$, které tvoří *ortonormální bázi* Hilbertova prostoru. Stav ψ qubitu tak může zapsat pomocí výše zavedeného vztahu pro skládání kvantových stavů (3.2) jako

$$\psi = \alpha\,|0\rangle + \beta\,|1\rangle\,. \tag{3.9}$$

Komplexní čísla α a β zde opět musí splňovat podmínku $|\alpha|^2 + |\beta|^2 = 1$.

Unitární operace lze provádět nad qubity, podobně jako nad klasickými bity provádíme operace logické. Všechny operace na qubitech však musí být na rozdíl od mnohých operací bitových **reverzibilní**. To znamená, že pro každý prvek z množiny možných vstupů musí existovat právě jeden prvek v množině výstupů a lze tedy najít inverzní funkci f' ke každé funkci f operující nad qubity takovou, že $f'(f(\psi)) = \psi$. Pro zajištění reverzibility některých unitárních operací je nutné přidat ke vstupu či výstupu navíc takzvaný *pomocný qubit* (angl. *ancilla qubit*).

Aplikaci unitárních operací na qubity si lze představit jako rotaci (vektorem reprezentovaného) stavu qubitu v Hilbertově prostoru. Pro výpočty s qubity je vhodné přepsat vztah 3.9 pro zápis stavu qubitu do podoby sloupcového vektoru jako

$$\psi = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}, \tag{3.10}$$

kde horní údaj α vždy odpovídá amplitudě stavu $|0\rangle$ a spodní údaj β amplitudě stavu $|1\rangle$. Čisté stavy $|0\rangle$ a $|1\rangle$ tak zapíšeme sloupcovými vektory

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \qquad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}.$$

Unitární operátory jsou popsány pomocí *unitárních matic*. Velikost matice závisí na počtu qubitů, které do operace vstupují. Do běžných unitárních operací vstupují jeden či dva qubity. Aplikace operace na qubit odpovídá **vynásobení** sloupcového vektoru jeho stavu unitární maticí. V kvantových obvodech jsou pak operace s qubity realizovány ***kvantovými hradly***. Bylo ukázáno, že k provedení jakékoli unitární operace na libovolném množství qubitů stačí sada jednobitových hradel a dvoubitového hradla *CNOT* plnícího funkci *výlučné nebo* [41]. Níže jsou uvedena některá základní kvantová hradla operující na jednom či na dvou qubitech.

Pauliho X hradlo je ekvivalentem k logické operaci NOT. Jeho operátor je popsán Pauliho maticí σ_x, operuje na jednom qubitu a má za následek překlopení stavu qubitu (např. $|0\rangle \rightarrow |1\rangle$). Obecně lze účinek operátoru $\hat{X}$ na qubit ve stavu $\alpha|0\rangle + \beta|1\rangle$ zapsat jako

$$\hat{X}\begin{pmatrix}\alpha\\ \beta\end{pmatrix} = \begin{pmatrix}\beta\\ \alpha\end{pmatrix}. \tag{3.11}$$

Hadamardovo hradlo je významné kvantové hradlo působící na jednom qubitu. Je-li qubit na vstupu v čistém stavu (tj. $|0\rangle$ či $|1\rangle$), na výstupu se ocitá ve stavu **superpozice**. Konkrétně pro vstupní stav qubitu $|0\rangle$ je výstupem stav $\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$ a pro vstup $|1\rangle$ je výstupem stav $\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$. To v obou případech znamená, že změřením výsledného qubitu dostaneme se stejnou pravděpodobností výsledek $|0\rangle$ jako výsledek $|1\rangle$. Operátor je reprezentován Hadamardovou maticí

$$\hat{H} = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}. \tag{3.12}$$

Hadamardovo hradlo lze také použít k přeměně stavu superpozice na stav čistý. Pro vstupní stav qubitu $\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$ je pak výstupem stav $|0\rangle$ a pro vstup $\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$ je výstupem stav $|1\rangle$.

CNOT (z angl. *controlled NOT*) je kvantové hradlo provádějící operaci *řízené negace*. Vstupují do něj dva qubity, jež si můžeme označit písmeny A a B. Je-li qubit A ve stavu $|1\rangle$, provede se na qubitu B operace NOT (jeho stav se překlopí). Pakliže je qubit A ve stavu $|0\rangle$ stav qubitu B se nemění.

Jsou-li tak qubity A a B v čistých stavech, tedy $|0\rangle$ či $|1\rangle$, plní kvantové hradlo *CNOT* logickou funkci *výlučné nebo* a její výstup zapisuje do qubitu B, označovaného jako *cílový*. Pokud se však qubit A nachází v jiném stavu než $|0\rangle$ a $|1\rangle$ vytvoří hradlo mezi qubity A a B **kvantové provázání** (3.1.5).

Operace *CNOT* je oproti jednoqubitovým unitárním operacím výrazně náročnější. Proto se výpočetní náročnost kvantového obvodu někdy uvádí v počtu *CNOT* hradel, jež ho utváří.

3.2.2 Princip kvantového počítače

Kvantový počítač je teoretický model výpočetního stroje, jenž ke zpracování informací přímo využívá *kvantové fyzikální jevy*. Jak je již zřejmé z předchozí sekce, klasické bity nahradí v kvantových obvodech *qubity*, mající tu vlastnost, že se mohou nacházet v jakékoli superpozici stavů $|0\rangle$ a $|1\rangle$. K tomu, abychom mohli teoretický koncept qubitu aplikovat ve skutečném stroji, musíme zvolit médium, které nám umožní qubit fyzicky reprezentovat. Takovým médiem může být jakýkoli *dvouhladinový kvantový systém*. Mezi dvouhladinové systémy vhodné k reprezentaci qubitu patří například

- **elektron**, jehož spin může nabývat hodnot 1 pro kladný směr otáčení, 0 pro záporný směr otáčení, či se nacházet v superpozici těchto hodnot,
- **atom vodíku**, jehož elektron se může nacházet v základním či excitovaném stavu (uvažujeme-li první dvě energetické hladiny), nebo v superpozici těchto stavů,
- **foton**, jehož rovina polarizace může být ve směru rovnoběžném či kolmém na polarizační rovinu měřicí báze, nebo v superpozici těchto směrů (viz sekce 3.1.7).

Jak qubity reprezentované spinem elektronu, tak qubity reprezentované energetickou hladinou elektronu lze dostat z již změřeného stavu ($|0\rangle$ či $|1\rangle$) do stavu superpozice tak, že jim laserem dodáme právě tolik energie, abychom mohli říct, že se jejich stav s určitou pravděpodobností překlopil a s určitou pravděpodobností zůstal stejný.

V sekci 3.2.1 jsme hovořili o *unitárních operacích*, které pracují s qubity a musí vždy vykazovat vlastnost *reverzibility*. To je důvodem, proč v průběhu výpočtu **nedochází k žádnému měření**, neboť měření v kvantové mechanice je, alespoň ve vztahu k pozorovateli, který je seznámen s jeho výsledky, zcela *ireverzibilní* (viz [43]). Změřen je tak až závěrečný výstup algoritmu. Aby však počítač pracoval korektně, nesmí docházet ani k žádné jiné formě interakce s vnějším prostředím. Proto musí být kvantový počítač od vnějšího prostředí dokonale izolován a udržován v teplotách blízkých *absolutní nule*.

Měření qubitu je zvláštní také tím, že ačkoli se qubit může nacházet v nekonečně mnoha možných stavech a teoreticky by do něj tak mělo být možné uložit nekonečné množství informace, měřením z něj lze získat pouze jediný *bit* informace. Tato skutečnost byla demonstrována na příkladu polarizace fotonu v sekci 3.1.7.

Žádným (von Neumannovým) měřením nelze získat více než jeden očekávaný bit informace z jakéhokoli daného qubitu. [23]

Aby bylo možné provádět výpočty na kvantovém počítači, je pochopitelně zapotřebí více než jeden qubit. K uchování stavu několika qubitů v kvantovém počítači slouží ***kvantové registry***, jejichž celkový stav lze reprezentovat *tenzorovým součinem* stavů jednotlivých qubitů. Stav vzniklý tenzorovým součinem stavů n qubitů je prvkem vícerozměrného Hilbertova prostoru H_n majícího 2^n dimenzí. Zásadní rozdíl oproti klasickým registrům je však ten, že zatímco klasický registr šířky n bitů se může nacházet vždy v jednom z 2^n různých stavů, kvantový registr se díky principu superpozice může nacházet **ve všech 2^n stavech zároveň**.

Schopnost registru nacházet se v superpozici několika rozlišitelných stavů najednou vede k fenoménu známému jako ***kvantový paralelismus***. Pakliže totiž hledáme hodnoty nějaké funkce pro více odlišných vstupů, s pomocí kvantového počítače můžeme aplikovat tuto funkci na superpozici daných vstupů. Výsledný stav je pak **superpozicí všech hledaných výstupů**. Místo abychom tak brali vstupy jeden po druhém a provedli funkci na každém zvlášť, bude stačit provést funkci pouze jednou. Kvantový paralelismus se liší od paralelismu v klasických počítačích, kde paralelní výpočty probíhají na odlišných obvodech.

Kvantový paralelismus sám o sobě však není příliš užitečný. Výsledný stav sice obsahuje informace o všech hledaných výsledcích, otázkou však zůstává jak z něj tyto informace získat. Pouhým změřením výsledného stavu bychom totiž, jak víme, způsobili kolaps tohoto stavu a obdržená hodnota by odhalila pouze jednu z hledaných odpovědí. S tímto problémem se různými způsoby vypořádávají konkrétní *kvantové algoritmy*.

3.2.3 Kvantové algoritmy

Kvantové algoritmy typicky kombinují kvantové výpočetní techniky s klasickými. Všechny algoritmy pro klasický počítač lze totiž provést také na počítači kvantovém. Je to však právě přidání kvantových výpočetních technik, využívajících zejména *principu superpozice* a *kvantového provázání*, co umožňuje exponenciálně snížit výpočetní složitost algoritmů pro řešení některých matematických problémů. Níže je uveden příklad kvantového algoritmu, jehož objevení představuje důležitý milník v dějinách kryptografie. Jedná se o *Shorův algoritmus*, jenž může posloužit k faktorizaci celých čísel, ale také např. k nalezení diskrétního logaritmu, což v obou případech představuje hrozbu pro metody používané v současné kryptografii. Implementací tohoto algoritmu by došlo jak k prolomení nejrozšířenější klasické asymetrické šifry RSA (1.3.2), tak Diffieho-Hellmanova protokolu pro výměnu tajného klíče, používaného v symetrické kryptografii.

Shorův algoritmus objevil Peter Shor v roce 1994 [45]. Primárním účelem algoritmu je rozklad celého čísla na jeho prvočinitele. Jedná se o *polynomiálně omezený* algoritmus, neboť jeho časová složitost $f(N)$, kde N je velikost rozkládaného čísla, lze vyjádřit mnohočlenem. Právě tato skutečnost proslavila Shorův algoritmus napříč vědeckými disciplínami vzhledem k tomu, že nejefektivnějším *klasickým* algoritmem pro faktorizaci velkých celých čísel je v současné době algoritmus *GNFS* [46] pracující s *exponenciální* složitostí.

Problém faktorizace čísla je v Shorově algoritmu převeden na problém nalezení periody funkce. Rozkládané číslo se reprezentuje jako periodický kvantový stav za pomoci *modulárního umocňování*. Jádrem algoritmu je pak ***kvantová Fourierova transformace*** [48], díky které jsme schopni získat frekvenční spektrum vlnové funkce popisující stav kvantového systému. Tuto významnou kvantovou techniku lze realizovat za použití relativně nízkého počtu hradel a je nesrovnatelně rychlejší než klasické *Fourierovy transformace*. Nalezená perioda je dále použita k nalezení prvočinitelů čísla za užití *klasické* výpočetní techniky *binárního umocňování*.

Podobně jako faktorizace celých čísel, také *výpočet diskrétního logaritmu* je možné převést na problém nalezení periody funkce. Shorův článek [45] představuje návrh řešení obou těchto problémů. Dosud ovšem nebyl sestrojen kvantový počítač natolik výkonný, aby ve spojení s Shorovým algoritmem představoval skutečnou hrozbu pro kryptosystémy stojící na obtížné řešitelnosti uvedených problémů. Nejvyšší číslo, jež se zatím podařilo úspěšně faktorizovat na kvantovém počítači, je 56 153 [49].

3.2.4 Využití kvantového počítače

Schopnost kvantového počítače řešit určité kategorie problémů s nesrovnatelně nižší časovou složitostí, než s jakou stejné problémy řeší počítače klasické, je známá pod pojmem ***kvantová nadřazenost***. V uplynulých letech byla již kvantová nadřazenost demonstrována v praxi na kvantových počítačích, kterými lidstvo v současnosti disponuje [50, 51]. Tyto stroje však stále nejsou natolik výkonné a spolehlivé, aby jich šlo v praxi valně využít. Přenesení teoretického modelu kvantového počítače do reálného světa se totiž ukazuje být nesmírně obtížným, zejména proto, že se vzrůstajícím počtem qubitů vzrůstá také míra chybovosti počítače. Současné kvantové počítače proto slouží především k výzkumným a vzdělávacím účelům.

Jednou z otázek, kterou se odvětví kvantových počítačů zabývá, je určení množiny matematických problémů, které podléhají *kvantové nadřazenosti*. S některými kategoriemi problému si totiž ani kvantový počítač nedovede poradit o nic lépe než počítač klasický a zdá se, že pro některé účely se budou dokonce klasické počítače vždy hodit lépe než kvantové. Je tedy pravděpodobné, že tak jako kvantová teorie fyziky nenahradila teorii klasickou, ani kvantový počítač klasickou výpočetní techniku zcela nenahradí. V určitých oblastech však může pomoci významně posunout hranice možností, za které se klasický počítač ze své fyzikální podstaty nedostane. Příchod dokonalejšího kvantového počítače by tak mohl v budoucnu znamenat významný pokrok například v oblasti farmacie, meteorologie či umělé inteligence.

Komplikovanější je vztah kvantového počítače k **datové bezpečnosti**. Na jednu stranu mají totiž kvantové technologie potenciál otevřít dveře novým možnostem zabezpečení informací, na stranu druhou však nutně znamenají znehodnocení mnohých stávajících. Přestože je příchod prakticky využitelného kvantového počítače nejistý a těžko předvídatelný, zabývat se otázkou zabezpečení dat v éře kvantových počítačů je rozhodně namístě již nyní. V okamžiku sestrojení plně funkčního kvantového počítače bude totiž drtivá většina klasicky šifrovaných dat již potenciálně vystavena nebezpečí a je proto třeba uvést kvantové a postkvantové kryptosystémy do praxe dříve než kvantový počítač jako takový.

3.2.5 Kvantový generátor náhodných čísel

Vedle kvantového počítače stojí za to na závěr této kapitoly zmínit ještě jednu významnou a výrazně triviálnější kvantovou technologii, která je s kryptografií úzce spjatá. Vzhledem k tomu, že výsledky měření v kvantové mechanice mají **nedeterministický** charakter, lze kvantové jevy využít jako zdroj náhodnosti v *kvantovém generátoru náhodných čísel*. Význam náhodných číselných posloupností, jež nelze nahradit pseudonáhodnými, v kryptografii byl již diskutován v předchozí kapitole 2 o nepodmíněné bezpečnosti a bude o něm dále řeč v kapitole 4 o kvantové kryptografii. Podobně důležité jsou generátory náhodných čísel také třeba pro *stochastické simulace*. Kvantové generátory náhodných čísel typicky využívají kvantových aspektů světla, kvantové fluktuace ve vakuu či radioaktivní přeměny.

Kapitola 4

Kvantová kryptografie

V předchozích kapitolách jsme se seznámili se základy klasické kryptografie a zdůvodnili potřebu nalezení kryptosystémů, jejichž bezpečnost by nebyla podmíněna výkonností dostupné výpočetní techniky. Představili jsme si také stěžejní principy kvantové fyziky a kvantového počítače, které nám vytvořily půdu pro pochopení fyzikální i informačně teoretické stránky nadcházející problematiky. Pojďme nyní propojit koncepty osvětlené v předchozích kapitolách a nahlédněme do nitra vědecké disciplíny, výsledky jejíchž výzkumů budou jednou dost možná klíčové pro zachování soukromí v digitálním prostoru. Řeč je samozřejmě o *kvantové kryptografii*. Nejrozvinutější oblastí kvantové kryptografie je bezesporu *kvantová distribuce klíče*. Proto je i v této práci věnována pozornost zejména této kategorii kvantových kryptografických protokolů. O praktickém využití protokolů a s ním spojených komplikacích dále pojednává závěrečná sekce kapitoly.

4.1 Kvantová distribuce klíčů (QKD)

Kvantová distribuce klíčů (dále *QKD* z angl. *Quantum Key Distribution*) je disciplínou kvantové kryptografie zkoumající způsoby bezpečného přenosu tajného šifrovacího klíče s využitím poznatků z kvantové fyziky. V kombinaci s Vernamovou šifrou lze mluvit o nepodmíněně bezpečném způsobu komunikace (viz kapitola 2). Protokoly QKD vychází zejména z *principu superpozice*, *stavu kvantové provázanosti* a specifických vlastností měření na kvantovém systému (3.1). Podobně jako algoritmy pro kvantové počítače, také QKD pracuje s kombinací kvantových a klasických postupů. Domluva klíče tak probíhá zčásti po kvantovém a zčásti po klasickém komunikačním kanále. Tajná zpráva zašifrovaná získaným klíčem je pak bezpečně poslána po klasickém (nezabezpečeném) komunikačním kanále.

Kvantový komunikační kanál slouží k přenosu qubitů, z nichž se poté utváří samotný tajný klíč. Vlivem fenoménů kvantové fyziky jako je *kvantová dekoherence* (narušení sytému měřením či pozorováním), *Heisenbergův princip neurčitosti* (3.1.4) či *no-cloning theorem* (3.1.6) totiž není principiálně možné provádět odposlech na kvantovém komunikačním kanále tak, aby nebyl zpozorovatelný. Měření provedené útočníkem na qubitech putujících po kvantovém kanále totiž ve většině případů naruší stav těchto qubitů, což **umožňuje odhalit přítomnost útočníka** na kanále. Mechanismus detekce odposlechu bude konkrétně popsán v sekcích pojednávajících o konkrétních protokolech. Médiem sloužícím k přenosu informace po kvantovém komunikačním kanále je typicky foton a v závislosti na použitém protokolu bývá informace kódována do jeho polarizace či spinu. Přenos fotonu se nejčastěji uskutečňuje po optickém vlákně, ale je možný také bezdrátově, pomocí satelitů [52]. O kvantovém komunikačním kanále se v přeneseném významu někdy mluví také v souvislosti s komunikací na bázi kvantového provázání, kdy je sdílení informace uskutečněno prostřednictvím provázaného fotonového páru, z nějž každá ze dvou komunikujících stran vlastní jeden foton.

Kvantová distribuce klíče je patrně nejznámější a nejprobádanější oblastí kvantové kryptografie. Pro tuto skutečnost však bývá někdy mylně považována za synonymum *kvantové kryptografie*. QKD se však zabývá pouze problémem bezpečné distribuce tajného a dokonale náhodného klíče, kterým je možné následně šifrovat komunikaci za pomoci symetrické šifry. V rámci QKD nejsou vytvářeny nové metody šifrování informace, metody umožňující autentizaci komunikujících stran ani metody pro tvorbu digitálního podpisu. Těmito a dalšími problémy se zabývají jiné domény kvantové kryptografie.

V rámci QKD bylo navrženo několik protokolů bezpečné výměny klíčů, využívajících různých aspektů kvantové mechaniky. Níže jsou popsány dva, jež se významným způsobem zapsaly do historie kvantové kryptografie. Jedná se o první kvantový kryptografický protokol *BB84* založený na polarizaci fotonů a protokol *E91*, který je jedním z prvních úkazů praktického využití *stavu kvantové provázanosti*. V sekci 4.1.3 jsou poté uvedeny některé další kvantové protokoly, jež vycházejí z protokolu *BB84* a odstraňují nedostatky, které na něm byly v průběhu let nalezeny.

4.1.1 BB84

Protokol ***BB84*** [1] navrhli Charles Bennett a Gilless Brassard v roce 1984. Protokol umožňuje bezpečnou distribuci tajného klíče pro šifrování *Vernamovou šifrou*. Vyšli z myšlenky Stephena Wiesnera, využít některých specifik kvantové fyziky k tvorbě nepadělatelných bankovek [54]. Ačkoli původní Wiesnerův návrh nebyl vědeckou komunitou přijat příliš vřele, zvláště proto, že by realizace takových bankovek byla těžce proděločná, Bennett s Brassardem prohlédli potenciál, který se ve Wiesnerových myšlenkách skrýval, a přenesli princip „kvantových peněz“ do kryptografie. Tak přišel na svět první kvantový kryptografický protokol.

Přenos tajného klíče je v protokolu *BB84* uskutečněn pomocí polarizovaných fotonů posílaných po kvantovém kanále. Z kvantové fyziky víme, že přesné zjištění neznámého stavu polarizace fotonu není žádným měřením možné (3.1.7), a víme také, že není možné vytvářet nezávislé identické kopie

fotonů v neznámém stavu (3.1.6). Tyto poznatky v kombinaci s faktem, že měřením na kvantovém systémů vzniká risk narušení stavu tohoto systémů, útočníkovi znemožňují provádět odposlech na kvantovém kanále a zaručují tak protokolu **nepodmíněnou teoretickou bezpečnost**.

Výměnu klíčů podle protokolu *BB84* lze rozdělit do několika fází.

1) Přípravná fáze

Aby mohla Alice odeslat Bobovi tajnou zprávu délky n za použití *Vernamovy šifry*, potřebuje s ním nejprve sdílet dokonale náhodný tajný klíč délky n (viz sekce 2.2). To je možné prostřednictvím protokolu *BB84* tak, že si Alice i Bob nejprve každý zvlášť vygenerují **náhodnou posloupnost bitů** délky m, k čemuž mohou využít *kvantový generátor náhodných čísel* (3.2.5). Platí, že $m \gg n$ z důvodů, jež vyplynou z dalších fází algoritmu. Tyto posloupnosti ještě nebudou sloužit jako šifrovací klíč, nýbrž budou určovat, jakou *bázi* použije Alice k polarizaci fotonů posílaných po kvantovém kanále (Alicina posloupnost) a v jaké *bázi* bude Bob přijímané fotony měřit (Bobova posloupnost). Skutečnost, že se jedná o binární posloupnosti již naznačuje, že bude na výběr ze dvou bází: *rektilineární báze* $+$ a *diagonální báze* $\times$. Alice a Bob se veřejně domluví, kterou bázi budou zastupovat nulové hodnoty v jejich posloupnostech, a kterou jedničkové. Jejich posloupnosti tak lze v podstatě zaznamenat jako posloupnosti $+$ a $\times$.

Rektilineární báze $(+)$ umožňuje, aby byl foton polarizován:

a) horizontálně, tj. pod úhlem 0° (zn. $\rightarrow$)

b) vertikálně, tj. pod úhlem 90° (zn. $\uparrow$)

Diagonální báze $(\times)$ umožňuje, aby byl foton polarizován:

a) diagonálně pod úhlem 45° (zn. $\nearrow$)

b) diagonálně pod úhlem 135° (zn. $\nwarrow$)

Alice a Bob se také veřejně domluví, kterou z dvojice polarizací v každé bázi má Bob interpretovat jako 0 a kterou jako 1, nalezne-li přijatý foton v příslušné polarizaci. Rektilineární polarizace → a diagonální polarizace ↗ například budou interpretovány jako 0, rektilineární polarizace ↑ a diagonální polarizace ↖ jako 1.

Alice si následně vygeneruje ještě jednu náhodnou binární posloupnost délky m, která již bude určovat konkrétní hodnoty klíče, který bude Bobovi odesílat. Celkem má tedy Alice připravené dvě stejně dlouhé náhodné posloupnosti a Bob jednu.

2) Přenosová fáze

Ve druhé fázi protokolu zakóduje Alice svou druhou náhodnou posloupnost bitů do polarizace fotonů a tyto fotony Bobovi odešle. Jeden bit vždy kóduje do jednoho fotonu. K dispozici má 4 zdroje světla vysílající fotony (qubity) 4 možných polarizací (→; ↑; ↗; ↖). Který zdroj fotonů použije pro zaslání k-tého fotonu v řadě vždy závisí na k-tých členech její první a druhé náhodné posloupnosti a na předchozí domluvě s Bobem. Jak by taková řada polarizovaných fotonů odeslaných po kvantovém kanále Bobovi mohla vypadat, je patrné z následujícího schématu.

Náhodná posloupnost bází	+	+	×	+	×	×	×	×
Náhodná posloupnost bitů klíče	0	1	0	0	0	1	1	0
Fotony vyslané Bobovi	→	↑	↗	→	↗	↖	↖	↗

Alice fotony vysílá v pravidelných časových intervalech a Bob na druhém konci kvantového komunikačního kanálu měří přijaté fotony vždy v příslušné bázi určené **jeho** náhodnou posloupností. K měření tak používá dva neortogonální lineární polarizační filtry např. ↑ a ↗ nebo ↑ a ↖, ... a přistupuje k přijatým fotonům tak, jako by je Alice polarizovala ve stejné bázi, v jaké je on měří, přestože ve skutečnosti použili každý jinou náhodnou posloupnost. V tuto chvíli si jednoduše zaznamenává hodnoty 0 a 1 v závislosti na tom, jak se foton na filtru zachová, a ignoruje skutečnost, že množství záznamů

neodpovídá skutečné polarizaci fotonu, neboť mnohdy použil opačnou bázi, diagonální vůči té, kterou použila Alice, a výsledek jeho měření na těchto fotonech je tak zcela náhodný. Chování fotonu při dopadu na filtr, jehož polarizační rovina je od polarizační roviny fotonu odkloněna o 45° bylo objasněno v sekci 3.1.7.

Oproti příkladu uvedenému v sekci 3.1.7 však Bob nepoužívá filtr na principu absorpce, neboť musí předpokládat, že v neideálních podmínkách dojde ke ztrátám některých fotonů během přenosu. V případě použití absorpčního filtru by tyto ztracené fotony mylně interpretoval jako pohlcené (tedy v polarizaci kolmé na filtr). Používá proto raději analyzátory založené na lomu či odrazu, které jsou pro dané účely vhodnější, a dvojici vhodně rozmístěných detektorů fotonů. Celkově tedy na jeho straně může vždy po uplynutí daného časového intervalu dojít ke třem situacím:

1. Foton je detekován a změřen v polarizaci rovnoběžné s filtrem.
2. Foton je detekován a změřen v polarizaci kolmé na filtr.
3. Foton není detekován.

3) Eliminační fáze

Komunikace mezi Alicí a Bobem ve třetí fázi protokolu probíhá již po klasickém, nezabezpečeném komunikačním kanále. Informace, které budou po tomto kanále sdílet, útočníkovi nemohou vyzradit nic užitečného o tajném klíči, který z protokolu vzejde, tudíž fakt, že útočník může provádět odposlech na tomto kanále, není pro Alici s Bobem překážkou.[1]

Bob nejprve informuje Alici o tom, které fotony se mu podařilo detekovat. Oba tak mohou vyřadit ze svých posloupností členy, které se nepodařilo k Bobovi doručit, popř. které jeho nedokonalé detektory nedokázaly zachytit. Bob následně sdělí Alici **posloupnost bází**, které použil k měření přijatých fotonů, **ne však posloupnost hodnot**, které měřením získal.

[1] Předpokladem je, že útočník nemá možnost modifikovat obsah zasílaných zpráv.

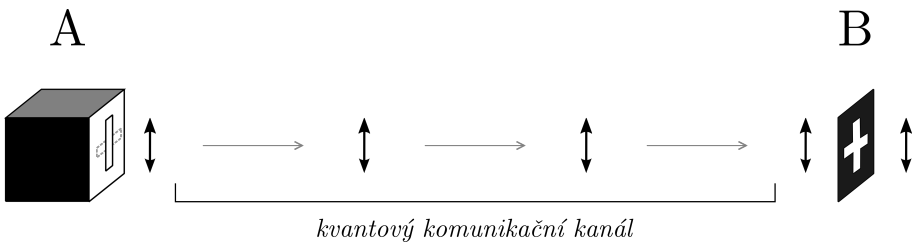
Alice porovná Bobovu posloupnost bází s posloupností, kterou pro volbu bází použila ona, a zpětně Boba informuje o tom, na kterých místech se jejich posloupnosti shodují. Bob tak ze svých záznamů vyloučí hodnoty, které naměřil s opačnou bází, neboť mají zcela náhodný charakter a nelze z nich získat žádnou užitečnou informaci o původní polarizaci Alicí vyslaného fotonu. Alice stejně tak vyřadí tyto členy z posloupnosti, kterou převáděla do odesílaných qubitů. Statisticky by takto měli vyřadit polovinu členů, neboť šance, že se oba trefili do stejné báze, je $\frac{1}{2}$. Na konci třetí fáze tedy Alice i Bob disponují posloupnostmi, které budou tvořit **základ tajného klíče**. Domnívají se totiž, že by nyní jejich posloupnosti měly být identické. Jisti si však být zatím nemohou, neboť stále neověřili, zda na kvantovém komunikačním kanále nedošlo k odposlechu či jinému rušení.

4) Ověřovací fáze

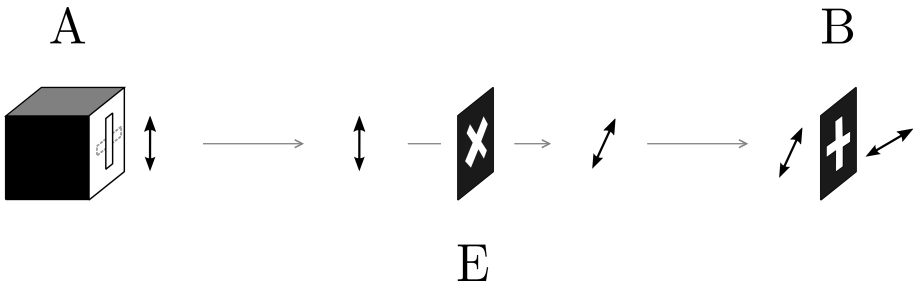
Již bylo nejednou řečeno, že protokoly kvantové kryptografie znemožňují útočníkovi vykonávat odposlech tak, aby nebyl odhalen. Takový typ odposlechu, který nemá vliv na obsah přenášených dat, nazýváme v kryptografii *pasivním*. Principy kvantové fyziky, jichž protokoly využívají, tak vynucují, že jakýmkoli mechanismem se útočník pokusí získat informace z qubitů přenášených po kvantovém kanále, vždy se bude jednat o odposlech *aktivní* – útočník odposlechem nutně poškodí přenášená data. Zamysleme se nyní, jaké možnosti odposlechu útočník má a jak by se takové počínání promítlo do přenášených dat.

K získání informace o polarizaci fotonu je třeba provést měření polarizace na tomto fotonu. Díky *no-cloning teorému* (3.1.6) víme, že kvantový systém v neznámém stavu není možné klonovat. Útočník (Eva) tudíž musí své měření provádět přímo na fotonech, které Alice Bobovi vyslala, nemůže si vytvořit vlastní kopie. K tomuto měření musí použít vždy jednu ze dvou možných bází ($+$ či $\times$). Neexistuje žádné zařízení, které by dokázalo měřit polarizaci fotonu v obou bázích zároveň, neboť neortogonální stavy polarizace (stavy, které na sebe nejsou kolmé) podléhají *Heisenbergovu principu*

neurčitosti (3.1.4) a nelze tak z principu v jediném okamžiku provádět měření v diagonální i rektilineární bázi zároveň. Protože Eva nezná posloupnost, dle které Alice volila pořadí bází, v nichž fotony polarizovala, nezbývá jí, než volit báze náhodně, podobně jako to dělá Bob. Ať Eva zvolí pořadí bází jakékoli, statisticky se také trefí zhruba jen v polovině případů. Pokaždé když zvolí opačnou bázi, nejenže získá náhodný výsledek, ale navíc **nevratně naruší původní stav fotonu** a ten tak k Bobovi dorazí s jinou polarizací, než s jakou jej Alice vyslala.



(a) **Příklad průběhu komunikace v nepřítomnosti útočníka.** Alice vyšle foton polarizovaný v rektilineární bázi vertikálně. Bob tento foton změří taktéž v rektilineární bázi a správně ho tudíž identifikuje jako vertikálně polarizovaný.



(b) **Příklad průběhu komunikace v přítomnosti útočníka.** Alice vyšle foton polarizovaný v rektilineární bázi vertikálně. Eva provede odposlech na kvantovém komunikačním kanále s použitím diagonální báze. Horizontálně polarizovaný foton se tak změní v náhodně diagonálně polarizovaný. Bob následně změří příchozí foton ve stejné bázi, v jaké jej Alice původně polarizovala, získá však s šancí 50% opačný výsledek.

Obrázek 4.1: Srovnání rozdílných průběhů komunikace dle protokolu *BB84* po kvantovém komunikačním kanále nez odpoclechu (a) a s odposlechem (b).

V důsledku Evina odposlechu vzniknou chyby v Bobových záznamech. Pakliže totiž Bob změří foton ve stejné bázi jako Alice (o čemž se přesvědčí v eliminační fázi protokolu) a tento foton byl po cestě změřen Evou v bázi opačné, s pravděpodobností $\frac{1}{2}$ získá Bob opačný výsledek, než by měl, protože se narušený foton bude nacházet v bázi diagonální vůči té, kterou Alice s Bobem použili. Čím více fotonů Eva odposlechem naruší, tím více chyb bude do Bobových záznamů zaneseno a tyto chyby v jeho posloupnosti zůstanou i po eliminační fázi, neboť jestliže se Bob s Alicí shodli na tom, že pro daný foton použili stejnou bázi, nemají důvod ho ze svých záznamů eliminovat. Jejich posloupnosti se tak budou lišit.

Čtvrtá, ověřovací fáze protokolu tedy spočívá v **určení míry neshody** v posloupnostech Boba a Alice, které vzešly z předchozí fáze protokolu. Zde je třeba uvést, že k rušení může na komunikačním kanále dojít i z jiných důvodů než vlivem odposlechu a chyba v datech tak nemusí nutně hned implikovat přítomnost útočníka na komunikačním kanále. Aby však bylo docíleno skutečně nepodmíněné bezpečnosti, musí tvůrci protokolů ke všem chybám vzniklým při přenosu klíče přistupovat tak, jako by je měl na svědomí útočník. Alice s Bobem si tak předem určí *přijatelnou míru neshody* ve svých posloupnostech, pro kterou je bezpečnostní riziko zanedbatelné. Pakliže míra neshody v jejich posloupnostech překročí tuto hranici, klíč nebudou moci k zašifrování tajné zprávy použít, neboť je pravděpodobné, že byl na kvantovém komunikačním kanále proveden odposlech ohrožující bezpečnost jejich komunikace.

Míru neshody (angl. *error rate*) určí Alice s Bobem tak, že jeden z nich jednoduše odtajní náhodnou podmnožinu bitů své posloupnosti a druhý sdělí, jak velká část této podmnožiny nesouhlasí s tím, jaké hodnoty si pro dané indexy poznamenal on. Vyberou-li dostatečně velkou podmnožinu, měli by být schopni případný odposlech spolehlivě detekovat. Zde je patrné, proč museli Alice s Bobem začít v první fázi s výrazně delšími posloupnostmi, než je délka klíče, který potřebují k zašifrování zprávy. Zhruba polovinu bitů vyřadili v eliminační fázi, neboť fotony použité k jejich přenosu polarizovali

v odlišných bázích, další část nyní obětují k ověření integrity svých posloupností. Pokud tedy shledají, že je míra neshody ve vybrané podmnožině jejich posloupností zanedbatelná, mohou ze zbylých (neodtajněných) bitů vybrat n, které budou tvořit jejich **tajný šifrovací klíč**. Bude-li však míra neshody v jejich posloupnostech příliš velká, zahodí je a opakují celý protokol od začátku, dokud se jim nepodaří získat bezpečný klíč.

Oprava a posílení bezpečnosti klíče

Původní verze protokolu *BB84* nabízí pouze teoretický model nepodmíněně bezpečné výměny klíče, podle kterého je klíč bezpečný tehdy, neshledají-li komunikující strany v podmnožinách svých posloupností *žádnou* neshodu. Výše jsme se však již zmínili o tom, že v důsledku neideálnosti reálného kvantového kanálu a měřicích přístrojů lze určitou míru neshody v posloupnostech očekávat vždy. Byly proto vyvinuty techniky, které v praxi umožňují dodatečně opravit některé chyby v posloupnostech Alice a Boba vzniklé během přenosu. Opravnými technikami lze tak snížit míru neshody v Alicině a Bobově verzi klíče. Technikami posilujícími bezpečnost klíče se dále eliminuje množství informace, které by mohl útočník o tajném klíči potenciálně mít. V anglické literatuře jsou techniky opravy a posílení bezpečnosti klíče známy pod pojmy *information reconcilliation*, popř. *error correction*, a *privacy amplification*.

Příkladem techniky pro opravu chyb v klíči je protokol *Cascade* [55], jehož spoluautorem je Gilles Brassard, jeden z autorů původního protokolu *BB84*. *Cascade* umožňuje najít neshody mezi Alicinou a Bobovou posloupností tak, že posloupnosti dělí na menší bloky a sdělují si *parity* těchto bloků. Je-li v Bobově bloku liché množství chyb jeho parita se bude od parity Alicina bloku lišit a za pomoci interaktivního binárního vyhledávání, tj. postupným půlením bloku a porovnávání parit jeho částí s Alicí, nakonec narazí na hledanou chybu. Touto cestou je možné výrazně snížit míru chybovosti klíče, avšak za cenu poskytnutí některých informací o klíči případnému útočníkovi. Proto by měla být na klíč následně aplikována některá z technik posilujících

bezpečnost. Alternativně lze k opravě chyb použít metody, které nevyžadují odtajnění takového množství informace o klíči (př. [56], [57], [58]).

Na rozdíl od klasických kryptografických protokolů pracují kvantové kryptografické protokoly s předem stanovenou konečnou délkou vstupu. Také míra informace, která by mohla potenciálně uniknout k útočníkovi, je tudíž konečná a lze pro ni určit horní mez. Díky tomu lze matematicky dokázat nepodmíněnou bezpečnosti protokolů QKD a také nalézt postupy, které horní mez odposlechnuté informace sníží natolik, aby nepředstavovala skutečné bezpečnostní riziko. Techniky *posílení bezpečnosti* [60] mají za úkol minimalizovat až zcela eliminovat množství informace, které by mohl útočník zjistit o výsledném klíči z dat, jež se mu podařilo odposlechnout během přenosu fotonů či během procesu opravy klíče. Posílení bezpečnosti klíče spočívá v aplikaci *hashovací funkce* na klíče Alice a Boba vzešlé z předchozí fáze. Výsledný klíč je kratší než klíč, jenž do funkce vstupoval, a míra jeho zkrácení typicky závisí na *míře chybovosti*, a tedy potenciální kompromitace vstupujícího klíče.

4.1.2 E91

Protokol ***E91*** [62] byl navržen Arturem Ekertem v roce 1991 a umožňuje komunikujícím stranám vytvořit sdílený nepodmíněně bezpečný náhodný šifrovací klíč za pomoci *kvantového provázání* (3.1.5). Níže je popsána modifikace tohoto protokolu využívající měření polarizace fotonů (3.1.7).

Kvantově provázaný systém se nachází ve stavu superpozice, dokud není alespoň jedna z jeho části změřena. Ve chvíli, kdy se tak stane, zkolabují všechny části do náhodných samostatných stavů, které jsou však v perfektní korelaci (či antikorelaci). Stav jejich vzájemné provázanosti v této chvíli zaniká. Toho lze využít v kryptografii k získání identických posloupností na obou stranách komunikace.

Podobně jako *BB84*, také protokol *E91* lze realizovat pomocí fotonů. Tentokrát však fotony nemusí odesílat jedna komunikující strana druhé, ale v podstatě jim provázaný fotonový pár může opatřit i libovolná třetí strana, (útočníka nevyjímaje). Stačí, aby byl vždy jeden foton z páru dopraven Alici a

druhý Bobovi ještě v nezměřeném, provázaném stavu. Teprve tehdy, až foton k oběma dorazí, je na něm provedeno měření, a to následujícím způsobem.

1. Alice pro změření polarizace fotonu zvolí vždy náhodně bázi z množiny $\{a_1, a_2, a_3\}$, kde jednotlivé báze odpovídají rektilineárnímu filtru $+$ z předchozího protokolu, otočenému o 0, $\frac{\pi}{8}$ a $\frac{\pi}{4}$ radiánu.

   Bob také náhodně volí měřící báze, pouze z množiny $\{b_1, b_2, b_3\}$, kde otočení bází odpovídá 0, $\frac{\pi}{8}$ a $-\frac{\pi}{8}$ radiánu.

2. Poté, co provedou měření a zaznamenají si výsledky, sdělí si Alice a Bob veřejně posloupnosti bází, které zvolili. Hodnoty, které naměřili ve stejných bázích, tj. (a_1, b_1) či (a_2, b_2), v posloupnostech ponechají a eventuálně použijí jako tajný klíč. Ostatní hodnoty zveřejní.

3. Na zveřejněných hodnotách je provedena statistická analýza s využitím poznatků fyzika Johna Bella o kvantově provázaných systémech, která určí koeficient korelace mezi posloupnostmi Boba a Alice. Pokud je zjištěno, že posloupnosti nekorelují tak, jak by se u provázaných fotonových párů očekávalo, je pravděpodobné, že došlo k odposlechu. Jinak může být tajná posloupnost použita jako šifrovací klíč.

Důvod proč by Evino měření ovlivnilo korelaci posloupností Boba a Alice spočívá v tom, že jakékoli měření provedené na provázaném stavu předtím, než jeho části dorazí k Bobovi a Alici, by vedlo k zániku tohoto stavu. Fotony by od toho okamžiku byly již na sobě nezávislé, což by se projevilo v měřeních Alice a Boba. Není žádná strategie, jak by mohla Eva získat informaci o tajném klíči z provázaných fotonů předtím, než je Alice s Bobem změří, neboť provázané fotony jako takové žádnou informaci o tomto klíči nenesou. Informace vzniká až v okamžiku, kdy Bob a Alice své fotony změří, a je závislá na tom, jaké báze k tomu použijí. Jelikož se Eva posloupnosti bází (stejně jako v předchozím protokolu) dozví až poté, co měření proběhlo, nemá žádnou cestu, jak provést odposlech aniž by byla odhalena a to ani tehdy, je-li ona sama zdrojem těchto provázaných fotonů.

4.1.3 Další protokoly kvantové distribuce klíčů

Ač jsou z pohledu teorie informace výše uvedené protokoly nepodmíněně bezpečné, realizovat je přesně v takové podobě, v jaké byly navrženy, je v praxi velmi obtížné. Pro implementaci protokolu *BB84* se ukázala být problematickou zejména konstrukce světelného zdroje vysílajícího samostatné fotony. V současné době bývají k tomuto účelu využívány lasery, vysílající krátké světelné impulsy, jež obsahují velice malá množství fotonů. Ukázalo se však, že vyslání i pouhých dvou fotonů na místo jednoho dává útočníkovi možnost uskutečnit na kvantovém kanále odposlech, který by nebylo možné odhalit. Teoreticky by totiž mohla Eva oddělit ze shluku fotonů jeden, který by poslala dále Bobovi, a na zbylých by provedla vlastní měření. Takový typ útoku se v kvantové kryptografii nazývá *photon number splitting attack* [63].

Mnohé novější kvantové protokoly proto hledají cestu, jak upravit schéma *BB84* tak, aby bylo možné útoku předejít i bez nároků na dokonalý zdroj samostatných fotonů. Příkladem takového protokolu je ***SARG04*** [64], který se od *BB84* liší pouze v eliminační a ověřovací fázi. Nejlepších výsledků však, co se týče odolnosti vůči *photon number splitting* útoku, doposud dosáhl protokol ***Decoy state*** [65], ve kterém Alice záměrně pracuje s různými intenzitami světla a kromě signálů nesoucích informaci o klíči vysílá navíc tzv. *návnadové stavy*. Pro svou bezpečnost, které lze navíc dosáhnout s již dnes dostupným vybavením, je *Decoy state* protokol v současnosti nejpoužívanějším protokolem QKD.

Známou úpravou protokolu *BB84* je také protokol ***B92***, jehož autorem je Charles Bennett a který pracuje pouze se dvěma možnými stavy polarizace namísto čtyř. Za zmínku stojí ještě první kvantový protokol se základem v asymetrické kryptografii [66], který na rozdíl od předchozích protokolů využívá dvou kvantových kanálů a žádného klasického – hodí se tedy pro situaci, kdy má útočník možnost modifikovat data sdílená po klasickém komunikačním kanále. Tak jako klasické protokoly s veřejným klíčem, je navíc jeho použití výhodné, účastní-li se komunikace více než dvě strany. Daní za to je však náročnější praktická implementace než u výše uvedených protokolů.

4.2 Praktické využití kvantové kryptografie

Všechny protokoly kvantové distribuce klíčů, o kterých byla v předchozí sekci řeč, s výjimkou posledního, mají společný jeden předpoklad: Část úmluvy klíče zde probíhá po klasickém kanále, na němž útočník nesmí mít možnost přenášená data ovlivňovat. Pokud by totiž byl útočník schopen nahradit například Bobem zveřejněnou posloupnost bází za vlastní posloupnost bází, mohl by si s Alicí v podstatě umluvit vlastní klíč a vylákat z ní tajnou zprávu zašifrovanou tímto klíčem, aniž by se Alice dozvěděla, že komunikuje s útočníkem, a nikoli s Bobem. Tento problém lze v kvantové kryptografii vyřešit podobně, jako bychom ho řešili v kryptografii klasické, tedy *autentizačním schématem*. Nepodmíněně bezpečných autentizačních schémat bylo navrženo několik, vesměs však všechny vyžadují, aby Alice s Bobem předem sdíleli nějaké tajemství, kterým si vzájemně prokáží své identity. Narážíme tak na paradoxní situaci, že aby si dvě strany mohly vytvořit společný tajný klíč, musí již předem nějakou tajnou informaci sdílet. Kvantová distribuce klíče tak v tomto případě slouží spíše k rozšíření tajné informace, kterou strany předem sdílí. Tomuto paradoxu se lze v zásadě vyhnout dvěma způsoby – použitím protokolu QKD, který lze realizovat čistě na kvantovém kanále, nebo použitím kvantového kryptografického protokolu, který klíčovou výměnu vůbec nevyžaduje (př. [67], [68]).

Patrně největší úskalí kvantové kryptografie tkví však v přenosu informace po kvantovém kanále. Již byla zmíněna obtížnost konstrukce zdrojů samostatných fotonů, potřebných k realizaci mnoha protokolů QKD. Samotný fyzikální princip protokolů, který jim na jednu stranu zaručuje nepodmíněnou bezpečnost, je však na druhou stranu v mnohém limitující. Protokoly QKD například mnohdy vděčí za svou bezpečnost skutečnosti, že nosičem informace jsou konkrétní fotony. K příjemci tak musí fyzicky dorazit přesně ten polarizovaný foton, který odesílatel vyslal. To v praxi znamená, že je vyloučeno použití jakékoli formy posílení signálu, na kterou jsme zvyklí z klasických komunikačních technologií. Přenosy po kvantovém komunikačním kanále jsou tak na dnešní poměry velice pomalé (řádově tisíce bitů za sekundu) a neprak-

tické vzhledem k objemům dat, které je potřeba bezpečně přenášet. Výzkum v oblasti kvantových technologií jde však stále kupředu a v budoucnu by tak s rychlostí přenosu dat po kvantovém kanále mohly vypomoci dokonalejší světelné zdroje a detektory fotonů či optická vlákna s nižším rušením.

V současné chvíli jsou již komerční řešení pro kvantovou distribuci klíčů nabízena několika společnostmi z různých koutů světa. Zájem o kvantové kryptosystémy jeví především bankovní společnosti, vlády a armády. Moderní technologický výzkum v oblasti kvantové kryptografie se zabývá zejména přenosem klíčů na velké vzdálenosti, a to ideálně vzduchem, za pomoci satelitů, tedy bez potřeby optického vlákna. Experimentálně se již podařilo úspěšně bezdrátově přenést kvantový klíč na vzdálenost 144 km [69] a také z letadla letícího rychlostí 290 km/h na zem [52].

Závěr

Jakkoli neuvěřitelné a šílené se zpočátku zdály myšlenky kvantové fyziky i nejšpičkovějším vědcům své doby, za méně než století jsme jako lidstvo dokázali nejen popsat celou řadu principů kvantové fyziky a experimentálně ověřit jejich platnost, ale dokonce pro ně nalézt praktické využití. To, zda se kdokoli z nás skutečně dožije doby, kdy budou využití kvantových počítačů a komunikace pomocí kvantových kryptografických protokolů součástí našeho každodenního života, zůstává ve hvězdách. Jisté ovšem je, že se pokrok v této oblasti nezastavuje a s trochou štěstí bychom snad měli mít možnost brzy běžně využívat technologie na bázi kvantové fyziky alespoň k experimentálním, ne-li praktickým, účelům.

Největší překážkou je v tomto směru pořizovací cena kvantové aparatury. I to je důvod, proč mnoho lidí spíše než na kvantové technologie sází na jejich klasické alternativy. V oblasti kryptografie takovou alternativu představuje *postkvantová kryptografie*. Ta totiž slibuje bezpečnost vzdorující výpočetnímu potenciálu kvantových počítačů i bez potřeby využití kvantových fyzikálních principů ve svých protokolech. Matematické problémy, na kterých jsou modelovány postkvantové kryptosystémy totiž, jak se zdá, nebudou snadno řešitelné ani kvantovým počítačem, tudíž pro ně jeho potenciální vznik nepředstavuje hrozbu. Příklady algoritmů postkvantové kryptografie jsou asymetrický šifrovací systém *NTRU* [70] založený na matematických *mřížích*, algoritmus *RLWE-KEX* [71] či *supersingulární eliptické kryptosystémy* [72]. I kdyby se ovšem kvantové kryptografické protokoly v jejich současné podobě nestaly přímo novým bezpečnostním standardem, poznatky vzešlé z výzkumů, do nichž vědci v této oblasti vložili své úsilí budou jistě v nějaké formě vědě i nadále užitečné.

V této práci byly představeny vybrané protokoly kvantové kryptografie a důvody, které vedly k jejich vzniku i fyzikální principy jež zaručují jejich nepodmíněnou teoretickou bezpečnost. V programovacím jazyce Python byla pak za pomoci simulátoru otevřených kvantových systémů *QuTip* [2] implementována simulace protokolu *BB84*, která umožňuje simulovat klíčovou výměnu popsanou v sekci 4.1.3 jak v přítomnosti, tak v nepřítomnosti útočníka na kvantovém komunikačním kanále. Zdrojový kód simulace je dostupný v online repozitáři [73].

Literatura

1. BENNETT, Charles H.; BRASSARD, Gilles. Quantum cryptography: Public key distribution and coin tossing. *Theoretical Computer Science*. 2014, roč. 560, s. 7–11. ISSN 0304-3975. Dostupné z DOI: https://doi.org/10.1016/j.tcs.2014.05.025.
2. JOHANSSON, J.R.; NATION, P.D.; NORI, Franco. QuTiP: An open-source Python framework for the dynamics of open quantum systems. *Computer Physics Communications*. 2012, roč. 183, č. 8, s. 1760–1772. ISSN 0010-4655. Dostupné z DOI: https://doi.org/10.1016/j.cpc.2012.02.021.
3. PIPER, F. C.; MURPHY, Sean. *Kryptografie*. Praha: Dokořán, 2006. ISBN 80-7363-074-5.
4. DOSEDĚL, Tomáš. *Počítačová bezpečnost a ochrana dat*. Brno: Computer Press, 2004. ISBN 80-251-0106-1.
5. SINGH, Simon. *Kniha kódů a šifer*. Praha: Dokořán, 2003. ISBN 80-86569-18-7.
6. JAŠEK, Roman. *Informační a datová bezpečnost*. Zlín: Univerzita Tomáše Bati ve Zlíně, 2006. ISBN 80-7318-456-7.
7. Advanced Encryption Standard (AES). *Federal Information Processing Standards*. 2001, roč. 197. Dostupné z DOI: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf.
8. OULEHLA, Milan; JAŠEK, Roman. *Moderní kryptografie*. Praha: IFP Publishing s.r.o., 2017. ISBN 978-80-87383-67-4.

9. RIVEST, R. L.; SHAMIR, A.; ADLEMAN, L. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*. 1978.

10. ARORA, Mohit. *How secure is AES against brute force attacks?* [Online]. 2012 [cit. 2021-02-11]. Dostupné z: https://www.eetimes.com/how-secure-is-aes-against-brute-force-attacks/#.

11. VERNAM, Gilbert Sandford. *Secret signaling system*. 1919. US Patent US1,310,719.

12. KISH, Laszlo B.; GRANQVIST, Claes-Goran. On the security of the Kirchhoff-law-Johnson-noise (KLJN) communicator. *CoRR*. 2013, roč. 13. Dostupné také z: http://arxiv.org/abs/1309.4112.

13. VADAI, G.; MINGESZ, R.; GINGL, Z. Generalized Kirchhoff-Law-Johnson-Noise (KLJN) secure key exchange system using arbitrary resistors. *Sci Rep*. 2015, roč. 5. Dostupné z DOI: https://doi.org/10.1038/srep13653.

14. HAO, Feng. Kish's key exchange scheme is insecure. *Information Security, IEE Proceedings*. Ledna 2007, roč. 153, s. 141–142. Dostupné z DOI: 10.1049/ip-ifs:20060068.

15. BENNETT, Charles H.; RIEDEL, C. Jess. *On the security of key distribution based on Johnson-Nyquist noise*. 2013. Dostupné z arXiv: 1303.7435 [quant-ph].

16. GUNN, Lachlan J; ALLISON, Andrew; ABBOTT, Derek. A new transient attack on the Kish key distribution system. *IEEE Access*. 2015, roč. 3, s. 1640–1648.

17. BENSON, Robert L. *The Venona Story*. Center for Cryptologic History, 2004. Dostupné také z: https://www.nsa.gov/News-Features/Declassified-Documents/Venona/.

18. ERSKINE, Ralph. Enigma's Security: What the Germans Really Knew. *Action this Day*. 2001, s. 370–386.

19. HUANG, Dazu; CHEN, Zhigang; GUO, Ying; HO LEE, Moon. Quantum Secure Direct Communication Based on Chaos with Authentication. *Journal of the Physical Society of Japan*. 2007, roč. 76, č. 12. Dostupné z DOI: 10.1143/JPSJ.76.124001.

20. ZHANG, Zhan-jun; LIU, Jun; WANG, Dong; SHI, Shou-hua. Comment on "Quantum direct communication with authentication". *Physical Review A*. 2007, roč. 75, č. 2. Dostupné z DOI: 10.1103/physreva.75.026301.

21. ALLÉAUME, R.; BRANCIARD, C.; BOUDA, J.; DEBUISSCHERT, T.; DIANATI, M.; GISIN, N.; GODFREY, M.; GRANGIER, P.; LÄNGER, T.; LÜTKENHAUS, N.; AL., et. Using quantum key distribution for cryptographic purposes: A survey. *Theoretical Computer Science*. 2014, roč. 560, s. 62–81. Dostupné z DOI: 10.1016/j.tcs.2014.09.018.

22. FORMÁNEK, Jiří. *Úvod do kvantové teorie I., II.* Academia, 2004. Advanced topics in computer science series. ISBN 80-200-1176-5.

23. GRUSKA, Jozef. *Quantum Computing*. McGraw-Hill, 1999. Advanced topics in computer science series. ISBN 9780077095031.

24. *Teorie a perspektiva kvantových počítačů* [online]. 2001 [cit. 2021-03-03]. Dostupné z: https://www2.karlin.mff.cuni.cz/~holub/soubory/qc/qc.html.

25. DIRAC, Paul Adrien Maurice. *The principles of quantum mechanics*. 4. vyd. Oxford University Press, 1958.

26. EVERETT, Hugh; DEWITT, Bryce Seligman; GRAHAM, Neill. *The many-worlds interpretation of quantum mechanics*. Princeton Univ. Press, 1973. Princeton series in physics. Dostupné také z: http://cds.cern.ch/record/426557.

27. HEISENBERG, Werner K. Uber den anschaulichen Inhalt der quanten theoretischen Kinematik und Mechanik. *Zeitschrift für Physik*. 1927, roč. 43, s. 172–198.

28. COLES, Patrick J.; KANIEWSKI, Jedrzej; WEHNER, Stephanie. Equivalence of wave–particle duality to entropic uncertainty. *Nature Communications*. 2014, roč. 5. Dostupné z DOI: 10.1038/ncomms6814.

29. KLYSHKO, D. N.; PENIN, A. N.; POLKOVNIKOV, B. F. Parametric Luminescence and Light Scattering by Polaritons. *Soviet Journal of Experimental and Theoretical Physics Letters*. Ledna 1970, roč. 11, s. 5. Dostupné také z: https://ui.adsabs.harvard.edu/abs/1970JETPL..11....5K.

30. CHOI, Charles Q. *Quantum Record! 3,000 Atoms Entangled in Bizarre State* [online]. 2015 [cit. 2020-05-11]. Dostupné z: https://www.livescience.com/50280-record-3000-atoms-entangled.html.

31. KULHÁNEK, Petr. Kvantová provázanost mnohačásticového systému. *Aldebaran Bulletin*. 25. kvetna 2018, roč. 16, č. 16. ISSN 1214-1674.

32. WOOTTERS, William K; ZUREK, Wojciech H. A single quantum cannot be cloned. *Nature*. 1982, roč. 299, č. 5886, s. 802–803.

33. DIEKS, D. Communication by EPR devices. *Physics Letters A*. 1982, roč. 92, č. 6, s. 271–272. ISSN 0375-9601. Dostupné z DOI: https://doi.org/10.1016/0375-9601(82)90084-6.

34. EBERHARD, P.H.; ROSS, R.R. Quantum field theory cannot provide faster-than-light communication. *Foundations of Physics Letters*. 1989, roč. 2, s. 127–149. Dostupné z DOI: 10.1007/BF00696109.

35. REICHL, Jaroslav; VŠETIČKA, Martin. *Encyklopedie fyziky* [online] [cit. 2021-03-23]. Dostupné z: http://fyzika.jreichl.com.

36. RIOUX, Frank. *The Three-Polarizer Paradox* [online]. College of Saint Benedict/Saint John's University, 2020 [cit. 2020-08-15]. Dostupné z: https://chem.libretexts.org/@go/page/140336.

37. FEYNMAN, Richard P. Simulating physics with computers. *International Journal of Theoretical Physics*. 1982, roč. 21, č. 6-7, s. 467–488. ISSN 0020-7748. Dostupné z DOI: 10.1007/bf02650179.

38. NIELSEN, Michael A; CHUANG, Isaac. *Quantum computation and quantum information*. American Association of Physics Teachers, 2002.

39. SCHUMACHER, Benjamin. Quantum coding. *Phys. Rev. A*. Dubna 1995, roč. 51, s. 2738–2747. Dostupné z DOI: 10.1103/PhysRevA.51.2738.

40. FEYNMAN, Richard P. Quantum mechanical computers. *Foundations of physics*. 1986, roč. 16, č. 6, s. 507–531.

41. BARENCO, Adriano; BENNETT, Charles H; CLEVE, Richard; DI-VINCENZO, David P; MARGOLUS, Norman; SHOR, Peter; SLEATOR, Tycho; SMOLIN, John A; WEINFURTER, Harald. Elementary gates for quantum computation. *Physical review A*. 1995, roč. 52, č. 5.

42. *Operations glossary – IBM Quantum* [online]. 2016 [cit. 2021-05-05]. Dostupné z: https://quantum-computing.ibm.com/composer/docs/iqx/operations_glossary.

43. ZUREK, Wojciech H. Quantum reversibility is relative, or does a quantum measurement reset initial conditions? *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*. 2018, roč. 376, č. 2123, s. 20170315.

44. VAN GAEL, Jurgen. *The Role of Interference and Entanglement in Quantum Computing*. 2005. Dis. Univeristy of Wisconsin-Madison.

45. SHOR, Peter W. Algorithms for quantum computation: discrete logarithms and factoring. In: *Proceedings 35th annual symposium on foundations of computer science*. 1994, s. 124–134.

46. LENSTRA, Arjen K; LENSTRA, Hendrik W; MANASSE, Mark S; POLLARD, John M. The number field sieve. In: *The development of the number field sieve*. Springer, 1993, s. 11–42.

47. GIDNEY, Craig. *Shor's Quantum Factoring Algorithm* [online]. 2017 [cit. 2021-05-18]. Dostupné z: https://algassert.com/post/1718.

48. COPPERSMITH, Don. An approximate Fourier transform useful in quantum factoring. *arXiv preprint quant-ph/0201067*. 2002.

49. ZYGA, Lisa. *New largest number factored on a quantum device is 56,153* [online]. 2014-11-28 [cit. 2021-05-18]. Dostupné z: https://phys.org/news/2014-11-largest-factored-quantum-device.html.

50. ARUTE, Frank; ARYA, Kunal; BABBUSH, Ryan; BACON, Dave; BARDIN, Joseph C; BARENDS, Rami; BISWAS, Rupak; BOIXO, Sergio; BRANDAO, Fernando GSL; BUELL, David A et al. Quantum supremacy using a programmable superconducting processor. *Nature*. 2019, roč. 574, č. 7779, s. 505–510.

51. GARISTO, Daniel. *Light-Based Quantum Computer Exceeds Fastest Classical Supercomputers* [online]. 2020-12-03 [cit. 2021-05-19]. Dostupné z: https://www.scientificamerican.com/article/light-based-quantum-computer-exceeds-fastest-classical-supercomputers/.

52. NAUERTH, Sebastian; MOLL, Florian; RAU, Markus; FUCHS, Christian; HORWATH, Joachim; FRICK, Stefan; WEINFURTER, Harald. Air-to-ground quantum communication. *Nature Photonics*. 2013, roč. 7, č. 5, s. 382–386.

53. GILBERT, Gerald; HAMRICK, Michael. Practical quantum cryptography: A comprehensive analysis (part one). *arXiv preprint quant-ph/0009027*. 2000.

54. WIESNER, Stephen. Conjugate Coding. *SIGACT News*. 1983, roč. 15, č. 1, s. 78–88. ISSN 0163-5700. Dostupné z DOI: 10.1145/1008908.1008920.

55. BRASSARD, Gilles; SALVAIL, Louis. Secret-Key Reconciliation by Public Discussion. In: HELLESETH, Tor (ed.). *Advances in Cryptology, EUROCRYPT '93*. Berlin, Heidelberg: Springer Berlin Heidelberg, 1994, s. 410–423.

56. BUTTLER, William T; LAMOREAUX, Steven K; TORGERSON, Justin R; NICKEL, GH; DONAHUE, CH; PETERSON, Charles G. Fast, efficient error reconciliation for quantum cryptography. *Physical Review A*. 2003, roč. 67, č. 5, s. 052303.

57. ELKOUSS, David; MARTINEZ-MATEO, Jesus; MARTIN, Vicente. *Information Reconciliation for Quantum Key Distribution*. 2011. Dostupné z arXiv: 1007.1616.

58. NIEMIEC, Marcin. Error correction in quantum cryptography based on artificial neural networks. *Quantum Information Processing*. 2019, roč. 18, č. 6, s. 1–18.

59. MEHIC, Miralem; NIEMIEC, Marcin; SILJAK, Harun; VOZNAK, Miroslav. *Reversible Computation: Extending Horizons of Computing: Selected Results of the COST Action IC1405*. Error Reconciliation in Quantum Key Distribution Protocols. Cham: Springer International Publishing, 2020. ISBN 978-3-030-47361-7. Dostupné z DOI: 10.1007/978-3-030-47361-7_11.

60. BENNETT, C.H.; BRASSARD, G.; CREPEAU, C.; MAURER, U.M. Generalized privacy amplification. *IEEE Transactions on Information Theory*. 1995, roč. 41, č. 6, s. 1915–1923. Dostupné z DOI: 10.1109/18.476316.

61. SERGIENKO, Alexander V. *Quantum communications and cryptography*. CRC press, 2006.

62. EKERT, Artur K. Quantum cryptography based on Bell's theorem. *Phys. Rev. Lett.* 1991, roč. 67, s. 661–663. Dostupné z DOI: 10.1103/PhysRevLett.67.661.

63. BRASSARD, Gilles; LÜTKENHAUS, Norbert; MOR, Tal; SANDERS, Barry C. Limitations on Practical Quantum Cryptography. *Physical Review Letters*. 2000, roč. 85, č. 6, s. 1330–1333. ISSN 1079-7114. Dostupné z DOI: 10.1103/physrevlett.85.1330.

64. SCARANI, Valerio; ACÍN, Antonio; RIBORDY, Grégoire; GISIN, Nicolas. Quantum Cryptography Protocols Robust against Photon Number Splitting Attacks for Weak Laser Pulse Implementations. *Physical Review Letters*. 2004, roč. 92, č. 5. ISSN 1079-7114. Dostupné z DOI: 10.1103/physrevlett.92.057901.

65. LO, Hoi-Kwong; MA, Xiongfeng; CHEN, Kai. Decoy state quantum key distribution. *Physical review letters*. 2005, roč. 94, č. 23.

66. SERNA, Eduin H. *Quantum Key Distribution Protocol with Private-Public Key*. 2012. Dostupné z arXiv: 0908.2146 [quant-ph].

67. NAGY, Marius; NAGY, Naya. Quantum-based secure communications with no prior key distribution. *Soft Computing*. 2016, roč. 20, s. 87–101. Dostupné z DOI: 10.1007/s00500-014-1555-7.

68. HILLERY, Mark; BUŽEK, Vladimír; BERTHIAUME, André. Quantum secret sharing. *Physical Review A*. 1999, roč. 59, č. 3, s. 1829–1834. ISSN 1094-1622. Dostupné z DOI: 10.1103/physreva.59.1829.

69. SCHMITT-MANDERBACH, T.; WEIER, H.; FÜRST, M.; URSIN, R.; TIEFENBACHER, F.; SCHEIDL, Th.; PERDIGUES, J.; SODNIK, Z.; KURTSIEFER, Ch.; RARITY, J.; ZEILINGER, A.; WEINFURTER, H. Experimental Demonstration of Free-Space Decoy-State Quantum Key Distribution over 144 km. In: *CLEO/Europe and IQEC 2007 Conference Digest*. Optical Society of America, 2007. Dostupné z DOI: 10.1364/IQEC.2007.IC6_1.

70. HOFFSTEIN, Jeffrey; PIPHER, Jill; SILVERMAN, Joseph H. NTRU: A ring-based public key cryptosystem. In: Springer Berlin Heidelberg, 1998, s. 267–288. Dostupné z DOI: 10.1007/BFb0054868.

71. *On Lattices, Learning with Errors,Random Linear Codes, and Cryptography*. 2004.

72. JAO, David; DE FEO, Luca. Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies. In: *International Workshop on Post-Quantum Cryptography*. 2011, s. 19–34.

73. *Simulace protokolu BB84 v jazyce Python s užitím simulátoru kvantových systémů QuTip*. Dostupné také z: https://github.com/lea318/BB84.