FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Zadání bakalářské práce

Název:	Protokoly pro kvantový přenos klíče
Student:	Michael Wagner
Vedoucí:	Ing. Ivo Petr, Ph.D.
Studijní program:	Informatika
Obor / specializace:	Bezpečnost a informační technologie
Katedra:	Katedra počítačových systémů
Platnost zadání:	do konce letního semestru 2023/2024

Pokyny pro vypracování

Pro navázání zabezpečeného spojení mezi dvěma komunikujícími stranami je zásadním problémem ustanovení společného klíče. Protokoly pro kvantový přenos klíče zakládají svoji bezpečnost na principech kvantové mechaniky a slibují také možnost detekce případného odposlechu kanálu. Práce se zaměřuje na studium známých protokolů pro kvantový přenos klíče a vytvoření ukázkových materiálů umožňujících demonstraci vlastností těchto protokolů.

- Seznamte se se základními principy využívanými v kvantové komunikaci.
- Popište principy vybraných protokolů pro kvantový přenos klíče (např. BB84, B92, E91), možnosti detekce odposlechu a kapacitu kanálu v těchto protokolech.
- Pomocí vhodně zvolených nástrojů (např. Qiskit) vytvořte ukázkové simulace přenosu klíče těmito protokoly.

Elektronicky schválil/a prof. Ing. Pavel Tvrdík, CSc. dne 14. ledna 2023 v Praze.

Bakalářská práce

PROTOKOLY PRO KVANTOVÝ PŘENOS KLÍČE

Michael Wagner

Fakulta informačních technologií
Katedra informační bezpečnosti
Vedoucí: Ing. Ivo Petr, Ph.D.
11. května 2023

Obsah

Seznam obrázků

Seznam tabulek

Seznam výpisů kódu

Rád bych poděkoval své rodině za bezmeznou podporu napříč celým studiem. Rovněž mé poděkování za odborné vedení, věnovaný čas a mnoho cenných rad patří Ing. Ivu Petrovi, Ph.D., bez něhož by tato práce nemohla vzniknout.

Prohlášení

Prohlašuji, že jsem předloženou práci vypracoval samostatně a že jsem uvedl veškeré použité informační zdroje v souladu s Metodickým pokynem o dodržování etických principů při přípravě vysokoškolských závěrečných prací.

Beru na vědomí, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., autorského zákona, ve znění pozdějších předpisů, zejména skutečnost, že České vysoké učení technické v Praze má právo na uzavření licenční smlouvy o užití této práce jako školního díla podle § 60 odst. 1 citovaného zákona.

V Praze dne 11. května 2023 .....

Abstrakt

V práci se zaměřuji na problematiku bezpečné distribuce klíče mezi komunikačními stranami s využitím zákonů kvantové mechaniky. Tento přístup umožňuje stranám kromě samotné distribuce klíče i metody, jak detekovat odposlech třetí strany na kvantovém kanále. V práci představuji základní koncepty kvantového počítání a protokoly BB84, B92 a E91, které kvantovou distribuci klíče umožňují. Ve vytvořeném řešení poskytuji způsob, jak se vypořádat s chybovým kvantovým kanálem pomocí lineárních kódů. U každého protokolu uvádím způsob možného odposlechu i prostředky, jak lze odposlech detekovat. Na základě zjištěných údajů vytvářím srovnání protokolů na komunikační a bezpečnostní úrovni. Na závěr práce tato srovnání potvrzuji pomocí výsledků simulací protokolů.

Klíčová slova kvantový přenos klíče, problém distribuce klíče, bezpečná komunikace, kvantový kanál, detekce odposlechu, Qiskit

Abstract

In my thesis, I focus on the issue of secure key distribution between communicating parties using the laws of quantum mechanics. This approach allows parties in addition to key distribution, the methods to detect eavesdropping by a third party on a quantum channel. In my thesis, I present the basic concepts of quantum computation and the BB84, B92 and E91 protocols that enable quantum key distribution. In the created solution, I provide a way to deal with the noisy quantum channel using linear codes. For each protocol, I list the method of possible eavesdropping and the means by which eavesdropping can be detected. Based on the collected data, I create a comparison of protocols on communication and security level. At the end of the thesis, I confirm these comparisons using the results from protocols simulation.

Keywords quantum key distribution, key distribution problem, secure communication, quantum channel, eavesdropping detection, Qiskit

Seznam zkratek

QKD	Kvantový přenos klíče
PQC	Post–kvantová kryptografie
SDK	Sada nástrojů pro vývoj softwaru

Úvod

Kvantová informatika je obor kombinující kvantovou mechaniku, teorii informace a klasickou informatiku za účelem pochopení a vývoje nových technologií, které využívají jedinečné vlastnosti kvantové mechaniky pro zpracování, ukládání a přenos informací. Umožňuje nám nejen hledání nových způsobů jak se vypořádat s problémy, u kterých nám v klasické informatice chybí efektivní a plně spolehlivá řešení, ale také vrhnout nové světlo na základní otázky kvantové mechaniky a povahu světa a informací jako takových.

S příchodem kvantových počítačů přibývá mnoho otázek v oblasti informatiky, zejména v oboru bezpečnosti a bezpečné komunikace. Mezi takové problémy patří distribuce klíčů, která je nezbytná pro symetrickou kryptografii. Distribuce klíčů umožňuje účastníkům komunikace společně sdílet tajný klíč, který je použit na šifrování a dešifrování jejich zpráv.

Aktuální řešení jsou založena na problémech faktorizace nebo diskrétního logaritmu, například se jedná o algoritmus RSA nebo algoritmy založené na principu eliptických křivek. Tyto zmíněné algoritmy nejsou odolné vůči Shorově algoritmu, který lze realizovat na kvantovém počítači. I když nemáme doposud dostatečně silný a spolehlivý kvantový počítač, abychom ohrozili naše aktuální zabezpečení, s myšlenkou na budoucí ohrožení se pracuje na nových klasických algoritmech, které jsou odolné i proti výkonosti kvantových počítačů. Tato skupina klasických algoritmů se označuje jako Post–kvantová kryptografie (PQC). V roce 2022 Národní institut standardů a technologie v USA oznámil výběr prvních standardizovaných algoritmů patřící do této skupiny. Kromě nových klasických algortimů existují i kvantová řešení jak k problému distribuce klíče přistupovat.

Kvantová distribuce klíče (QKD) je metoda bezpečné komunikace, která implementuje protokol, pomocí kterého mohou být sdíleny bity tajného klíče přes veřejný kanál mezi dvěma stranami. Bezpečnost výsledného klíče je zaručena vlastnostmi kvantové mechaniky, a proto je podmíněna pouze tím, že základní fyzikální zákony jsou správné. Důležitou a jedinečnou vlastností kvantové distribuce klíčů je schopnost dvou komunikujících uživatelů detekovat přítomnost jakékoli třetí strany, která se snaží získat znalost klíče. Bohužel, i když je matematický koncept na kterém je možnost detekce odposlechu založena teoreticky bezpečný, stále se v dnešní době setkáváme s problémy samotné realizace přenosu. Dosavadní realizace se setkávají především s problémem přenosu na delší vzdálenost a vysoké chybovosti, aktuálně se tedy pohybujeme na vzdálenosti přenosu ve stovkách kilometrů a chybovostí v jednotkách procent a více.

Cílem teoretické části práce je vybudovat základní principy využití kvantového počítání v oboru informační bezpečnosti, především poskytnout přehled a využití různých typů protokolů pro kvantový přenos klíče. Mimo jiné, se práce kromě samotného přenosu klíče také zabývá detekcí možného odposlechu na komunikačním kanále při jeho vytváření.

Praktická část práce se zaměřuje na samotnou implementaci kvantových protokolů pro přenos klíče. Kromě samotného přenosu klíče jsou součástí implementace metody, jakými lze poznat přítomnost odposlouchávajícího na kanále.

Kapitola 1
Základní koncepty

V této kapitole poskytneme čtenáři základní vhled do principů a pojmů kvantové informatiky. Vhodným jazykem pro popis kvantového světa je lineární algebra, a proto předpokládáme v tomto textu její základní znalost. Tato kapitola poskytuje základní informace, definice a koncepty a vychází z knihy [1].

▶ Notace 1.1. V textu budeme používat tzv. Bra-ketový formalismus, který se běžně využívá pro zápis vektorů v kvantové mechanice a kvantovém počítání. Vektory budeme zapisovat $|\psi\rangle$ a o označovat jménem *kety*, jejich komplexní sdružení a transpozici zapisovat $\langle\phi|$ a nazývat *bra*.

▶ **Definice 1.2** (Skalární součin)**.** *Nechť je V vektorový prostor nad $\mathbb{C}$. Zobrazení $\langle\cdot,\cdot\rangle : V\times V \to \mathbb{C}$ nazýváme skalární součin, platí-li pro všechny vektory $\mathbf{x},\mathbf{y},\mathbf{z} \in V$ a každý skalár $\alpha,\beta \in \mathbb{C}$ následující axiomy:*

$$\langle \mathbf{x}, \alpha\mathbf{y} + \beta\mathbf{z}\rangle = \alpha\langle \mathbf{x},\mathbf{y}\rangle + \beta\langle \mathbf{x},\mathbf{z}\rangle, \tag{1.1}$$

$$\langle \mathbf{x},\mathbf{y}\rangle = \langle \mathbf{y},\mathbf{x}\rangle^*, \tag{1.2}$$

$$\langle \mathbf{x},\mathbf{x}\rangle \geq 0 \text{ a } \langle \mathbf{x},\mathbf{x}\rangle = 0 \text{ pouze pokud } \mathbf{x} = \mathbf{0}, \tag{1.3}$$

*kde * značí komplexní sdružení a $\mathbf{0}$ značí nulový vektor.*

▶ **Příklad 1.3.** Pro konečnědimenzionální vektorový prostor V můžeme skalární součin vektorů $|\psi\rangle$ a $|\phi\rangle$ popsat maticovým násobením jako

$$\langle |\psi\rangle, |\phi\rangle\rangle =: \langle\psi|\phi\rangle = \begin{pmatrix}\psi_1^* & \psi_2^* & \dots & \psi_N^*\end{pmatrix} \cdot \begin{pmatrix}\phi_1\\ \phi_2\\ \vdots\\ \phi_N\end{pmatrix}, \tag{1.4}$$

kde $\langle\psi|$ je *bra* a $|\phi\rangle$ je *ket*. Jejich skalární součin $\langle\psi|\phi\rangle$ nazýváme *bra-ket*.

► **Příklad 1.4.** Pro konečnědimenzionální vektorový prostor V můžeme vnější součin vektorů $|\psi\rangle$ a $|\phi\rangle$ popsat maticovým násobením jako

$$|\psi\rangle\langle\phi| = \begin{pmatrix} \psi_1 \\ \psi_2 \\ \vdots \\ \psi_N \end{pmatrix} \cdot \begin{pmatrix} \phi_1^* & \phi_2^* & \dots & \phi_N^* \end{pmatrix}, \tag{1.5}$$

a říkáme, že vnější součin definuje operátor na V.

1.1 Kvantový bit

Stav kvantového systému je dán stavovým vektorem, prvkem Hilbertova prostoru $\mathcal{H}$ nad tělesem komplexních čísel $\mathbb{C}$. I když v kvantové mechanice setkáváme spíše s nekonečnědimenzionálním prostorem, v kvantovém počítání se pohybujeme pouze v prostorech konečné dimenze.

Základním kamenem kvantové informatiky je koncept kvantového bitu, zvaný *qubit*, který je kvantovou obdobou klasického bitu. Stejně jako klasický bit má stav, a to pouze 0 nebo 1, náš qubit má svůj stav také. Abstraktně je qubit vektorem dvoudimenzionálního Hilbertova prostoru $\mathcal{H} = \mathbb{C}^2$, ale na rozdíl od klasického bitu, jeden qubit může být v lineární kombinaci dvou stavů. Kvantový systém se však může skládat z více kvantových stavů, čímž vznikne nový kvantový systém, tento jev označujeme jako *kvantová superpozice*. Pokud v $\mathcal{H}$ definujeme ortonormální bázi pomocí vektorů $|0\rangle$ a $|1\rangle$, definované

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \tag{1.6}$$

pak libovolný vektor z $\mathcal{H}$ lze vyjádřit jako jejich lineární kombinaci

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle, \quad \alpha, \beta \in \mathbb{C}. \tag{1.7}$$

Koeficienty α, β nazýváme amplitudy.

Bornovo pravidlo nám říká, že je pravděpodobnost přechodu stavu $|\psi\rangle$ do stavu $|0\rangle$, resp. do stavu $|1\rangle$, vyjádřena jako

$$P_{|0\rangle}(|\psi\rangle) = |\alpha|^2, \quad P_{|0\rangle}(|\psi\rangle) = |\beta|^2, \tag{1.8}$$

kde obecně značíme $P_{|\phi\rangle}(|\psi\rangle)$ jako pravděpodobnost přechodu ze stavu $|\phi\rangle$ do stavu $|\psi\rangle$. Tento vztah poté implikuje, že součet pravděpodobností všech možných jevů musí být roven 1, pro jeden qubit $|\psi\rangle$ tedy platí $|\alpha|^2 + |\beta|^2 = 1$, stavový vektor proto musí být normalizovaný na 1. Více o měření obecného kvantového systému se dozvíme v podkapitole 1.3.3.

Další důležitou vlastností qubitu je fáze. Globální fáze je pouze artefakt matematického aparátu, který používáme. Pokud se stavy liší pouze svou globální fází, představují stejný fyzikální systém, neboť je žádným měřením nelze rozlišit. Můžeme tedy říct, že globální fázi nelze zpozorovat.

► **Příklad 1.5.** Mějme dva qubity $|\psi\rangle$ a $|\phi\rangle$, pro $\theta \in \mathbb{R}, \varphi \in \mathbb{R}, \gamma \in \mathbb{R}$, které jsou ve stavech

$$|\psi\rangle = e^{i\gamma}\left(\cos\frac{\theta}{2}|0\rangle + e^{i\phi}\sin\frac{\theta}{2}|1\rangle\right), \qquad \theta \in \langle 0, \pi), \ \phi \in \langle 0, 2\pi). \tag{1.9}$$

$$|\phi\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\phi}\sin\frac{\theta}{2}|1\rangle, \qquad \theta \in \langle 0, \pi), \ \phi \in \langle 0, 2\pi) \tag{1.10}$$

U stavu $|\psi\rangle$ si můžeme povšimnout násobení číslem $e^{i\gamma}$, toto číslo je ale globální fází, a proto stavy $|\psi\rangle$ a $|\phi\rangle$ představují stejný kvantový systém.

Pokud se ale systémy liší ve své relativní fázi, představují pak jiný stav kvantového systému.

▶ **Příklad 1.6.** Vektory $|+\rangle, |-\rangle$ určené

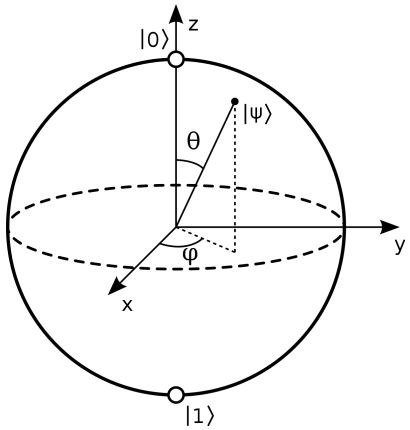
$$|+\rangle = \left(\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle\right), \qquad |-\rangle = \left(\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle\right), \tag{1.11}$$

se liší ve své relativní fázi, tudíž jejich stav je jiný a pomocí vhodně zvolené báze při meření je lze odlišit. Například měřením v bázi $(|0\rangle, |1\rangle)$ stavy nerozlišíme, ale rozlišíme je měřením v bázi $(|+\rangle, |-\rangle)$.

Qubit lze také interpretovat geometricky při použití parametrizace pomocí, $\theta \in \mathbb{R}, \phi \in \mathbb{R}$, jako

$$|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\phi}\sin\frac{\theta}{2}|1\rangle, \qquad \theta \in \langle 0, \pi), \ \phi \in \langle 0, 2\pi). \tag{1.12}$$

Pomocí geometrického vyjádření lze qubit znázornit na 3-dimenzionální sféře, tzv. Blochově sféře. Za zmínku stojí, že Blochova sféra pracuje pouze s jedním qubitem, systémy s mnoha qubity nelze na sféře znázornit.



■ **Obrázek 1.1** Blochova sféra reprezentující jeden qubit [1]

1.2 Kvantový registr

Kvantový registr označuje systém více qubitů, který je tvořen pomocí tenzorového součinu Hilbertových prostorů jednotlivých qubitů.

▶ **Definice 1.7** (Kroneckerův součin)**.** *je typ tenzorového součinu dvou matic libovolných rozměrů. Mějme matice* $\mathbf{A}^{m\times n}$ *a* $\mathbf{B}^{p\times q}$*, pak výsledná matice* $\mathbf{C}^{mp\times nq}$ *Knockerova součinu matic* $\mathbf{A}$*,* $\mathbf{B}$ *je maticově reprezentována jako*

$$\mathbf{C} = \mathbf{A}\otimes\mathbf{B} = \begin{pmatrix} a_{11}B & a_{12}B & \cdots & a_{1n}B \\ a_{21}B & a_{22}B & \cdots & a_{2n}B \\ \vdots & \vdots & \vdots & \vdots \\ a_{m1}B & a_{m2}B & \cdots & a_{mn}B \end{pmatrix}. \tag{1.13}$$

V textu dále budeme používat pouze obecné označení tenzorový součin a budeme ho používat pro vektory i zobrazení.

▶ Notace 1.8. Tenzorový součin ketů lze zapisovat různými způsoby, například $|0\rangle \otimes |1\rangle$, pouze $|0\rangle\,|1\rangle$ nebo nejčastěji $|01\rangle$. V textu budeme využívat všechny tři způsoby z důvodu přehlednosti v konkrétních případech.

▶ **Příklad 1.9.** Tenzorový součin dvou qubitů ve stavech $|0\rangle$ a $|1\rangle$ odpovídá

$$|01\rangle = |0\rangle \otimes |1\rangle = \begin{pmatrix}1\\0\end{pmatrix} \otimes \begin{pmatrix}0\\1\end{pmatrix} = \begin{pmatrix}1\cdot 0\\1\cdot 1\\0\cdot 0\\0\cdot 1\end{pmatrix}. \tag{1.14}$$

Pokud vezmeme dvouqubitový kvantový registr dostáváme tenzorový součin dvou Hilbertových prostorů

$$\mathcal{H} \otimes \mathcal{H} = \mathcal{H}^{\otimes 2} = \mathcal{C}^2 \otimes \mathcal{C}^2. \tag{1.15}$$

Pro standardní bázi tenzorového součinu $\mathcal{H}^{\otimes 2}$ používáme zápis

$$|00\rangle = \begin{pmatrix}1\\0\\0\\0\end{pmatrix}, |01\rangle = \begin{pmatrix}0\\1\\0\\0\end{pmatrix}, |10\rangle = \begin{pmatrix}0\\0\\1\\0\end{pmatrix}, |11\rangle = \begin{pmatrix}0\\0\\0\\1\end{pmatrix}. \tag{1.16}$$

Stav systému dvou qubitů bude tedy obecně dán vektorem

$$|\psi\rangle = a\,|00\rangle + b\,|01\rangle + c\,|10\rangle + d\,|11\rangle\,, \quad a,b,c,d \in \mathbb{C}. \tag{1.17}$$

Prostor $\mathcal{H}^{\otimes n}$ pro libovolné $n \in \mathbb{N}$ nazýváme n-qubitový kvantový registr s dimenzí rovnou 2^n.

▶ Notace 1.10. Standardně zapisujeme standardní báze stavu systému qubitů pomocí binárního rozvoje. Nechť máme $x \in \{0,\dots,2^{n-1}\}$ pro zvolené $n \in \mathbb{N}$, zápis standardní báze systému qubitů $|x_0x_1\dots x_{n-1}\rangle$ je dán jako $x = x_{n-1}2^{n-1} + x_{n-2}2^{n-2} + \cdots + x_0 2^0$.

▶ **Tvrzení 1.11.** *Obecně pro libovolný systém n qubitů, kde* $x \in \{0,\dots,2^{n-1}\}$, $n \in \mathbb{N}$, $N = 2^n$ *a* $\alpha_x \in \mathbb{C}$ *platí, že stavový vektor je lineární kombinací*

$$|\psi\rangle = \sum_{x=0}^{N-1} \alpha_x\,|x\rangle \tag{1.18}$$

kde

$$||\,|\psi\rangle\,||^2 = \sum_{x=0}^{N-1} |\alpha_x|^2 = 1. \tag{1.19}$$

1.3 Kvantové počítání

Změny v diskrétních časových okamžicích u kvantových systémů se dají popsat pomocí kvantového počítání. Tak, jako jsou naše klasické počítače z elektrických obvodů obsahující dráty a logické hradla, kvantový počítač lze sestavit z kvantových obvodů a kvantových hradel. Pro manipulaci s kvantovými stavy používáme pouze unitární matice, ale jelikož použití matic u vícedimenzionálních stavů může nabývat obrovských rozměrů, používáme pro jejich popis právě kvantová hradla.

▶ **Definice 1.12** (Hermitovské sdružení)**.** *Na konečnědimenzionálním Hilbertově prostoru $\mathcal{H}$ můžeme každý operátor vyjádřit pomocí jeho matice v dané bázi. Hermitovský operátor H je takový lineární operátor $H : \mathcal{H} \mapsto \mathcal{H}$, pro jehož matici v libovolné bázi platí*

$$\mathbf{H} = \mathbf{H}^\dagger, \tag{1.20}$$

kde † značí transpozici matice a komplexní sdružení jejich prvků. Matici $\mathbf{H}^\dagger$ nazýváme Hermitovsky sdruženou k matici $\mathbf{H}$.

▶ **Věta 1.13.** *V prostoru konečné dimenze je spektrum operátoru totožné s množinou vlastních čísel. Hermitovský operátor má tu vlastnost, že jeho vlastní čísla jsou vždy reálná, jeho vlastní vektory jsou na sebe kolmé a lze z nich vybrat ortonormální bázi $\mathcal{H}$*

▶ **Definice 1.14** (Unitární matice)**.** *Říkáme, že čtvercová komplexní matice $\mathbf{U}$ je unitární, jestliže platí*

$$\mathbf{U}\mathbf{U}^\dagger = \mathbf{U}^\dagger\mathbf{U} = \mathbf{I}, \tag{1.21}$$

kde $\mathbf{I}$ je jednotková matice.

Důležitou vlastností unitárních matic je, že jsou invertibilní, jelikož $\mathbf{U^{-1}} = \mathbf{U}^\dagger$. To nám říká, že na rozdíl od výpočtů na klasickém počítači, kdy jednotlivé operace jako NAND, AND . . . nejsou reverzibilní, u kvantových počítačů lze každou operaci vrátit zpět. S tím přichází i obtíže, jelikož nemůžeme aplikovat jednoduchá klasická hradla, která nejsou popsány unitární maticí, a proto musíme každou tuto operaci převést na hradlo, které je popsáno unitární maticí. Přitom každá unitární matice popisuje validní kvantové hradlo. Tato vlastnost je hojně používána řadou algoritmů a má mnohá využití. Jedinou vyjímkou je operace měření, jak se dozvíme v 1.3.3, kdy po jejím aplikování dochází ke kolapsu vlnové funkce a tedy dochází ke ztrátě informace.

▶ **Tvrzení 1.15.** *Ze Schrödingerovy rovnice plyne, že systém, který v čase t_0 byl ve stavu $|\psi\rangle$, je v čase $t \geq t_0$ v jednoznačně určeném stavu $|\psi(t)\rangle$, pokud na něm nebylo provedeno měření. Existuje tedy lineární operátor $U(t, t_0)$, pro který platí*

$$|\psi\rangle = U(t, t_0)\,|\psi\rangle\,. \tag{1.22}$$

Tento operátor se nazývá evoluční operátor. Lze dokázat, že tento operátor je vždy unitární. Z důvodu složitosti tento důkaz vynecháme.

▶ **Důsledek 1.16.** *Časový vývoj systému vždy probíhá působením unitárního operátoru, kvantová hradla jsou tedy vždy unitární a cokoliv, co chceme se stavem provést, musíme provést unitárně* [2].

1.3.1 Jednoqubitová hradla

Jednoqubitová hradla jsou unitární matice o rozměru 2×2, které aplikujeme právě na jeden qubit. Na začátek si představíme množinu základních hradel identity a Pauliho matic a jaký mají efekt na qubit ve standardní bázi. Mějme $|\psi\rangle = a\,|0\rangle + b\,|1\rangle$.

$$\mathbf{I} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \qquad \mathbf{I}\,|\psi\rangle = a\,|0\rangle + b\,|1\rangle\,, \tag{1.23}$$

$$\mathbf{X} = \sigma_X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \qquad \mathbf{X}\,|\psi\rangle = b\,|0\rangle + a\,|1\rangle\,, \tag{1.24}$$

$$\mathbf{Y} = \sigma_Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \qquad \mathbf{Y}\,|\psi\rangle = -ib\,|0\rangle + a\,|1\rangle\,, \tag{1.25}$$

$$\mathbf{Z} = \sigma_Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \qquad \mathbf{Z}\,|\psi\rangle = a\,|0\rangle - b\,|1\rangle\,. \tag{1.26}$$

Z pozorování si můžeme všimnout, že hradlo **X** prohodí amplitudy a je tudíž kvantovou obdobou logického hradla NOT, proto je též často nazýváno jako NOT-hradlo. V sekci 1.2 jsme si vysvětlili pojem relativní fáze. Při použití hradla **Z** došlo ke změně znaménka, tedy ke změně relativní fáze qubitu, a proto nový stav popisuje jiný kvantový systém než před jeho použitím.

Mezi základní a nejčastěji využívané hradlo patří tzv. Hadamardovo hradlo **H**, které je dáno maticí

$$\mathbf{H} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}. \tag{1.27}$$

Hadamardovo hradlo je velice specifické svým použitím, jeho aplikováním na stavy $|0\rangle$ a $|1\rangle$ je nastaví do tzv. vyváženého stavu, kdy pravděpodobnost naměření obou stavů ve standardní bázi je stejná $\left(\frac{1}{2}\right)$.

▶ Notace 1.17. Jelikož se jedná o jednu z nejčastěji používaných operací, tak pro srozumitelnost a přehlednost používáme pro popis stavů $|0\rangle$ a $|1\rangle$ po použití Hadamardova hradla **H** notaci $|+\rangle$ a $|-\rangle$ kdy

$$|+\rangle = \frac{1}{\sqrt{2}} \left(|0\rangle + |1\rangle\right), \tag{1.28}$$

$$|-\rangle = \frac{1}{\sqrt{2}} \left(|0\rangle - |1\rangle\right). \tag{1.29}$$

▶ **Příklad 1.18.** Použitím Hadamardova hradla namapujeme stavy $|0\rangle$ na $|+\rangle$ a $|1\rangle$ na $|-\rangle$.

$$\mathbf{H}\,|0\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = |+\rangle \tag{1.30}$$

$$\mathbf{H}\,|1\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = |-\rangle \tag{1.31}$$

Pokud bychom se chtěli pokusit tuto operaci vizualizovat na Blochově sféře 1.1, mohli bychom si ji představit pouze jako operaci dvou rotací, kdy vektor rotujeme o 90° podle osy y a následně podle osy x o 180°.

Pro úplnost si představíme také jednoqubitová hradla, která provádí rotaci o úhel δ kolem osy x, y nebo z. Operátory rotací jsou dány maticemi

$$\mathbf{R}_x(\delta) = \begin{pmatrix} \cos\frac{\delta}{2} & -i\sin\frac{\delta}{2} \\ -i\sin\frac{\delta}{2} & \cos\frac{\delta}{2} \end{pmatrix}, \tag{1.32}$$

$$\mathbf{R}_y(\delta) = \begin{pmatrix} \cos\frac{\delta}{2} & -\sin\frac{\delta}{2} \\ \sin\frac{\delta}{2} & \cos\frac{\delta}{2} \end{pmatrix}, \tag{1.33}$$

$$\mathbf{R}_z(\delta) = \begin{pmatrix} e^{-i\frac{\delta}{2}} & 0 \\ 0 & e^{i\frac{\delta}{2}} \end{pmatrix}. \tag{1.34}$$

Existuje nekonečně mnoho libovolných 2×2 unitárních matic a tudíž existuje i nekonečně jednoqubitových hradel. Ukazuje se však, že vlastnosti jakékoli kompletní množiny lze pochopit z vlastností mnohem menší množiny. Tak jako jsme se se v příkladu (1.18) snažili vysvětlit, jaké rotace na sféře Hadamardovo hradlo způsobuje, lze ukázat, že jeho matice lze rozložit na matice jednotlivých rotací (1.32),(1.33) a (1.34) podle os. To ovšem neplatí jen pro Hadamardovu matici. Skládáním rotací kolem os x, y a z se lze na jednotkové kouli dostat do libovolného bodu. To znamená, že každou unitární 2×2 matici lze rozložit na součin rotací (1.33) a (1.34), tedy lze vizualizovat jako rotaci na Blochově sféře.

▶ **Věta 1.19.** *Předpokládejme, že* $\mathbf{U}$ *je unitární operace na jednom qubitu. Pak existují* $\alpha, \beta, \gamma, \delta \in \mathbb{R}$ *taková, že platí*

$$\mathbf{U} = e^{i\alpha}\mathbf{R}_z(\beta)\,\mathbf{R}_y(\gamma)\,\mathbf{R}_z(\delta) = e^{i\alpha}\begin{pmatrix} e^{-i\frac{\delta}{2}} & 0 \\ 0 & e^{i\frac{\delta}{2}} \end{pmatrix}\begin{pmatrix} \cos\frac{\delta}{2} & -\sin\frac{\delta}{2} \\ \sin\frac{\delta}{2} & \cos\frac{\delta}{2} \end{pmatrix}\begin{pmatrix} e^{-i\frac{\delta}{2}} & 0 \\ 0 & e^{i\frac{\delta}{2}} \end{pmatrix}. \tag{1.35}$$

1.3.2 Vícequbitová hradla

Zatím jsme si představili hradla působící pouze na jednotlivé qubity. Ale jako u klasických počítačů, kdy potřebujeme mít operace působící na dva bity, v kvantové informatice potřebujeme operace ovlivňující více qubitů. Nejdůležitějším hradlem pracujícím se dvěma qubity je tzv. **CNOT** hradlo, které je kvantovou obdobou hradla XOR. U klasického hradla XOR, ale narážíme na problém, že tato operace není reverzibilní, a proto se nemůže považovat za validní operaci kvantového hradla 1.14. Způsob jakým tento problém vyřešíme je, že jeden qubit označíme jako kontrolní a druhý jako cílový. Je-li hodnota kontrolního qubitu 0, cílový qubit se nezmění, ale pokud má kontrolní qubit hodnotu 1, hodnota cílového qubitu se změní aplikováním $\mathbf{X}$ hradla. Operaci CNOT můžeme tedy zapsat maticí

$$\mathbf{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}. \tag{1.36}$$

▶ **Příklad 1.20.** Obecný předpis hradla **CNOT**, kdy první qubit je kontrolní a druhý cílový:

$$\mathbf{CNOT}\,|A, B\rangle = |A, A \oplus B\rangle \tag{1.37}$$

Působení hradla **CNOT** na bazické stavy:

$$\mathbf{CNOT}\,|00\rangle = |00\rangle \quad \mathbf{CNOT}\,|01\rangle = |01\rangle \quad \mathbf{CNOT}\,|10\rangle = |11\rangle \quad \mathbf{CNOT}\,|11\rangle = |10\rangle \tag{1.38}$$

Poslední hradlo, které si v této kapitole představíme bude Toffoliho hradlo CCX. Jedná se o hradlo působící na 3 qubity. Toffoliho hradlo je rozšíření hradla **CNOT** do tří qubitů, kde první dva qubity jsou kontrolní a poslední je cílový. Hilbertův prostor tří qubitů má dimenzi 8, tedy naše unitární matice bude rozměru 8×8 a je zapsána jako

$$\mathbf{CCX} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}. \tag{1.39}$$

1.3.3 Kvantové měření

Kvantové měření je proces, kterým zjistíme informace o kvantovém systému, tedy přeměňuje kvantový stav na klasickou informaci. Měření je popsáno sadou měřících operátorů $\left\{M_{|\phi\rangle}\right\}$, které působí na stavovém prostoru měřeného systému, kde $|\phi\rangle$ odpovídá možným stavům, do kterých může při měření systém přejít. Měřící operátory jsou Hermitovské a jedná se o projektory. Tedy pro každý měřící operátor $M_{|\phi\rangle}$ platí $M^2_{|\phi\rangle} = M_{|\phi\rangle}$.

► **Tvrzení 1.21.** *Pokud máme kvantový systém, který je přesně před měřením ve stavu $|\psi\rangle$ tak pravděpodobnost přechodu do stavu $|\phi\rangle$ je*

$$P_{|\phi\rangle}\left(|\psi\rangle\right) = \langle\psi|M_{|\phi\rangle}^{\dagger}M_{|\phi\rangle}|\psi\rangle\,, \tag{1.40}$$

Stav systému hned po změření bude

$$\frac{M_{|\phi\rangle}\,|\psi\rangle}{\sqrt{\langle\psi|M_{|\phi\rangle}^{\dagger}M_{|\phi\rangle}|\psi\rangle}}. \tag{1.41}$$

Měřící operátory, kde $n \in \mathbb{N}$ určuje počet možných stavů $|\phi\rangle$, do kterých systém může přejít, splňují

$$\sum_{i=1}^{n} M_{|\phi_i\rangle}^{\dagger}M_{|\phi_i\rangle} = I, \tag{1.42}$$

a součet pravděpodobností přechodu je pak roven jedné:

$$\sum_{i=1}^{n} P_{|\phi\rangle}\left(|\psi\rangle\right) = \sum_{i=1}^{n} \langle\psi|M_{|\phi_i\rangle}^{\dagger}M_{|\phi_i\rangle}|\psi\rangle = 1. \tag{1.43}$$

► **Příklad 1.22.** Uvažujme měření jednoho qubitu s dvěma možnými výsledky měření $(|0\rangle, |1\rangle)$ definované dvěma měřícími operátory $M_{|0\rangle} = |0\rangle\langle 0|$ a $M_{|1\rangle} = |1\rangle\langle 1|$. Mějme qubit, který chceme změřit, ve stavu $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$. Nyní už snadno ověříme, že pravděpodobnost přechodu do stavu $|0\rangle$, resp. $|1\rangle$ je opravdu

$$P_{|0\rangle}\left(|\psi\rangle\right) = \langle\psi|M_{|0\rangle}^{\dagger}M_{|0\rangle}|\psi\rangle = \langle\psi|M_{|0\rangle}|\psi\rangle = |\alpha|^2\,, \tag{1.44}$$

$$P_{|1\rangle}\left(|\psi\rangle\right) = \langle\psi|M_{|1\rangle}^{\dagger}M_{|1\rangle}|\psi\rangle = \langle\psi|M_{|1\rangle}|\psi\rangle = |\beta|^2 \tag{1.45}$$

jak jsme si ukázali v (1.8). Můžeme z tohoto příkladu vypozorovat, že měřící operátory jsou opravdu Hermitovské, a že se jedná o projektory, tedy platí $M_{|0\rangle}^2 = M_{|0\rangle}$, $M_{|1\rangle}^2 = M_{|1\rangle}$ a $M_{|0\rangle}^{\dagger}M_{|0\rangle} + M_{|1\rangle}^{\dagger}M_{|1\rangle} = M_{|0\rangle} + M_{|1\rangle} = I$.

Nyní se podíváme na speciální typ měření, nazývaný *projektivní měření* [3].

► **Tvrzení 1.23.** *Nechť je $\mathbf{M} \in \mathbb{C}^{n\times n}$ Hermitovská matice pro $n \in \mathbb{N}$ a $|\varphi_1\rangle, |\varphi_2\rangle \ldots |\varphi_n\rangle$ jsou normalizované vlastní vektory matice $\mathbf{M}$ s vlastními čísly $m_1, m_2 \ldots m_n$, pak můžeme $\mathbf{M}$ přepsat jako*

$$\mathbf{M} = \sum_{i=1}^{n} m_i\,|\varphi_i\rangle\langle\varphi_i|\,, \tag{1.46}$$

kde $|\varphi_i\rangle\langle\varphi_i|$ je projektor na vlastní prostor $\mathbf{M}$ s vlastním číslem m_i.

► Notace 1.24. Projektor $|\varphi_i\rangle\langle\varphi_i|$ budeme dále zapisovat jako $\mathbf{P}_{|\varphi_i\rangle}$ s vlastním číslem $m_{|\varphi_i\rangle}$.

► **Příklad 1.25.** Projektory $\mathbf{P}_{|0\rangle}, \mathbf{P}_{|1\rangle}, \mathbf{P}_{|+\rangle}, \mathbf{P}_{|-\rangle}$ spočteme následujícím způsobem:

$$\mathbf{P}_{|0\rangle} = |0\rangle\langle 0| = \begin{pmatrix}1\\0\end{pmatrix}\cdot\begin{pmatrix}1 & 0\end{pmatrix} = \begin{pmatrix}1 & 0\\0 & 0\end{pmatrix}, \tag{1.47}$$

$$\mathbf{P}_{|1\rangle} = |1\rangle\langle 1| = \begin{pmatrix}0\\1\end{pmatrix}\cdot\begin{pmatrix}0 & 1\end{pmatrix} = \begin{pmatrix}0 & 0\\0 & 1\end{pmatrix}, \tag{1.48}$$

$$\mathbf{P}_{|+\rangle} = \left(|0\rangle + |1\rangle\right)\left(\langle 0| + \langle 1|\right) = \begin{pmatrix}1\\1\end{pmatrix}\cdot\begin{pmatrix}1 & 1\end{pmatrix} = \begin{pmatrix}1 & 1\\1 & 1\end{pmatrix}, \tag{1.49}$$

$$\mathbf{P}_{|-\rangle} = \left(|0\rangle - |1\rangle\right)\left(\langle 0| - \langle 1|\right) = \begin{pmatrix}1\\-1\end{pmatrix}\cdot\begin{pmatrix}1 & -1\end{pmatrix} = \begin{pmatrix}1 & -1\\-1 & 1\end{pmatrix}. \tag{1.50}$$

▶ **Důsledek 1.26.** *Měřením stavu $|\psi\rangle$ získáváme pravděpodobnost přechodu do stavu $|\phi\rangle$:*

$$P_{|\phi\rangle}\left(|\psi\rangle\right) = \langle\psi|\,\mathbf{P}_{|\phi\rangle}\,|\psi\rangle\,. \tag{1.51}$$

▶ **Příklad 1.27.** Mějme bázi určenou vektory $|0\rangle$ a $|1\rangle$, kterou nazýváme jako **Z**-bázi, kde $|0\rangle$ a $|1\rangle$ jsou vzájemně kolmými vlastními vektory operátoru **Z**, který lze zapsat jako

$$\mathbf{Z} = m_{|0\rangle}\mathbf{P}_{|0\rangle} + m_{|1\rangle}\mathbf{P}_{|1\rangle} = 1\cdot\begin{pmatrix}1 & 0\\ 0 & 0\end{pmatrix} - 1\cdot\begin{pmatrix}0 & 0\\ 0 & 1\end{pmatrix}. \tag{1.52}$$

Pokud bychom měřili systém ve stavu $|\psi\rangle = |0\rangle$, vždy měřením systém přejde do stavu $|0\rangle$, nikdy $|1\rangle$, tedy pro stav $|\psi\rangle$ je pravděpodobnost přechodu do stavu $|0\rangle$:

$$P_{|0\rangle}\left(|\psi\rangle\right) = \langle 0|\,\mathbf{P}_{|0\rangle}\,|0\rangle = \begin{pmatrix}1 & 0\end{pmatrix}\cdot\begin{pmatrix}1 & 0\\ 0 & 0\end{pmatrix}\cdot\begin{pmatrix}1\\ 0\end{pmatrix} = 1. \tag{1.53}$$

Pravděpodobnost přechodu do $|1\rangle$ pro stav $|\psi\rangle$

$$P_{|1\rangle}\left(|\psi\rangle\right) = \langle 0|\,\mathbf{P}_{|1\rangle}\,|0\rangle = \begin{pmatrix}1 & 0\end{pmatrix}\cdot\begin{pmatrix}0 & 0\\ 0 & 1\end{pmatrix}\cdot\begin{pmatrix}1\\ 0\end{pmatrix} = 0. \tag{1.54}$$

Pro přechod do stavu $|1\rangle$ pro stav $|\psi\rangle = |1\rangle$ to funguje identicky. Z pozorování si můžeme povšimnout, že v **Z**-bázi se jedná o jediné dva stavy, které lze jednoznačně rozlišit.

▶ **Příklad 1.28.** Pokud bychom měli systém ve stavu $|0\rangle$ nebo $|1\rangle$ a vzali jiné dva vektory, do kterých bychom chtěli přejít, např. $|+\rangle$ a $|-\rangle$, nelze je v **Z**-bázi odlišit:

$$P_{|+\rangle}\left(|0\rangle\right) = P_{|+\rangle}\left(|1\rangle\right) = P_{|-\rangle}\left(|0\rangle\right) = P_{|-\rangle}\left(|1\rangle\right) = \frac{1}{2}. \tag{1.55}$$

To ale neznamená, že je nelze odlišit nikdy. V případě vhodně zvolené báze tyto vektory rozlišit umíme. Když pro měření těchto vektorů zvolíme **X**-bázi, definovanou operátorem **X**, kde

$$\mathbf{X} = m_{|+\rangle}\mathbf{P}_{|+\rangle} + m_{|-\rangle}\mathbf{P}_{|-\rangle} = 1\cdot\begin{pmatrix}1 & 1\\ 1 & 1\end{pmatrix} - 1\cdot\begin{pmatrix}1 & -1\\ -1 & 1\end{pmatrix}, \tag{1.56}$$

měřením vektoru $|+\rangle$ v **X**-bázi vždy přejdeme do stavu $|+\rangle$, zatímco měřením vektoru $|-\rangle$ vždy $|-\rangle$, vyjádřeno pravděpodobnostmi:

$$P_{|+\rangle}\left(|+\rangle\right) = 1 \qquad P_{|+\rangle}\left(|-\rangle\right) = 0 \tag{1.57}$$

$$P_{|-\rangle}\left(|+\rangle\right) = 0 \qquad P_{|-\rangle}\left(|-\rangle\right) = 1 \tag{1.58}$$

Pomocí projektivního měření pak lehce můžeme získat střední hodnotu měřícího operátoru.

▶ **Tvrzení 1.29.** *Střední hodnota měření systému ve stavu $|\psi\rangle$ v bázi M je definována následovně*

$$E(M) = \langle\psi|M|\psi\rangle\,. \tag{1.59}$$

▶ Poznámka 1.30. Důležitým poznatkem je, že pokud výsledek meření fyzikálního systému nabývá hodnot +1 nebo -1, kde tato hodnota odpovídá vlastnímu číslu projektoru $\mathbf{P}_{|\psi\rangle}$ stavu $|\psi\rangle$, ve kterém se systém po měření nachází. Hodnoty +1 a -1 poté v kvantové informatice kódujeme do binárního stavu, na který jsme zvyklý z klasické informatiky, kde $+1 = 0$ a $-1 = 1$.

Kapitola 2
Kvantová distribuce klíče

Bezpečná komunikace a kryptografie se stávají v dnešní době stále důležitějšími, protože technologie nám umožňují se okamžitě propojit po celém světě. Abychom chránili naše citlivé informace a komunikaci, musíme používat techniky šifrování a nejlepší postupy, aby naše zprávy byly přístupné pouze zamýšleným příjemcům bez jakéhokoliv narušení. V této kapitole si představíme význam a důležitost distribuce klíče a metodu QKD. Seznámíme se s základními principy, na kterých protokoly QKD stojí, požadavky pro jejich bezpečnost a přípravu.

2.1 Úvod do kryptografie

Kryptografie je praxe zabezpečování informací pomocí kódů nebo šifer tak, aby mohly být informace přístupné pouze oprávněným účastníkům. To zahrnuje použití algoritmů k šifrování dat, čímž se stávají nečitelnými pro kohokoli, kdo nemá klíč k jejich dešifrování. Existuje několik různých kryptografických postupů, které lze použít k ochraně dat. Rozlišujeme především symetrické šifrování, asymetrické šifrování a hashování.

Symetrické šifrování je technika, která používá jediný klíč k šifrování i dešifrování dat. To znamená, že jak odesílatel, tak příjemce musí mít stejný klíč, aby mohli komunikovat bezpečně. Na druhé straně asymetrické šifrování používá dva různé klíče: veřejný klíč a soukromý klíč. Veřejný klíč může být sdílen s kýmkoli, zatímco soukromý klíč je tajný a používá se k dešifrování zpráv, které byly šifrovány pomocí veřejného klíče.

Symetrickou i asymetrickou kryptografii lze používat samostatně k zabezpečení komunikace a ochraně citlivých informací. Avšak obě techniky mohou být použity společně pro zvýšení bezpečnosti komunikace. Tato technika se nazývá hybridní kryptografie a je v nynějších modelech bezpečné komunikace nejčastěji využívána. Při hybridní kryptografii se používá symetrická kryptografie pro šifrování samotné zprávy a asymetrická kryptografie pro bezpečnou výměnu tajného klíče, který se používá k šifrování a dešifrování zprávy. Zde si představíme, jak obecný koncept hybridní kryptografie funguje:

1. Odesílatel vygeneruje náhodný tajný klíč pro symetrickou kryptografii.
2. Odesílatel šifruje zprávu pomocí tajného klíče a symetrické kryptografie.
3. Odesílatel šifruje tajný klíč pomocí veřejného klíče příjemce a asymetrické kryptografie.
4. Jak šifrovaná zpráva, tak šifrovaný tajný klíč jsou odeslány přes nezabezpečenou síť.
5. Příjemce používá svůj soukromý klíč k dešifrování šifrovaného tajného klíče.
6. Příjemce používá dešifrovaný tajný klíč k dešifrování šifrované zprávy.

Hybridní kryptografie kombinuje výhody symetrické a asymetrické kryptografie. Symetrická kryptografie je rychlejší a účinnější pro velké množství dat, zatímco asymetrická kryptografie umožňuje výměnu klíčů bez toho, aby se strany fyzicky setkaly. Tento způsob se široce používá v bezpečných komunikačních protokolech, jako je SSL/TLS.

Jedním z algoritmů, který je součástí tzv. SSL handshake, kdy se komunikující strany domluví na společném klíči pro symetrickou kryptografii, je asymetrická kryptografická technika s názvem RSA [4]. Bezpečnost RSA je založena na faktorizaci složených čísel na prvočísla. Velká složená čísla, například 2048–bitová, nedokážeme z důvodu nedostatku dosavadní výpočetní síly našich klasických počítačů efektivně rozložit a to zaručuje bezpečnost schémat založených na tomto problému. To stejné platí pro schéma Diffie-Hellmanovy výměny klíče, který je založený na problému diskrétního logaritmu.

V roce 1994 americký matematik Peter Shor navrhnul kvantový algoritmus pro efektivní faktorizaci velkých složených celých čísel. Algoritmus je založen na odhadu fáze vlastního čísla, pomocí (inverzní) Kvantové Fourierovy transformace. Shorův algoritmus ale ve skutečnosti řeší obecnější problém hledání periody určité periodické funkce. Ukazuje se, že kvantové počítače mohou prolomit mnoho běžně používaných algoritmů pro asymetrickou kryptografii založených na problému faktorizace nebo diskrétního logaritmu. Jedná se tedy o známé algoritmy jako RSA, Diffie-Hellman pracující s konečnou grupou $\mathbb{Z}_p^*$, kde $\mathbb{Z}_p^* = \mathbb{Z}_p \setminus \{0\}$ a p je prvočíslo, a Diffie-Hellman s využitím eliptických křivek.

Nicméně praktická implementace Shorova algoritmu je v současnosti omezena technickými výzvami spojenými s výstavbou a provozem kvantových počítačů s dostatečným množstvím qubitů k faktorizaci velkých celých čísel [5]. Přesto potenciál Shorova algoritmu a dalších kvantových algoritmů vedl k zvýšenému zájmu a výzkumu v oblasti kvantových výpočtů a post-kvantové kryptografie (PQC).

2.2 Principy QKD

Bezpečnost metod zmíněných v kapitole 2.1 je založena na výpočetní náročnosti matematických problémů. Při zvýšení výpočetní síly kvantových počítačů, je potřeba hledat nová řešení jak nahradit schémata, která by v budoucnosti mohla být lehce prolomena. Mezi nejpravděpodobnější uchazeče na náhradu patří právě QKD a algoritmy spadající do PQC.

PQC si klade za cíl vyvinout nové kryptografické algoritmy, které jsou odolné vůči výpočetní síle kvantových počítačů, při zachování stejné úrovně zabezpečení jako stávající klasické kryptografické algoritmy. Jedním z nejslibnějších přístupů je kryptografie založena na matematických vlastnostech tzv. mřížky ve vysoce dimenzionálních prostorech [6]. Tento přístup se zda být velice příznivý jelikož implementace těchto algoritmů je pouze softwarovou záležitostí, tudíž lze k jejich využívání používat osvedčené hardwarové moduly. Nicméně, jelikož se jedná stále o problémy matematického typu, nemůžeme si býti jisti, že se nenajdou algoritmy, které dokáží tyto schémata efektivně rozbít [7].

QKD je naproti tomu založeno na principech kvantové mechaniky, a tudíž na základních fyzikálních zákonech jako takových. Fyzicky jsou kvantové sítě implementovány pomocí přenosu polarizovaných fotonů a různých druhů signálů. Jednou z velikých výhod QKD je, že poskytuje bezpodmínečné zabezpečení, což znamená, že je teoreticky nemožné, aby odposlouchávající zachytil klíč, aniž by byl detekován.

Zákony kvantové mechaniky říkají, že je nemožné vytvořit nezávislou a identickou kopii libovolného neznámého kvantového stavu [8]. Předpokládejme, že máme libovolný neznámý stav $|\psi\rangle$, který chceme nakopírovat do stavu $|\phi\rangle$. A předpokládejme, že existuje unitární operátor U,

pomocí kterého dokážeme libovolný stav qubitu zkopírovat do jiného qubitu. Potom platí

$$U\left(|\psi\rangle \otimes |0\rangle\right) = |\psi\rangle \otimes |\psi\rangle \tag{2.1}$$
$$U\left(|\phi\rangle \otimes |0\rangle\right) = |\phi\rangle \otimes |\phi\rangle \tag{2.2}$$
$$\tag{2.3}$$

Skalární součin takových vektorů je roven

$$\left(\langle\phi| \otimes \langle 0|\right) U^\dagger U \left(|\psi\rangle \otimes |0\rangle\right) = \left(\langle\phi| \otimes \langle\phi|\right)\left(|\psi\rangle \otimes |\psi\rangle\right) = \langle\phi|\psi\rangle \langle\phi|\psi\rangle = \left(\langle\phi|\psi\rangle\right)^2 . \tag{2.4}$$

Současně ale musí díky unitaritě U platit

$$\left(\langle\phi| \otimes \langle 0|\right) U^\dagger U \left(|\psi\rangle \otimes |0\rangle\right) = \left(\langle\phi| \otimes \langle 0|\right)\left(|\psi\rangle \otimes |0\rangle\right) = \langle\phi|\psi\rangle \langle 0|0\rangle = \langle\phi|\psi\rangle . \tag{2.5}$$

Tyto dvě rovnice nám dávají

$$\left(\langle\phi|\psi\rangle\right)^2 = \langle\phi|\psi\rangle . \tag{2.6}$$

To znamená, že buď $\langle\phi|\psi\rangle = 1$ nebo $\langle\phi|\psi\rangle = 0$, takže $|\psi\rangle = |\phi\rangle$ nebo jsou vektory $|\psi\rangle$ a $|\phi\rangle$ ortogonální, což je spor s naším předpokladem, že lze klonovat libovolné vektory $|\psi\rangle$ a $|\phi\rangle$.

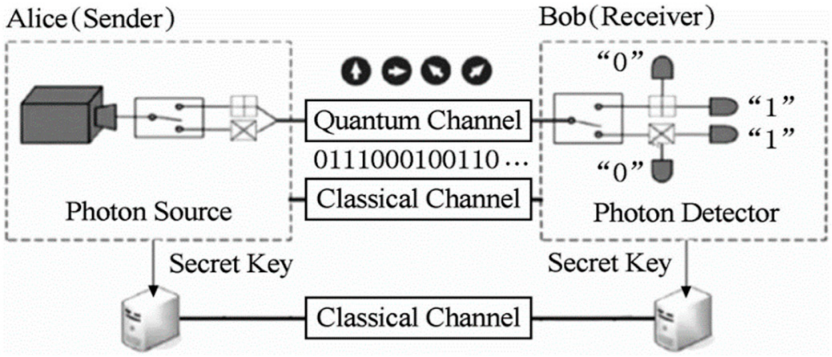
Nemožnost klonování je zcela zásadní vlastnost pro bezpečnost QKD. Odposlouchávající na kvantovém kanále nedokáže procházející qubity zkopírovat, proto jak dále uvidíme, je jedinou možností rovnou qubity změřit, čímž dojde ke kolapsu kvantového stavu. Díky tomu pak účastníci komunikace dokáží zjistit, že někdo neověřený je na jejich komunikačním kvantovém kanále a odposlouchává jejich přenos qubitů.

2.2.1 Fyzická realizace QKD

Provedení QKD vyžaduje přenos jednotlivých fotonů přes optická vlákna, což je velmi citlivý proces, který vyžaduje značnou technickou preciznost a silná bezpečnostní opatření. Proces začíná vysláním světelných signálů (fotonů) z optického zdroje. Vlákno musí být zcela izolováno od vnějších vlivů, aby se minimalizovaly ztráty fotonů a zajistila se co nejvyšší úroveň přesnosti. Při přenosu fotonů mohou být vystaveny různým druhům šumu, které mohou snížit kvalitu a bezpečnost přenosu. Jedním z nejvýznamnějších faktorů šumu je degradace signálu v důsledku jeho interakce s prostředím, ve kterém se přenos uskutečňuje. Další významným faktorem jsou nečistoty v optickém vláknu, jako jsou nehomogenity a nedostatky v materiálu vlákna. To může vést k rozptýlení světla a ztrátě fotonů. Aby se minimalizovaly účinky těchto šumů a zajistila se co nejvyšší kvalita přenosu, jsou při QKD používány různé techniky. To znamená, že musí být použity kvalitní materiály a omezit se rušení v oblasti přenosového kanálu, například elektromagnetickými vlnami [9].

Jedním z nejdůležitějších prvků pro přípravu a měření poslaných qubitů je použití polarizačních filtrů. Polarizační filtry umožňují vysílací straně ovládat polarizaci fotonů, aby bylo možné vytvořit klíč s předem definovanými polarizacemi. Směr polarizace představuje stavy qubitu, například horizontální polarizací kódujeme stav $|0\rangle$ a vertikální polarizací stav $|1\rangle$. Tyto polarizace musí být přesně definovány a chráněny před vnějšími vlivy, aby bylo možné zajistit úspěšnost přenosu. Přijímající strana musí použít stejné polarizační filtry k přesnému měření polarizace fotonů. Pokud je polarizace fotonu správně naměřena, je považován za úspěšně přenesený a použit pro vytvoření sdíleného tajného klíče.

Dalším důležitým bodem, který je potřebné podotknout je, že samotné schéma QKD stojí na dvou komunikačních kanálech, jak můžeme vidět v (2.1). Jedním z nich je veřejný kvantový kanál, přes který probíhá přenos polarizovaných fotonů. Druhým kanálem je veřejný klasický kanál, kde si obě strany veřejně sdělují doplňkové informace k měření qubitů. Pro správný chod protokolů, účastníci musí být na klasickém kanále autentizováni.



Obrázek 2.1 Základní schéma realizace QKD pro přenos polarizovaných fotonů [10]

Pokud mluvíme o kvantových sítích, mluvíme o skutečné technologii, která se vyvíjí a začíná nacházet své uplatnění v průmyslu a vědě. Kromě mezinárodních organizacích, které se aktivně podílí na vývoji této technologie, začíná vznikat více komerčních firem nabízejících QKD systémy. Tento seznam představuje kvantové sítě, které jsou už v běhu a byla na nich provedena QKD:

1. Kvantová síť DARPA (Agentura pro pokročilé obranné výzkumné projekty) v USA: síť vznikla v roce 2004 v Massachusetts a skládá se z 10 komunikačních stran.

2. SwissQuantum: byla založena roku 2007 komerční firmou ID Quantique v Ženevě, tento projekt byl jeden z prvních, který potvrdil reálné využití QKD pro šifrovací systémy.

3. SECOQC (Bezpečná komunikace založená na kvantové kryptografii): jedná se o první počítačovou síť, která byla plně zabezpečena pomocí QKD, využitím více než 200km optických kabelů v roce 2008 ve Vídni.

4. Tokyo QKD Network: jedná se o největší mezinárodní projekt implementující QKD systémy, společně s Japonským Národním institutem pro informační a komunikační technologie dokázali při QKD dosáhnout rychlosti až 1,25Gb/s na vzdálenost 100km.

Aktuálním rekordem na nejdelší úspěšnou vzdálenost je přenos realizovaný v Číně v roce 2020 a to na 1120km při rychlosti vytvoření klíče 0.12 bitů za vteřinu, tento přenos byl uskutečněn mezi satelitem a zemskou stanicí [11].

2.3 Kvantové provázání

Kvantové provázání je fenomén kvantové mechaniky. Jedná se o koncept, s kterým se v klasické mechanice nesetkáme. Jedná se o stav dvou nebo více kvantových systémů, které jsou vzájemně provázány tak, že změna stavu jednoho systému okamžitě ovlivní stav druhého systému, bez ohledu na to, jak daleko jsou od sebe. V kvantové mechanice jsou kvantové systémy reprezentovány kvantovými stavy, které mohou být superpozicemi několika jiných stavů. Když jsou dva kvantové systémy provázány, jejich stavy jsou v kvantové superpozici a nelze je popsat jako oddělené systémy. Kvantové provázání je tedy stav, kdy je více kvantových systémů propojeno tak, že jsou v jednom kvantovém stavu. Kvantově provázané stavy využíváme i pro komunikaci, kdy se stranám posílá jeden qubit z provázaného páru.

▶ **Definice 2.1** (Kvantové provázání)**.** *Mějme fyzikální systém $\mathcal{S}$ se stavovým prostorem $\mathcal{H}$ a nechť je tento systém složen ze dvou podsystémů $\mathcal{S}_1$ a $\mathcal{S}_2$ se stavovými prostory $\mathcal{H}_1$ a $\mathcal{H}_2$. O stavu $|\psi\rangle$ popisující systém $\mathcal{S}$ řekneme, že je kvantově provázaný, pokud tento stav nelze zapsat*

jako tenzorový součin stavů prvního a druhého podsystému, tedy platí

$$|\psi\rangle \neq |\psi_1\rangle \otimes |\psi_2\rangle\,, \qquad |\psi\rangle \in \mathcal{H},\ |\psi_1\rangle \in \mathcal{H}_1,\ |\psi_2\rangle \in \mathcal{H}_2. \tag{2.7}$$

► **Příklad 2.2.** Provázaným stavem je například

$$|\beta_{00}\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right). \tag{2.8}$$

Při měření obou qubitů přejde stav $|\beta_{00}\rangle$ do stavu $|00\rangle$ s pravděpodobností $\frac{1}{2}$, kdy je výsledkem měření 00. Do stavu $|11\rangle$ přejde také s pravděpodobností $\frac{1}{2}$ s výsledkem měření 11. V žádném případě nemůžeme po změření provázaného stavu $|\beta_{00}\rangle$ dostat výsledek měření 01 nebo 10. Jelikož je $|\beta_{00}\rangle$ provázaný stav, nedokážeme ho zapsat jako $|\psi_1\rangle \otimes |\psi_2\rangle$.

2.3.1 Bellovy Stavy

Bezpochyby nejznámějším příkladem provázaných stavů jsou tzv. Bellovy stavy, které představují nejjednodušší způsob kvantového provázání. Vytvoření Bellových stavů lze provést např. na obvodu, jenž má na vstupu dva qubity inicializované ve stavu $|00\rangle$. Na první qubit se aplikuje Hadamardovo hradlo, které první qubit uvede do superpozice, a ten je pak kontrolním qubitem pro hradlo **CNOT**, které invertuje druhý qubit, pouze pokud je kontrolní ve stavu $|1\rangle$, a tímto vytvoříme Bellův stav $|\beta_{00}\rangle$. Bellovy stavy jsou provázané stavy dvou qubitů a mají tvar:

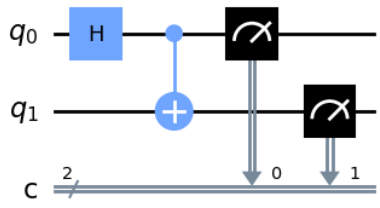
$$\begin{aligned}
|\beta_{00}\rangle &= \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right), \\
|\beta_{01}\rangle &= \frac{1}{\sqrt{2}}\left(|01\rangle + |10\rangle\right), \\
|\beta_{10}\rangle &= \frac{1}{\sqrt{2}}\left(|00\rangle - |11\rangle\right), \\
|\beta_{11}\rangle &= \frac{1}{\sqrt{2}}\left(|01\rangle - |10\rangle\right).
\end{aligned} \tag{2.9}$$

Tyto stavy se také někdy nazývají EPR stavy nebo EPR páry, jelikož z jejich pozoruhodných vlastností vychází slavný EPR paradox od A. Einsteina, B. Podolského a N. Rosena z roku 1935 [12].

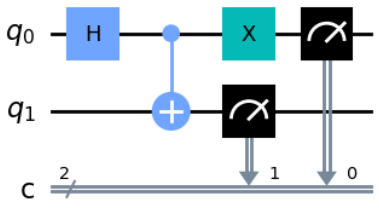
Ti považovali kvantovou mechaniku za neúplnou teorii a až v roce 1964 byl tento paradox vyřešen J. S. Bellem v teorému, jenž si přiblížíme v podkapitole 5.1.

S Bellovými stavy se setkáme v různých aplikacích jako např. superhusté kódování nebo kvantová teleportace.

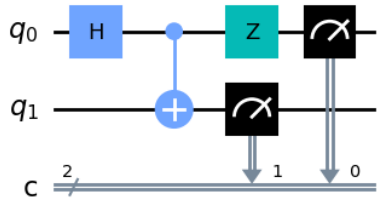
Na obrázcích 2.2a, 2.2b, 2.2c a 2.2d vidíme obvody pro vytvoření Bellových stavů. Označení q_0, q_1 je pro qubity a c je označení pro 2–bitový klasický registr, kam ukládáme výsledky měření. Druhé hradlo použíté v obvodu je hradlo **CNOT** a každý z obvodů je zakončený měřením.



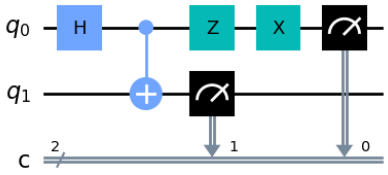
(a) Kvantový obvod pro přípravu $|\beta_{00}\rangle$



(b) Kvantový obvod pro přípravu $|\beta_{01}\rangle$



(c) Kvantový obvod pro přípravu $|\beta_{10}\rangle$



(d) Kvantový obvod pro přípravu $|\beta_{11}\rangle$

Obrázek 2.2 Kvantové obvody pro přípravu Bellových stavů [13]

2.3.2 Superhusté kódování

Superhusté kódování je označení pro komunikační protokol, při kterém si dvě komunikující strany dokáží pomocí jednoho qubitu přenést dva bity informace [14].

Pro zahájení komunikace například Alice a Boba, musí mít každá ze stran jeden qubit z provázaného páru qubitů

$$|\beta_{00}\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right). \tag{2.10}$$

Alice vlastní první qubit a Bob druhý. Pokud Alice chce přeposlat zprávu skládající se ze dvou bitů, musí nejdříve aplikovat kvantová hradla na svůj qubit, aby zprávu zakódovala. Kódování její zprávy, je vlastně přípravou Bellových stavů (2.3.1) kde indexy x,y v označení $|\beta_{xy}\rangle$ odpovídají zprávě xy a jsou dány následující tabulkou:

$$00 : |\beta_{00}\rangle \tag{2.11}$$

$$01 : |\beta_{00}\rangle \xrightarrow{\mathbf{X}} |\beta_{01}\rangle \tag{2.12}$$

$$10 : |\beta_{00}\rangle \xrightarrow{\mathbf{Z}} |\beta_{10}\rangle \tag{2.13}$$

$$11 : |\beta_{00}\rangle \xrightarrow{\mathbf{ZX}} |\beta_{11}\rangle \tag{2.14}$$

Po zakódování zprávy Alice pošle svůj qubit Bobovi. Tudíž Bob bude mít ve svém vlastnictví oba qubity. Kdyby Bob své dva qubity změřil, došel by k neodpovídajícímu výsledku, protože by měřil ve standardní bázi (1.16) a ne v bázi Bellových stavů (2.9), kde stavy od sebe nemůže jednoznačně rozpoznat. Aby se Bob dostal k původní zprávě, musí provést inverzní operace k původním operacím, aby efektivně měřil v bázi Bellových stavů, Aplikuje tedy hradlo **CNOT**, kde Alicin qubit je kontrolní, a poté aplikuje **H** hradlo na Alicin qubit, provede měření a získá původní zprávu [15].

▶ **Příklad 2.3.** Alice i Bob obdrželi své qubity a jejich systém je ve stavu $|\beta_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ a Alice se rozhodne, že chce poslat Bobovi zprávu 10. Musí tedy na svůj qubit aplikovat hradlo **Z**:

$$\mathbf{Z}\left(\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)\right) = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)\,, \tag{2.15}$$

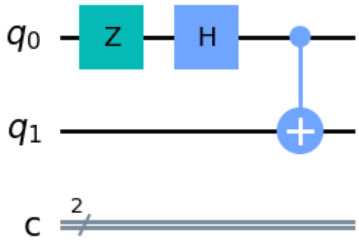
a pošle svůj qubit Bobovi. Alice může na svůj qubit aplikovat **Z** hradlo před i po použití hradel **CNOT** a **H**, jelikož obdrží stejný stav. Bob obdrží od Alice její qubit a použije hradlo **CNOT**, kde Alicin qubit je kontrolní,

$$\mathbf{CNOT}\left(\frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)\right) = \frac{1}{\sqrt{2}}(|00\rangle - |10\rangle)\,. \tag{2.16}$$

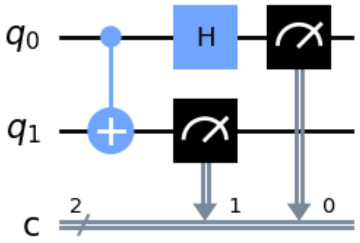
Poté aplikuje **H** hradlo na Alicin qubit

$$\mathbf{H}\left(\frac{1}{\sqrt{2}}(|00\rangle - |10\rangle)\right) = |10\rangle\,. \tag{2.17}$$

Nakonec provede měření stavu $|10\rangle$ a obdrží zamýšlenou zprávu 10.



(a) Kvantový obvod pro zakódování zprávy 10



(b) Kvantový obvod pro dekódování zprávy

■ **Obrázek 2.3** Kvantové obvody pro Superhusté kódování [13]

Kapitola 3
Provoz na klasickém kanále

V této kapitole si představíme úvod do lineárních kódů, které budeme využívat na klasickém kanále pro detekci a opravu chyb vytvořených kvantovým kanálem. Dále si představíme techniku posílení soukromí a sladění informací, kterou budeme používat pro lepší opravu chyb a snížení informace, která může být odposlechnuta. V této kapitole vždy předpokládáme přítomnost dvou komunikujících stran, Alice a Boba, a případnou třetí stranu Evu, která chce jejich sdílení klíče odposlechnout.

3.1 Lineární kódy

V kvantové informatice je oprava chyb velkým tématem stejně jako u klasické informatiky. Při přenosu qubitů se chybovost s našimi dnešními technologiemi silně projevuje. Po distribuci klíče ale potřebujeme, aby klíče pro budoucí komunikaci byly naprosto shodné a i chyby v jednotkách bitů dělají klíče nepoužitelné. Při kvantovém počítání nám šum zhoršuje výpočetní schopnosti. Abychom se s následky šumu nějak vypořádali, používáme různých technik kvantové opravy chyb. Avšak během přenosu klíče, komunikující strany musí ihned měřit příchozí qubity a nemají možnost je nějakým způsobem ukládat. Chybí jim tzv. kvantová paměť, tudíž nemají možnost využít uložených qubitů pro kvantovou opravu chyb. Obrátíme se tedy na klasickou opravu chyb probíhající přes klasický kanál.

Obecně můžeme definovat lineární kódy na libovolném konečném tělesu $\mathcal{F}_x$ s x prvky. Budeme však pouze pracovat s binárními tělesy $\mathcal{F}_2$ s prvky $\{0, 1\}$ a všechny aritmetické operace, které budeme u prvků používat budeme uvažovat modulo 2 [16].

▶ **Definice 3.1** (Lineární kód)**.** *Lineární kód $\mathcal{C}$ délky n a stupně k, pro $n \in \mathbb{N}$ a $k \in \mathbb{N}$, je lineární podprostor dimenze k binárního vektorového prostoru $\mathcal{F}_2^n$, tedy $\mathcal{C} \subseteq \mathcal{F}_2^n$.*

▶ **Tvrzení 3.2.** *Vektorový prostor $\mathcal{F}_2^n$ obsahuje 2^n prvků, které lze chápat jako n–bitové řetězce, a prostor lineárního kódu $\mathcal{C}$ obsahuje 2^k prvků.*

▶ Notace 3.3. Tyto lineární kódy budeme v textu značit jako $[n, k]$ kódy. Prvkům vektorového prostoru $\mathcal{F}_2^n$ budeme říkat slova, prvkům $\mathcal{C}$ kódová slova a budeme je značit n–bitovým vektorem.

▶ **Tvrzení 3.4.** *Pro $[n, k]$ lineární kód, je k počet bitů zakódovaných do kódového slova délky n. Platí, že je 2^k zpráv možných zpráv, které můžeme zakódovat a tedy 2^k kódových slov.*

Zbylých $n - k$ bitů kódových slov jsou redundantní a nazýváme je *kontrolní bity.*

▶ **Definice 3.5** (Hammingova váha)**.** *Hammingova váha kódového slova je počet nenulových bitů v kódovém slově. Minimální váha kódu $\mathcal{C}$ je značena d a jedná se o váhu kódového slova s minimální váhou, kromě kódového slova pouze s 0.*

▶ **Věta 3.6.** *Lineární kód $\mathcal{C}$, který je [n, k], dokáže detekovat $u = d-1$ chyb a opravit $t = \lfloor \frac{d-1}{2} \rfloor$ chyb.*

▶ **Příklad 3.7.** Mějme [7, 4] Hammingův kód $\mathcal{C}$, který obsahuje 2^4 kódových slov délky 7 bitů. V každém kódovém slově jsou 4 bity obsahující zprávu a $7 - 4 = 3$ kontrolních bitů. Kód $\mathcal{C}$ je dán následovně

$$\mathcal{C} = \{0000000, 0001011, 0010101, 0011110, 0100111, 0101100, 0110010, 0111001, \tag{3.1}$$
$$1000110, 1001101, 1010011, 1011000, 1100001, 1101010, 1110100, 1111111\}. \tag{3.2}$$

Můžeme snadno vypozorovat, že minimální váha je $d = 3$. Pomocí minimální váhy pak vypočítáme, že tento Hammingův kód dokáže detekovat 2 chyby a opravit 1 chybu. Ukážeme si příklad chybového přenosu a schopnost detekování chyby

$$1000110 \xrightarrow{1 \text{ chyba}} 0000110 \qquad \text{dokážeme detekovat a opravit} \tag{3.3}$$
$$1000110 \xrightarrow{2 \text{ chyby}} 0100110 \qquad \text{dokážeme detekovat}$$
$$1000110 \xrightarrow{3 \text{ chyby}} 0000000 \qquad \text{nedokážeme detekovat}$$

▶ **Věta 3.8.** *Pro váhu d pro [n, k] kód platí*

$$d \leq n - k + 1 \tag{3.4}$$

(viz [17]*) a pro počet chyb t, který je kód schopen opravit, pak platí*

$$t \leq \left\lfloor \frac{n-k}{2} \right\rfloor. \tag{3.5}$$

Ke každému $[n, k]$ lineárnímu kódu máme generující matici $\mathbf{G}^{k\times n}$, která ho generuje, a jejíž k řádků je tvořeno lineárně nezávislými vektory. Matice $\mathbf{G}^{k\times n}$ pro $[n, k]$ lineární kód je standardně ve tvaru

$$\mathbf{G} = (\mathbf{E}|\mathbf{P}), \tag{3.6}$$

kde $\mathbf{E}^{k\times k}$ je jednotková matice a $\mathbf{P}^{k\times(n-k)}$ je libovolná matice.

Každý lineární kód $\mathcal{C}$ leží v jádru nějaké matice $\mathbf{H}$, které říkáme kontrolní matice. Kontrolní matice $\mathbf{H}^{(n-k)\times n}$ pro $[n, k]$ lineární kód je standardně ve tvaru

$$\mathbf{H} = \left(-\mathbf{P}^T|\mathbf{E}\right), \tag{3.7}$$

kde $\mathbf{E}^{(n-k)\times(n-k)}$ je jednotková matice

▶ **Příklad 3.9.** Pro [7, 4] Hammingův kód $\mathcal{C}$, máme generující matici $\mathbf{G}$, která je popsána

$$\mathbf{G} = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}. \tag{3.8}$$

Matice $\mathbf{G}$ pak generuje $\mathcal{C}$:

$$\mathcal{C} = \{\alpha_1(1000110) + \alpha_2(0100111) + \alpha_3(0010101) + \alpha_4(0001011) \mid \forall\alpha_i \in \{0, 1\}\} \subseteq \mathcal{F}_2^7 \tag{3.9}$$

▶ **Příklad 3.10.** Pro [7, 4] Hammingův kód $\mathcal{C}$, máme kontrolní matici $\mathbf{H}$, která je popsána

$$\mathbf{H} = \begin{pmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{pmatrix}. \tag{3.10}$$

▶ **Definice 3.11** (Duální kód)**.** *Pro každý $[n, k]$ lineární kód $\mathcal{C}$ s generující maticí $\mathbf{G}^{k\times n}$ existuje $[n, n-k]$ lineární kód $\mathcal{C}^\perp$, který je generován řádky kontrolní matice $\mathbf{H}^{n-k\times n}$. Kód $\mathcal{C}^\perp$ se nazývá duální kód.*

▶ **Příklad 3.12.** Pro [7, 4] Hammingův kód $\mathcal{C}$ kontrolní matice $\mathbf{H}$ generuje $\mathcal{C}^\perp$:

$$\mathcal{C}^\perp = \{\alpha_1 (1110100) + \alpha_2 (1101010) + \alpha_3 (0111001) \mid \forall \alpha_i \in \{0, 1\}\} \subseteq \mathcal{F}_2^7 \tag{3.11}$$

3.1.1 Detekce a oprava chyb

Při detekci a opravě chyb využíváme tzv. syndromy, které jsou určeny pomocí kontrolní matice.

▶ **Definice 3.13** (Syndrom)**.** *Pro [n, k] lineární kód $\mathcal{C}$ s odpovídající kontrolní maticí $\mathbf{H}$, pro $x \in \mathcal{F}_2^n$ platí*

$$s = \mathbf{H}x^T \in \mathcal{F}_2^{n-k}, \tag{3.12}$$

kde s nazýváme syndromem x.

Uvažujme scénář, kdy nám přijde slovo r ovlivněno nějakou chybou, tedy $r = c+e$, kde $c \in \mathcal{C}$ je původní slovo a $e \in \mathcal{F}_2^n$ je možná chyba. Syndrom příchozího slova r je poté

$$s = \mathbf{H}r^T \in \mathcal{F}_2^{n-k}. \tag{3.13}$$

Pokud je ve zprávě méně než t chyb platí

$$s = \mathbf{H}r^T = \mathbf{H}c^T + \mathbf{H}e^T = \mathbf{H}e^T \tag{3.14}$$

a máme 2^{n-k} různých syndromů. Pokud $s = (0, 0, \ldots, 0)$ tak se ve zprávě neobjevuje žádná chyba, jinak se chyba vyskytuje a syndrom s odpovídá jednomu z možných chybových vektorů e.

Chybu bychom tedy opravili tím, že bychom si připravili tabulků syndromů s chybovými vektory. Pokud nám přijde zpráva r, spočítáme syndrom s, který nám v tabulce udává chybový vektor e, pak stačí odečíst od přijaté zprávy chybu a získáme původní slovo, tedy $c = r - e$.

▶ **Příklad 3.14.** Příklad možné tabulky syndromů pro [7,4] kód :

$$s_0 = \begin{pmatrix}0\\0\\0\end{pmatrix} \to e = 0000000 \qquad s_1 = \begin{pmatrix}1\\1\\0\end{pmatrix} \to e = 1000000 \tag{3.15}$$

$$s_2 = \begin{pmatrix}1\\1\\1\end{pmatrix} \to e = 0100000 \qquad s_3 = \begin{pmatrix}1\\0\\1\end{pmatrix} \to e = 0010000 \tag{3.16}$$

$$s_4 = \begin{pmatrix}0\\1\\1\end{pmatrix} \to e = 0001000 \qquad s_5 = \begin{pmatrix}1\\0\\0\end{pmatrix} \to e = 0000100 \tag{3.17}$$

$$s_6 = \begin{pmatrix}0\\1\\0\end{pmatrix} \to e = 0000010 \qquad s_7 = \begin{pmatrix}0\\0\\1\end{pmatrix} \to e = 0000001 \tag{3.18}$$

3.1.2 Kosety

Koncept kosetů pro nás bude velice důležitý pro zrealizování bezpečného protokolu v dalších kapitolách a proto si v této podkapitole uvedeme jejích základní myšlenku a principy.

▶ **Definice 3.15** (Koset)**.** *Pro lineární kód $\mathcal{C}$ a slovo $x \in \mathcal{F}_2^n$, definujeme koset $x + \mathcal{C}$ jako*

$$x + \mathcal{C} = \{x + c \mid c \in \mathcal{C}\}. \tag{3.19}$$

▶ **Věta 3.16.** *Mějme slova $x_1, x_2 \in \mathcal{F}_2^n$, pokud $x_2 \in x_1 + \mathcal{C}$, kde $\mathcal{C}$ je [n, k] lineární kód, pak platí*

$$x_2 + \mathcal{C} = x_1 + \mathcal{C} \tag{3.20}$$

▶ **Důsledek 3.17.** *Koset $x_2 + \mathcal{C}$ je pro každý prvek $x_2 \in x_1 + \mathcal{C}$ identický a každý prvek je jiný. Tedy 2^k různých slov patří do stejného kosetu.*

▶ **Věta 3.18.** *Mějme slova $x_1, x_2 \in \mathcal{F}_2^n$, pokud $x_2 \notin x_1 + \mathcal{C}$, kde $\mathcal{C}$ je [n, k] lineární kód, pak platí*

$$x_2 + \mathcal{C} \cap x_1 + \mathcal{C} = \emptyset \tag{3.21}$$

▶ **Důsledek 3.19.** *Jelikož jsou kosety $x_2 + \mathcal{C}$ a $x_1 + \mathcal{C}$ disjunktní, počet unikátních kosetů $\mathcal{C}$ v $\mathcal{F}_2^n$ je $\frac{2^n}{2^k} = 2^{n-k}$.*

▶ **Věta 3.20.** *Uvažujme $[n, k_1]$ lineární kód $\mathcal{C}_1$ a $[n, k_2]$ lineární kód $\mathcal{C}_2$, který je netriviálním podprostorem $\mathcal{C}_1$. Pro $x_1, x_2 \in \mathcal{C}_1$ platí,*

$$x_2 \in x_1 + \mathcal{C}_2 \implies x_2 + \mathcal{C}_2 = x_1 + \mathcal{C}_2 \tag{3.22}$$

$$x_2 \notin x_1 + \mathcal{C}_2 \implies x_2 + \mathcal{C}_2 \cap x_1 + \mathcal{C}_2 = \emptyset. \tag{3.23}$$

▶ **Důsledek 3.21.** *Počet kosetů $\mathcal{C}_2$ v $\mathcal{C}_1$ je $2^{k_1 - k_2}$.*

3.2 Posílení soukromí a sladění informací

Při QKD se setkáváme s problémem, kdy se hodnota klíče na jedné straně může lišit od hodnoty na straně druhé, například kvůli šumu nebo odposlechu na kanále. Klíče lišící se už v jednom bitu jsou pro následné použití v symetrické kryptografii nepoužitelné. Jak tedy zajistit, aby obě komunikující strany měly stejné klíče, a co nejméně z nich bylo prozrazeno třetí straně? Technice, která tento problém řeší se říká *posílení soukromí a sladění informací.*

První částí je sladění informací, což označuje proces, při kterém dochází k detekování a odstranění chyb mezi řetězci vlastněnými Alicí a Bobem na klasickém kanále, aby získali totožný řetězec X a přitom prozradili, co nejméně informací Evě. Řekněme, že Eva po tomto procesu vlastní řetězec Y, který je částečně korelován s řetězcem X. Součástí druhého procesu posílení soukromí, je aby Alice a Bob ze svých řetězců X vybrali kratší řetězec S, který bude mít hodnotu korelace s Evy řetězcem Y menší než je chtěná hranice.

Jednou z možných realizací posílení soukromí je využití třídy univerzálních hašovacích funkcí $\mathcal{G}$, která mapuje množinu n–bitových řetězců $\mathcal{A}$ na množinu m–bitových řetězců $\mathcal{B}$. Platí, že pokud je funkce g z třídy $\mathcal{G}$ vybrána zcela náhodně, pro řetězce $a_1, a_2 \in \mathcal{A}$ je pravděpodobnost, že je jejich zahašovaná hodnota bude stejná, tedy $g(a_1) = g(a_2)$, rovna $\frac{1}{|\mathcal{B}|}$ [1].

▶ **Tvrzení 3.22** (Pravděpodobnost kolize)**.** *Nechť je X náhodná diskrétní veličina nad abecedou $\mathcal{X}$ a pravděpodobnostní distribucí P_{X}. Pravděpodobnost kolize $P_c(\mathsf{X})$ veličiny X je definována jako pravděpodobnost, že X nabude dvakrát stejné hodnoty pro dva nezávislé experimenty:*

$$P_c(\mathsf{X}) = \sum_{\forall x \in \mathsf{X}} P_{\mathsf{X}}(x)^2. \tag{3.24}$$

▶ **Definice 3.23** (Entropie kolize)**.** *Pro náhodnou diskrétní veličinu X s pravděpodobností kolize $P_c(\mathsf{X})$ je entropie kolize definována jako*

$$H_c(\mathsf{X}) = -\log_2 P_c(\mathsf{X}). \tag{3.25}$$

▶ **Definice 3.24** (Sdružená entropie)**.** *Sdružená entropie pro náhodné veličiny* X *a* Y *s pravděpodobností* $P_{\mathsf{X},\mathsf{Y}}(\cdot,\cdot)$ *je definována jako*

$$H(\mathsf{X},\mathsf{Y}) = -\sum_{\forall x\in\mathsf{X},\forall y\in\mathsf{Y}} P_{\mathsf{X},\mathsf{Y}}(x,y)\log_2 P_{\mathsf{X},\mathsf{Y}}(x,y). \tag{3.26}$$

Entropie pro náhodnou veličinu X *za podmínky, že známe* Y*, se nazývá podmíněná entropie a platí pro ni*

$$H(\mathsf{X}|\mathsf{Y}) = H(\mathsf{X},\mathsf{Y}) - H(\mathsf{Y}). \tag{3.27}$$

▶ **Definice 3.25** (Sdílená informace)**.** *Sdílená informace* $I(\cdot:\cdot)$ *určuje množství informací, které v sobě má jedna náhodná veličina o druhé náhodné veličině. Pro náhodné veličiny* X *a* Y *je definována jako*

$$I(\mathsf{X}:\mathsf{Y}) = \sum_{\forall x\in\mathsf{X},\forall y\in\mathsf{Y}} P_{\mathsf{X},\mathsf{Y}}(x,y)\log_2\left(\frac{P_{\mathsf{X},\mathsf{Y}}(x,y)}{P_{\mathsf{X}}(x)\,P_{\mathsf{Y}}(y)}\right). \tag{3.28}$$

Těchto definic využijeme, abychom si mohli ukázat větu o univerzálních hašovacích funkcích, která je velmi důležitá při posílení soukromí [18].

▶ **Věta 3.26.** *Nechť je* X *náhodná veličina nad abecedou* $\mathcal{X}$ *s pravděpodobnostní distribucí* P_{X} *a kolizní entropií* $H_c(\mathsf{X})$*. Náhodná velična* G *nám poté náhodně určuje hašovací funkci z třídy univerzálních hašovacích funkcí s definičním oborem* $\mathcal{X}$ *a oborem hodnot* $\{0,1\}^m$*. Poté platí*

$$H(\mathsf{G}(\mathsf{X})|\mathsf{G}) \geq H_c(\mathsf{G}(\mathsf{X})|\mathsf{G}) \geq m - 2^{m-H_c(\mathsf{X})}. \tag{3.29}$$

Při posílení soukromí si tedy Alice s Bobem veřejně vyberou hašovací funkci $g \in \mathcal{G}$ a použijí ji na svůj klíč X, aby získali bezpečnější a kratší klíč S, čímž ještě sníží Evy znalost. Pokud by Evy znalost X byla $Y = y$ a kolizní entropií byla zespodu ohraničená nějakým číslem d, tedy $H_c(X|Y=y) > d$, ze vztahu (3.29) získáváme spodní hranici po aplikování hašovací funkce g:

$$H_c(S|G,Y=y) \geq m - 2^{m-d}. \tag{3.30}$$

Tato nerovnost nám říká, že čím kratší bude výstupní hodnota m hašovací funkce g, tím menší znalost bude Eva o ní mít.

Získali jsme kontrolu nad tím, kolik Eva získá informace z procesu posílení soukromí, teď se ale vrátíme zpět k fázi sladění informací, která také probíhá přes veřejný klasický kanál. Řekněme, že před sladěním informací Alice má řetězec A a Bob má řetězec B, které se od sebe nejspíše liší. Alice pro opravu chyb musí sestrojit zprávu u, která se skládá z původního klíče délky n a k kontrolních bitů, a poslat ji Bobovi. Při přenosu dochází k odposlechu od Evy a ta získá o klíči informaci $U = u$.

▶ **Věta 3.27.** *Nechť jsou* X *a* U *náhodné veličiny nad abecedou* $\mathcal{X}$ *a* $\mathcal{U}$*, kde* X *má pravděpodobnostní distribuci* P_{X} *a* U *je sdružená s* X *s distribucí* $P_{\mathsf{X},\mathsf{U}}$*. Pak s pravděpodobností alespoň* $1-2^{-s}$ U *nabývá hodnoty* u*, pro které platí*

$$H_c(\mathsf{X}|\mathsf{U}=u) \geq H_c(\mathsf{X}) - 2\log|\mathcal{U}| - 2s, \tag{3.31}$$

pro libovolný parametr $s > 0$*.*

Parametr s, kterému říkáme *bezpečnostní parametr*, si Alice a Bob můžou vybrat libovolně pro sladění informací aby omezili Evy kolizní entropii $H_c(\mathsf{X}|\mathsf{Y}=y,\mathsf{U}=u) \geq d-2k-2s$ s pravděpodobností alespoň $1-2^{-s}$. Poté po posílení soukromí je Evy informace o klíči menší než $2^{m-d+2k+2s}$.

Tento souhrn informací nám dává dohromady obecnou mez, kterou můžeme odhadnout Evy informaci po celém procesu.

▶ **Důsledek 3.28.** *Nechť je W náhodný n–bitový řetězec s rovnoměrným rozdělením $\{0,1\}^n$ a nechť $V = e(W)$ je odposlechnutý řetězec pro libovolnou funkci $e : \{0,1\}^n \to \{0,1\}^r$ s parametrem e_t. Buď $s < n - r$ libovolný bezpečnostní parametr a nechť $m = n - r - s$. Pokud si Alice s Bobem zvolí $K = \mathsf{G}(W)$ jako jejich klíč, kde g je jejich společná a náhodně zvolená hašovací funkce z univerzální třídy hašovacích funkcí G z $\{0,1\}^n$ do $\{0,1\}^m$ poté je Evy očekávaná informace o klíči omezena takto:*

$$I(K : gV) \leq \frac{2^{-s}}{\ln 2}, \tag{3.32}$$

kde $I(K : gV)$ značí Evy informaci o sdíleném klíči K pro danou hašovací funkci g a odposlechnutý řetězec V [19].

▶ **Příklad 3.29.** Uvažujme situaci kdy Alice a Bob mají společný n–bitový řetězec například $x = 101110$, kde $n = 6$ a $t = 1$ znamená maximální počet chyb, který dokáží opravit. Navíc předpokládejme, že předpovídají, že Evy znalost ohledně jejich klíče je $r = 2$ bitů, což by znamenalo, že mají zkrátit svoji delku klíče alespoň o 2 bity. Vygenerují si náhodně společnou hašovací funkci, která je dána maticí $\mathbf{G}^{m\times 7}$, kde $m = n - r = 6 - 2 = 4$ a použijí ji na svůj řetězec

$$\mathbf{G} \cdot x^T = \begin{pmatrix} 0 & 1 & 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 0 \\ 1 \\ 1 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 1 \end{pmatrix} \tag{3.33}$$

Jejich sdílený klíč by byl 0101. Pokud by si ale nebyli jistí a chtěli by mít bezpečnější klíč zvolili by si bezpečnostní parametr s, například $s = 3$ a podle toho odpovídající hašovací funkci, danou maticí $\mathbf{G}^{m\times 7}$, kde $m = n - r - s = 6 - 2 - 3 = 1$. S tímto bezpečnostním parametrem by mohli vypočítat horní mez pro Evy informaci o klíčí, tedy $\frac{2^{-3}}{\ln 2} \approx 0,18$ bitů.

Kapitola 4

Protokoly založené na přípravě a měření

V této kapitole si představíme protokoly, založené na principu prvotní přípravy a následovného měření. V těchto protokolech vždy předpokládáme přítomnost dvou komunikujících stran, Alice a Boba, a případnou třetí stranu Evu, která chce jejich sdílení klíče odposlechnout.

4.1 BB84

Prvním QKD protokolem, jenž si ukážeme bude známý protokol BB84, který byl poprvé představen Ch. Bennettem a G. Brassardem v roce 1984. Tento protokol využívá pro fyzickou realizaci polarizaci fotonů pro přenos informace a je nejčastěji realizovaný přenosem přes optická vlákna. Bezpečnost protokolu vychází ze zakódování informace do neortogonálních stavů. BB84 používá dva páry stavů, kde tyto stavy v jednom páru jsou ortogonální a páry samotné představují jednotlivé báze jednoho qubitu. Obvyklá polarizace stavů je v lineární (+) bázi, tedy **Z**-bázi, nebo v diagonální (×) bázi, tedy **X**-bázi. U lineární báze se jedná o polarizaci ve směru 0° ($|0\rangle$) a 90° ($|1\rangle$), u diagonální je to 45° ($|+\rangle$) a 135° ($|-\rangle$) [20].

Tabulka 4.1 Zakódování bitu do qubitu u protokolu BB84

	Bity	
Báze	0	1
+	$\|0\rangle$	$\|1\rangle$
×	$\|+\rangle$	$\|-\rangle$

Algoritmus 1 protokol BB84 za ideálních podmínek

1. Alice si nejdříve musí vygenerovat sekvenci náhodných bitů a_0. Pokud mají v plánu si vygenerovat klíč délky n, měla by si Alice připravit alespoň $2n$ bitů.
2. Alice si poté vygeneruje sekvenci náhodných bitů b_0 stejné délky jako a_0, které budou určovat báze, v kterých Alice své bity zakóduje do qubitů. Pokud příslušný bit z b_0 bude 0, zakóduje bit do báze $\{|0\rangle, |1\rangle\}$, pokud bude 1 tak do báze $\{|+\rangle, |-\rangle\}$.
3. Bob si náhodně vygeneruje sekvenci bitů b_1, které pro každý bit určují **Z**-bázi, pokud $b_1 = 0$, nebo **X**-bázi, když $b_1 = 1$.

4. Alice pak přepošle Bobovi jednotlivé qubity přes nezabezpečený kvantový kanál.

5. Bob oznámí úspěšné přijmutí qubitů a v bázích b_1, které si Bob vygeneroval, provede měření přicházejících qubitů a získá výsledek a_1.

6. Alice i Bob si poté přes klasický kanál zveřejní informace o tom v jakých bázích pro každý bit pracovali. Všechny bity, v kterých se neshodli na vybraných bází, zahodí. Mají u každého qubitu pravděpodobnost $\frac{1}{2}$, že zvolili stejné báze, a tudíž střední hodnota počtu správně změřených qubitů je n. Pokud jim nezůstane alespoň n bitů, zruší průběh protokolu a začnou znovu.

7. Alice si ze svých zbývajících bitů a_0 vybere posloupnost přesně n bitů, pokud jich zbylo více než n. Tyto bity budou sloužit jako klíč a Alice oznámí Bobovi, jaké jsou pozice bitů, které vybrala.

4.1.1 Odposlech protokolu BB84

Jako při každém typu komunikace, musíme pracovat s faktem, že nás někdo může odposlouchávat, při distribuci klíče to není jiné. Dokonce můžeme říct, že je to více pravděpodobné a nebezpečné. Představíme si bezpečnostní prvky protokolu BB84 a možný scénář odposlechu od třetí strany Evy.

Aby Alice a Bob zjistili přítomnost Evy na kanále, provádí obětování několika kontrolních bitů. Tento proces je založen na myšlence, že pokud zvolili stejné báze ($b_0 = b_1$), měli by se rovnat hodnoty jejich odpovívajících bitů ($a_0 = a_1$). Pokud se tyto hodnoty nerovnají, může to být způsobeno chybovostí kanálu nebo přítomností Evy.

Algoritmus 2 protokol BB84 s detekcí odposlechu

---

1. Alice si nejdříve musí vygenerovat sekvenci náhodných bitů a_0. Pokud mají v plánu si vygenerovat klíč délky n, měla by si Alice připravit alespoň $2\,(n+m)$ bitů, kde m udává počet kontrolních bitů, které budou obětovány pro detekci Evy.

2. Alice si poté vygeneruje sekvenci náhodných bitů b_0 stejné délky jako a_0, které budou určovat báze, v kterých Alice své bity zakóduje do qubitů. Pokud příslušný bit z b_0 bude 0, zakóduje bit do báze $\{|0\rangle, |1\rangle\}$, pokud bude 1 tak do báze $\{|+\rangle, |-\rangle\}$.

3. Bob si náhodně vygeneruje sekvenci bitů b_1, které pro každý bit určují **Z**-bázi, pokud $b_1 = 0$, nebo **X**-bázi, když $b_1 = 1$.

4. Alice pak přepošle Bobovi jednotlivé qubity přes nezabezpečený kvantový kanál.

5. Bob oznámí úspěšné přijmutí qubitů a v bázích b_1, které si Bob vygeneroval, provede měření přicházejících qubitů a získá výsledek a_1.

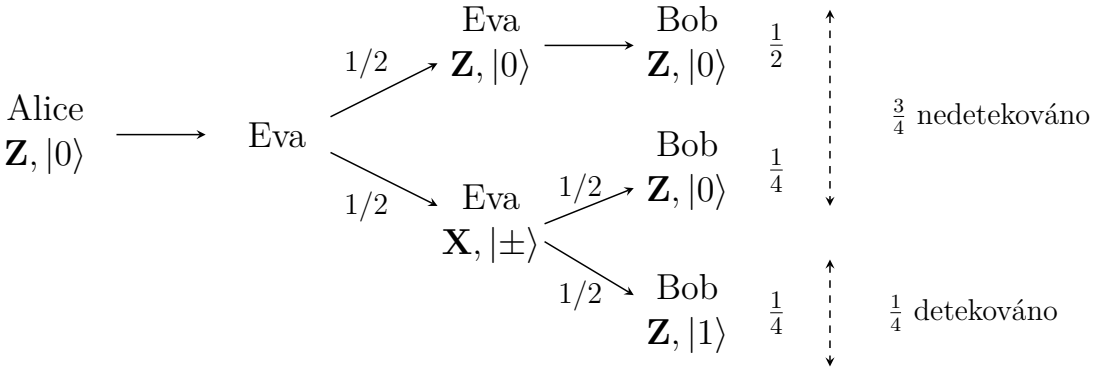
6. Alice i Bob si poté přes klasický kanál zveřejní informace o tom v jakých bázích pro každý bit pracovali. Všechny bity, v kterých se neshodli na vybraných bází, zahodí. Mají u každého qubitu pravděpodobnost $\frac{1}{2}$, že zvolili stejné báze, a tudíž střední hodnota počtu správně změřených qubitů je $n+m$. Pokud jim nezůstane alespoň $n+m$ bitů, zruší průběh protokolu a začnou znovu.

7. Alice si ze svých zbývajících bitů a_0 vybere posloupnost alespoň m bitů, tak aby jí přesně n bitů zůstalo. Tyto bity budou sloužit pro kontrolu průběhu přenosu a Alice oznámí Bobovi, jaké jsou pozice bitů, které vybrala.

8. Alice s Bobem si spolu veřejně porovnají hodnoty vybraných kontrolních bitů. Pokud se neshodují v nějakém bitu, nejspíše došlo k odposlechu nebo chybnému přenosu, proto opustí protokol a začnou znovu.

9. Alice s Bobem nyní sdílí posloupnost n bitů a ty tvoří jejich klíč.

Eva má mnoho možností útoku, které může provést. Jedním z nich je útok založený na změření a přeposlání fotonů, kdy Eva změří fotony poslané Alicí, a poté přepošle fotony připravené ve stavu, které sama naměří. Eva nemá jinou možnost než fotony změřit, jelikož platí nemožnost klonování, a tedy při jejich měření dojde ke kolapsu poslaného stavu. Stejně jako Bob, Eva také nemá žádné informace o tom, jaké polarizace Alice zvolila a tudíž ji nezbývá nic jiného než pouze hádat. Pokud Eva zvolila bázi správně, změří správný stav, který Alice poslala, a přepošle i správný stav Bobovi, který nemá šanci to poznat. Ovšem pokud Eva vybrala špatnou bázi, její výsledek měření je náhodný a s pravděpodobností $\frac{1}{2}$ nebude správný, tedy Bob někdy obdrží jiný než původní stav. Pravděpodobnosti možných výsledků mohou býti vyjádřeny tímto diagramem:



Obrázek 4.1 Pravděpodobnost detekování odposlechu u protokolu BB84

Z 4.1 lze jednoduše vyčíst, že Alice s Bobem mají u každého qubitu pravděpodobnost $\frac{1}{4}$ na detekování Evy. To znamená, že pokud si Alice a Bob vymění m kontrolních bitů, pravděpodobnost, že naleznou neshodující se bity a poznají Evy přítomnost na kanále je

$$P_d = 1 - \left(\frac{3}{4}\right)^m. \tag{4.1}$$

Pro představu, pokud by si Alice s Bobem vyměnili 41 kontrolních bitů, měli by pravděpodobnost $P_d = 0,999992\ldots$, že dokáží detekovat Evu [21]. V tomto případě se jedná o bezchybový kanál, při samotném přenosu pracujeme s kanálem, který je nějakým způsobem chybový. To pro nás znamená, že můžeme detekovat chybu na kontrolních bitech, která je způsobena pouze kanálem, proto do naší pravděpodobnosti musíme přidat i možnost chybné detekce odposlechu a pravděpodobnost detekce odposlechu bude vypadat takto:

$$P_d = 1 - \left(\frac{3}{4}\right)^m - \left(\frac{1}{4}\delta\right)^m, \tag{4.2}$$

kde δ je pravděpodobnost chyby qubitu na kanále.

Ostatní strategie útoků jsou často založeny na principu změření a přeposlání fotonů s přidáním nějakých prvků navíc, například posílání světelných pulzů do přijímacího zařízení. Tyto typy útoků jsou nad rámec tohoto textu a proto si je zde nebudeme uvádět.

Tabulka 4.2 Příklad protokolu BB84 s detekcí odposlechu s 14 qubity

	1	2	3	4	5	6	7	8	9	10	11	12	13	14
Alice bity	1	1	0	1	1	1	1	0	1	1	1	0	1	1
Alice bity báze	0	1	1	0	1	0	0	0	1	0	0	0	1	1
Alice báze	+	×	×	+	×	+	+	+	×	+	+	+	×	×
Alice přepošle	$\|1\rangle$	$\|-\rangle$	$\|+\rangle$	$\|1\rangle$	$\|-\rangle$	$\|1\rangle$	$\|1\rangle$	$\|0\rangle$	$\|-\rangle$	$\|1\rangle$	$\|1\rangle$	$\|0\rangle$	$\|-\rangle$	$\|-\rangle$
Bobovy bity báze	1	1	0	0	1	1	0	0	0	0	1	0	1	0
Bobova báze	×	×	+	+	×	×	+	+	+	+	×	+	×	+
Bob změří	$\|+\rangle$	$\|-\rangle$	$\|0\rangle$	$\|1\rangle$	$\|-\rangle$	$\|-\rangle$	$\|1\rangle$	$\|1\rangle$	$\|0\rangle$	$\|1\rangle$	$\|+\rangle$	$\|0\rangle$	$\|-\rangle$	$\|1\rangle$
Hodnoty měření	0	1	0	1	1	1	1	0	0	1	0	0	1	1
Veřejná diskuze		1		1	1		1	0		1		0	1	
Sdílený klíč		1			1			0					1	

4.1.2 Realizace protokolu BB84 s chybovým kanálem

Kromě přítomnosti odposlouchávajícího se musíme vypořádat i s dalšími problémy omezující bezpečnost, takovým problémem je samotný přenos, který je s dnešní realizací těžký vyřešit bez chybovosti. Mezi chyby, se kterými se setkáváme na kvantovém kanále patří chyby v převrácení bitu a fáze. Při převrácení bitu dochází k změně stavu qubitu, kdy je hodnota změřeného bitu převrácena a při převrácení fáze dochází ke změně relativní fáze qubitu.

V našem algoritmu 3 používáme sadu kontrolních bitů, které využíváme k detekci odposlechu na kanále. Pokud se nějaká dvojice bitů nerovná, můžeme se domnívat, že došlo k předešlému narušení kvantového stavu a došlo k odposlechu. Problém s tímto schématem je takový, že pracujeme s kanály, které se svojí chybovostí pohybují v jednotkách procent, z toho důvodu by bylo předčasné se domnívat, že pokud se naše bity nerovnají, je to způsobeno třetí stranou. Jak se tedy tohoto problému zbavit? Využijeme techniky posílení soukromí a sladění informací 3.2

Algoritmus 3 protokol BB84 s chybovým kanálem

1. Alice si nejdříve musí vygenerovat sekvenci náhodných bitů a_0. Pokud mají v plánu si vygenerovat klíč délky n, měla by si Alice připravit alespoň $2(n+m+v)$ bitů, kde m udává počet kontrolních bitů, které budou obětovány pro detekci Evy, a v udává počet bitů, které budou použity pro finální posílení soukromí a sladění informace.

2. Alice si poté vygeneruje sekvenci náhodných bitů b_0 stejné délky jako a_0, které budou určovat báze, v kterých Alice své bity zakóduje do qubitů. Pokud příslušný bit z b_0 bude 0, zakóduje bit do báze $\{|0\rangle, |1\rangle\}$, pokud bude 1 tak do báze $\{|+\rangle, |-\rangle\}$.

3. Bob si náhodně vygeneruje sekvenci bitů b_1, které pro každý bit určují **Z**-bázi, pokud $b_1 = 0$, nebo **X**-bázi, když $b_1 = 1$.

4. Alice pak přepošle Bobovi jednotlivé qubity přes nezabezpečený kvantový kanál.

5. Bob oznámí úspěšné přijmutí qubitů a v bázích b_1, které si Bob vygeneroval, provede měření přicházejících qubitů a získá výsledek a_1.

6. Alice i Bob si poté přes klasický kanál zveřejní informace o tom v jakých bázích pro každý bit pracovali. Všechny bity, v kterých se neshodli na vybraných bází, zahodí. Mají u každého qubitu pravděpodobnost $\frac{1}{2}$, že zvolili stejné báze, a tudíž střední hodnota počtu správně

změřených qubitů je $n + m + v$. Pokud jim nezůstane alespoň $n + m + v$ bitů, zruší průběh protokolu a začnou znovu.

7. Alice si ze svých zbývajících bitů a_0 vybere posloupnost alespoň m bitů, tak aby jí přesně $n + v$ bitů zůstalo. Tyto bity budou sloužit pro kontrolu průběhu přenosu a Alice oznámí Bobovi, jaké jsou pozice bitů, které vybrala.

8. Alice s Bobem si spolu veřejně porovnají hodnoty vybraných kontrolních bitů. Pokud se neshodují ve větším počtu bitů než je nastavená hranice t určená experimentálním testováním chybovosti kanálu, nejspíše došlo k odposlechu nebo chybnému přenosu, proto opustí protokol a začnou znovu.

9. Alice a Bob na závěr mohou provést posílení soukromí a sladění informací na zbývajích $n+v$ bitech, aby získali n bitů sdíleného klíče.

Nyní se podíváme na konkrétní realizaci bezpečného protokolu, jehož posílení soukromí a sladění informací bude stát na myšlence lineárních kosetů 3.1.2 vyvořených pomocí lineárních kódů $\mathcal{C}_1$ a $\mathcal{C}_2$. Kód $\mathcal{C}_1$ bude sloužit k sladění informací, tedy opravě chyb, kdy si Alice bude náhodně vybírat kódové slovo z $\mathcal{C}_1$, pomocí kterého Bob svoji zprávu opraví. Kód $\mathcal{C}_2$ poté hraje roli v posílení soukromí, kdy jeho koset v $\mathcal{C}_1$ bude sloužit k vygenerování finálního klíče [22].

Aby protokol správně fungoval musí se Alice s Bobem před spuštěním protokolu dohodnout na volbě $\mathcal{C}_1$ a $\mathcal{C}_2$. Výběr kódů pak musí splňovat tyto podmínky:

- Kód $\mathcal{C}_1$ je $[n_1, k_1]$ lineární kód, který dokáže opravit až t chyb.
- Kód $\mathcal{C}_2$ je $[n_1, k_2]$ lineární kód, pro který platí $\mathcal{C}_2 \subset \mathcal{C}_1$, kdy duální kód $\mathcal{C}_2^{\perp}$ dokáže opravit až t chyb.
- Pro dimenze k_1 a k_2 platí, že $k = k_1 - k_2$ se rovná délce chtěného klíče.

▶ Poznámka 4.1. Výběr kódů, aby dokázali opravit t chyb, je rozhodnut podle předešlých testování chybovosti kanálu.

Algoritmus 4 bezpečný protokol BB84

---

1. Alice si nejdříve musí vygenerovat sekvenci náhodných bitů a_0. Pokud mají v plánu si vygenerovat klíč délky n, měla by si Alice připravit alespoň $2\,(wn_1 + m)$ bitů, kde m udává počet kontrolních bitů, které budou obětovány pro detekci Evy a $w = \frac{n}{\log_2\left(2^{k_1 - k_2}\right)}$.

2. Alice si poté vygeneruje sekvenci náhodných bitů b_0 stejné délky jako a_0, které budou určovat báze, v kterých Alice své bity zakóduje do qubitů. Pokud příslušný bit z b_0 bude 0, zakóduje bit do báze $\{|0\rangle, |1\rangle\}$, pokud bude 1 tak do báze $\{|+\rangle, |-\rangle\}$.

3. Bob si náhodně vygeneruje sekvenci bitů b_1, které pro každý bit určují **Z**-bázi, pokud $b_1 = 0$, nebo **X**-bázi, když $b_1 = 1$.

4. Alice si náhodně vygeneruje w kódových slov $v_i \in \mathcal{C}_1$ pro $i = 1, \ldots, w$, která jsou o délce n_1.

5. Alice pak přepošle Bobovi jednotlivé qubity, které reprezentují náhodné bity a_0, přes nezabezpečený kvantový kanál.

6. Bob oznámí úspěšné přijmutí qubitů a v bázích b_1, které si Bob vygeneroval, provede měření přicházejících qubitů a získá výsledek a_1.

7. Alice i Bob si poté přes klasický kanál zveřejní informace o tom v jakých bázích pro každý bit pracovali. Všechny bity, v kterých se neshodli na vybraných bází, zahodí. Mají u každého qubitu pravděpodobnost $\frac{1}{2}$, že zvolili stejné báze, a tudíž střední hodnota počtu správně změřených qubitů je $wn_1 + m$. Pokud jim nezůstane alespoň $wn_1 + m$ bitů, zruší průběh protokolu a začnou znovu.

8. Alice si ze svých zbývajících bitů a_0 vybere posloupnost alespoň m bitů, tak aby jí wn_1 bitů zůstalo. Tyto bity budou sloužit pro kontrolu průběhu přenosu a Alice oznámí Bobovi, jaké jsou pozice bitů, které vybrala.

9. Alice s Bobem si spolu veřejně porovnají hodnoty vybraných kontrolních bitů. Pokud se neshodují ve větším počtu bitů než je nastavená hranice t určená experimentálním testováním chybovosti kanálu, nejspíše došlo k odposlechu nebo chybnému přenosu, proto opustí protokol a začnou znovu.

10. Alici po kontrole zůstal wn_1–bitový řetězec x a Bobovi zůstal řetězec $x+e$, kde e značí chybu. Alice s Bobem rozdělí své řetězec do w bloků o délce n_1, které značíme x_i pro $i = 1, \ldots, w$.

11. Alice provede $x_i - v_i$ pro všechny své řetězce a zveřejní výsledky. Bob tyto zprávy odečte od svých řetězců, tedy $(x_i + e_i) - (x_i - v_i)$ a pomocí tabulky syndromů pro kód $\mathcal{C}_1$ opraví chyby e_i, aby získal v_i.

12. Alice s Bobem vypočítají koset $v_i + \mathcal{C}_2$ v $\mathcal{C}_1$ pro všechna v_i, kde index kosetu, do kterého $v_i + \mathcal{C}_2$ patří, tvoří $\log_2\left(2^{k_1-k_2}\right)$ bitů jejich sdíleného klíče o délce n.

▶ **Příklad 4.2.** Nechť Alice s Bobem používají pro svoji komunikaci [7, 4] Hammingův kód $\mathcal{C}_1$ a [7, 3] kód $\mathcal{C}_2$, který je určený duálním kódem $\mathcal{C}_1$, tedy $\mathcal{C}_2 = \mathcal{C}_1^{\perp}$, pro který platí $\mathcal{C}_2 \subset \mathcal{C}_1$.

Alice původní vygenerované bity klíče byly $x = 1101010$ a náhodně si vygenerovala kódové slovo $v = 0011110 \in \mathcal{C}_1$. Uvažujme situaci kdy Bob změřením qubitů získá zprávu s převráceným prvním bitem $x+e = 1101010+1000000 = 0101010$. Alice poté zveřejní řetězec $x-v = 1110100$, jelikož ten se skládá z dvou náhodných neveřejných řetězců, jejich výsledek po odečtení se veřejně chová také jako náhodný, jelikož z něj nejdou s jistotou zrekonstruovat původní řetězce. Po přijmutí si Bob odečte přijatou zprávu od svého chybného řetězce:

$$r = (x + e) - (x - v) = 0101010 - 1110100 = 1011110. \tag{4.3}$$

Bob poté vypočítá syndrom s, aby identifikoval pomocí tabulky syndromů 3.14 chybu e:

$$s = \mathbf{H}r^T = \begin{pmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 0 \\ 1 \\ 1 \\ 1 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}, \tag{4.4}$$

$$s = \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} \rightarrow e = 1000000. \tag{4.5}$$

Pomocí chyby pak získá kódové slovo v:

$$v = r - e = 1011110 - 1000000 = 0011110. \tag{4.6}$$

Víme, že pro $\mathcal{C}_2 \subset \mathcal{C}_1$ existuje $2^{4-3} = 2$ unikátních kosetů. Tyto kosety jsou idexovány binárním číslem a popsány následovně

$$0 = \{0000000, 0011110, 0100111, 0111001, 1001101, 1010011, 1101010, 1110100\} \tag{4.7}$$

$$1 = \{0001011, 0010101, 0101000, 0110010, 1000110, 1011000, 1100001, 1111111\} \tag{4.8}$$

Alice s Bobem nakonec spočítají do jakého kosetu jejich kódové slovo patří

$$v = 0011110 \rightarrow v + \mathcal{C}_2 = \{0000000, 0011110, \ldots, 1101010, 1110100\} \tag{4.9}$$

Alice s Bobem tímto způsobem získali index kosetu, do kterého patří jejich kódové slovo v, a tím získali jeden bit společného a naprosto bezpečného klíče $k = 0$.

4.2 B92

V roce 1992, Charles Bennett navrhnul ve své práci [23] novou modifikaci protokolu BB84, která nese název B92. Hlavním rozdílem mezi protokoly je, že zatímco BB84 využívá 4 polarizační stavy fotonu, protokol B92 využívá pouze 2 polarizační stavy. Jedná se o polarizační stavy lineární báze ve směru 0° ($|0\rangle$) a diagonální báze ve směru 45° ($|+\rangle$).

Algoritmus 5 protokol B92

1. Alice si nejdříve musí vygenerovat sekvenci náhodných bitů a_0.Pokud mají v plánu si vygenerovat klíč délky n, měla by si Alice připravit alespoň $4\,(n + m + v)$ bitů, kde m udává počet kontrolních bitů, které budou obětovány pro detekci Evy, a v udává počet bitů, které budou použity pro finální posílení soukromí a sladění informace.
2. Každý qubit pak zakóduje podle hodnoty odpovídajícího bitu. Pokud se bit bude rovnat 0, qubit připraví ve stavu $|0\rangle$, pokud se bude rovnat 1, připraví ho ve stavu $|+\rangle$
3. Bob si náhodně vygeneruje sekvenci bitů a_1, které pro každý bit určují **Z**-bázi, pokud $a_1 = 0$, nebo **X**-bázi, když $a_1 = 1$.
4. Alice pak přepošle Bobovi jednotlivé qubity přes kvantový kanál.
5. Bob oznámí úspěšné přijmutí qubitů a v bázích a_1, které si Bob vygeneroval, provede měření přicházejících qubitů a získá výsledek b_1.
6. Bob veřejně sdělí Alici výsledek měření b_1.
7. Alice i Bob si poté ze svých bitů a_0,a_1 nechají jen ty páry, pro které, byl výsledek měření $b_1 = 1$. Pokud jich nezůstane alespoň $n + m + v$, přeruší průběh protokolu a začnou znovu.
8. Alice si ze svých zbývajících bitů a_0 vybere posloupnost alespoň m bitů, tak aby jí zůstalo $n + v$ bitů. Tyto bity budou sloužit pro kontrolu průběhu přenosu a Alice oznámí Bobovi, jaké jsou pozice bitů, které vybrala.
9. Alice s Bobem si spolu veřejně porovnají hodnoty vybraných kontrolních bitů. Pokud se neshodují ve větším počtu bitů než je nastavená hranice t určená experimentálním testováním chybovosti kanálu, nejspíše došlo k odposlechu nebo chybnému přenosu, proto opustí protokol a začnou znovu.
10. Alice a Bob na závěr mohou provést posílení soukromí a sladění informací na zbývajích $n+v$ bitech, aby získali n bitů sdíleného klíče.

► Poznámka 4.3. Využití lineárních kódů jako posílení soukromí a sladění informací v BB84, může být použito stejným způsobem pro B92.

Můžeme si všimnout, že pokud platí $a_0 = a_1$, výsledkem Bobova měření bude vždy $b_1 = 0$. Pouze pokud $a_0 \neq a_1$ může výsledkem Bobova měření s pravděpodobností $\frac{1}{2}$ být $b_1 = 1$. Dále můžeme vypozorovat zásadní rozdíl oproti protokolu BB84, kdy ve veřejné diskuzi sdílí informace pouze Bob a sděluje výsledky svého měření namísto bází, ve kterých měřil. Výsledný klíč je tedy vytvořen sekvencí bitů původně určující báze a ne výsledky měření. Bity určující báze jsou ale pro výsledek $b_1 = 1$ vždy opačné, pro vytvoření finálního klíče si Bob vždy své bity a_1 ponechá a Alice své bity a_0 zneguje. Posledním značným rozdílem je, že uskutečnění protokolu B92 je mnohem náročnější na počet qubitu. Zatímco u BB84 mají strany pravděpodobnost $\frac{1}{2}$, že si vyberou stejné báze, u B92 mají pravděpodobnost pouze $\frac{1}{4}$, že hodnota bitu b_1 se bude rovnat 1, znázorněno v 4.3 [24].

Tabulka 4.3 Mechanismus protokolu B92

Alice vygenerované bity	$a_0 = 0$				$a_0 = 1$			
Alice posílá stav	$\|0\rangle$				$\|+\rangle$			
Bobovy vygenerované bity	$a_1 = 0$		$a_1 = 1$		$a_1 = 0$		$a_1 = 1$	
Bobovy báze	+		×		+		×	
Bobovy výsledky měření	$\|0\rangle$	$\|1\rangle$	$\|+\rangle$	$\|-\rangle$	$\|0\rangle$	$\|1\rangle$	$\|+\rangle$	$\|-\rangle$
Hodnoty měření	0	-	0	1	0	1	0	-
Pravděpodobnost	1	0	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$	1	0

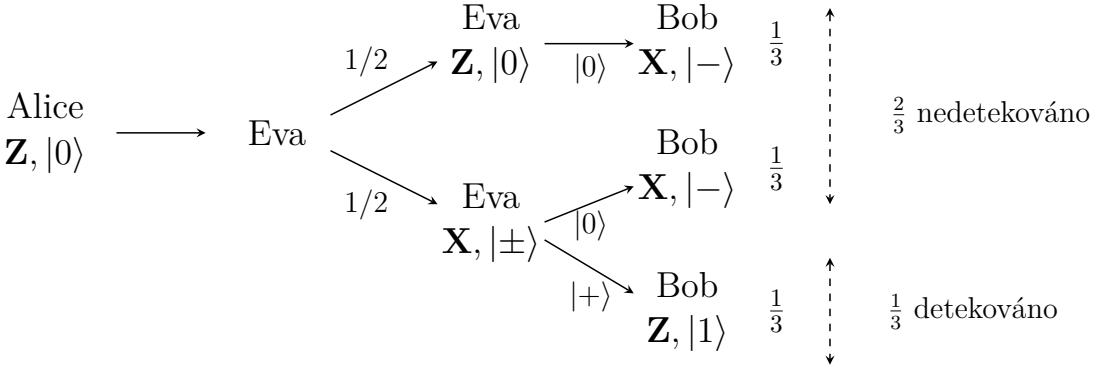
Tabulka 4.4 Příklad protokolu B92 s 14 qubity

	1	2	3	4	5	6	7	8	9	10	11	12	13	14
Alice bity	0	1	1	0	0	1	0	1	1	1	0	0	0	1
Alice báze	+	×	×	+	+	×	+	×	×	×	+	+	+	×
Alice přepošle	$\|0\rangle$	$\|+\rangle$	$\|+\rangle$	$\|0\rangle$	$\|0\rangle$	$\|+\rangle$	$\|0\rangle$	$\|+\rangle$	$\|0\rangle$	$\|0\rangle$	$\|0\rangle$	$\|0\rangle$	$\|-\rangle$	$\|+\rangle$
Bobovy bity	1	1	0	0	1	1	0	0	0	1	0	1	0	0
Bobova báze	×	×	+	+	×	×	+	+	+	×	+	×	+	+
Bob změří	$\|-\rangle$	$\|+\rangle$	$\|0\rangle$	$\|0\rangle$	$\|-\rangle$	$\|+\rangle$	$\|0\rangle$	$\|1\rangle$	$\|1\rangle$	$\|+\rangle$	$\|0\rangle$	$\|+\rangle$	$\|0\rangle$	$\|0\rangle$
Hodnoty měření	1	0	0	0	1	0	0	1	1	0	0	0	0	0
Veřejná diskuze	1				1			0	0					
Sdílený klíč					1			0						

4.2.1 Odposlech protokolu B92

Aby Alice a Bob zjistili přítomnost Evy na kanále, provádí obětování několika kontrolních bitů. Tento proces je založen na myšlence, že pokud Bobův výsledek měření bitu b_1 byl roven 1, museli s Alicí zvolit opačné báze $a_0 \neq a_1$. Pokud se hodnoty jejich bází rovnají, může to být způsobeno chybovostí kanálu nebo přítomností Evy.

Ukážeme si případ kdy si Eva zvolí stejný typ útoku založený na změření a přeposlání fotonů jako jsme si ukázali v podkapitole 4.1.1. Eva si opět bude generovat náhodně v jaké bázi bude měřit a změří přicházející fotony. Evy optimální strategie se odvíjí od výsledku, který z měření získá. Pokud získá 1, musela mít jinou bázi než v které Alice qubit zakódovala, jak vídíme v tabulce 4.3, a tedy qubit, který chce poslat Bobovi, zakóduje v jiné bázi než v které měřila. Pokud ale získá 0, podle pravděpodobnosti je rozumné se domnívat, že zvolila stejnou bázi jako Alice, a proto v této bázi také zakóduje qubit, který pošle Bobovi. Pravděpodobnosti možných výsledků mohou býti vyjádřeny diagramem na obrázku 4.2.



Obrázek 4.2 Pravděpodobnost detekování odposlechu u protokolu B92

Z diagramu 4.2 lze jasně vyčíst, že Alice s Bobem mají u každého qubitu pravděpodobnost $\frac{1}{3}$ na detekování Evy. To znamená, že pokud si Alice s Bobem vymění m kontrolních bitů, pravděpodobnost, že naleznou neshodující se bity a poznají Evy přítomnost na kanále je

$$P_d = 1 - \left(\frac{2}{3}\right)^m. \tag{4.10}$$

Pro představu, pokud by si Alice s Bobem vyměnili 29 kontrolních bitů, měli by pravděpodobnost $P_d = 0,999992\ldots$, že dokáží detekovat Evu. Na kanále s pravděpodobností chyby qubitu δ je pravděpodobnost detekce

$$P_d = 1 - \left(\frac{2}{3}\right)^m - \left(\frac{1}{3}\delta\right)^m. \tag{4.11}$$

4.2.2 Srovnání protokolu B92 s BB84

Naše porovnání protokolů bude probíhat zejména ve dvou kategoriích. První kategorií je náročnost přípravy a komunikace jako takové. Druhá kategorie se zabývá bezpečností a odhadu Evy informace o klíči. Techniky pro opravu chyb a získání vyšší bezpečnosti pomocí úprav na finálním klíči nebudou v porovnání, jelikož jsou pro oba protokoly stejné.

Protokol BB84 využívá 4 polarizační stavy, zatímco protokol B92 jen 2 stavy. B92 je tedy jednodušší na přípravu pro zdroj fotonů, který kvantovou komunikaci zprostředkovává. Z experimentálních výsledků se ale ukazuje, že samotný přenos na dlouhé vzdálenosti je méně chybový a více stabilní pro protokol BB84 [25]. Tento výsledek je způsoben částečně tím, že tyto

2 polarizační stavy využívající se u B92 jsou k sobě vzdálenostně bližší. Z toho důvodu, na delší vzdálenosti při chybovějších kvantových kanálech a detekovacích optických zařízení jsou lehce náchylnější k záměně těchto stavů. Další nevýhodou B92 oproti BB84 je potřeba pro vyšší počet qubitů v přenosu. Tato potřeba je způsebena tím, že při BB84 je střední hodnota pravděpodobnosti pro získání bitu na vytvoření klíče 50%, kdežto u B92 je pouze 25%. To znamená, že B92 potřebuje dvojnásobné množství qubitů pro stejný počet bitů na klíč. I když u B92 probíhá více kvantové komunikace, probíhá při něm méně klasické komunikace, jelikož Bobovi stačí zveřejnit výsledky měření a nemusí si vyměnit informace o bázích, v kterých oba pracovali jako u BB84.

Finální délka klíče závisí jak na původních přeposlaných qubitech, tak na chybovosti způsobenou šumem nebo Evou. U obou protokolů můžeme prohlásit, že obecně platí, čím více qubitů posláno, tím větší délka klíče může být. Zaprvé si můžeme všimnout, že Evy informace o klíči u měření je rozdílná. V protokolu B92 má Eva 25% šanci, že získá výsledek bitu 1, jestliže naměří výsledek 0, neví o původní bázi nic. Bob má též šanci 25% na naměření 1, jinak bit nebude použit. U BB84 má Eva šanci 50%, že vybere správnou bázi a Bob také 50%, aby byl bit použit. Pro srovnání Alice s Bobem mají u každého bitu, který chtějí použít pro svůj klíč, pravděpodobnost 75% u B92 a 50% u BB84, že Eva nenese informaci o hodnotě tohoto bitu jejich klíče. Dalším porovnávacím kritériem je kolik kontrolních bitů musí Alice s Bobem obětovat pro detekování Evy. Pro B92 máme pro m kontrolních bitů pravděpodobnost detekování Evy $P_d = 1 - \left(\frac{2}{3}\right)^m$, zatímco u BB84 máme $P_d = 1 - \left(\frac{3}{4}\right)^m$. Pokud bychom chtěli mít $P_d = 0,999992\ldots$, musíme použít 29 kontrolních bitů u B92 a u BB84 41 bitů. Na závěr můžeme prohlásit, že i když u obou protokolů můžeme dosáhnout stejné úrovně bezpečnosti, předpoklady pro její dosažení jsou rozdílné.

Kapitola 5

Protokoly založené na kvantovém provázání

5.1 Bellovy nerovnosti

5.1.1 EPR paradox

V roce 1935, Einstein, Podolsky a Rosen publikovali práci [12] se jménem „*Může být kvantově mechanický popis světa považován za úplný?*“, ve které se zaměřovali na nedostatky a neúplnost kvantové mechaniky. Einstein ve své Teorii relativity pracuje s myšlenkou, že se nic prostorem nemůže pohybovat rychleji než rychlost světla. Tato představa, že žádný vliv se nemůže šířit rychleji než světlo, se nazývá *lokálnost*. V jejich práci pak využívají myšlenky lokálnosti, s kterou vznikají pochybnosti nad úplností kvantové mechaniky.

Abychom si vysvětlili hlavní myšlenku EPR paradoxu, začneme s myšlenkovým experimentem, kdy Alice i Bob mají jeden qubit z páru popsaným Bellovým stavem $|\beta_{00}\rangle$. Nyní uvažujme, že Alice změří svůj qubit a Bob změří svůj qubit ihned poté. Pokud by tedy Alicin qubit přešel do stavu $|0\rangle$, Bobův by musel přejít též do stavu $|0\rangle$, protože prvním Aliciným měřením by provázaný stav přešel do stavu $|00\rangle$. Znamená to tedy, že pokud by byl Bob dostatečně daleko se svým provázaným qubitem, informace o přechodu stavu Bobova qubitu by se propagovala rychleji než je rychlost světla? EPR paradox tedy říká, že aby toto bylo možné, výsledek měření musí být předem určený nějakou *skrytou proměnnou*, s kterou kvantová mechanika nepočítá. Této domněnce, která říká, že qubity mají nějaké předdefinované reálné hodnoty před samotným měřením se říká *realismus*.

EPR paradox nepracuje s myšlenkou nesprávnosti kvantové mechaniky, ale s její neúplností. Domnívali se, že přijde nová teorie, která tyto jevy skryté proměnné vysvětlí a nahradí tak kvantovou mechaniku. Tento paradox byl publikován v době, kdy nebyla k dispozici potřebná hardwarová vybavení k provedení experimentů pro potvrzení těchto teorií. Až s příchodem potřebného vybavení, výsledky experimentů hovořily ve prospěch kvantové mechaniky namísto lokálního realismu [12].

5.1.2 Bellova a CHSH nerovnost

První návrh experimentu potvrzující zákony kvantové mechaniky oproti teoriím skryté proměnné byl publikován v roce 1964 J. S. Bellem [26]. Předpokládejme, že máme zdroj, který připraví dvě částice a pošle jednu Alici a druhou Bobovi, s možností kdykoliv tento proces opakovat. Alice i Bob mají každý své dva měřící aparáty a můžou si zvolit, kterou vlastnost budou měřit.

Těmto vlastnostem odpovídají různé báze měření a vybrané vlastnosti označíme A_0, A_1 pro Alici a B_0, B_1 pro Boba. Dále předpokládejme, že hodnota vlastnosti A_0 je označována jako a_0 a může nabývat pouze výsledků +1 a -1, pro ostatní vlastnosti funguje stejně. Nechť měření Alice i Boba probíhají současně, tedy jejich výsledky měření se nemohou navzájem ovlivňovat. Uvažujme kombinaci naměřených hodnot vyjádřenou jako:

$$a_0b_0 + a_0b_1 + a_1b_0 - a_1b_1 = (a_0 + a_1)\, b_0 + (a_0 - a_1)\, b_1. \tag{5.1}$$

Víme, že a_0 i a_1 mohou nabývat pouze hodnot ± 1, tedy musí platit buď $a_0 = a_1$ nebo $a_0 = -a_1$. Z toho vyplývá, že buď $(a_0 + a_1)\, b_0 = 0$ nebo $(a_0 - a_1)\, b_1 = 0$. To znamená, že pokud je jedna část rovna 0, druhá část musí nutně nabývat hodnot ± 2. Alice s Bobem ale nemůžou vyhodnotit výsledky měření obou stran rovnice jedním měřením, jelikož můžou pro každé měření zvolit pouze jednu kombinaci A a B, tento experiment provedou několikrát, aby získali střední hodnoty pro různé kombinace.

Nechť $P\,(a_0, a_1, b_0, b_1)$ je pravděpodobnost, že je systém před měřením ve stavu kde $A_0 = a_0$, $A_1 = a_1$, $B_0 = b_0$ a $B_1 = b_1$. Pro zjištění očekávaných hodnot experimentu budeme uvažovat střední hodnotu těchto hodnot. Pak platí

$$\begin{aligned} E\,(A_0B_0 + A_0B_1 + A_1B_0 - A_1B_1) &= \sum_{a_0,a_1,b_0,b_1} P\,(a_0, a_1, b_0, b_1)\,(a_0b_0 + a_0b_1 + a_1b_0 - a_1b_1) \\ &\leq \sum_{a_0,a_1,b_0,b_1} 2P\,(a_0, a_1, b_0, b_1) \\ &\leq 2. \end{aligned} \tag{5.2}$$

Tyto střední hodnoty se též nazývají jako *korelační koeficienty*. Z linearity střední hodnoty dostáváme z rovnice (5.2) jednu z Bellových nerovností, konkrétně CHSH nerovnost zapsanou

$$S = E\,(A_0B_0) + E\,(A_0B_1) + E\,(A_1B_0) - E\,(A_1B_1) \leq 2. \tag{5.3}$$

Několikanásobným opakováním experimentu pak lze tyto korelační koeficienty určit. Z tohoto statistického testu získáváme závěr, že pokud $S \leq 2$, zdroj, který poskytuje qubity, byl předem přednastavený a dokáže predikovat výsledky jejich měření [27].

Nyní pracujme s předpokladem, že máme zdroj, který připraví provázaný pár ve stavu $|\psi\rangle = \frac{1}{\sqrt{2}}\,(|00\rangle + |11\rangle)$ a první qubit pošle Alici, druhý Bobovi. Alice i Bob si zvolí své měřící aparáty jako

$$A_0 = X \qquad A_1 = Z \qquad B_0 = \frac{1}{\sqrt{2}}\,(X + Z) \qquad B_1 = \frac{1}{\sqrt{2}}\,(X - Z)\,,$$

detaily výběru těchto aparátů v textu vynecháme.

Pokud by Alice s Bobem opět počítali korelační koeficienty, získali by pro A_0B_0 hodnotu

$$\begin{aligned} E\,(A_0B_0) &= \langle\psi|\, A_0 \otimes B_0\, |\psi\rangle = \langle\psi|\, X \otimes \frac{1}{\sqrt{2}}\,(X + Z)\, |\psi\rangle \\ &= \frac{1}{2\sqrt{2}} \begin{pmatrix} 1 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \\ 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix} \\ &= \frac{1}{\sqrt{2}}. \end{aligned} \tag{5.4}$$

Ostatní korelační koeficienty lze získat analogicky:

$$E(A_0B_1) = \frac{1}{\sqrt{2}} \qquad E(A_1B_0) = \frac{1}{\sqrt{2}} \qquad E(A_1B_1) = -\frac{1}{\sqrt{2}}. \tag{5.5}$$

Pokud sečteme tyto korelační koeficienty získáme rovnici ve tvaru

$$S = E(A_0B_0) + E(A_0B_1) + E(A_1B_0) - E(A_1B_1) = 2\sqrt{2}. \tag{5.6}$$

Z tohoto závěru vidíme, že kvantová mechanika je v rozporu s CHSH nerovností (5.3), jelikož predikuje $S = 2\sqrt{2}$, zatímco jakákoliv teorie skryté proměnné predikuje $|S| \leq 2$. Hodnotu S určujeme experimentálně, tedy pokud dostaneme hodnotu S větší než 2, teorie skrytých proměnných neplatí a fungují zákony kvantové mechaniky.

Tsirelsonova nerovnost nám říká, že hodnota S z (5.6) je maximální hodnota, kterou můžeme v kvantové mechanice dosáhnout [28]. Jedná se o maximální hodnotu, kterou můžeme CHSH nerovnost přesáhnout a tedy platí:

$$|S| \leq 2\sqrt{2}. \tag{5.7}$$

▶ Pozorování 5.1. O Bellových stavech (2.9) říkáme, že jsou maximálně provázané stavy, jelikož je pro ně hodnota S vždy rovna její maximální hodnotě $2\sqrt{2}$. Maximální provázanost nám poté říká, že pokud změříme stav jednoho qubitu z provázaného páru, vždy dokážeme podle výsledku měření prvního qubitu jistě předpovědět i výsledek měření druhého qubitu.

5.2 E91

Návrh protokolu E91 byl poprvé představen Arturem Ekertem v roce 1991 v [29]. Schéma protokolu E91 je založeno na párově provázaných párech fotonů. Tyto provázané fotony můžou být poskytnuty kýmkoliv, tedy například Alicí, Bobem nebo i jakýmkoliv neověřeným zdrojem, klidně i samotným odposlouchávajícím. Fotony jsou na začátku protokolu distribiuovány tak, aby Alice i Bob měli každý k dispozici jeden foton z provázaného páru. Protokol E91 je 3-stavový protokol a je popsán různými polarizacemi EPR páru.

Velkým rozdílem oproti protokolům založených na přípravě a měření je, že k detekování odposlechu využívá principů Bellovy nerovnosti. Při návrhu tohoto protokolu autorovi došlo, že u ostatních protokolů se zbytečně plýtvá prostředky, které byly už přeneseny a nebyly změřeny ve stejné bázi. Pro fungování těchto protokolů je půlka qubitů zahozena, kvůli špatně vybraným bázím, a z té druhé půlky, se teprve vybírá část, která bude sloužit pro detekci případného odposlechu. V protokolu E91 se po veřejné diskuzi hodnot tzv. analyzátorů (5.8) (5.9) rozdělí bity do dvou skupin. První skupina obsahuje bity, ve kterých se Alice a Bob shodli na analyzátorech. Druhá skupina obsahuje všechny ostatní bity. Aby nedošlo opět k dalšímu rozdělení prvotního klíče a zahození přenesených bitů, druhá skupina je ta, která slouží pro detekci odposlechu.

Schéma protokolu je navrženo tak, že po distribuování fotonů, Alice i Bob používají k měření měřící operátor určený jedním ze tří směrů popsaných jednotkovými vektory a_i pro Alici a b_i pro Boba kde i = 1,2,3. Vektory a_i, b_i leží v rovině určené lineární polarizací a jsou určeny úhlem θ kolem této roviny:

$$\theta_{a_1} = 0 \qquad \theta_{a_2} = \frac{1}{4}\pi \qquad \theta_{a_3} = \frac{1}{2}\pi \tag{5.8}$$

$$\theta_{b_1} = \frac{1}{4}\pi \qquad \theta_{b_2} = \frac{1}{2}\pi \qquad \theta_{b_3} = \frac{3}{4}\pi \tag{5.9}$$

Tyto vektory jsou často označovány jako analyzátory. Měřící operátory jsou poté pro Alici, resp. Boba určeny jednoznačně vnějším součinem jejich analyzátoru, tedy

$$M_{a_i} = |a_i\rangle\langle a_i| \qquad M_{b_i} = |b_i\rangle\langle b_i| \tag{5.10}$$

a jsou pro každé měření vybrány zcela náhodně. Důležitou vlastností, kterou je potřeba podotknout je, že pro volbu stejných analyzátorů, výsledky měření pro Alici i Boba budou vždy stejné.

▶ Poznámka 5.2. Hodnoty úhlů analyzátorů v tomto protokolu nejsou pevně určené. Tyto hodnoty byly vybrány v původním návrhu [29] a v praxi se často setkáváme s různými hodnotami.

Algoritmus 6 protokol E91

1. Pro požadovanou délku klíče n, libovolný zdroj vytvoří alespoň $\frac{9}{2}n$ EPR párů. Vždy jeden qubit z páru bude přes kvantový kanál poslán Alici, druhý Bobovi.
2. Alice i Bob si náhodně vygenerují analyzátory ze svých množin popsaných v (5.8) a (5.9) , pomocí kterých budou měřit a změří svoje qubity.
3. Alice i Bob přes klasický kanál zveřejní, jaké analyzátory použili.
4. Alice i Bob rozdělí své naměřené bity do dvou skupin. Skupina $\mathcal{G}_k$ obsahuje bity s použitými stejnými analyzátory a slouží jako klíč. Skupina $\mathcal{G}_d$ obsahuje všechny ostatní bity a slouží k detekci odposlechu. Pokud prvků v $\mathcal{G}_k$ bude méně než n, přeruší průběh protokolu a začnou znovu.
5. Alice i Bob si přes klasický kanál nasdílí skupinu $\mathcal{G}_d$ a provedou na ní statistický test $\mathcal{S}$, konkrétně test CHSH nerovnosti.
6. Pokud jejich statistický test $\mathcal{S}$ byl neúspěšný, tedy $|\mathcal{S}| \leq 2$, nejspíše došlo k odposlechu Evou nebo qubity, které jim zdroj poslal, byly předem nějakým způsobem předpřipraveny, a tudíž ovlivnily výsledek měření.
7. Pokud byl statistický test $\mathcal{S}$ úspěšný, tedy $|\mathcal{S}| > 2$, skupina $\mathcal{G}_k$ tvoří bezpečný klíč.

Pokud chceme otestovat Bellovu nerovnost typu CHSH, musíme provést test S, který je součet všech korelačních koeficientů, pro které Alice a Bob zvolili jiné směry analyzátorů, vyjádřeno rovnicí

$$S = E\left(a_1 b_1\right) - E\left(a_1 b_3\right) + E\left(a_3 b_1\right) + E\left(a_3 b_3\right), \tag{5.11}$$

Tyto korelační koeficienty vektorů a_i, b_j jsou

$$E\left(a_i, b_j\right) = P_{++}\left(a_i, b_j\right) + P_{--}\left(a_i, b_j\right) + P_{+-}\left(a_i, b_j\right) - P_{-+}\left(a_i, b_j\right), \tag{5.12}$$

kde $P_{\pm\pm}$ je pravděpodobnost naměření ± 1 pro a_i a ± 1 pro b_i [29].

Pokud bychom chtěli udělat celkové srovnání využití prostředků, řekli bychom, že $\frac{2}{9}$ EPR párů bude využito pro tvorbu klíče, s $\frac{4}{9}$ párů se bude provádět statistický test a $\frac{1}{3}$ párů zůstane nevyužita.

5.2.1 Odposlech protokolu E91

První strategií pro odposlech, kterou může Eva zvolit, je odposlech na jednom z kvantových kanálů, na kterém zdroj posílá Alici nebo Bobovi jeden qubit z EPR páru. Pokud Eva poslaný qubit například Bobovi změří, je kvůli kvantovému provázání hodnota měření Alicina qubitu už předem určena před Aliciným měřením. To znamená, že se u Alice jedná o deterministické měření, pro které nefungují zákony kvantové mechaniky, ale fungují zákony té klasické. Pokud

Eva poté pošle svůj připravený qubit Bobovi a ten ho změří, výsledek jeho měření už nebude korelovaný s Aliciným měřením. Když v závěru Alice s Bobem provedou na svých naměřených bitech statistický test $\mathcal{S}$, s jistotou obdrží hodnotu $|\mathcal{S}| < 2$ a prohlásí přenos za odposlechnutý.

Druhá strategie, kterou Eva může mít, je být zdroj EPR párů, které bude posílat Alici a Bobovi. V tomto případě se Eva může rozhodnout posílat páry qubitů ve stavech $|0\rangle \otimes |0\rangle$ a $|1\rangle \otimes |1\rangle$ namísto maximálně provázaných EPR párů, aby jistě věděla, jaké hodnoty Alice s Bobem pro svůj klíč naměří. Naneštěstí pro Evu, tyto stavy mají deterministický výsledek měření, a tedy výsledek měření mluví ve prospěch lokálního realismu. Pokud se Alice s Bobem rozhodnou provést statistický test $\mathcal{S}$, měli by experimentálně obdržet hodnotu testu kolem 0 a opustit protokol. Aby Eva zvýšila své šance pro nedetekování při testu, může posílat tyto stavy s upravenými amplitudami, například $\frac{1}{\sqrt{5}}|00\rangle + \frac{2}{\sqrt{5}}|11\rangle$, kde Eva ví, že naměření hodnoty 1 bude 4x pravděpodobnější než naměření 0. Obecně platí, že čím budou tyto dvě amplitudy bližší, tím menší mají šanci Alice s Bobem na detekování Evy pomocí statistického testu. Bohužel pro Evu, čím bližší hodnoty jsou, tím menší má znalost nad klíčem, jelikož pravděpodobnosti pro naměření 0 a 1 jsou bližší.

5.2.2 Porovnání E91 s BB84 a B92

Naše porovnání bude probíhat zejména ve dvou kategoriích. První kategorií je náročnost přípravy a komunikace jako takové. Druhá kategorie se zabývá bezpečností a odhadu Evy informace o klíči.

Protokoly BB84 a B92 pracují s přeposláním jednotlivých qubitů, zatímco E91 využívá EPR párů. EPR páry jsou mnohem náročnější na přípravu než samostatné qubity, s dosavadní technologií je využití E91 zatím neaktuální. Na počet přenesených qubitu je E91 nejnáročnější, jelikož u každého měření je šance pouze $22,22\ldots\%$ oproti 25% u B92 a 50% u BB84, že bit bude použit pro tvorbu klíče. Kromě toho se u E91 musí přenést dvojnásobné množství, jelikož pracujeme s provázanými páry.

Pro detekování odposlechu u BB84 a B92 se využívají bity, u jejichž naměření byly použity stejné báze, a proto se obětují bity z klíče. Protokol E91 však využívá ke kontrole odposlechu bity, u kterých se měřilo v jiných bázích, a proto se nemusí obětovat žádné bity z klíče. Porovnání pomocí kontrolních bitů u BB84 a B92 je více určené podle chybovosti kanálu a z toho důvodu více záleží na individuálním přístupu k určení hranice pro detekci. U E91 provádíme statistický test, který je více objektivní a sám stanovuje hodnotu detekce odposlechu, kterou bychom se měli řídit.

Kapitola 6
Simulace protokolů

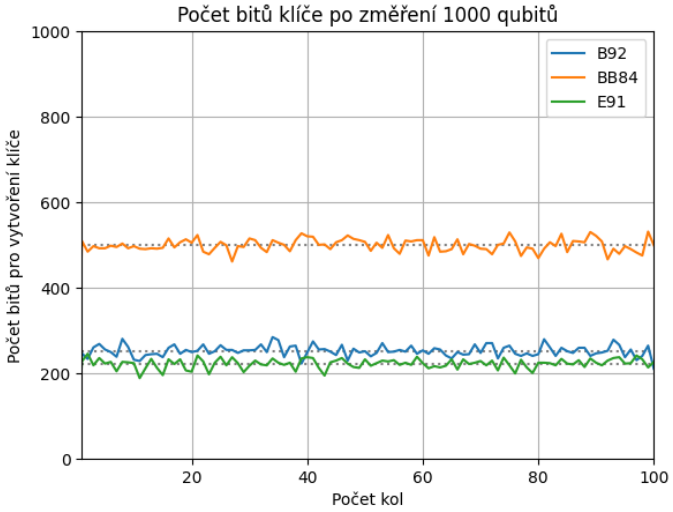
V této kapitole si ukážeme výsledky simulací protokolů BB84, B92 a E91. Budeme hodnotit různé aspekty distribuce klíčů, jako náročnost komunikace na počet qubitů, šanci na detekování odposlechu, úroveň bezpečnosti a Evy znalost o klíči. Představíme si také odhad počtu qubitů a bitů u jednotlivých protokolů potřebných pro symetrickou šifru AES.

Pro simulaci protokolů budeme využívat SDK jménem Qiskit.[13] Qiskit byl vyvinut firmou IBM pod open source licencí MIT a zveřejněn v roce 2017 společně s OpenQASM. OpenQASM je název instrukční sady komunikující s hardwarem pro kvantové počítání, do které se programy vytvořené ve vyšších jazycích překládají. Qiskit obsahuje nástroje pro tvorbu kvantových programů a jejich spuštění na lokálním nebo vzdáleném zařízení. Ke vzdálenému zařízení se přistupuje prostřednictvím služby IBM cloudu, které umožňuje odeslat programy ke spuštění na skutečném kvantovém počítači. Mimo to, lze náš kvantový program pouze odsimulovat na dostupných simulátorech. Simulátory narozdíl od kvantových počítačů netrpí na chybovost, ale i tu je možné v programech nasimulovat.

Jelikož v našem případě nedokážeme uskutečnit skutečný přenos fotonů na kvantové síti, budeme chod protokolů simulovat přes simulátory poskytnuté v Qiskit. Kódy protokolů jsou psané v jazyce Python a dostupné pro otestování na přiloženém médiu.

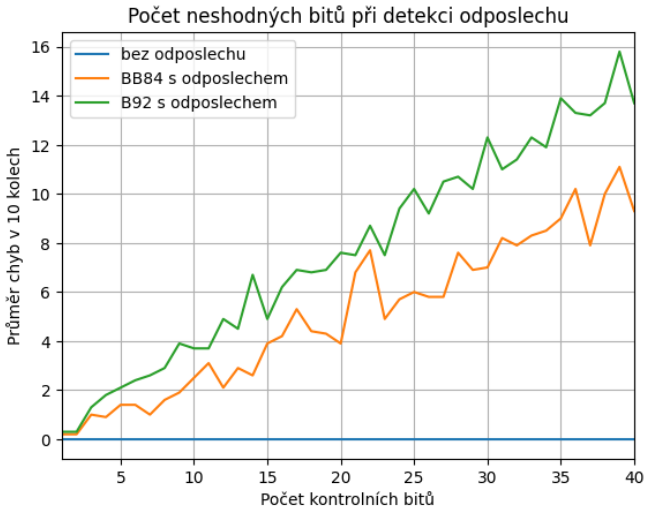
6.1 Testování protokolů

První důležitou fází při přenosu je kódování a měření přenesených fotonů. Na obrázku 6.1 můžeme vidět srovnání protokolů, v jakém poměru mají počet přeposlaných qubitů k počtu správně zvolených bází pro vytvoření klíče. Protokoly byly odsimulovány 100× s 1000 přeposlanými qubity, v případě E91 se bavíme o 1000 provázaných párech.Vidíme, že protokoly se pohybují kolem svých teoretických předpokladů, protokol BB84 se pohybuje kolem 50% zbylých bitů, B92 kolem 25% bitů a E91 kolem 22.22…%.

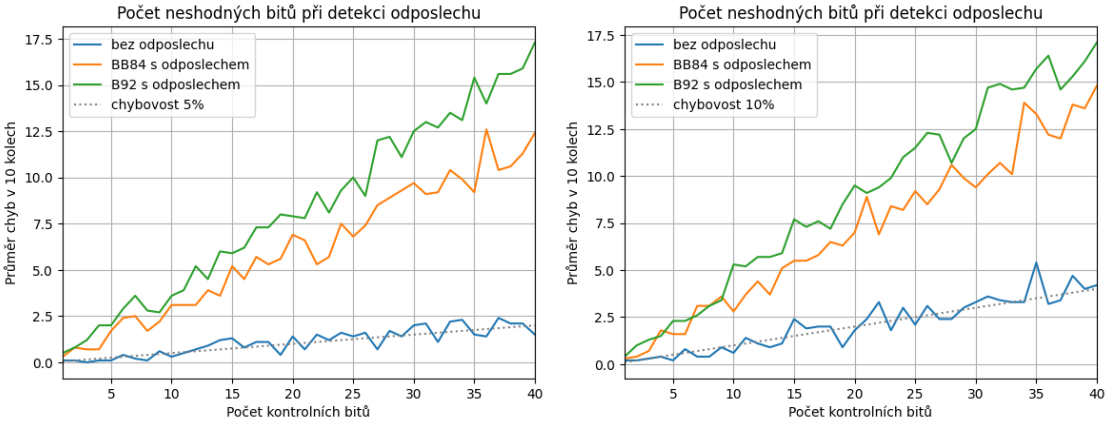


Obrázek 6.1 Počet bitů klíče po změření 1000 qubitů

U protokolů BB84 a B92 využíváme sady bitů, kterým říkáme kontrolní bity, pro detekci odposlechu na kvantovém kanále. Jedním z problémů, s kterým se při kontrole shody bitů setkáváme, je neschopnost zjistit, jestli byla chyba způsobena odposlechem nebo chybovostí kanálu. Na obrázcích 6.2, 6.3a a 6.3b vidíme výsledky porovnání kontrolních bitů s různě chybovými kanály.



Obrázek 6.2 Detekování odposlechu s ideálním kanálem



(a) Detekování odposlechu s chybovostí 5%

(b) Detekování odposlechu s chybovostí 10%

Obrázek 6.3 Detekování odposlechu s chybovým kanálem

Z obrázků lze vypozorovat, že pokud použijeme více bitů pro kontrolu u obou protokolů, je detekce odposlechu pravděpodobnější. Navíc si můžeme povšimnout, že pokud otestujeme chybovost našeho kvantového kanálu a získáme tak odhad pravděpodobnosti chyby, je u více použitých kontrolních bitů lehké nastavit hranici mezi šumem a odposlechem.

Mimo naší detekci Evy je také důležité, kolik toho Eva o našem klíči po odposlechu ví. U protokolu BB84 má u každého qubitu šanci 50% na to, že zjistí zakódovaný bit a u B92 pouze 25%. Celkový počet Evy bitů shodných s klíčem Alice a Boba je ale větší, jelikož pokud se Eva netrefí výběrem báze, je její hodnota bitu náhodná. Na obrázku 6.4 vidíme porovnání počtu bitů, které Eva dokázala úspěšně odposlechnout.

Obrázek 6.4 Odposlouchávajícího znalost klíče

U protokolu E91 používáme pro otestování bezpečnosti Bellovy nerovnosti 5.1.2, kdy provedeme statistický test $\mathcal{S}$ na qubitech, které nepoužijeme pro tvorbu klíče. E91 považujeme za bezpečný, pokud náš statistický test nabývá hodnoty větší než 2, u maximálně provázaných stavů je $\mathcal{S} = 2\sqrt{2}$.

Provedli jsme 1000 běhů protokolu a získali výběrový průměr $\overline{\mathcal{S}} = 2,8175$ a výběrovou

směrodatnou odchylku $s = 0,2012$. Na základě předpokladu bezpečnosti a těchto dat bychom chtěli na hladině významnosti 5% otestovat, jestli je střední hodnota $\mathcal{S}$ menší nebo rovna 2,6, nebo jestli je významně vyšší. Chceme testovat nulovou hypotézu $H_0 = \mu \leq 2,6$ proti alternativní hypotéze $H_A = \mu > 2,6$. Provedeme testovou statistiku T při neznámem rozptylu ve tvaru

$$T = \frac{\overline{\mathcal{S}} - 2,6}{s}\sqrt{n} = \frac{2,8175 - 2,6}{0,2012}\sqrt{1000} = 34,1846. \tag{6.1}$$

Testujeme na hladině významnosti 5%, takže zkoumáme, zda je testová statistika větší než kritická hodnota Studentova rozdělení $t_{0,05,999}$:

$$T = 34,1846 > 1,646 = t_{0,05,999}. \tag{6.2}$$

Na hladině významnosti 5% zamítáme nulovou hypotézu ve prospěch alternativy, že je střední hodnota $\mathcal{S}$ významně vyšší než 2,6, což potvrzuje bezpečnost přenosu.

Jelikož v protokolu používáme EPR stavy, které jsou maximálně provázané, chtěli bychom otestovat konkrétnější hypotézu pro naší bezpečnost, a to jestli je střední hodnota $\mathcal{S}$ rovna $2\sqrt{2}$ nebo nikoliv. Chceme testovat nulovou hypotézu $H_0 = \mu = 2\sqrt{2}$ proti alternativní hypotéze $H_A \neq 2\sqrt{2}$ na hladině významnosti 5%. Test provedeme pomocí p–hodnoty, kterou získáme z našich naměřených dat z minulého příkladu. Pro naše data se p–hodnota rovná 0,087. Je-li p-hodnota menší než naše požadovaná hladina významnosti, zamítáme H_0. V našem případě je hodnota p větší než hladina významnosti α

$$p = 0,087 > 0,05 = \alpha, \tag{6.3}$$

a tudíž hypotézu H_0 o rovnosti střední hodnoty nezamítáme na hladině významnosti 5%.

6.2 Odhad množství prostředků pro AES

Symetrická šifra AES využívá pro své fungování klíče o délkách 128, 192 nebo 256 bitů. Nyní si ukážeme odhad pro vygenerování těchto klíčů pomocí našich QKD protokolů. Při odhadu počtu qubitů, které posíláme na kvantovém kanále, budeme pracovat se scénářem, že chceme u protokolů s detekcí pomocí kontrolních bitů pravděpodobnost detekce alespoň $P_d = 0,99999$. To znamená, že budeme využívat počty kontrolních bitů $m_{BB84} = 41$ a $m_{B92} = 29$.

Tabulka 6.1 Odhad počtu qubitů pro AES

	délka klíče v bitech		
protokoly	128	196	256
BB84 s bezchybným přenosem	338	474	594
BB84 s [7, 4] a [7, 3] lin. kódy	1874	2826	3666
B92 s bezchybným přenosem	628	900	1140
B92 s [7, 4] a [7, 3] lin. kódy	3700	5604	7284
E91	576 párů	882 párů	1152 párů

Z tabulky lze jednoduše vypozorovat, jak moc náročnými na počet qubitů jsou protokoly, které dokáží detekovat a opravit chyby způsobené kanálem.

Dalším odhadem je počet bitů, které si Alice s Bobem musí přeposlat na klasickém kanále pro správné fungování protokolů. Odhady jsou minimální a nezapočítáváme do nich zprávy, u kterých

nedokážeme odhadnout počet bitů, například úspěšné ohlášení příchodu qubitů nebo pozice qubitů, které byly zvoleny pro nějaké operace. Posuzujeme pouze velikost obsahu důležitých zpráv týkající se samotného klíče a bází.

Tabulka 6.2 Odhad počtu bitů pro AES

	délka klíče v bitech		
protokoly	128	196	256
BB84 s bezchybným přenosem	758	1030	1270
BB84 s [7, 4] a [7, 3] kódy	4179	7106	9206
B92 s bezchybným přenosem	1471	2083	26323
B92 s [7, 4] a [7, 3] kódy	8511	12855	16703
E91	200	300	400

Závěr

Cílem této práce bylo představit a naimplementovat různé protokoly pro kvantový přenos klíče a úvést argumenty týkající se jejich bezpečnosti. Konkrétně se jedná o známé a často uváděné protokoly BB84, B92 a E91.

V úvodu teoretické části práce jsme zavedli pojmy pro základní pochopení kvantové informatiky jako takové. Vysvětlili jsme s jakými fyzikálními systémy v kvantové informatice pracujeme, a co s nimi můžeme provést. Začali jsme s pochopením systémů s jedním qubitem a poté rozšířili na systémy pracující s více qubity, s kterými jsme se naučili manipulovat pomocí kvantových hradel, a skončili u získání klasické informace z těchto kvantových systémů, tedy měřením.

Na těchto vybudovaných základech jsme poté ukázali, jak s těmito systémy pracujeme pro přenos informace s využitím kvantového i klasického kanálu. Poté jsme přešli na konkrétní využití kvantového kanálu, a to na kvantový přenos klíče. Uvedli jsme možné přístupy pro přenos qubitů při vytváření klíče, první přístup s přenosem předpřipravených samostatných qubitů a druhý přístup s využitím kvantového provázání dvou qubitů. Detekci odposlechu přenosu u protokolů BB84 a B91 jsme řešili přenosem kontrolních klasických bitů, zatímco u protokolu E91 jsme využili Bellových nerovností pro detekci skrytých proměnných v našem systému.

Na základě zpracované teorie jsme zmiňované prokoly implementovali s využitím SDK Qiskit v jazyce Python, která slouží pro práci s kvantovými systémy od firmy IBM. Z důvodu nedostatečné potřebné kvantové výpočetní síly a nemožnosti pracovat se samotnými kvantovými sítěmi, chod protokolů pouze simulujeme. V simulovaných prostředí však nepracujeme s přenosem ovlivněným chybovostí, ale pracujeme s bezchybným přenosem. Pro protokoly BB84, B92 a E91 jsme mimo jiné vytvořili i varianty s odposlechem na kvantovém kanále, s kterými jsme se vypořádali pomocí metod vysvětlených v teoretické části.

Výsledná práce nezahrnuje pohled do hloubky na samotnou fyzickou realizaci kvantového přenosu. Kvůli tomu se i vyhýbá podrobnému popisu přístupů pro napadení přenosu, které jsou realizovány spíše na hardwarové úrovni. V této oblasti by práci šlo rozšířit o různé metodiky útoků.

Bibliografie

1. NIELSEN, M. A.; CHUANG, I. L. *Quantum Computation and Quantum Information: 10th Anniversary Edition*. Cambridge University Press, 2010. ISBN 9781107002173. Dostupné z DOI: 10.1017/CBO9780511976667.
2. HLAVATÝ, L.; ŠTEFAŇÁK, M. *Slabikář kvantové mechaniky* [online]. 2018. [cit. 2023-04-20]. Dostupné z: https://physics.fjfi.cvut.cz/files/predmety/02KVAN/02KVAN.
3. PRESKILL, J. Lecture Notes for Physics: Quantum Information and Computation [online]. 2018, roč. 3, s. 4–10 [cit. 2023-05-02]. Dostupné z: http://theory.caltech.edu/~preskill/ph219/chap3_15.pdf.
4. RIVEST, R. L.; SHAMIR, A.; ADLEMAN, L. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM* [online]. 1978, roč. 21, č. 2, s. 120–126 [cit. 2023-01-02]. Dostupné z DOI: https://doi.org/10.1145/359340.359342.
5. SHOR, P. W. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. *SIAM Journal on Computing* [online]. 1997, roč. 26, č. 5, s. 1484–1509 [cit. 2023-04-05]. Dostupné z DOI: https://doi.org/10.1137/s0097539795293172.
6. AJTAI, M. Generating Hard Instances of Lattice Problems. *Electronic Colloquium on Computational Complexity*. 1996, roč. 3.
7. COMPUTER SECURITY DIVISION, Information Technology Laboratory. *Post-Quantum Cryptography — CSRC — CSRC* [online]. 2017-01. [cit. 2023-02-26]. Dostupné z: https://csrc.nist.gov/projects/post-quantum-cryptography.
8. WOOTTERS, W. K.; ZUREK, W. H. A single quantum cannot be cloned. *Nature*. 1982, roč. 299, č. 5886, s. 802–803. Dostupné z DOI: https://doi.org/10.1038/299802a0.
9. RIBORDY, G.; GAUTIER, J. D. Fast and user-friendly quantum key distribution. *Journal of Modern Optics* [online]. 2000, roč. 47, č. 2-3, s. 517–531 [cit. 2023-03-30]. Dostupné z DOI: https://doi.org/10.1080/09500340008244057.
10. B, Zhao; X, Zha; Z, Chen; R, Shi; D, Wang; T, Peng; L, Yan. *Quantum key distribution (QKD) based on polarization encoding* [online]. 2020. [cit. 2023-04-18]. Dostupné z: https://www.mdpi.com/2076-3417/10/8/2906.
11. YIN, J.; LI, YH.; LIAO, SK.; et. al. et. Entanglement-based secure quantum cryptography over 1,120 kilometres. *Nature* [online]. 2020, roč. 582, č. 7813, s. 501–505 [cit. 2023-05-11]. Dostupné z DOI: https://doi.org/10.1038/s41586-020-2401-y.
12. EINSTEIN, A.; PODOLSKY, B.; ROSEN, N. Can Quantum-Mechanical Description of Physical Reality Be Considered Complete? *Description of Physical Reality* [online]. 1935, vol. 47, no. 10, s. 777–800 [cit. 2023-04-22]. Dostupné z DOI: 10.1103/physrev.47.777.

13. CONTRIBUTORS, Qiskit. *Qiskit: An Open-source Framework for Quantum Computing* [online]. 2023. [cit. 2023-05-05]. Dostupné z DOI: 10.5281/zenodo.2573505.
14. CONTRIBUTORS, Qiskit. *Superdense Coding* [online]. [B.r.]. [cit. 2023-05-01]. Dostupné z: https://learn.qiskit.org/course/ch-algorithms/superdense-coding.
15. MCMAHON, D. Applications of Entanglement: Teleportation and Superdense Coding. In: *Quantum Computing Explained*. 2008, s. 236–237. Dostupné z DOI: 10.1002/9780470181386.ch10.
16. BHANDARI, Ramesh. *Quantum Error Correcting Codes and the Security Proof of the BB84 Protocol* [online]. 2011. [cit. 2023-04-29]. Dostupné z: https://arxiv.org/ftp/arxiv/papers/1409/1409.1452.pdf.
17. SINGLETON, R. Maximum distance q-nary codes. *IEEE Transactions on Information Theory* [online]. 1964, roč. 10, č. 2, s. 116–118 [cit. 2023-04-04]. Dostupné z DOI: https://doi.org/10.1109/tit.1964.1053661.
18. DATTA, N. Course 9 - Quantum Entropy and Quantum Information. In: BOVIER, A.; DUNLOP, F.; AL., et. (ed.). *Mathematical Statistical Physics* [online]. Elsevier, 2006, sv. 83, s. 395–466 [cit. 2023-05-08]. Les Houches. ISSN 0924-8099. Dostupné z DOI: https://doi.org/10.1016/S0924-8099(06)80046-6.
19. BENNETT, C.H.; BRASSARD, G.; CREPEAU, C.; MAURER, U.M. Generalized privacy amplification. *IEEE Transactions on Information Theory* [online]. 1995, roč. 41, č. 6, s. 1915–1923 [cit. 2023-05-06]. Dostupné z DOI: 10.1109/18.476316.
20. BENNETT, Ch. H.; BRASSARD, G. Quantum cryptography: Public key distribution and coin tossing. *Theoretical Computer Science* [online]. 2014, roč. 560, č. 1, s. 7–11 [cit. 2023-03-06]. Dostupné z DOI: https://doi.org/10.1016/j.tcs.2014.05.025.
21. WONG, T. G. *Introduction to classical and quantum computing* [online]. Omaha: Rooted Groove. Copyright, 2022 [cit. 2023-04-08]. ISBN 9798985593105. Dostupné z: https://www.thomaswong.net/introduction-to-classical-and-quantum-computing-1e3p.pdf.
22. WATANABE, S.; MATSUMOTO, R.; UYEMATSU, R. Noise tolerance of the BB84 protocol with random privacy amplification. In: *Proceedings. International Symposium on Information Theory, 2005. ISIT 2005.* 2005, s. 1013–1017. Dostupné z DOI: 10.1109/ISIT.2005.1523492.
23. BENNETT, Ch. H. Quantum cryptography using any two nonorthogonal states. *Physical Review Letters*. 1992, roč. 68, č. 21, s. 3121–3124. Dostupné z DOI: https://doi.org/10.1103/physrevlett.68.3121.
24. ELBOUKHARI, M.; AZIZI, M.; AZIZI, A. Achieving unconditional security by quantum cryptography [online]. 2010 [cit. 2023-03-15]. Dostupné z: https://www.researchgate.net/publication/228669847_Achieving_unconditional_security_by_quantum_cryptography.
25. ETENGU, R.; ABBOU, F. M.; WONG, H. Y.; ABID, A.; NORTIZA, N.; SETHARAMAN, A. Performance Comparison of BB84 and B92 Satellite-Based Free Space Quantum Optical Communication Systems in the Presence of Channel Effects [online]. 2011, roč. 32, č. 1, s. 37–47 [cit. 2023-05-01]. Dostupné z DOI: doi:10.1515/joc.2011.007.
26. BELL, J. S. On the Einstein Podolsky Rosen paradox. *Physics Physique* [online]. 1964, vol. 1, no. 3, s. 195–200 [cit. 2023-04-15]. Dostupné z DOI: https://doi.org/10.1103/physicsphysiquefizika.1.195.
27. HENSEN, B.; BERNIEN, H.; DRÉAU, A. E. et. al. Loophole-free Bell inequality violation using electron spins separated by 1.3 kilometres. *Nature*. 2015, roč. 526, č. 7575, s. 682–686. Dostupné z DOI: https://doi.org/10.1038/nature15759.

28. CIREL'SON, B. S. Quantum generalizations of Bell's inequality. *Letters in Mathematical Physics* [online]. 1980, roč. 4, č. 2, s. 93–100 [cit. 2023-04-20]. Dostupné z DOI: https://doi.org/10.1007/bf00417500.

29. EKERT, A. Quantum cryptography based on Bell's theorem. *Physical review letters* [online]. 1991, roč. 67, č. 6, s. 661–663 [cit. 2023-05-06]. Dostupné z DOI: https://doi.org/10.1103/PhysRevLett.67.661.

Obsah přiloženého média

- `readme.txt` ..... stručný popis obsahu média
- `notebooks` ..... notebooky ukázky protokolů
  - `BB84.ipynb` ..... notebook protokolu BB84
  - `B92.ipynb` ..... notebook protokolu B92
  - `E91.ipynb` ..... notebook protokolu B91
- `text` ..... text práce
  - `thesis.pdf` ..... text práce ve formátu PDF