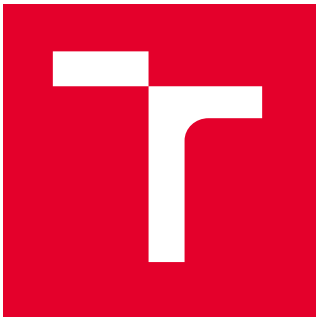


VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION

ÚSTAV TELEKOMUNIKACÍ

DEPARTMENT OF TELECOMMUNICATIONS

LABORATORNÍ ÚLOHA – KVANTOVÁ DISTRIBUCE KLÍČŮ ZALOŽENÁ NA POLARIZACI

LABORATORY TASK - POLARIZATION-BASED QUANTUM KEY DISTRIBUTION

BAKALÁŘSKÁ PRÁCE

BACHELOR'S THESIS

AUTOR PRÁCE — **Sylva Poláková**

AUTHOR

VEDOUCÍ PRÁCE — **Ing. Ondřej Klíčník**

SUPERVISOR

BRNO 2024

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

Bakalářská práce

bakalářský studijní program **Informační bezpečnost**

Ústav telekomunikací

Studentka: Sylva Poláková ***ID:*** 211208

Ročník: 3 ***Akademický rok:*** 2023/24

NÁZEV TÉMATU:

Laboratorní úloha – Kvantová distribuce klíčů založená na polarizaci

POKYNY PRO VYPRACOVÁNÍ:

Cílem bakalářské práce je provést detailní rozbor problematiky kvantové distribuce klíčů (QKD), zejména pak jednosměrných protokolů (one-way prepare-and-measure) s diskrétní proměnnou (DV-QKD) a polarizačním kódováním. Dále bude rozebrána polarizace jakožto fyzikální jev a součástí práce bude i rešerše aktuálně platných standardů od organizací jako ETSI, ITU-T, IEEE nebo ISO. V rámci praktické části pak bude navržena laboratorní úloha zaměřená na názornou demonstraci významu polarizace u vybraných QKD protokolů. Tato úloha bude fyzicky sestavena, otestována a dodána včetně doprovodných výukových materiálů.

DOPORUČENÁ LITERATURA:

Podle pokynů vedoucího práce

Termín zadání: 5.2.2024 ***Termín odevzdání:*** 28.5.2024

Vedoucí práce: Ing. Ondřej Klíčník

doc. Ing. Jan Hajný, Ph.D.
předseda rady studijního programu

ABSTRAKT

Tato bakalářská práce se zaměřuje na detailní rozbor problematiky kvantové distribuce klíčů (QKD) se zaměřením na jednosměrné prepare-and-measure protokoly s diskrétní proměnnou (DV-QKD) a polarizačním kódováním. Práce se člení na část teoretickou a praktickou. V úvodní teoretické části práce je poskytnut komplexní přehled o polarizaci jako zásadním fyzikálním jevu, který je nezbytný pro pochopení fungování QKD protokolů. Jsou rozebrány různé aspekty polarizace, včetně Jonesových vektorů, Stokesových parametrů a Poincarého koule. Další část se věnuje základům kvantové mechaniky s důrazem na qubit a reprezentaci kvantových stavů. Dále práce přechází k samotné kvantové distribuci klíčů, kde jsou vysvětleny základní principy QKD, a rovněž jsou zde analyzovány nejvýznamnější protokoly. Práce obsahuje i rešerši aktuálně platných standardů. V praktické části je navržena laboratorní úloha, která má za cíl demonstrovat význam polarizace v kontextu QKD protokolů.

KLÍČOVÁ SLOVA

DV-QKD, kvantová distribuce klíčů (QKD), kvantová mechanika, polarizace, protokol BB84

ABSTRACT

This bachelor thesis focuses on a detailed analysis of quantum key distribution (QKD) with a focus on one-way prepare-and-measure protocols with discrete variable (DV-QKD) and polarization coding. The thesis is divided into a theoretical and practical part. The introductory theoretical part of the thesis provides a comprehensive overview of polarization as a fundamental physical phenomenon that is essential for understanding the operation of QKD protocols. Various aspects of polarization are discussed, including Jones vectors, Stokes parameters, and the Poincaré sphere. The next section covers the basics of quantum mechanics with a focus on qubit and the representation of quantum states. The work then moves on to quantum key distribution itself, where the basic principles of QKD are explained, and the most important protocols are also analysed. In the practical part, a laboratory task is designed to demonstrate the importance of polarization in the context of QKD protocols.

KEYWORDS

DV-QKD, polarization, protocol BB84, quantum key distribution (QKD), quantum mechanics

POLÁKOVÁ, Sylva. *Laboratorní úloha – Kvantová distribuce klíčů založená na polarizaci*. Bakalářská práce. Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav telekomunikací, 2023. Vedoucí práce: Ing. Ondřej Klíčník

Prohlášení autora o původnosti díla

Jméno a příjmení autora:	Sylva Poláková
VUT ID autora:	211208
Typ práce:	Bakalářská práce
Akademický rok:	2023/24
Téma závěrečné práce:	Laboratorní úloha – Kvantová distribuce klíčů založená na polarizaci

Prohlašuji, že svou závěrečnou práci jsem vypracovala samostatně pod vedením vedoucí/ho závěrečné práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou všechny citovány v práci a uvedeny v seznamu literatury na konci práce.

Jako autorka uvedené závěrečné práce dále prohlašuji, že v souvislosti s vytvořením této závěrečné práce jsem neporušila autorská práva třetích osob, zejména jsem nezasáhla nedovoleným způsobem do cizích autorských práv osobnostních a/nebo majetkových a jsem si plně vědoma následků porušení ustanovení § 11 a následujících autorského zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů, včetně možných trestněprávních důsledků vyplývajících z ustanovení části druhé, hlavy VI. díl 4 Trestního zákoníku č. 40/2009 Sb.

Brno ....

podpis autorky*

*Autor podepisuje pouze v tištěné verzi.

PODĚKOVÁNÍ

Ráda bych poděkovala vedoucímu bakalářské práce panu Ing. Ondřeji Klíčníkovi za odborné vedení, konzultace, trpělivost a podnětné návrhy k práci.

Obsah

Seznam obrázků

Seznam tabulek

Úvod

V posledních několika desetiletích se kvantová kryptografie, zejména kvantová distribuce klíčů (QKD), stala předmětem rozsáhlého výzkumu a inovací. Tento narůstající zájem je způsoben nejen rychlým pokrokem v kvantových technologiích, ale také rostoucí poptávkou po bezpečné komunikaci. Současná asymetrická kryptografie, jež je založena na složitých matematických problémech, je vystavena potenciálním hrozbám, které může účinně překonat právě kvantová distribuce klíčů. QKD využívá základní principy kvantové mechaniky k vytváření a distribuci klíčů, což zajišťuje vysokou úroveň bezpečnosti garantovanou fyzikálními zákony.

Tato bakalářská práce se věnuje komplexnímu pohledu na problematiku polarizace a její aplikaci v oblasti QKD. První kapitola se zaměřuje na základní principy polarizace jako fyzikálního jevu, přičemž jsou popsány druhy polarizace, metody jejich reprezentace a vizualizace. Následuje stručný přehled kvantové mechaniky a různých způsobů vyjádření kvantových stavů.

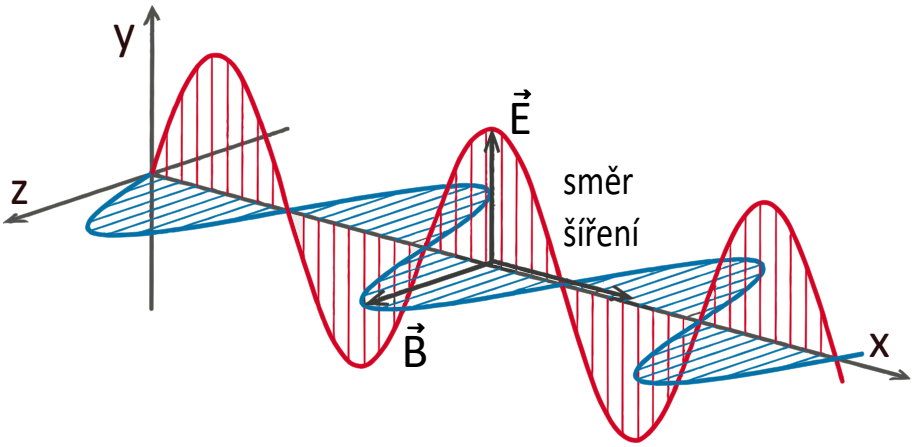
V dalších kapitolách se pozornost soustředí na klíčové téma práce, kterým je samotná kvantová distribuce klíčů (QKD). Jsou analyzovány hlavní aspekty QKD, včetně procesů výměny, prosévání a destilace klíčů. Další část se věnuje jednosměrným DV-QKD protokolům s detailním pohledem na jednotlivé protokoly jako BB84, B92, T12, SARG04 a SSP. Následně se práce zabývá standardizací v oblasti QKD a rolí mezinárodních organizací, přičemž jsou popsány jak aktuálně platné standardy, tak standardy ve vývoji.

Praktickou část bakalářské práce tvoří laboratorní úloha, která má za cíl demonstrovat význam polarizace v QKD protokolech. Skládá se z několika částí, které umožňují propojit teoretické znalosti s experimentálním testováním v laboratoři.

1 Polarizace jako fyzikální jev

1.1 Polarizace světla

Polarizace je fyzikální vlastnost elektromagnetického vlnění, jako je světlo, při které se oscilace elektromagnetického vlnění omezuje nebo orientuje do určitého směru. To se dá popsat dvěma vektory: vektorem elektrického pole $\vec{E}$ a vektorem magnetického pole $\vec{B}$. Vektory $\vec{E}$ i $\vec{B}$ jsou navzájem kolmé a zároveň leží v rovině, která je kolmá ke směru šíření vlnění [1].



Obr. 1.1: Elektromagnetická vlna a její složky [2].

Pokud se směr i velikost vektoru $\vec{E}$ nahodile mění, jedná se o nepolarizované světlo. U polarizovaného světla vektor $\vec{E}$ kmitá v jedné konkrétní rovině (lineární polarizace), nebo v určitém směru, jako je kruh nebo elipsa (kruhová nebo eliptická polarizace). Polarizované světlo se dá získat několika způsoby: odrazem, lomem, dvojlomem a průchodem polaroidem [1].

Vektor elektrického pole $\vec{E}$ lze pro jakýkoliv stav polarizace světelné vlny rozložit do dvou složek E_x a E_y v rovině xy, která je kolmá na směr šíření paprsku. Výsledek lze popsat pomocí rovnice

$$\vec{E} = \hat{e}_x E_x + \hat{e}_y E_y, \tag{1.1}$$

kde $\hat{e}_x$ je jednotkový vektor ve směru osy x, $\hat{e}_y$ je jednotkový vektor ve směru osy y a

$$E_x = E_{0x} \cos\left(kz - \omega t + \varphi_x\right), \tag{1.2}$$

$$E_y = E_{0y} \cos\left(kz - \omega t + \varphi_y\right), \tag{1.3}$$

kde E_{0x} a E_{0y} jsou amplitudy, k je vlnové číslo, ω je úhlová frekvence, t je čas, φ_x a φ_y jsou odpovídající fáze. Druh polarizace světla se určuje na základě rozdílu ve fázových posunech mezi složkami elektrického pole [3, 4].

1.2 Druhy polarizace

Základní rozdělení polarizace světla je možné určit podle rozdílu ve fázích $\varphi_x - \varphi_y$. Rozlišují se tři typy polarizace [1, 3]:

- **Lineární polarizace:** Fázový posun je 0 nebo π. Vektor $\vec{E}$ kmitá stále v jedné rovině, to znamená, že jeho směr je stále konstantní nebo se mění na přesně opačný, mění svou velikost.
- **Kruhová polarizace:** Fázový rozdíl je roven $\frac{\pi}{2}$. Vektor $\vec{E}$ opisuje kruh, to znamená že jeho velikost je konstantní, ale mění se jeho směr.
- **Eliptická polarizace:** Fázový rozdíl může nabývat jakékoli hodnoty z $(0, \pi)$ mimo konkrétní hodnoty pro lineární či kruhovou polarizaci. Vektor $\vec{E}$ opisuje elipsu, mění se jak směr, tak i velikost.

Lineární a kruhová polarizace jsou tak speciálními případy eliptické polarizace.

1.3 Reprezentace polarizace

Existuje několik metod, které lze použít k reprezentaci polarizace:

- **Matematický popis:** Polarizace světla může být reprezentována matematicky pomocí různých metod. Mezi tyto metody patří použití **Jonesových vektorů** a **Stokesových parametrů**. **Jonesovy** a **Muellerovy matice** umožňují popsat vliv optických komponent na polarizační stavy světla.
- **Grafické znázornění:** Kromě matematického popisu lze polarizaci také reprezentovat vizuálně. **Poincarého koule** je jedním z nejznámějších nástrojů pro tento účel. **Polarizační elipsa**, která je matematickým konceptem, může být rovněž zobrazena graficky.

1.3.1 Jonesovy vektory

Polarizované světlo se dá popsat pomocí Jonesových vektorů, které byly pojmenovány po americkém fyzikovi Robertu Clarku Jonesovi. Tento popis platí pro již zcela polarizované světlo, nedá se použít pro částečnou polarizaci (tu je možné popsat pomocí Stokesových parametrů viz kapitola 1.3.2) [5].

Typicky je reprezentován jako dvourozměrný komplexní vektor, kde každá složka vektoru reprezentuje elektrické pole ve dvou vzájemně kolmých směrech (typicky označovaných jako horizontální a vertikální složka). Obecný tvar Jonesova vektoru lze zapsat jako:

$$\vec{J} = \begin{bmatrix} E_x \\ E_y \end{bmatrix} = \begin{bmatrix} E_{0x} e^{j\varphi_x} \\ E_{0y} e^{j\varphi_y} \end{bmatrix}, \tag{1.4}$$

kde E_{0x} a E_{0y} jsou amplitudy elektrického pole v daném směru, φ_x a φ_y jsou příslušné fáze [5]. Pro lineární horizontální polarizaci (LHP) bude Jonesův vektor vypadat následovně:

$$\vec{J}_{\mathrm{LHP}} = \begin{bmatrix} E_x \\ 0 \end{bmatrix} = \begin{bmatrix} E_{0x} e^{j\varphi_x} \\ 0 \end{bmatrix}, \tag{1.5}$$

kde složka ve směru y je nulová, což znamená, že neexistuje žádná složka elektrického pole ve vertikálním směru. Obdobně lze odvodit i Jonesův vektor pro lineární vertikální polarizaci (LVP):

$$\vec{J}_{\mathrm{LVP}} = \begin{bmatrix} 0 \\ E_y \end{bmatrix} = \begin{bmatrix} 0 \\ E_{0y} e^{j\varphi_y} \end{bmatrix}, \tag{1.6}$$

kde složka ve směru x je nulová [5].

Dále se provádí normalizace, která slouží ke zjednodušení vyjádření. Proces normalizace probíhá tak, že se vypočítá norma vektoru, a poté se každá složka vektoru dělí touto normou. U lineární horizontální či vertikální polarizace se nastaví hodnoty E_x nebo E_y na 1. V těchto případech je fázový posun mezi složkami irelevantní, což znamená, že neovlivňuje stav polarizace. Jonesovy vektory v normalizované normě budou mít výslednou podobu [5]:

$$\vec{J}_{\mathrm{LHP}} = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \quad \text{a} \quad \vec{J}_{\mathrm{LVP}} = \begin{bmatrix} 0 \\ 1 \end{bmatrix}. \tag{1.7}$$

1.3.2 Stokesovy parametry

Dalším matematickým způsobem jak reprezentovat polarizaci jsou Stokesovy parametry, které poprvé definoval George Gabriel Stokes. Na rozdíl od Jonesových vektorů, které jsou omezeny na popis výhradně plně polarizovaného světla, umožňují Stokesovy parametry zachytit také stav částečně polarizovaného světla [5].

Stokesovy parametry jsou reprezentovány čtyřmi hodnotami, které společně popisují stav polarizace světla. Tyto parametry jsou obvykle označovány jako S_0, S_1, S_2 a S_3 a jsou definovány následovně:

$$S_0 = E_{0x}^2 + E_{0y}^2, \tag{1.8}$$

$$S_1 = E_{0x}^2 - E_{0y}^2, \tag{1.9}$$

$$S_2 = 2E_{0x}E_{0y}\cos\varphi, \tag{1.10}$$

$$S_3 = 2E_{0x}E_{0y}\sin\varphi, \tag{1.11}$$

kde $\varphi = \varphi_y - \varphi_x$, parametr S_0 popisuje celkovou intenzitu světla, druhý parametr S_1 popisuje rozdíl mezi intenzitami lineárně polarizovaného světla v horizontálním

a vertikálním směru. Pokud je S_1 kladný ($S_1 > 0$), znamená to, že horizontální polarizace převažuje. Naopak, pokud je S_1 záporný ($S_1 < 0$), převažuje vertikální polarizace. Třetí parametr S_2 charakterizuje lineárně polarizované světlo pod úhlem $45°$ ($S_2 > 0$) nebo pod úhlem $-45°$ ($S_2 < 0$) vzhledem k horizontální ose. Poslední parametr S_3 poskytuje informace o kruhové polarizaci světla. Jeho hodnota určuje, zda světlo vykazuje pravotočivou ($S_3 > 0$) nebo levotočivou ($S_3 < 0$) kruhovou polarizaci. Mezi Stokesovými parametry platí následující vztah:

$$S_0^2 = S_1^2 + S_2^2 + S_3^2. \tag{1.12}$$

Kvadratická hodnota parametru S_0 reprezentující celkovou intenzitu světla, se rovná součtu kvadratických hodnot zbývajících tří parametrů S_1, S_2 a S_3, které společně charakterizují různé aspekty polarizace světla [5, 6].

Pomocí Stokesových parametrů lze popsat stupeň polarizace DOP (Degree of polarization), který vyjadřuje, do jaké míry je světlo polarizováno:

$$\mathrm{DOP} = \frac{I_{\text{polarizované}}}{I_{\text{celkové}}} = \frac{\sqrt{S_1^2 + S_2^2 + S_3^2}}{S_0}, \tag{1.13}$$

kde $I_{\text{polarizované}}$ značí intenzitu polarizovaného světla a $I_{\text{celkové}}$ značí celkovou intenzitu světla. DOP nabývá hodnot od 0 do 1: nepolarizované světlo má stupeň polarizace 0, úplně polarizované světlo má stupeň polarizace 1 a částečně polarizované světlo nabývá hodnot mezi 0 a 1 [6].

Soubor Stokesových parametrů lze zapsat do formy sloupcového vektoru, který se nazývá Stokesův vektor [6]:

$$\begin{bmatrix} S_0 \\ S_1 \\ S_2 \\ S_3 \end{bmatrix} = \begin{bmatrix} E_{0x}^2 + E_{0y}^2 \\ E_{0x}^2 - E_{0y}^2 \\ 2E_{0x}^2 E_{0y}^2 \cos\varphi \\ 2E_{0x}^2 E_{0y}^2 \sin\varphi \end{bmatrix}. \tag{1.14}$$

Tab. 1.1: Stokesovy a Jonesovy vektory pro některé polarizační stavy [5].

Polarizační stav	**Stokesův vektor**	**Jonesův vektor**
Lineární horizontální polarizace	$\begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \end{bmatrix}$	$\begin{bmatrix} 1 \\ 0 \end{bmatrix}$
Lineární vertikální polarizace	$\begin{bmatrix} 1 \\ -1 \\ 0 \\ 0 \end{bmatrix}$	$\begin{bmatrix} 0 \\ 1 \end{bmatrix}$
Lineární polarizace pod úhlem 45°	$\begin{bmatrix} 1 \\ 0 \\ 1 \\ 0 \end{bmatrix}$	$\frac{1}{\sqrt{2}}\begin{bmatrix} 1 \\ 1 \end{bmatrix}$
Lineární polarizace pod úhlem −45°	$\begin{bmatrix} 1 \\ 0 \\ -1 \\ 0 \end{bmatrix}$	$\frac{1}{\sqrt{2}}\begin{bmatrix} 1 \\ -1 \end{bmatrix}$
Kruhová levotočivá polarizace	$\begin{bmatrix} 1 \\ 0 \\ 0 \\ -1 \end{bmatrix}$	$\frac{1}{\sqrt{2}}\begin{bmatrix} 1 \\ i \end{bmatrix}$
Kruhová pravotočivá polarizace	$\begin{bmatrix} 1 \\ 0 \\ 0 \\ 1 \end{bmatrix}$	$\frac{1}{\sqrt{2}}\begin{bmatrix} 1 \\ -i \end{bmatrix}$
Nepolarizované světlo	$\begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}$	neexistuje

1.3.3 Jonesovy a Muellerovy matice

Jonesovy a Muellerovy matice jsou dvě hlavní metody používané pro popis chování polarizovaného světla při průchodu optickými komponentami a pro analýzu polarizačních stavů a jejich transformací. Jonesovy matice reprezentují transformaci pouze plně polarizovaného světla, Muellerovy matice jsou schopny popsat transformace plně i částečně polarizovaného světla. Z toho vyplývá, že Muellerovy matice jsou obecnější a umožňují reprezentovat širší spektrum polarizačních stavů [7].

Jonesovy matice

Jonesova matice je čtvercová matice o rozměrech 2×2 používaná k popisu polarizační transformace plně polarizovaného světla. To lze vyjádřit rovnicí:

$$\vec{J}_2 = \boldsymbol{J} \cdot \vec{J}_1, \tag{1.15}$$

kde $\vec{J}_1$ označuje Jonesův vektor reprezentující počáteční polarizační stav, který do soustavy vstoupil, $\vec{J}_2$ označuje Jonesův vektor reprezentující koncový polarizační stav, který vystoupí ze soustavy a $\boldsymbol{J}$ je příslušná Jonesova matice. Po rozepsání se získá [5, 8]:

$$\begin{bmatrix} E_{2x} \\ E_{2y} \end{bmatrix} = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} \begin{bmatrix} E_{1x} \\ E_{1y} \end{bmatrix}, \tag{1.16}$$

$$\begin{aligned} E_{2x} &= a_{11}E_{1x} + a_{12}E_{1y}, \\ E_{2y} &= a_{21}E_{1x} + a_{22}E_{1y}. \end{aligned} \tag{1.17}$$

Lineární polarizátory jsou optické prvky, které propouštějí světlo určité polarizace a blokují světlo jiné polarizace. Například lineární polarizátor orientovaný vertikálně propustí vertikálně polarizované světlo a blokuje horizontálně polarizované světlo [8]. Obecný tvar Jonesovy matice pro lineární polarizátor je následující:

$$\boldsymbol{J}_{\text{lineární}} = \begin{pmatrix} p_x & 0 \\ 0 & p_y \end{pmatrix}, \quad 0 \leq p_x, p_y \leq 1, \tag{1.18}$$

kde prvky p_x a p_y reprezentují propustnost polarizátoru pro horizontálně a vertikálně polarizované složky světla. Jejich hodnoty nabývají mezi 0 a 1, kde 1 znamená plnou propustnost a 0 znamená nepropustnost pro danou složku polarizace. Ideální lineární horizontální a lineární vertikální polarizátor lze popsat následujícími maticemi [7]:

$$\boldsymbol{J}_{\text{LHP}} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \quad \boldsymbol{J}_{\text{LVP}} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}. \tag{1.19}$$

Muellerovy matice

Muellerovy matice se využívají v kombinaci se Stokesovými parametry, které mají tu vlastnost, že popisují jak plně polarizované, tak i částečně polarizované světlo. Matice jsou čtvercové s rozměrem 4×4, používají se podobným způsobem jako Jonesovy matice:

$$\vec{S}_2 = \boldsymbol{M} \cdot \vec{S}_1, \tag{1.20}$$

kde $\vec{S}_1$ je Stokesův vektor popisující vstupní polarizační stav, $\vec{S}_2$ je výsledný polarizační stav a $\boldsymbol{M}$ je Muellerova matice. Ideální lineární horizontální a lineární vertikální polarizátor se dá popsat pomocí následujících Muellerových rovnic [8]:

$$\boldsymbol{M}_{\mathrm{LHP}} = \frac{1}{2}\begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}, \quad \boldsymbol{M}_{\mathrm{LVP}} = \frac{1}{2}\begin{pmatrix} 1 & -1 & 0 & 0 \\ -1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}. \tag{1.21}$$

1.3.4 Polarizační elipsa

Polarizační elipsa je grafické znázornění stavu polarizace světla, které poskytuje vizuální představu o tom, jak elektrické pole světelné vlny kmitá v čase. Z rovnic 1.2 a 1.3 je patrné, že mají společný člen $kz - \omega t$ (tzv. časoprostorový propagátor). Eliminací tohoto členu z obou rovnic se získá rovnice pro polarizační elipsu

$$\frac{E_x^2}{E_{0x}^2} + \frac{E_y^2}{{E_{0y}}^2} - 2\frac{E_x}{E_{0x}}\frac{E_y}{E_{0y}}\cos\varphi = \sin^2\varphi, \tag{1.22}$$

kde $\varphi = \varphi_y - \varphi_x$ [7].

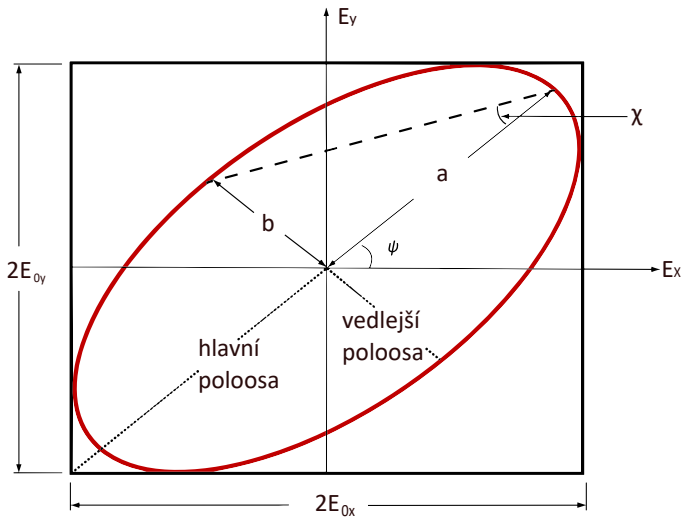
Polarizační elipsu lze charakterizovat dvěma úhly, které se nazývají azimut ψ a elipticita χ. Azimut ψ je úhel mezi hlavní osou elipsy a osou x, a lze jej definovat následovně:

$$\tan 2\psi = \frac{2E_{0x}E_{0y}}{E_{0x}^2 - E_{0y}^2}\cos\varphi, \quad 0 \leq \psi \leq \pi, \tag{1.23}$$

elipticita χ určuje poměr mezi délkami hlavní a vedlejší osy elipsy a má následující tvar:

$$\sin 2\chi = \frac{2E_{0x}E_{0y}\sin\varphi}{E_{0x}^2 + E_{0y}^2}, \quad -\pi/4 < \chi \leq \pi/4. \tag{1.24}$$

Polarizační elipsa slouží k vizualizaci polarizovaného světla. Nicméně, s výjimkou základních (degenerovaných) stavů polarizace, je v praxi velmi složité určit úhly, které tvoří elipsu. Dále jsou výpočty, které jsou nutné pro zjištění změn úhlů polarizovaného světla procházející jedním či více polarizačními prvky, složité a časově náročné. Tyto problémy překonává přehlednější vizualizace pomocí Poincarého koule, která je popsána v kapitole 1.3.5. [7, 9].



Obr. 1.2: Polarizační elipsa [9].

1.3.5 Poincarého koule

Poincarého koule je geometrická reprezentace stavů polarizace světla. Tento model je pojmenován po francouzském matematikovi jménem Jules Henri Poincaré. Umožňuje vizuálně zobrazit různé stupně polarizace (DOP): od bodu ve středu koule, který reprezentuje nepolarizované světlo (DOP = 0), přes body uvnitř koule, jež symbolizují částečně polarizované stavy (0 < DOP < 1), až po body na povrchu koule, kde každý z nich odpovídá plně polarizovanému světlu (DOP = 1). Povrchové body zahrnují všechny typy polarizace - lineární, kruhovou a eliptickou [6, 10].

Pokud se koule přirovná zeměkouli, tak lineární polarizace je znázorněna body na rovníku koule, kruhová polarizace se nachází na pólech. Eliptická polarizace je zobrazena všemi ostatními body na povrchu koule, které neleží přímo na rovníku nebo na pólech [6].

Polarizační stavy jsou určeny pomocí azimutálního úhlu (2ψ) a úhlu elipticity (2χ), které lze převést na kartézské souřadnice x, y a z na jednotkové kouli podle následujících vztahů:

$$x = \cos(2\chi)\cos(2\psi), \quad 0 \leq \psi < \pi, \tag{1.25}$$

$$y = \cos(2\chi)\sin(2\psi), \; -\frac{\pi}{4} < \chi \leq \frac{\pi}{4}, \tag{1.26}$$

$$z = \sin(2\chi). \tag{1.27}$$

kde platí $x^2 + y^2 + z^2 = 1$ [7].

Polarizační stavy lze na Poincarého kouli popsat i pomocí Stokesových parametrů. Stokesovy parametry S_1, S_2 a S_3 odpovídají souřadnicím x, y a z v trojrozměrném prostoru koule, lze je tedy chápat jako kartézské souřadnice, které určují polohu bodu na Poincarého kouli [6]. Tyto parametry jsou úzce spojeny s úhly polarizace, jako jsou azimutální úhel ψ a úhel elipticity χ, které pomáhají popsat orientaci a tvar polarizační elipsy. Vztah mezi Stokesovými parametry a těmito úhly lze popsat následovně [7]:

$$S_1 = S_0 \cos(2\chi)\cos(2\psi) \tag{1.28}$$

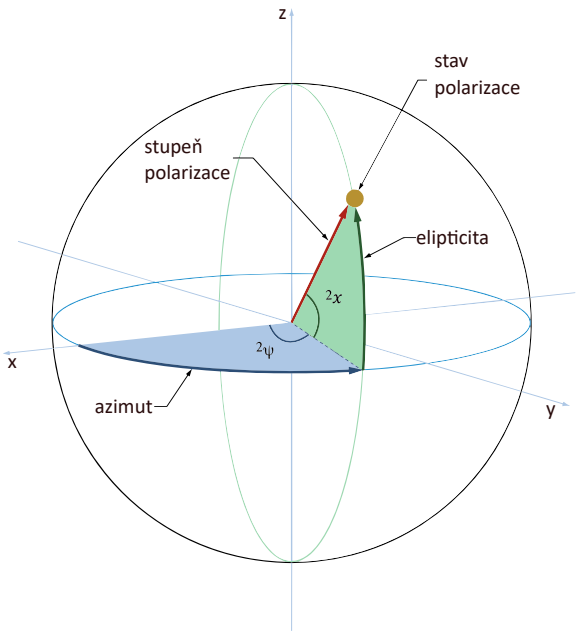
$$S_2 = S_0 \cos(2\chi)\sin(2\psi) \tag{1.29}$$

$$S_3 = S_0 \sin(2\chi), \tag{1.30}$$

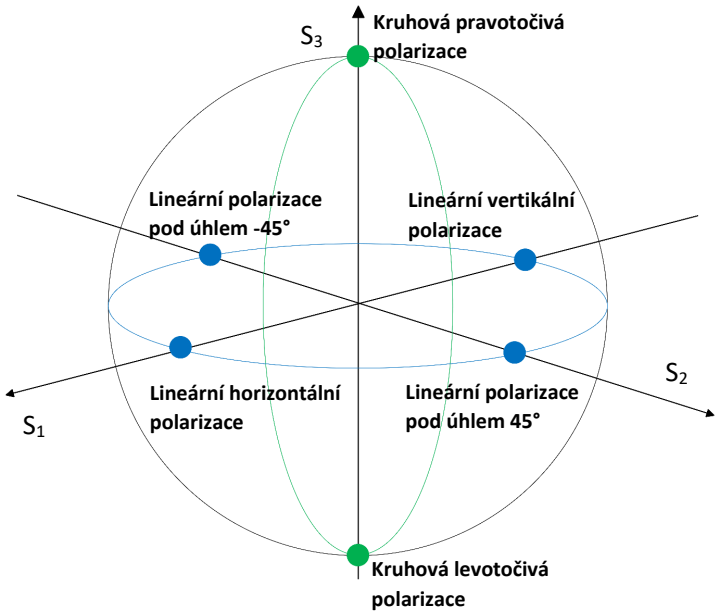
kde $S_0 = I$, a úhly lze vyjádřit:

$$\psi = \frac{1}{2}\tan^{-1}\left(\frac{S_2}{S_1}\right), \quad 0 \leq \psi \leq \pi, \tag{1.31}$$

$$\chi = \frac{1}{2}\sin^{-1}\left(\frac{S_3}{S_0}\right), \quad -\frac{\pi}{4} \leq \chi \leq \frac{\pi}{4}. \tag{1.32}$$



Obr. 1.3: Poincarého koule [11].



Obr. 1.4: Poincarého koule s vyznačenými polarizačními stavy [11].

2 Kvantová mechanika

Kvantová distribuce klíčů QKD je založena na základních principech kvantové mechaniky. Klíčové koncepty kvantové mechaniky, jako jsou superpozice, kvantová provázanost a princip neurčitosti, hrají stěžejní roli v procesu vytváření a distribuce klíčů v QKD systémech.

2.1 Základní koncepce kvantové mechaniky

Klasická mechanika je efektivní pro popis a předpovídání jevů v makrosvětě, přičemž se řídí zákony formulovanými Newtonem a dalšími, které účinně popisují pohyb a interakce objektů v našem okolí. Avšak při zkoumání mikrosvěta, který zahrnuje atomy a subatomové částice, se zjistilo, že klasická mechanika je nedostatečná pro popis jevů na této úrovni. Z tohoto důvodu byla vyvinuta kvantová mechanika, která umožňuje přesněji popsat a predikovat chování těchto částic. V této kapitole budou velmi stručně vysvětleny základní principy kvantové mechaniky [12].

Heisenbergův princip neurčitosti
Heisenbergův princip neurčitosti, pojmenovaný po německém fyzikovi Werneru Heisenbergovi, je jedním z klíčových konceptů v kvantové mechanice. Tento princip říká, že není možné současně a přesně určit některé páry kvantových vlastností, jako jsou poloha a hybnost částice. Čím přesnější je snaha změřit polohu částice, tím méně přesně jsme schopni určit její hybnost, a naopak. Když se změří jedna z těchto vlastností, dojde k ovlivnění stavu částice [12].

Teorém o neklonovatelnosti
Tento teorém říká, že není možné vytvořit dokonalou kopii libovolného neznámého kvantového stavu. Pokud by bylo možné přesně měřit všechny parametry bez narušení kvantového stavu, teoreticky by bylo možné tento stav duplikovat. S tím však souvisí Heisenbergův princip neurčitosti, podle kterého nelze získat veškeré informace o kvantovém systému. To znamená, že jakýkoli pokus o změření stavu nezbytně ovlivní jeho vlastnosti, a tím pádem jej není možné replikovat [13].

Princip superpozice
Kvantová superpozice je princip, podle kterého může být částice v několika stavech současně. Tento princip umožňuje kvantovým částicím existovat v kombinaci všech možných kvantových stavů až do momentu měření, kdy dochází ke kolapsu vlnové funkce na jeden konkrétní stav [14].

Kvantová provázanost
Kvantová provázanost nastává, když se stav jedné z dvojice nebo skupiny kvantových částic stane neoddělitelně spojeným se stavem ostatních. To se děje bez ohledu na vzdálenost mezi nimi [14].

Vlnově-částicový dualismus
Vlnově-částicový dualismus je princip, podle kterého mohou kvantové objekty projevovat vlastnosti jak vln, tak částic [12].

Vlnová funkce a kolaps
Vlnová funkce je základním matematickým aparátem popisující úplný stav kvantového systému. Systém může být před měřením v superpozici, což znamená, že existuje ve více stavech současně. Při měření dochází k jevu známému jako kolaps vlnové funkce. Tento kolaps převede superpozici na jeden konkrétní stav, který odpovídá výsledku měření. Před měřením nelze s jistotou určit, do kterého konkrétního stavu se systém zhroutí, ale lze určit pravděpodobnost různých možných výsledků. Tento jev úzce souvisí s dualismem částice a vlny, který je jedním ze základních principů kvantové mechaniky. Dualismus znamená, že kvantové objekty vykazují jak vlastnosti částic (diskrétní stavy), tak vln (superpozice stavů), a kolaps vlnové funkce představuje přechod z vlnového do konkrétního částicového stavu [14].

2.2 Qubit

Qubit, základní jednotka kvantové informace, se liší od tradičního bitu svou schopností existovat v několika stavech současně. Zatímco klasický bit může nabývat pouze jedné ze dvou hodnot (0 nebo 1), qubit, neboli kvantový bit, může reprezentovat 0, 1, nebo libovolnou kombinaci těchto stavů současně - tzv. superpozice. Tato vlastnost umožňuje qubitům zpracovávat a uchovávat větší množství informací než klasické bity, což vede k výrazně rychlejším a efektivnějším výpočetním schopnostem [15].

Qubit může být implementován různými fyzikálními způsoby, jedním z těchto způsobů je využití polarizace fotonů. Tento přístup využívá různých polarizačních stavů fotonů, jako jsou horizontální a vertikální polarizace, k reprezentaci kvantových stavů qubitu. V QKD se qubity často implementují právě pomocí polarizace fotonů [15].

Každý kvantový stav je možné popsat pomocí vektoru v Hilbertově prostoru. Pro každou dimenzi v Hilbertově prostoru existuje odpovídající základní (nebo vlastní) stav. Tyto základní stavy, které odpovídají různým dimenzím, jsou navzájem ortogonální. Pro vyjádření kvantového bitu, který nabývá hodnot 0 a 1, používáme dva základní stavy v rámci dvoudimenzionálního Hilbertova prostoru, který má následující bázové vektory [16, 17]:

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

Matematicky lze libovolný stav qubitu vyjádřit jako lineární superpozice těchto bázových stavů:

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

kde $|\psi\rangle$ je vektor popisující kvantový stav qubitu, koeficienty α a β jsou komplexní čísla popisující pravděpodobnostní amplitudy [15, 17].

Vizuálně je možné qubit znázornit pomocí Blochovy koule, která je více popsána v kapitole 2.3.3

2.3 Reprezentace kvantových stavů

2.3.1 Vlnová funkce a Diracova notace

Vlnová funkce je základním konceptem kvantové mechaniky poskytující kompletní informace o stavu kvantového systému. Tato komplexní funkce, označená jako

$$\psi(x, y, z, t) = \psi(\vec{r}, t), \tag{2.2}$$

zahrnuje reálné proměnné, kterými jsou prostorové souřadnice $\vec{r}$ a čas t [18].

Absolutní hodnota čtverce vlnové funkce $|\psi(\vec{r}, t)|^2$ udává pravděpodobnostní hustotu. To znamená, že popisuje pravděpodobnost nalezení částice v určitém místě prostoru v určitém čase. Z tohoto důvodu se vlnová funkce někdy označuje jako amplituda pravděpodobnosti [18].

Vlnovou funkci je možné zapsat v Diracově notaci, známé také jako bra-ket notaci, což je způsob, jakým se v kvantové mechanice zapisují kvantové stavy. Používá se ke zjednodušení a zobecnění výpočtů [19].

Vlnová funkce v bra-ket notaci má označení $|\psi\rangle$, kde symbol $|\,\rangle$ značí sloupcový vektor nazývaný jako „ket“ vektor. V případě, kdy je použit symbol $\langle\,|$, jedná se o „bra“ vektor, který je vzhledem k původnímu „ket“ vektoru transponovaný a komplexně sdružený vektor. Je zobrazen ve formě řádku [19].

2.3.2 Pauliho matice

Pauliho matice jsou souborem tří komplexních unitárních matic o rozměru 2×2. Využívají se zejména v teorii spinu částic, umožňují reprezentovat spinový stav částic. Každá Pauliho matice předsatvuje spin podél os x, y, z. Značí se $\sigma_x, \sigma_y, \sigma_z$ a jsou definovány následovně [20]:

$$\text{První Pauliho matice:} \quad \sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \tag{2.3}$$

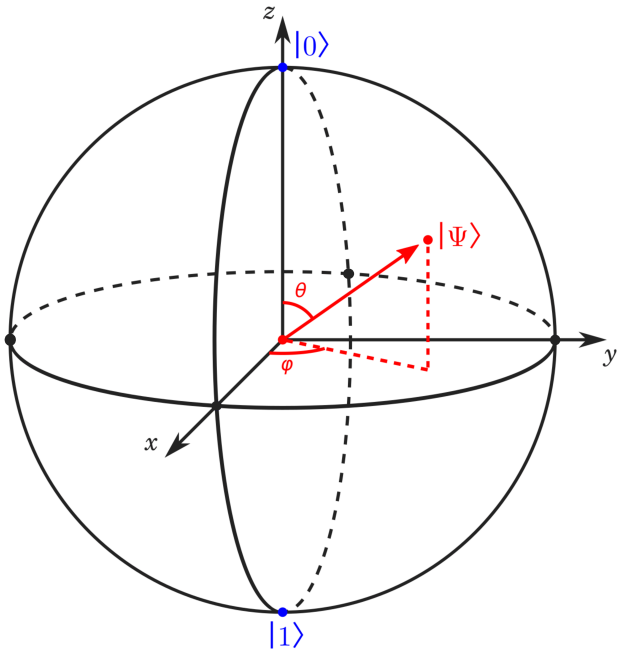
$$\text{Druhá Pauliho matice:} \quad \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \tag{2.4}$$

$$\text{Třetí Pauliho matice:} \quad \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \tag{2.5}$$

Pauliho matice σ_x a σ_z jsou v kvantové mechanice často popisovány jako reprezentace bit-flip (bitového převrácení) a phase-flip (fázového převrácení) operací. Pauliho matice σ_x mění stav qubitu z $|0\rangle$ na $|1\rangle$ a naopak. Na druhou stranu, matice σ_z mění fázi stavu $|1\rangle$, ale ponechává stav $|0\rangle$ nezměněn, což odpovídá fázovému převrácení. Matice σ_y lze pak chápat jako kombinaci obou těchto operací, bitového a fázového převrácení [20].

2.3.3 Blochova koule

Blochova koule slouží ke grafickému znázornění kvantového bitu, což umožňuje vizuální představu o tom, jak se qubit může nacházet ve stavu, který není čistě $|0\rangle$ nebo $|1\rangle$. Každý bod na povrchu Blochovy koule odpovídá možnému stavu qubitu. Na severním a jižním pólu koule existují dva základní stavy, které jsou vůči sobě ortogonální. Stav $|0\rangle$ je reprezentován bodem na severním pólu koule, stav $|1\rangle$ je reprezentován bodem na jižním pólu koule [21].



Obr. 2.1: Blochova koule [22].

Matematický zápis qubitu na Blochově kouli je

$$|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\phi}\sin\frac{\theta}{2}|1\rangle, \tag{2.6}$$

kde úhel θ nabývá hodnot v rozmezí 0 až π, což znamená že se může pohybovat od severního pólu k jižnímu. Když je $\theta = 0$, qubit je ve stavu $|0\rangle$, a když je $\theta = \pi$, qubit je ve stavu $|1\rangle$. Úhel ϕ má hodnoty v rozmezí od 0 do 2π, což umožňuje reprezentovat pohyb po celém obvodu koule v její rovníkové oblasti. Tento úhel reprezentuje fázovou rotaci okolo z-osy na Blochově kouli [21].

2.4 Analogické struktury mezi klasickou optikou a kvantovou mechanikou

Ačkoli se může zdát, že rozdíly mezi klasickou optikou a kvantovou mechanikou jsou významné, mnoho z těchto rozdílů pramení z odlišného názvosloví. Oba obory využívají podobné matematické struktury a transformace pro popis a manipulaci se stavy systémů. Ať už se jedná o polarizaci světla v rámci klasické optiky nebo kvantové stavy v kvantové mechanice, základní principy a postupy mají mnoho společného [23, 24].

Polarizace světla může být reprezentována pomocí Poincarého koule, zatímco kvantové stavy jsou reprezentovány na Blochově kouli. Blochova a Poincarého koule jsou matematicky ekvivalentní struktury, neboť obě představují jednotkové koule ve třírozměrném prostoru, které vizualizují stav systému. Střed Blochovy koule představuje maximálně smíšený stav, zatímco na povrchu jsou čisté stavy. Analogicky, střed Poincarého koule reprezentuje nepolarizované světlo, zatímco na povrchu je zcela polarizované světlo. Další analogií jsou Jonesovy a Pauliho matice, které sdílejí podobnou matematickou strukturu. Obě jsou 2x2 matice a reprezentují transformace stavů ve svých příslušných oblastech. Jonesovy matice mění polarizační stavy světla v klasické optice, zatímco Pauliho matice mění kvantové stavy qubitů v kvantové mechanice [23, 24].

Jonesův vektor, který popisuje stav polarizace světla, se dá zapsat jako

$$\vec{J} = \begin{bmatrix} \alpha \\ \beta \end{bmatrix}, \tag{2.7}$$

kde α je amplituda elektrického pole ve směru horizontální polarizace a β je amplituda elektrického pole ve směru vertikální polarizace. Každý kvantový stav je možné popsat pomocí vektoru v Hilbertově prostoru. Základními stavy tohoto prostoru jsou $|0\rangle$ a $|1\rangle$

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

Obecný stav qubitu lze vyjádřit jako lineární kombinaci těchto základních stavů:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle, \tag{2.8}$$

kde $|\psi\rangle$ je vektor popisující kvantový stav qubitu, α je amplituda pravděpodobnosti stavu $|0\rangle$ a β je amplituda pravděpodobnosti stavu $|1\rangle$. Oba popisy, jak Jonesův vektor, tak vlnová funkce, využívají komplexní amplitudy k charakterizaci stavu systému [15, 23].

3 Kvantová distribuce klíčů (QKD)

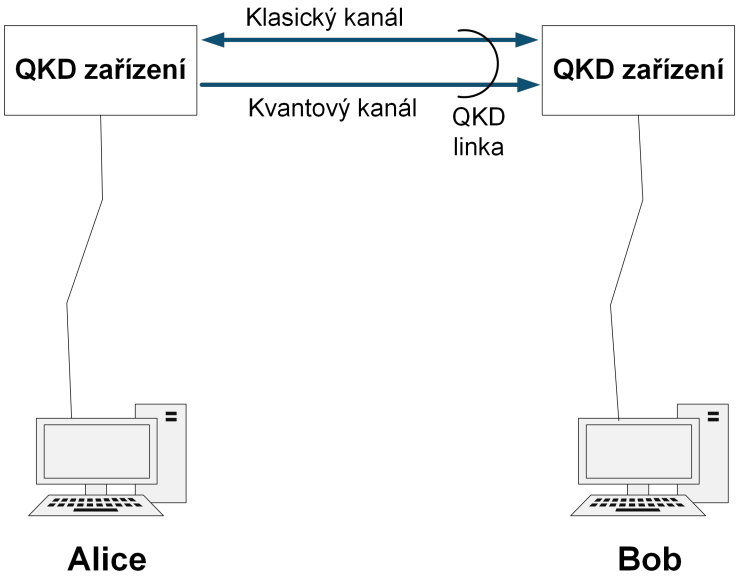
V dnešní době, kdy dochází k dynamickému rozvoji technologií umožňujících rychlé propojení na globální úrovni, je bezpečnost komunikace klíčová. Prostřednictvím internetu se již běžně přenáší citlivé údaje a je nezbytné zajistit, aby zasílané zprávy byly přístupné pouze těm, pro něž jsou určeny.

Kvantová distribuce klíčů poskytuje vysokou úroveň bezpečné komunikace a slibuje v zásadě takzvanou bezpodmínečnou bezpečnost. Na rozdíl od klasické kryptografie, jejíž bezpečnost je založena na složitosti řešení určitých matematických úloh, zabezpečení QKD není závislé na žádných výpočetních předpokladech. Pojem bezpodmínečná bezpečnost v kontextu QKD slibuje zabezpečení čistě na zákonech fyziky, konkrétně vychází ze základních principů kvantové mechaniky. Jakýkoli pokus o odposlech naruší kvantový stav přenášených částic. Tuto změnu je možné detekovat jako chybu, čímž se signalizuje možná přítomnost odposlouchávače. Bezpečnost je tak zajištěna bez ohledu na technologický pokrok nebo vývoj v oblasti výpočetní techniky, což činí QKD obzvláště odolnou proti pokročilým kryptografickým útokům, jako je například i útok pomocí kvantového počítače [25].

3.1 Základní princip QKD

QKD je metoda pro bezpečnou distribuci klíčů mezi dvěma komunikujícími stranami. Zatímco klasické kryptografické postupy se zabývají šifrováním zpráv a spoléhají převážně na matematické metody, kvantová kryptografie řeší systém distribuce klíčů a opírá se o základní fyzikální zákony kvantové mechaniky, které ji poskytují vysokou úroveň zabezpečení [26].

Obecný princip fungování QKD systému lze popsat následovně. Na obrázku 3.1 je znázorněno, že QKD systém má dva kanály, kvantový a klasický kanál. Tyto kanály dohromady tvoří QKD linku. Kvantový kanál slouží k přenosu a sdílení tajného klíče, který je kódován do kvantových stavů fotonů. Klasický kanál komunikující strany používají k řízení celého procesu a k ustanovení sdíleného klíče. Prostřednictvím tohoto kanálu dochází ke vzájemné komunikaci mezi oběma účastníky, z tohoto důvodu je kanál obousměrný [27, 28].



Obr. 3.1: Obecné schéma QKD.

Dva uživatelé, Alice (odesílatel) a Bob (příjemce), chtějí mezi sebou sdílet tajný klíč. Distribuce sdíleného klíče a následné post-procesní fáze se dají shrnout do tří částí, které budou popsány v následujících podkapitolách.

3.1.1 Výměna hrubého klíče (Raw key exchange)

Jediná část komunikace, která probíhá přes kvantový kanál.

- Alice si vygeneruje náhodnou posloupnost bitů, zakóduje je do jednotlivých fotonů jako různé stavy polarizace a odešle je Bobovi.
- Bob přijímá zakódované kvantové stavy fotonů a provede měření v různých bázích. Výsledky si poznamená [29].

3.1.2 Prosévání klíče (Key sifting)

Tato fáze a veškerá následující komunikace probíhá přes klasický kanál. Po přenosu kvantových stavů spolu Alice s Bobem komunikují, aby zjistili, ve kterých případech jsou výsledky měření kompatibilní. V případě, že by třetí strana neoprávněně vstoupila do komunikačního kanálu snažíc se odposlouchávat, její aktivita by ovlivnila kvantové stavy fotonů. Obě komunikující strany by mohly tuto změnu detekovat a dozvědět se tak o pokusu o odposlech [29].

- Bob sdělí Alici výsledky svého měření.
- Alice porovná výsledky měření a vybírá ty kvantové stavy fotonů, jež byly měřeny stejným způsobem. Porovnávají informace o základních stavech, které

použili pro přípravu a měření, ale nevyměňují si samotné výsledky měření. Výsledky, které nesouhlasí, jsou z hrubého klíče vyřazeny. Shodné výsledky jsou použity k vytvoření tzv. prosetého klíče (sifted key) [29, 30].

3.1.3 Destilace klíče (Key distillation)

Tato post-procesní fáze je důležitá součást QKD k zajištění efektivity celého procesu. Je klíčová pro zvýšení přesnosti, neboť umožňují identifikaci a opravu chyb, které se objevily během přenosu. Dále přispívají k lepší bezpečnosti tím, že zajišťují bezpečný přenos dat a prevenci jejich zneužití. V rámci této činnosti se uplatňují následující metody:

- **Korekce chyb (Error reconciliation):** Cílem korekce chyb je zajistit, aby obě strany měly identickou kopii klíče po procesu prosévání. Kvantový přenos může být náchylný k chybám nejen kvůli potenciálnímu rušení ze strany odposlouchávače, jako je Eva, ale také kvůli omezením a nepřesnostem přístrojového vybavení. Alice a Bob porovnají určité aspekty svých klíčů, aby identifikovali nesrovnalosti [31]. Tím získají QBER (Quantum Bit Error Rate), neboli kvantovou bitovou chybovost, která určuje chybovost přenosu. Pokud je hodnota QBER pod stanovenou mez, proces pokračuje a tajný klíč postupuje do další fáze destilace klíče. Naopak, pokud QBER překročí tuto prahovou hodnotu, tajný klíč je zahozen, jelikož vysoká chybovost bitů naznačuje možný odposlech. V takovém případě je nutné zahájit nový cyklus kvantové distribuce klíčů [32].
- **Zesílení soukromí (Privacy amplification):** Proces zesílení soukromí je realizován s cílem eliminovat informace, které mohla Eva získat o klíči. Během tohoto kroku dochází ke kompresi klíčového materiálu v poměru odpovídajícím hodnotě QBER. V případě, že je QBER vysoké, je vyžadována intenzivnější komprese, aby se minimalizovala možnost, že Eva má znalost některých bitů klíče [32].
- **Autentizace (Authentication):** Nakonec je nutné provést autentizaci, jež slouží k prevenci útoků typu „Man-in-the-middle“. Autentizace zajišťuje, že komunikace probíhá mezi oprávněnými stranami, tedy že Alice komunikuje skutečně s Bobem a naopak. Existuje riziko, že Eva rozdělí komunikační kanál mezi Alicí a Bobem. Při interakci s Alicí se Eva představuje jako Bob, zatímco v komunikaci s Bobem se vydává za Alici. Proto využívají předsdílený klíč, který využijí na počátku vzájemné komunikace. K příští autentizaci použijí část klíče, který byl získán během procesu kvantové distribuce klíčů [33].

3.2 Klasifikace protokolů

Existuje mnoho různých protokolů pro implementaci QKD, přičemž se nabízí různé přístupy pro jejich klasifikaci. Tyto protokoly mohou být obecně rozděleny na několik kategorií, z nichž dvě nejzákladnější jsou tzv. Prepare and Measure (PM) protokoly a protokoly založené na kvantovém provázání (Entanglement-Based, EB).

- **PM protokoly**: Tento protokol se skládá ze dvou kroků:
  1. Příprava (prepare): Alice připraví kvantový stav, který chce přenést, a pošle jej Bobovi.
  2. Měření (measure): Bob měří kvantový stav, který obdržel od Alice.
- **EB protokoly**: Na rozdíl od předchozího typu protokolu, kde dochází k využívání jednotlivých fotonů, zde hrají klíčovou roli provázané páry fotonů. Entanglement, neboli kvantové provázaní, znamená, že stav jedné částice je přímo spojen se stavem druhé [28].

Další možné rozdělení je podle typu kódování a dekódování, a to konkrétně QKD s diskrétní proměnnou (DV-QKD) a QKD se spojitou proměnnou (CV-QKD):

- **DV-QKD**: V těchto schématech dochází ke kódování přenášené informace do kvantových stavů jednotlivých částic, typicky fotonů. K detekci se používají jednofotonové detektory, které jsou schopné detekovat přítomnost či nepřítomnost jednotlivých fotonů.
- **CV-QKD**: Informace se kóduje do speciálních kvantových stavů, které mají kontinuální spektrum hodnot, např. amplitudy a fází světelných vln. Příklady takových stavů zahrnují kvantové stavy světla, jako jsou koherentní stavy nebo stlačené stavy. K detekci se používá homodynní či heterodynní detektor [34].

Podle směru, ve které komunikace probíhá, se rozlišují jednosměrné protokoly (one-way protocols) a dvousměrné protokoly (two-way protocols):

- **Jednosměrné protokoly**: Výměna klíče probíhá pouze jedním směrem.
- **Dvousměrné protokoly**: Komunikace probíhá oběma směry a výměna klíče probíhá obousměrně.

3.3 Alternativní metody

Ve světě, kde se výpočetní technologie neustále vyvíjí a s nimi i potenciální hrozba kvantových počítačů, se QKD stává jednou z nejperspektivnějších metod v zajištění bezpečnosti komunikace v budoucnosti. Nicméně, i přes své silné stránky, QKD má své nevýhody: vysoké náklady na infrastrukturu potřebnou k jeho implementaci a omezení vzdálenosti, na kterou lze klíče poslat. Z toho důvodu se vyvíjí i další mechanismy, které by byly schopny odolat kvantovým počítačům a kvantovým útokům.

Jedním z klíčových aspektů současné kryptografie, která reaguje na výzvy spojené s kvantovými technologiemi, je kryptografická agilita. Tato vlastnost umožňuje efektivně přecházet mezi různými kryptografickými schématy bez nutnosti výměny celého systémů nebo složitého zasahování do stávající infrastruktury. Kryptografická agilita zahrnuje schopnost rychle se přizpůsobit a implementovat nové algoritmy nebo upravit stávající, pokud se ukážou být zranitelné. Implementace není jednoduchá kvůli potřebě zpětné kompatibility, tedy aby systémy umožňovaly používat různé sady kryptografických algoritmů současně, a také kvůli požadavku na snadnou výměnu [35, 36].

3.3.1 Postkvantová kryptografie (PQC)

Postkvantová kryptografie, která se také označuje jako kvantově odolná kryptografie nebo kvantově bezpečná kryptografie (QSC – Quantum-Safe Cryptography), je souhrn kryptografických algoritmů s veřejnými klíči, které budou odolávat kvantovým hrozbám. Je založena na matematických problémech, u nichž se předpokládá, že budou neřešitelné jak pro klasické, tak pro kvantové počítače [35].

PQC je vnímána řadou bezpečnostních institucí jako nejefektivnější cesta, jak vzdorovat kvantovým výzvám. Na rozdíl od QKD, které pro svou implementaci vyžaduje speciální hardware, postkvantové algoritmy lze vykonávat i na klasických počítačích. V současné době se tyto algoritmy zaměřují na kryptografii na bázi kódů, na mřížkách, na hashích či na multivariační kryptografii [35, 36].

Tab. 3.1: Srovnání QKD a PQC [37].

	QKD	**PQC**
Úroveň bezpečnosti	„Bezpodmínečně bezpečné“, bezpečnost založena na zákonech fyziky.	Vysoce bezpečné, ale neexistuje matematický důkaz o neprolomitelnosti.
Princip fungování	Založena na principech fyziky, konkrétně kvantové mechaniky.	Založena na matematických algoritmech, u kterých se předpokládá, že budou neřešitelné.
Implementace	Vyžaduje speciální hardware.	Nevyžaduje speciální hardware.
Cena	Dražší než PQC (potřeba hardwaru a změn v infrastruktuře).	Levnější než QKD.
Dlouhodobá udržitelnost	Komunikace nemůže být retrospektivně dešifrována, klíče nelze kopírovat ani ukládat → Vhodné k dlouhodobému utajení informace.	Zranitelná vůči budoucím pokrokům v matematice, komunikace může být zpětně dešifrována → Nevhodné k dlouhodobému utajení informace.
Dosah	Omezený.	Neomezený.
Škálovatelnost	Vyžaduje speciální infrastrukturu, což může být technicky náročné na široké nasazení.	Využívá podobných algoritmů, možno implementovat jako software do nynějších systémů bez nutnosti zásadních hardwarových změn.

3.3.2 Symetrická kryptografie s délkou klíče 256 bitů

Jako další variantu lze zmínit i symetrickou kryptografii s klíčem o délce 256 bitů. Taková délka klíče je považována za kvantově odolnou. Avšak je třeba mít na paměti, že symetrická kryptografie vyžaduje bezpečný způsob distribuce klíčů mezi oběma stranami, což je problém, který QKD umí vyřešit. Výhradní použití symetrické kryptografie by vedlo ke ztratě přínosů, které nabízí kryptografie s veřejnými klíči [35].

3.4 Proč je QKD v současné době důležité?

Současná bezpečnost internetových služeb je založena na využívání asymetrické kryptografie, která je založena na dosud nevyřešených matematických problémech, z nichž některé základní jsou faktorizace velkých čísel nebo počítání diskrétního logaritmu. Současné počítače tyto matematické úlohy nespočítají. S příchodem kvantových počítačů se objevuje hrozba, že tyto metody budou jednoduše prolomeny, jelikož kvantové počítače mají potenciál tato matematická omezení překonat rychleji [25, 38].

QKD je klíčovou technologií pro budoucnost, která bude moci nabídnout zabezpečení při přenosu informací i v prostředí, kde současná kryptografie selhává. Tato metoda distribuce klíčů bude poskytovat bezpečnost i v případě vzniku kvantového počítače. Kvantová kryptografie využívá principů kvantové mechaniky, což zaručuje, že jakákoli informace přenášená pomocí fotonů se při pokusu o odposlech třetí stranou nevyhnutelně změní. To umožňuje komunikujícím stranám detekovat jakékoli narušení [28, 39].

4 Jednosměrné DV-QKD protokoly

Jednosměrné DV-QKD protokoly jsou základním stavebním kamenem QKD. Jsou považovány za nejstarší a obecně jsou lépe srozumitelné než CV-QKD. Klíčovým prvkem je využití kvantových vlastností částic, jako jsou fotony, pro přenos informací. Nejčastější formou kódování je využití diskrétních kvantových stavů, jako jsou polarizační stavy fotonů. Jak je patrné z názvu, přenášená informace probíhá pouze jedním směrem [16].

Prepare and Measure protokoly
Jak již bylo zmíněno v kapitole 3.2, tyto protokoly zahrnují dvě základní fáze: přípravu (prepare) kvantových stavů a jejich následné měření (measure). Bezpečnostní aspekty těchto protokolů jsou zakotveny v základních principech kvantové mechaniky, konkrétně v principu neurčitosti a nemožnosti kopírování kvantových stavů. Tyto charakteristiky zajistí, že jakýkoliv pokus o neoprávněné odposlechnutí způsobí narušení kvantového stavu, což lze detekovat jako chybu během přenosu [28].

4.1 Protokol BB84

Protokol BB84 položil základy pro další výzkum a vývoj v oblasti QKD, jelikož se jedná o první takový protokol. Byl navržen v roce 1984 dvěma americkými vědci Charlesem H. Bennettem a Gillesem Brassardem a je stále považován za jeden z nejdůležitějších protokolů v tomto odvětví.

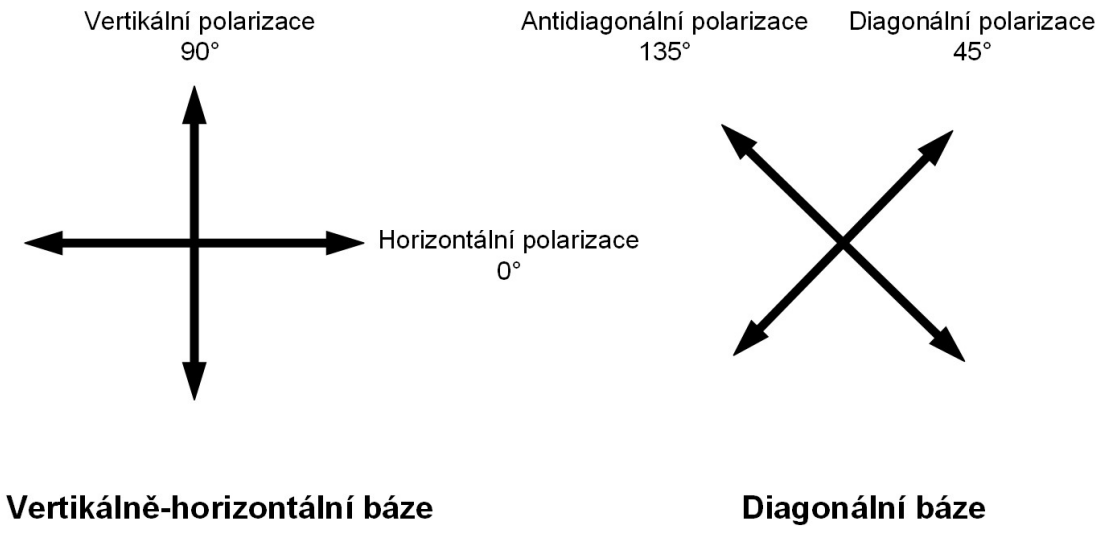
4.1.1 Obecný princip

Tento protokol pracuje s polarizací fotonů, přičemž se používají následující čtyři stavy:

- **Horizontální polarizace:** Foton je polarizován pod úhlem 0°.
- **Vertikální polarizace:** Foton je polarizován pod úhlem 90°.
- **Diagonální polarizace:** Foton je polarizován pod úhlem 45°.
- **Antidiagonální polarizace:** Foton je polarizován pod úhlem 135°.

Polarizace fotonů se měří ve dvou polarizačních bázích, ve kterých mohou fotony oscilovat:

- **Vertikálně-horizontální báze:** Značí se $\oplus$ a výsledkem měření polarizace mohou být kvantové stavy $\{|\rightarrow\rangle, |\uparrow\rangle\}$.
- **Diagonální báze:** Značí se $\otimes$ a výsledkem měření polarizace mohou být kvantové stavy $\{|\nearrow\rangle, |\nwarrow\rangle\}$ [28, 17].



Obr. 4.1: Polarizační báze protokolu BB84

Každému stavu v bázi je přidělena binární hodnota 0 a 1 pro vyjádření bitů. To znamená, že jedničkový bit je reprezentován dvěma stavy a nulový bit také dvěma stavy.

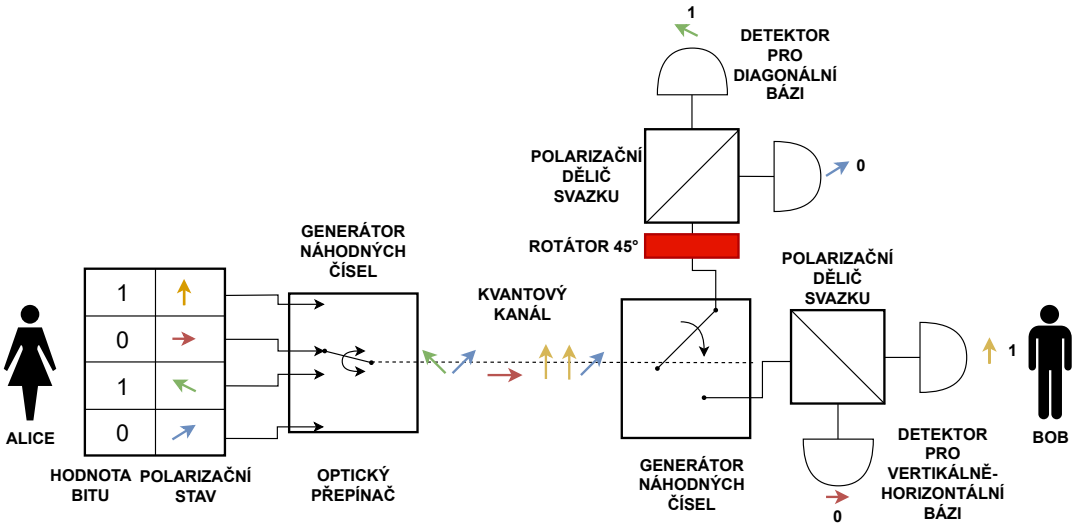
Tab. 4.1: Přiřazené bitové hodnoty jednotlivým stavům [40].

Stav polarizovaného fotonu	**Bitová hodnota**	**Báze**
$\rightarrow$	0	$\oplus$
$\uparrow$	1	$\oplus$
$\nearrow$	0	$\otimes$
$\nwarrow$	1	$\otimes$

Výměna klíče probíhá v několika krocích:

- **Příprava a odeslání fotonů Alicí:** Alice nejprve vybere náhodný bitový řetězec a náhodnou sekvenci polarizačních bází $\otimes, \oplus$. Tato komunikace probíhá přes kvantový kanál. Alice odesílá směrem Bobovi sérii fotonů, přičemž každý foton reprezentuje jeden bit z řetězce v bázi vybrané pro danou pozici bitu. Přiřazené bitové hodnoty jednotlivým stavům jsou znázorněny v tabulce 4.1.
- **Příjem a měření fotonů Bobem:** Bob přijímá jednotlivé fotony, náhodně volí polarizační bázi a získané výsledky si zaznamenává. Výsledek měření interpretuje jako binární nulu nebo jedničku.
- **Sdělení výsledků:** Následující kroky protokolu probíhají přes běžný veřejný komunikační kanál. Bob sdělí Alici své výsledky, a to konkrétně jaké typy bází

pro jednotlivě přijaté fotony použil. Alice sdělí, kdy došlo ke shodě. Protože jsou jen dvě možné báze a výběr je zcela náhodný, pravděpodobnost, že Bob zvolí stejnou bázi jako Alice, je 50%. Shodná série bitů tak tvoří klíč, ostatní bity jsou zahozeny [41].



Obr. 4.2: Obecné schéma protokolu BB84 [42]

.

Tab. 4.2: Průběh přenosu klíče pomocí protokolu BB84 [28].

Aliciny bity	1	0	1	1	0	0	0	1
Aliciny báze	⊕	⊗	⊕	⊕	⊗	⊗	⊕	⊗
Aliciny fotony	↑	↗	↑	↑	↗	↗	→	↖
Bobovy náhodné báze	⊗	⊕	⊗	⊕	⊗	⊗	⊗	⊗
Bobovy bity	0	0	1	1	0	0	0	1
Bob Alici sdělí báze	⊗	⊕	⊗	⊕	⊗	⊗	⊗	⊗
Alice sdělí shodu bází	X	X	X	✓	✓	✓	X	✓
Sdílený klíč	-	-	-	1	0	0	-	1

4.1.2 Detekce odposlechu

Alice a Bob mohou provést kroky k ověření, zda nedošlo k odposlechu během jejich komunikace. Pokud by se Eva, coby třetí strana, snažila zachytit a analyzovat kvantové signály určené pro Boba, musela by se spolehnout na svůj odhad při volbě polarizačních bází. Vzhledem k tomu, že Eva nemá přesné informace o použitých bázích, její pokusy o měření nevyhnutelně naruší původní polarizační stavy některých fotonů. Tyto narušení se pak projeví jako chyby ve finálním sdíleném klíči, které Alice a Bob mohou identifikovat a použít jako indikaci potenciálního odposlechu.

Při odposlechu Eva zachytává Aliciny fotony a stejně jako Bob vybírá náhodně ze dvou polarizačních bází. Pravděpodobnost, že zvolí stejnou bázi jako Alice, je 50 % (v takovém případě se stav fotonu nezmění a nikdo nepozná, že došlo k odposlechu). Pokud Eva zvolí špatnou bázi, k Bobovi se dostanou nezměněné fotony v původní podobě opět s 50% pravděpodobností. Součinem zmíněných pravděpodobností lze určit, že Eva svým odposlechem způsobí chyby ve 25 % případů. Tedy pravděpodobnost, že chyba nenastane, je $\frac{3}{4}$ (75 %). Aby Alice a Bob mohli zjistit, jestli došlo k odposlechu, vymění si n bitů a porovnají výsledky. Pokud se hodnoty neshodují, chyba v těchto bitech může signalizovat přítomnost Evy. Pravděpodobnost, že Eva zůstane neodhalená po n porovnáních, je $\left(\frac{3}{4}\right)^n$. Pravděpodobnost, že Eva bude odhalena, se dá spočítat jako $1 - \left(\frac{3}{4}\right)^n$. Obětované fotony jsou zahozeny a nejsou již použity k vytvoření klíče [26, 33].

4.2 Protokol B92

Protokol B92 byl vyvinut Charlesem H. Bennettem v roce 1992 jako jednodušší alternativa k jeho předchozímu protokolu BB84. Klíčovým rozdílem je počet polarizačních stavů fotonů. Zatímco BB84 využívá čtyři polarizační stavy, B92 využívá pouze dva stavy, které jsou vzájemně neortogonální [28].

- **Příprava a odeslání fotonů Alicí:** Alice si zvolí pro horizontální stav $|\rightarrow\rangle$ bitovou hodnotu 0, pro diagonální stav $|\nearrow\rangle$ bitovou hodnotu 1 a tuto informaci sdělí Bobovi. Kvantovým kanálem odešle Bobovi jednotlivé fotony [26, 43].
- **Příjem a měření fotonů Bobem:** Bob náhodně volí polarizační báze ($\otimes, \oplus$) a výsledky měření si zaznamenává. Následně budou rozebrány možnosti, které mohou nastat:
    1. **Bob zvolí $\oplus$ bázi:** Pokud výsledkem jeho měření je stav $|\uparrow\rangle$, Alice zaslala $|\nearrow\rangle$ a hodnota bitu je 1. Pokud je výsledkem měření stav $|\rightarrow\rangle$, Alice mohla zaslat foton ve stavu $|\rightarrow\rangle$ nebo $|\nearrow\rangle$. V takovém případě není schopen určit hodnotu bitu.

2. **Bob zvolí ⊗ bázi:** Pokud výsledkem jeho měření je stav $|\nwarrow\rangle$, znamená to, že Alice poslala stav $|\rightarrow\rangle$. Tento výsledek reprezentuje hodnotu bitu 0. Pokud zaznamená výsledek $|\nearrow\rangle$, znamená to, že Alice poslala buď stav $|\nearrow\rangle$ nebo $|\rightarrow\rangle$. Tento výsledek neumožňuje určit konkrétní bit [26, 43].

- **Sdělení výsledků:** Bob přes veřejný kanál sděluje Alici pozici fotonů, které byl schopný identifikovat. Série bitů bude použita k vytvoření klíče [26, 43].

4.3 Šestistavový protokol

Six-State Protocol, neboli šestistavový protokol je rozšířením protokolu BB84. Zatímco BB84 využívá čtyř kvantových stavů, obvykle reprezentovaných dvěma ortogonálními bázemi, Six-State Protocol, jak je již z názvu patrné, tuto sadu rozšiřuje na šest stavů. Kromě lineární a diagonální polarizace se zde využívá i polarizace kruhová, která zahrnuje pravotočivou $|\circlearrowright\rangle$ a levotočivou $|\circlearrowleft\rangle$ kruhovou polarizaci. Tím se zvyšuje bezpečnost protokolu proti odposlechu, protože útočník má menší šanci správně uhodnout bázi ze tří možností, nikoli jen ze dvou jako je tomu u BB84. Způsobí tak větší množství chyb, které jsou následně detekované. Princip komunikace je jinak zcela shodný s protokolem BB84 [16].

4.4 Protokol T12

Protokol T12, který byl představen společností Toshiba v roce 2012, je variantou kvantového protokolu pro distribuci klíčů (QKD). Je založen na populárním BB84 protokolu, ale zahrnuje několik důležitých vylepšení pro zvýšení jeho praktičnosti a bezpečnosti [44].

Tento protokol využívá tzv. návnadové stavy (decoy states), jejichž hlavním účelem je detekovat pokusy o odposlech a zvýšit bezpečnost kvantové komunikace. Toho je dosaženo tím, že Alice připraví sadu dodatečných stavů - návnadových - kromě standardních stavů používaných pro generování klíčů. Hlavním rozdílem mezi návnadovými stavy a standardními stavy je jejich intenzita, neboli distribuce počtu fotonů [45].

Stejně jako v protokolu BB84 Alice vybírá mezi dvěma bázemi Z $\{|\rightarrow\rangle, |\uparrow\rangle\}$ a X $\{|\nearrow\rangle, |\nwarrow\rangle\}$. Báze jsou vybírány s pravděpodobností $p_z \geq \frac{1}{2}$ a $p_x = 1 - p_z$. Z toho vyplývá, že báze Z je majoritní a je vybírána častěji, zatímco báze X je minoritní. Alice dále vybírá intenzitu světla ze tří typů, které se označují u, v a w. Každý z nich představuje různou úroveň intenzity fotonů: u (signál) - signální pulzy nesoucí kvantovou informaci, v (vakuum) - pulz neobsahuje žádný foton, w (weak decoy

states - slabé návnadové stavy) - pulzy s nižší intenzitou než signální pulzy, obsahující menší průměrný počet fotonů [44, 45].

Hlavní výhodou protokolu T12 oproti BB84 je asymetrická pravděpodobnost používání bází. V protokolu BB84 Alice a Bob vybírají báze se stejnou pravděpodobností, tedy $p_x = p_z = 50$ %. V průběhu prosévání klíče tak dojde k eliminaci 50 % bitů a pouze polovina bitů je použita pro vytvoření klíče. V protokolu T12 jsou vybírány báze s různými pravděpodobnostmi, typicky pravděpodobnost výběru majoritní báze p_z je nastavena na $\frac{15}{16}$ a p_x na $\frac{1}{16}$. Pravděpodobnost, že vyberou různé báze, je $\frac{15}{16} \cdot \frac{1}{16} = \frac{15}{256}$ pro každou kombinaci (Z od Alice, X od Boba, a naopak). Celková pravděpodobnost, že báze budou odlišné, a tedy bit bude eliminován, je součet těchto pravděpodobností: $\frac{15}{256} + \frac{15}{256} = \frac{30}{256}$. Díky nerovnoměrnému rozložení vybírání bází je eliminováno pouze 11,7 % bitů během prosévání klíče, což zvyšuje efektivitu přenosu ve srovnání s BB84, kde je eliminováno 50 %. Více bitů je tak použito pro generování klíče, zatímco menší počet bitů je eliminován během prosévání [44].

Informace z minoritní báze jsou klíčové pro zajištění bezpečné komunikace. Pokud Alice a Bob zaznamenají vysokou chybovost v této bázi, může to naznačovat přítomnost Evy. Vzhledem k tomu, že báze X se využívá méně často, každý bit v této bázi má větší váhu pro detekci anomálií [44].

4.5 Protokol SARG04

Protokol SARG04 je pojmenován podle iniciál jeho čtyř vynálezců: Scarani, Acin, Ribordy a Gisin, a roku 2004, kdy byl vytvořen. Jedná se o alternativu k již existujícímu protokolu BB84, nabízí však větší odolnost proti útokům typu PNS (Photon Number Splitting Attack) - útok dělením počtu fotonů [16].

Nejdříve je přiřazena každému polarizačnímu stavu bitová hodnota. Nyní je zvolena pro stavy $|\uparrow\rangle$ a $|\rightarrow\rangle$ bitová hodnota 1, stavy $|\nearrow\rangle$ a $|\nwarrow\rangle$ jsou reprezentovány bitovou hodnotou 0. Následující komunikace probíhá stejně jako u protokolu BB84: Alice připravuje a vysílá fotony ve čtyřech různých možných stavech, Bob pro každý přijatý foton náhodně volí bázi a výsledek si poznamená [26].

Rozdíl nastává ve sdělení výsledků. V protokolu BB84 Bob informuje Alici o bázích, které zvolil pro měření fotonů. V protokolu SARG04 Alice poskytne Bobovi dva neortogonální kvantové stavy, přičemž jeden z nich byl použit pro odeslání zprávy. Alice tedy může odesílat následující kombinace: $\{|\rightarrow\rangle, |\nwarrow\rangle\}$, $\{|\rightarrow\rangle, |\nearrow\rangle\}$, $\{|\uparrow\rangle, |\nwarrow\rangle\}$ a $\{|\uparrow\rangle, |\nearrow\rangle\}$ [16].

Alice odešle foton ve stavu $|\uparrow\rangle$, Bob volí $\otimes$ bázi a naměří $|\nwarrow\rangle$. Alice mu zašle dvojici fotonů $\{|\uparrow\rangle, |\nearrow\rangle\}$. Pokud Bob pozoruje, že polarizace fotonu, který změřil, je kolmá na polarizaci jednoho z páru fotonů zaslané Alicí, dojde k závěru, že si nevybral správnou polarizační bázi, protože by měla být polarizace obou fotonů

stejná. V důsledku toho může Bob s jistotou určit, že druhý foton v páru byl odeslán Alicí. V tomto případě tedy zhodnotí, že Alice zaslala $|\uparrow\rangle$ a zapíše hodnotu 1 [26].

Pokud Alice odešle foton ve stavu $|\uparrow\rangle$, Bob volí $\otimes$ bázi, ale tentokrát naměří $|\nearrow\rangle$. Alice mu zašle dvojici fotonů $\{|\uparrow\rangle, |\nearrow\rangle\}$. Pokud Bob zjistí, že polarizace fotonu, který změřil, odpovídá polarizaci některého z fotonů ve skupině, nemůže s určitostí říci, jestli tento foton s konkrétní polarizací poslala Alice, nebo zda došlo k chybě při výběru polarizační báze na jeho straně. V takovém případě Bob výsledek svého měření zahodí. Po odeslání a naměření všech fotonů Bob informuje Alici o bitech, u kterých byl schopen určit jejich stav. Tyto bity následně tvoří surový klíč [26].

5 Standardizace v oblasti QKD

Kvantová distribuce klíčů se v posledních letech vyvíjí rychlým tempem, avšak aby se tato technologie mohla plně rozvinout a stát se široce dostupnou, je nezbytná standardizace. Tento proces je klíčovým prvkem pro zajištění interoperability a integrace QKD systémů do stávajících telekomunikačních sítí. Standardy umožňují systémům od různých výrobců vzájemně komunikovat a spolupracovat tak bez problémů. Tímto způsobem se zvyšuje možnost širšího nasazení QKD technologií. Standardy definují bezpečnostní prvky, které musí QKD systémy splňovat. Tím zajišťují, že systémy budou navrženy tak, aby odolávaly útokům a zvyšovaly úroveň bezpečnosti [46, 47].

Standardy jsou definovány především mezinárodními organizacemi, které jsou rozebrány v následujících podkapitolách. Seznam aktuálně platných standardů i návrhů standardů od jednotlivých organizací je součástí přílohy A.

5.1 ETSI

ETSI (European Telecommunications Standards Institute) je evropská nezisková organizace, jež byla založena v roce 1988. Její sídlo se nachází ve Francii. Tato organizace je jednou ze tří evropských standardizačních organizací (ESO), jejichž klíčovou úlohou je vytváření a správa standardů v Evropské unii. Pouze normy vytvořené institucemi ETSI, CEN a CENELEC jsou oficiálně uznávané jako evropské normy [48].

ETSI je rozsáhlá instituce, zahrnuje několik skupin zaměřené na různé oblasti. ISG (Industry Specification Group) jsou pracovní skupiny v rámci ETSI, které se zaměřují na určitou oblast standardizace nebo technologické odvětví. Tyto skupiny mají za úkol urychlit proces vývoje standardizace v reakci na nové technologické výzvy. V roce 2008 tak byla vytvořena pracovní skupina ISG-QKD speciálně pro standardizaci QKD. Úkolem této skupiny je vypracovat technické specifikace pro implementaci kvantové distribuce klíčů. K tomu využívá dva druhy dokumentů, které následně zveřejňuje ETSI [47, 48]:

- **Group Specification (GS)**: Technický dokument obsahující konkrétní technické požadavky, vysvětlující materiál, nebo obojí.
- **Group Report (GR)**: Dokument obsahující pouze informativní prvky.

Skupina ETSI ISG-QKD vydala již přes 20 dokumentů, které se zabývaly oblastí aplikačního rozhraní (GS QKD 004), bezpečnostními důkazy (GS QKD 005), charakterizací komponentů (GS QKD 011) či specifikací parametrů (GS QKD 012). Mezi důležité dokumenty patří i GS QKD 014, který se zaměřuje na protokoly

a formáty dat rozhraní REST API pro doručení klíčů, který umožňuje interoperabilitu mezi různými zařízeními [46, 48]. V lednu roku 2024 vyšla aktualizovaná verze dokumentu GS QKD 016, který se jako první zabýval profilem ochrany pro QKD systémy. Tento standard definuje bezpečnostní požadavky, které musí QKD systémy splňovat, a tím pomáhá zajistit, že QKD systémy budou považovány za bezpečné a důvěryhodné [48].

V současné době několik publikací prochází revizí, které budou brzy dostupné v novější verzi, a vytváří se nové návrhy dokumentů [48]:

- **ETSI GS QKD 010**: Zabývá se ochranou QKD systémů proti útokům trojským koněm.
- **ETSI GS QKD 013**: Charakterizuje specifické vlastnosti vysílacích modulů QKD.
- **ETSI GR QKD 017**: Provádí průzkum různých síťových architektur.
- **ETSI GR QKD 019**: Technická zpráva o návrhu rozhraní pro systémy QKD, které zahrnují autentizaci.
- **ETSI GS QKD 020**: Specifikuje protokoly a formáty dat rozhraní REST API pro interoperabilitu systému správy klíčů.
- **ETSI GS QKD 021**: Zabývá se rozhraním mezi orchestrátorem SDN a kontrolérem SDN pro interoperabilní systém správy klíčů.
- **ETSI GS QKD 022**: Specifikace architektury sítě.
- **ETSI GS QKD 023**: Definice rozhraní a datového modelu pro monitorování QKD.

5.2 ITU-T

ITU-T (International Telecommunication Union Telecommunication Standardization Sector) je jeden ze tří sektorů organizace ITU (International Telecommunication Union), která spadá pod OSN. Byla založena v roce 1865 a její sídlo se nachází ve švýcarské Ženevě. ITU-T se zaměřuje na standardizaci v oblastech telekomunikací a informačních technologií [49].

Studijní skupiny (SG) jsou základními prvky ITU-T, kde se formují technické standardy a doporučení. Každá studijní skupina se zaměřuje na specifická témata a oblasti. SG11 (Protokoly) se zabývá klasickými protokoly a rozhraními pro QKDN, SG13 (Budoucí sítě) se obecně zabývá funkčními požadavky pro QKDN a SG17 (Bezpečnost) se věnuje kybernetické bezpečnosti a bezpečnostním architekturám. Dokumenty jsou organizovány do řady různých sérií, kdy každá série se soustředí na specifickou oblast. V procesu standardizace QKD jsou využívány tři typy dokumentů ITU-T [47, 49]:

- **ITU-T Q**: Přepínání a signalizace a související testy a měření.
- **ITU-T X**: Datové sítě, komunikace v otevřeném systému a zabezpečení.
- **ITU-T Y**: Globální informační infrastruktura a aspekty internetových protokolů.

Organizace vydala již několik desítek standardů zabývajícími se QKD, kompletní přehled se nachází v příloze A.2.

5.3 IEEE

IEEE (Institute of Electrical and Electronics Engineers) je mezinárodní nezisková organizace založená v roce 1963. Její centrála se nachází v USA ve státě New Jersey. Její hlavní činností je vývoj standardů v oblasti elektrotechniky, informatiky a elektroniky. SA (Standards Association) je odpovídajícím orgánem za vývoj a publikaci standardů. Od roku 2017 bylo založeno několik pracovních skupin, které se věnují standardizaci v oblasti kvantové technologie. V současné době se vyvíjí dva standardy, které se vztahují ke QKD [47, 50]:

- **IEEE P7130**: Poskytuje definici termínů používaných v kvantových technologiích a pomáhá standardizovat terminologii v celém oboru.
- **IEEE P1913**: Definuje model YANG pro softwarově kvantovou komunikaci. Vytváří standardizovaný způsob správy, kontroly a konfigurace zařízení v kvantové komunikaci.

5.4 ISO/IEC

ISO (International Organization for Standardization) a IEC (International Electrotechnical Commission) jsou organizace zabývající se přípravou a publikací standardů a obě sídlí v Ženevě ve Švýcarsku. Tyto dvě instituce spolupracují prostřednictvím společné technické komise ISO/IEC JTC 1 (Joint Technical Committee 1), která je zodpovědná za mezinárodní standardizaci v oblasti informačních technologií. Pod vedením JTC 1 existuje několik subkomisí SC (Sub-Committee), z nichž každá se zaměřuje na specifickou oblast. V rámci pracovní skupiny ISO/IEC JTC 1/SC 27, která se zabývá bezpečností informací, kybernetickou bezpečností a ochranou soukromí, byly ve druhé polovině roku 2023 vydány dva standardy o QKD [51, 52]:

- **ISO/IEC 23837-1**: První část standardu se zabývá bezpečnostními požadavky. které by měly QKD systémy splňovat. Poskytuje komplexní pohled na systém, zahrnující jak fyzické komponenty, tak samotný software a protokoly.

- **ISO/IEC 23837-2**: Druhá část dokumentu popisuje testovací a vyhodnocovací metody. Tyto metody kontrolují, zda byly splněny bezpečnostní požadavky definované v první části dokumentu. Tyto kroky jsou nezbytné pro zajištění bezpečnosti QKD systémů před jejich implementací v reálném prostředí.

6 Bezpečnost práce s lasery

Dodržovat bezpečnostní pravidla a pokyny při práci s lasery je nezbytně důležité pro všechny, kteří s nimi přichází do styku. Manipulace s těmito zařízeními je potenciálně nebezpečná a může vést k vážným zraněním, jako je trvalé poškození zraku nebo popálení kůže. Z toho důvodu je nezbytné, aby osoby pracující s lasery znaly a dodržovaly bezpečnostní předpisy a používaly ochranné vybavení.

6.1 Fyziologický vliv laseru na lidský organismus

Tab. 6.1: Přehled zdravotních rizik spojených s nadměrným vystavením tkání světlu [53].

Spektrální oblast	**Oko**	**Pokožka**
Ultrafialová C (180 nm až 280 nm)	Zánět rohovky	Opálení, zrychlené stárnutí pokožky, zvýšená pigmentace
Ultrafialová B (280 nm až 315 nm)	Zánět rohovky	Opálení, zrychlené stárnutí pokožky, zvýšená pigmentace
Ultrafialová A (315 nm až 400 nm)	Fotochemický šedý zákal	Ztmavnutí pigmentu, fotosenzitivní reakce, spálení pokožky
Viditelná (400 nm až 780 nm)	Fotochemické a tepelné poškození sítnice	Ztmavnutí pigmentu, fotosenzitivní reakce, spálení pokožky
Infračervená A (780 nm až 1400 nm)	Šedý zákal, spálení sítnice	Spálení pokožky
Infračervená B (1,4 µm až 3,0 µm)	Zkalení rohovky, šedý zákal, spálení rohovky	Spálení pokožky
Infračervená C (3,0 µm až 1 mm)	Spálení rohovky	Spálení pokožky

Laserové záření může mít různé fyziologické účinky na lidský organismus v závislosti na intenzitě, vlnové délce nebo době trvání záření. Pro lidské oko je laserový paprsek extrémně nebezpečný, obzvláště ve viditelné (400–700 nm) a blízké infračervené (780–1400 nm) spektrální oblasti, protože oko je přirozeně přizpůsobeno k přijímání světla. Vysoké dávky mohou způsobit poškození struktur oka jako je rohovka

nebo sítnice. Zatímco poškození zraku je běžně známým rizikem, vyšší třídy laseru mohou poškodit i kůži a způsobit vážné popáleniny. Přestože pokožka je více odolnější vůči množství energie z laseru než oko, při nadměrném ozáření laserem ve viditelné (400–700 nm) a infračervené (> 700 nm) spektrální oblasti může dojít k poranění. Nejdříve pokožka zrudne, poté se mohou vytvářet bolestivé puchýře. V tabulce 6.1 se jsou tyto informace shrnuty a popsány účinky různých spektrálních oblastí na tyto dvě oblasti lidského těla [53].

6.2 Třídy bezpečnosti laseru

Třídy bezpečnosti laserů jsou stanoveny technickou normou ČSN EN 60825-1 (367750), která se zabývá bezpečnostními aspekty laserových zařízení. Tato norma specifikuje různé úrovně rizika a příslušná ochranná opatření pro různé třídy laserů od 1 do 4. Třída 1 je obecně bezpečná, zatímco lasery třídy 4 mohou způsobit vážné poškození, a to i z odraženého světla. Každé zařízení musí být viditelně označeno štítkem, do které kategorie patří, aby uživatel věděl o potenciálních rizicích a bezpečnostních opatřeních. [54, 53].

Třída 1 – Lasery třídy 1 jsou považovány za bezpečné za všech podmínek běžného použití. Nepůsobí škodlivě na oči nebo na pokožku, a to ani při dlouhodobé expozici. Jsou bezpečné i při pozorování pomocí optických pomůcek jako jsou lupy či dalekohledy [53].

Třída 1M – Lasery třídy 1M jsou považovány za bezpečné za normálních podmínek používání, ale při použití optických pomůcek mohou být nebezpečné. Tyto lasery vysílají záření v rozsahu vlnových délek od 302,5 nm do 4000 nm [53].

Třída 1C – Jedná se o lasery běžně používané při lékařských či kosmetických procedurách (redukce vrásek, odstranění ochlupení), proto jsou navrženy tak, aby byly bezpečné pro přímý kontakt s kůží nebo jinými částmi těla [53].

Třída 2 – Lasery v této kategorii vysílají záření ve viditelné oblasti od 400 nm do 700 nm. Obvykle jsou považovány za bezpečné pro krátkodobé vystavení očí, pokud doba nepřesáhne 0,25 sekund. Bezpečnost vychází z přirozené lidské reakce na světlo, jako je mrkání nebo odvrácení pohledu, které zabrání poškození oka [54]

Třída 2M – Lasery této třídy jsou podobné laserům třídy 2 – také vyzařují světlo ve viditelném spektru a jsou obecně považovány za bezpečné pro krátkodobé vystavení očí. Nicméně, na rozdíl od laserů třídy 2, jsou lasery třídy 2M nebezpečné při použití optických pomůcek a dochází k výraznému zvýšení rizika poškození očí [54].

Třída 3R – Laserová zařízení v této třídě jsou určena pro viditelné spektrum světla, mají maximální výkon do 5 mW. Jedná se o lasery poměrně bezpečné s nízkým rizikem poškození, ale měly by být nasazeny pouze v prostředích, kde je minimální riziko přímého pohledu do svazku [53].

Třída 3B – Lasery v této kategorii mají maximální výkon mezi 5 mW a 500 mW. Přímý pohled do svazku může způsobit vážné poškození očí a laserové paprsky mohou zapříčinit drobné popáleniny kůže. Při použití těchto laserů je nutné dodržovat bezpečnostní opatření, jako je nošení ochranných brýlí [53].
Třída 4 – Tato třída představuje nejnebezpečnější kategorii laserů. Lasery této kategorie mohou způsobit okamžité poškození zraku a poranění kůže nejen při přímém kontaktu tkáně, ale i při odrazu paprsku. Lasery jsou natolik silné, že existuje riziko vzniku požáru [54].

7 Laboratorní úloha

Cílem bakalářské práce je navrhnout laboratorní úlohu, která je zaměřená na názornou demonstraci významu polarizace u vybraných QKD protokolů. Tento návrh zahrnuje praktické pokusy a měření, které umožní lépe porozumět teoretickým konceptům, které byly zmíněny v předchozích kapitolách, a zároveň si osvojit praktické dovednosti v oblasti kvantové kryptografie. Úloha umožňuje experimentálně prozkoumat a porozumět základním principům polarizace a vlivu různých optických komponent na polarizované světlo.

Úloha začíná teoretickým úvodem, který objasňuje základy kvantové distribuce klíčů, principy polarizace světla a jejich aplikaci v QKD s důrazem na protokol BB84. Dále poskytuje výčet potřebných optických komponent a důležité pokyny k vypracování.

Návrh se skládá z několika experimentů, které na sebe navazují. Nejdříve probíhá pozorování změn intenzity světla při průchodu dvěma polarizátory. Poté se přidáním dalšího polarizátoru pozorují změny intenzity světla při průchodu třemi polarizátory. Třetí část se věnuje praktické simulaci protokolu BB84 a poslední část poukazuje na rozdíly mezi různými typy optických vláken na polarizaci světla.

V úloze se vyskytují kontrolní otázky, které napomáhají hlubšímu porozumění látky. Otázky jsou koncipovány tak, aby vedly k přemýšlení nad daným pozorováním. V případě, že je potřeba zapsat výsledky pozorování, jsou zde připraveny tabulky, do kterých je možné výsledky zapsat. Vypracovaná laboratorní úloha se nachází v příloze B a simulace dílčích úloh v prostředí Virtual Lab od Quantum Flytrap je v příloze C.

7.1 Komponenty a vybavení

Pro realizaci laboratorní úlohy bylo nutné zajistit a shromáždit vhodné komponenty a vybavení. Většinu komponent bylo potřeba objednat od specializovaných firem jako Thorlabs a Eksma Optics, zatímco některé byly již k dispozici v laboratoři. Držáky, úchyty a stojany byly navrhnuty a vytisknuty na 3D tiskárně. Níže je uveden detailní seznam všech komponent.

Nově objednané komponenty

- **Lineární polarizátor LPVISE050-A** – Lineární polarizátor propouští světlo s kmitáním elektrického pole v určitém směru, zatímco světlo polarizované v jiném směru blokuje nebo snižuje jeho intenzitu. Bylo potřeba pořídit tři lineární polarizátory od firmy Thorlabs, které mají průměr 12,7 mm a jsou optimalizovány pro vlnovou délku 400–700 nm. Polarizátory jsou vyrobeny z materiálu

N-BK7, což je speciální typ borosilikátového skla, který se vyznačuje vynikající optickou kvalitou a vysokou propustností světla zejména ve viditelném spektru. Díky těmto vlastnostem se stal oblíbeným materiálem pro různé optické aplikace.

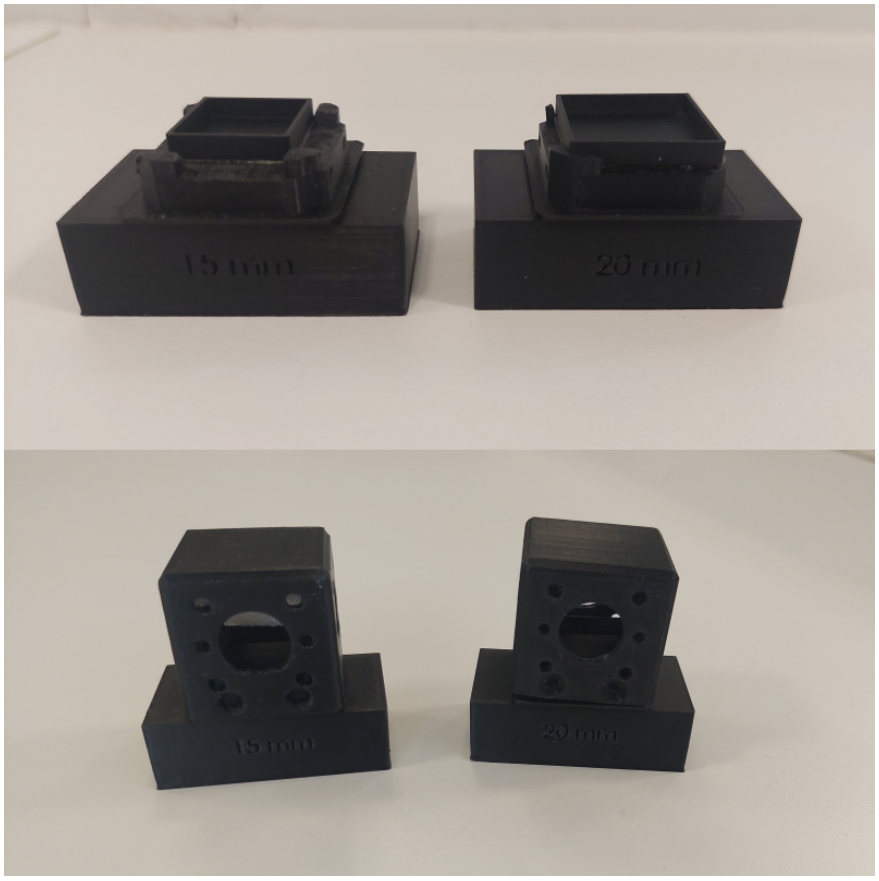
- **Rotační držák pro polarizátor RSP05/M** – Pro umístění lineárních polarizátorů byly pořízeny tři rotační držáky RSP05/M rovněž od firmy Thorlabs. Tyto držáky umožňují přesné nastavení úhlu polarizátoru v krocích po 2°.
- **Polarizační dělič svazku 430-0154** – Pro rozdělení světelného paprsku podle polarizace byly objednány dva polarizační děliče svazku 430-0154 od firmy Eksma Optics. Tyto děliče svazku mají tvar krychle s hranou délky 15 mm, jsou vyrobeny z N-BK7 a jsou navrženy pro vlnovou délku 633 nm.
- **Polarizační rotátor 470-4634** – Polarizační rotátor 470-4634 od firmy Eksma Optics je navržen tak, aby otáčel polarizační rovinu světla o 45° při vlnové délce 633 nm. Je vyroben z monokrystalického křemene a má průměr 25,4 mm.
- **Montážní základna BA1S/M** – Nastavitelné montážní základny od firmy Thorlabs slouží ke stabilnímu a přesnému umístění optických komponent do optického stolu.

Komponenty dostupné v laboratoři

- **Kolimátor PAF-X-5-C** – K dispozici jsou dva kolimátory PAF-X-5-C od firmy Thorlabs, které slouží k zaostření laserového paprsku. Usměrňují rozbíhavé nebo sbíhavé paprsky do paralelního svazku, čímž mění divergující nebo konvergující světlo na rovnoběžné paprsky.
- **Dělič svazku** – Dále byl dostupný dělič svazku od Melles Griot, ke kterému nebylo k dispozici více informací o jeho specifikacích. Proto bylo potřeba otestovat a ověřit, zdali skutečně rozděluje paprsek v poměru 50:50 (viz 7.1.1). Tak jako v případě polarizačního děliče svazku se jedná o krychli, jejíž délka hrany je 20 mm.
- **HeNe Laser 05-LHP-171** – Laser 05-LHP-171 od firmy Melles Griot je HeNe (hélium-neonový) laser, který vyzařuje lineárně polarizovaný paprsek s vlnovou délkou 632,8 nm a výstupním výkonem 15 mW. Napájecí zdroj pro toto zařízení je model 05-LPL-903-070. Laser patří do třídy 3B, což je nebezpečné pro oči při přímém pohledu do paprsku. Je potřeba mít nasazené ochranné brýle.
- **Držáky na sloupky a sloupky**
- **Optická vlákna**
- **Měřič optického výkonu SAT-4EX**
- **Čistící pero na vláknovou optiku**
- **Ochranné brýle**

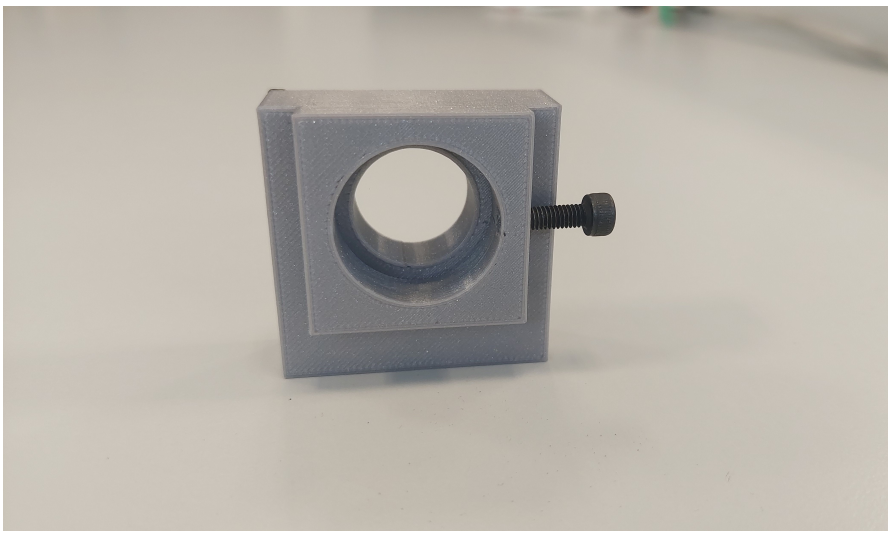
3D tištěné držáky, sloupky

- **Držák děliče svazku** – Byly navrženy dvě varianty uchycení děliče svazku pro různé velikosti, které umožňují bezpečné upevnění a ochranu komponenty. Konstrukce umožňuje uzavření shora, čímž se minimalizuje riziko poškození během manipulace a montáže. Dělič svazku je tak chráněn před mechanickým poškozením.



Obr. 7.1: Držák děliče svazku.

- **Držák na polarizační rotátor** – Polarizační rotátor se vloží do připraveného otvoru, který je vybaven šroubem umožňující pevné upevnění rotátoru na místě. Tím se zajistí jeho stabilita během měření.



Obr. 7.2: Držák polarizačního rotátoru.

- **Držák kolimátoru** – Kolimátor se vloží do otvoru a upevní se pomocí šroubů.

Obr. 7.3: Držák kolimátoru.

- **Držák sloupku, sloupek a montážní základna** – V laboratorním prostředí již byla k dispozici základní sada komponent, jako jsou držáky sloupků, samotné sloupky a montážní základny. Nicméně bylo potřeba navrhnout a vytisknout další, aby bylo k dispozici větší množství těchto dílů.

Obr. 7.4: Držák sloupku, sloupek a montážní základna.

7.1.1 Ověření funkce děliče svazku

Bylo potřeba ověřit, zda dostupný dělič svazku rozděluje vstupní světelný paprsek rovnoměrně v poměru 50:50, tedy jestli rozděluje světlo na dvě části se stejnou intenzitou. K ověření správnosti byl nejprve změřen a zaznamenán výkon laseru před vložením děliče svazku, což poskytlo základní referenční hodnotu pro další porovnávání. Následně se do cesty paprsku vložil dělič svazku a byly zaznamenány hodnoty na obou výstupech. V ideálním případě by mělo dojít k poklesu o 3 dB, což odpovídá snížení výkonu na polovinu.

Tab. 7.1: Měřené hodnoty výkonu před a po použití děliče svazku.

Popis měření	**Výkon [dBm]**	**Rozdíl od vstupu [dB]**
Vstupní paprsek	$-11,75$	-
Výstupní paprsek 1	$-14,66$	$2,91$
Výstupní paprsek 2	$-14,79$	$3,04$

V tabulce 7.1 se nachází veškeré potřebné zaznamenané údaje. Naměřené hodnoty jsou velmi blízké teoretickému očekávání ($-14,75$ dBm), rozdíly mezi dvěma výstupy jsou zanedbatelné a je možné konstatovat, že dělič svazku opravdu rozděluje paprsek rovným dílem v poměru 50:50.

7.2 Bezpečnostní pokyny a instrukce

Při práci s laserem třídy 3B je důležité dodržovat bezpečnostní opatření, aby nedošlo k poranění. Laser používaný v laboratoři, který vysílá lineárně polarizovaný paprsek s vlnovou délkou 632,8 nm a výstupním výkonem 15 mW, je dostatečně silný na to, aby způsobil poškození zraku i při krátkodobé expozici. Při práci s laserem třídy 3B je vždy potřeba pracovat s ochrannými brýlemi. Tyto brýle musí chránit před vlnovou délkou, kterou vysílá dané zařízení, tzn. v tomto případě 632 nm.

Dále je potřeba zajistit, aby se v blízkosti experimentu nenacházely žádné další osoby. Okolo zařízení by neměly být žádné lesklé nebo reflexní povrchy, od kterých by se mohl paprsek odrážet. V případě jejich přítomnosti je potřeba tyto povrchy zakrýt matným materiálem. V žádném případě není dovoleno dívat se přímo do výstupního otvoru laseru nebo laser zaměřovat na jiné osoby. Před každým použitím je potřeba zkontrolovat, že laser a jeho součásti nejsou poškozené a fungují správně.

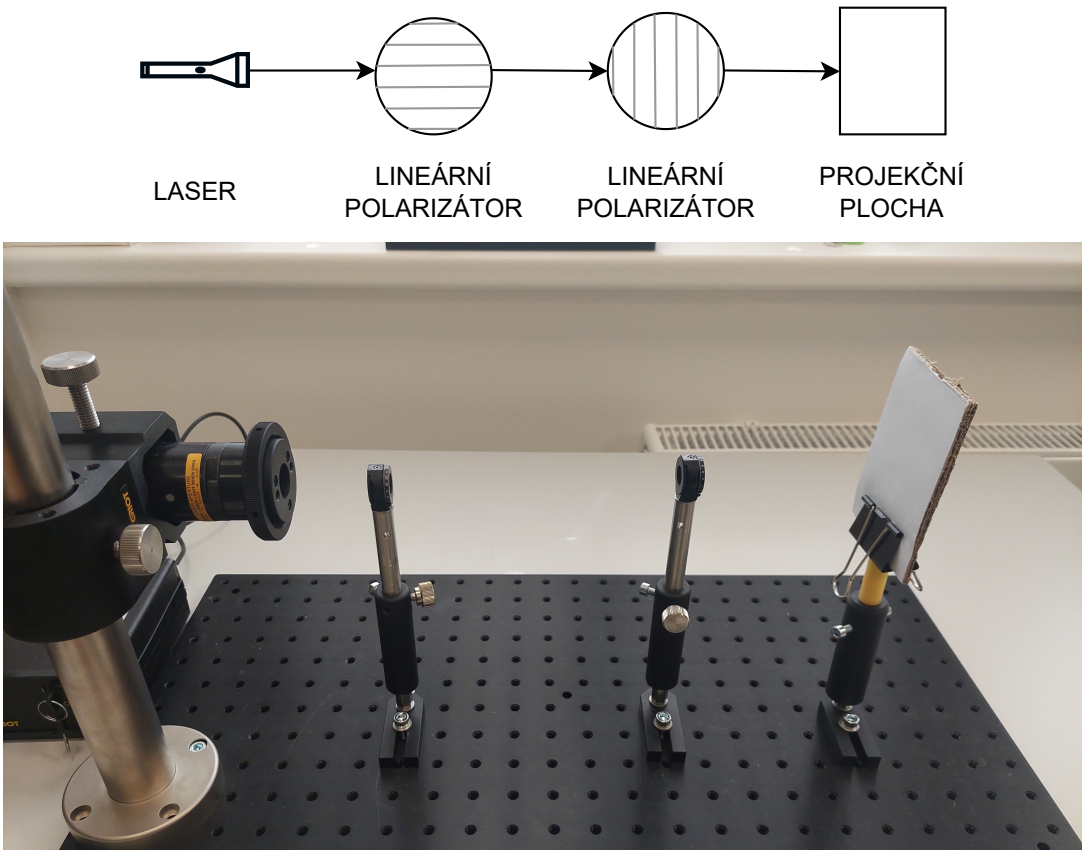
7.3 Realizace pracoviště

Před samotným otestováním a realizací laboratorní úlohy bylo potřeba připravit a správně nastavit potřebné komponenty a vybavení. Laser byl umístěn na optický stůl a upevněn na stabilní rameno. Pomocí nastavitelného šroubu bylo potřeba zajistit, že zdroj světla bude pevně zafixován.

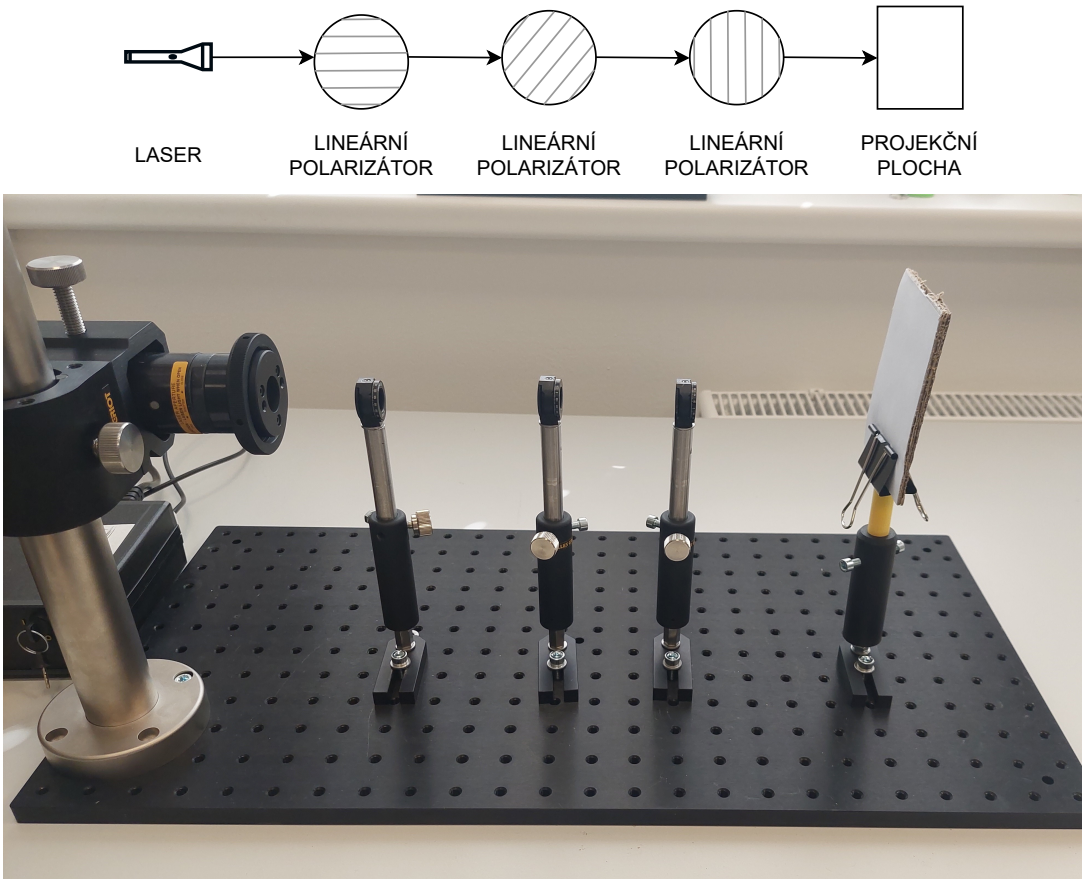
Všechny komponenty byly vyčištěny, aby na povrchu nezůstaly částice prachu nebo otisky prstů, což by mohlo vést k ovlivnění výsledku měření. Po očištění byly umístěny do příslušných držáků, ve kterých budou po celou dobu laboratorní úlohy. Tím se zabrání potenciálnímu poškození neopatrnou manipulací.

Při přípravě pracoviště bylo zásadní nastavit správně orientaci lineárních polarizátorů vzhledem k polarizaci vysílaného paprsku. Polarizátor byl umístěn na optický stůl tak, aby paprsek procházel jeho středem. Následně se pomocí kolimátoru a měřiče optického výkonu měřila intenzita procházejícího světla při různých úhlech. Maximální zaznamenaná intenzita světla indikovala, že polarizační osa polarizátoru je přesně zarovnána s polarizací vysílaného paprsku. Tento úhel byl nastaven jako 0° na stupnici rotačního držáku. Stejný postup byl opakován pro každý polarizátor.

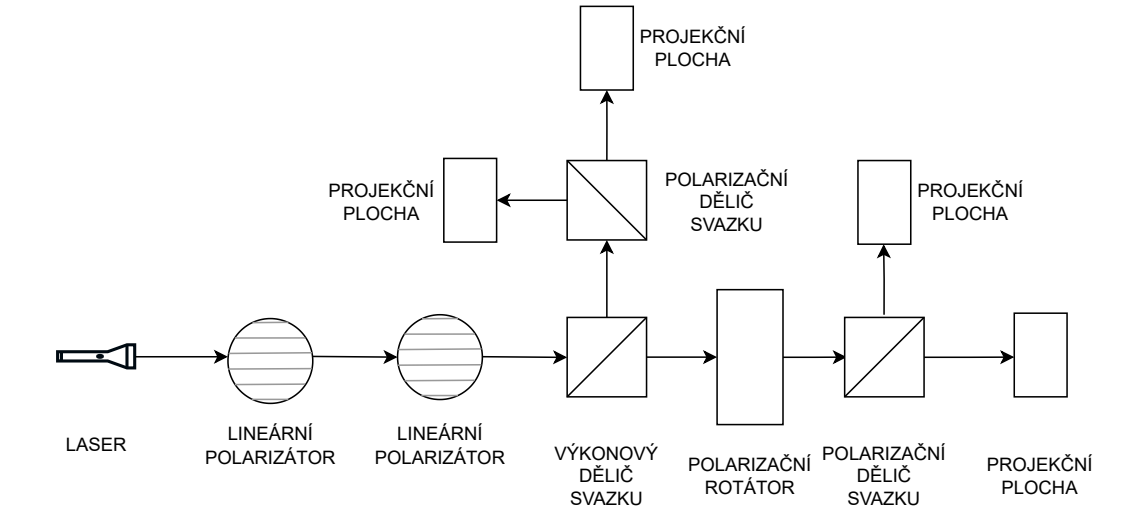
Následně byla celá laboratorní úloha několikrát úspěšně realizována. Pro názornou ukázku byly pořízeny fotografie jednotlivých experimentálních sestav. Aby bylo snadnější porozumět kontextu, nad každou fotografií se nachází schéma aparatury, které je pak doplněno o snímek z praktického provedení v laboratoři.

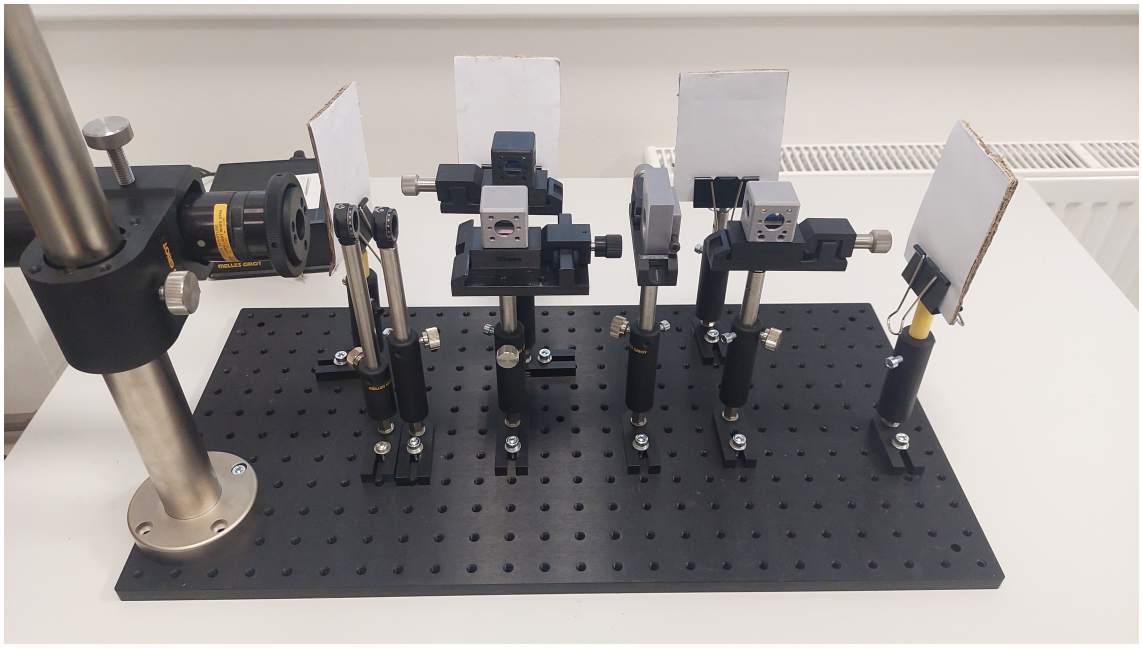


Obr. 7.5: Pozorování změny intenzity světla se dvěma polarizátory.

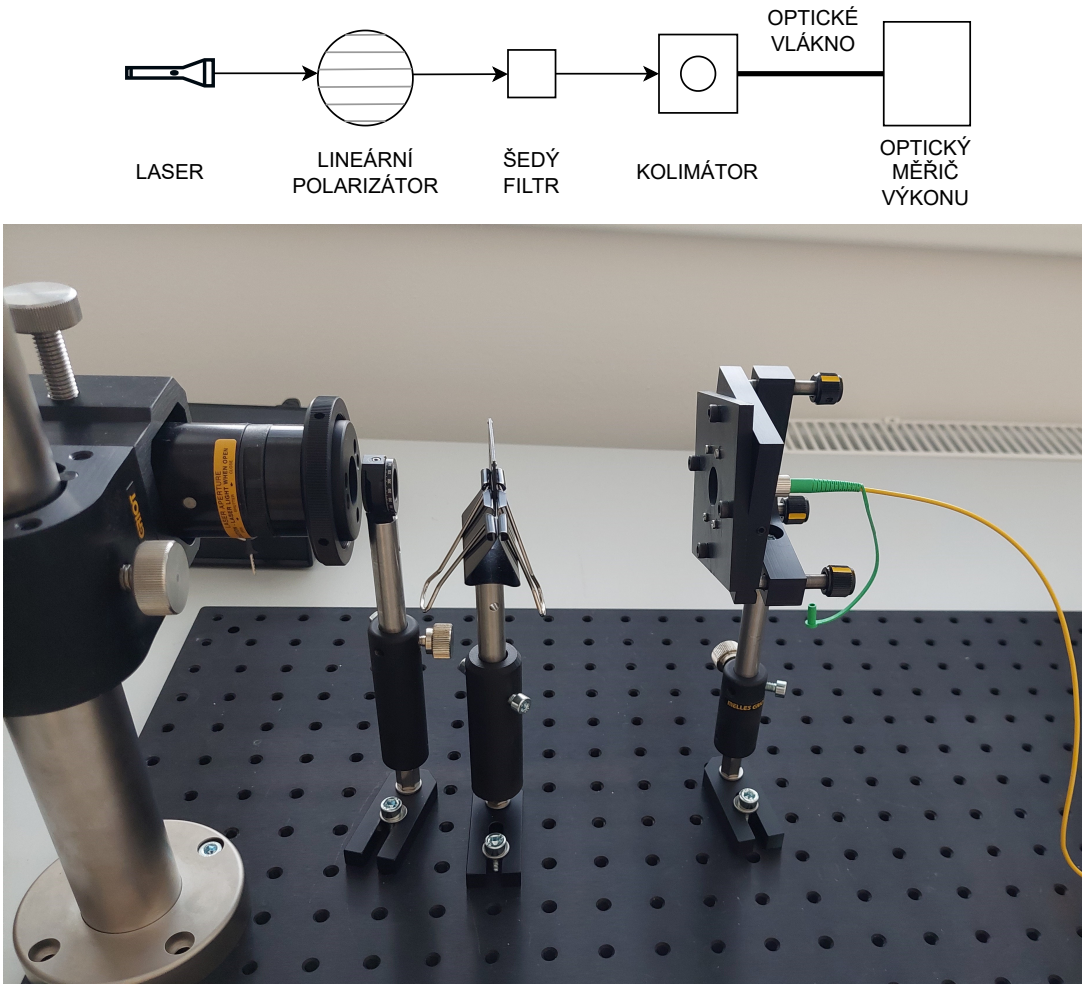


Obr. 7.6: Pozorování změny intenzity světla se třemi polarizátory.





Obr. 7.7: Praktická simulace protokolu BB84.



Obr. 7.8: Vliv různých typů optických vláken na polarizaci světla.

Závěr

V této bakalářské práci byla provedena podrobná analýza využití polarizace světla v kontextu kvantové distribuce klíčů (QKD), přičemž bylo zdůrazněno, že polarizace světla je klíčová pro bezpečný přenos informací v rámci QKD, a to díky využití jedinečných kvantových vlastností fotonů. Významná pozornost byla věnována jednosměrným prepare-and-measure protokolům s diskrétní proměnnou DV-QKD.

V teoretické části byly rozebrány základní principy polarizace, její význam v QKD a přehled různých metod reprezentace, včetně Jonesových vektorů, Stokesových parametrů a Poincarého koule. V rámci této části práce byl také poskytnut základní úvod do kvantové mechaniky a její důležitosti v QKD. Následně byl detailně rozepsán princip kvantové distribuce klíčů s charakterizací jednotlivých protokolů. Závěrečná část obsahuje informace o standardizaci v oblasti QKD a rešerši aktuálně platných či vyvíjených standardů.

Podrobný návrh praktické laboratorní úlohy, který byl součástí bakalářské práce, měl za cíl demonstrovat význam polarizace v QKD protokolech, poskytnout zkušenosti a hlubší pochopení smyslu polarizace v kontextu QKD. Zásadní byl také výběr vhodných komponentů potřebných pro provedení úlohy. Úloha byla navržena, následně otestována a realizována v laboratoři.

Literatura

[1] REICHL, Jaroslav a VŠETIČKA, Martin. Polarizace světla. *Encyklopedie fyziky*. 2017. Dostupné také z: http://fyzika.jreichl.com/main.article/view/462-polarizace-svetla.

[2] KUBERA, Miroslav; NEČAS, Tomáš a BENEŠ, Vojtěch. Polarizace světelných vln. Online. *E-MANUEL: Online učebnice fyziky pro gymnázia*. 2022. Dostupné z: https://e-manuel.cz/kapitoly/vlnova-optika/vyklad/polarizace-svetelnych-vln/. [cit. 2023-12-03].

[3] KOHOUTKOVÁ, Anna. *Princip polarizace světla a jeho využití v optometrii*. Online, Diplomová práce, vedoucí Mgr. Pavel Kříž. Masarykova univerzita, Lékařská fakulta, 2015. Dostupné z: https://is.muni.cz/th/sueyp/Princip_polarizace_svetla_a_jeho_vyuziti_v_optometrii_Anna_Kohoutkova.pdf. [cit. 2023-11-23].

[4] MORÁVKOVÁ, Iva. *Měření polarizace světla ve školní laboratoři*. Online, Bakalářská práce, vedoucí RNDr. Daniel Jezbera. Hradec Králové: Univerzita Hradec Králové, Přírodovědecká fakulta, Katedra fyziky, 2022. Dostupné z: https://theses.cz/id/71sj75/STAG98226.pdf. [cit. 2023-12-08].

[5] HECHT, Eugene. *Optics*. Online. Fifth edition, global edition. Boston: Pearson Education Limited, 2017. ISBN 978-1-292-09693-3. Dostupné z: https://edisciplinas.usp.br/pluginfile.php/5054148/mod_resource/content/1/Hecht-optics-5ed.pdf. [cit. 2023-11-24].

[6] ŠIMÁK, Petr. *Využití polarizačních rovin šíření světla pro vysokorychlostní přenosy optickými vlákny*. Online, Bakalářská práce, vedoucí prof. Ing. Miloslav Filka, CSc. Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav telekomunikací, 2016. Dostupné z: https://www.vut.cz/www_base/zav_prace_soubor_verejne.php?file_id=129397. [cit. 2023-11-25].

[7] COLLETT, Edward. *Field Guide to polarization*. Bellingham, Washington USA: SPIE Vol. FG05, 2005. ISBN 9780819458681.

[8] FIALOVÁ, Lenka. *Určování polarizačního stavu záření pro spektrometr na měření Ramanovy optické aktivity*. Online, Diplomová práce, vedoucí RNDR. Josef Kapitán, PhD. Olomouc: Univerzita Palackého v Olomouci, Přírodovědecká fakulta, Katedra optiky, 2013. Dostupné z: https://theses.cz/id/nofthr/7730488. [cit. 2023-12-08].

[9] How is the polarization ellipse related to the polarization state? Online. 2020. Dostupné z: https://www.thorlabs.com/newgrouppage9.cfm?objectgroup_id=14199. [cit. 2023-12-08].

[10] DESCHAMPS, G. a MAST, P. Poincaré sphere representation of partially polarized fields. Online. *IEEE Transactions on Antennas and Propagation*. 1973, roč. 21, č. 4, s. 474-478. ISSN 0096-1973. Dostupné z: https://doi.org/10.1109/TAP.1973.1140516. [cit. 2023-11-25].

[11] How is a Poincare Sphere useful for representing polarization states? Online. 2020. Dostupné z: https://www.thorlabs.com/newgrouppage9.cfm?objectgroup_id=14200. [cit. 2023-12-03].

[12] KULHÁNEK, Petr. *TF2: Kvantová teorie*. Online. Praha: AGA, 2016. Dostupné z: https://www.aldebaran.cz/studium/kvantovka.pdf. [cit. 2023-11-26].

[13] ZHOU, Tianqi; SHEN, Jian; LI, Xiong; WANG, Chen a SHEN, Jun. Quantum Cryptography for the Future Internet and the Security Analysis. Online. *Security and Communication Networks*. 2018, roč. 2018, s. 1-7. ISSN 1939-0114. Dostupné z: https://doi.org/10.1155/2018/8214619. [cit. 2024-05-22].

[14] TYC, Tomáš. *Základy kvantové mechaniky*. Online. Brno: Masarykova univerzita, Přírodovědecká fakulta, Ústav teoretické fyziky a astrofyziky, 2006. Dostupné z: https://www.physics.muni.cz/~tomtyc/kvantovka.pdf. [cit. 2023-11-26].

[15] KŘELINA, Michal. Kvantový seriál — díl 2. — Kvantové počítače — Qubit. Online. *Qubits.cz*. 2020. Dostupné z: https://qubits.cz/serialy/kvantovy-serial-dil-2-kvantove-pocitace-qubit/. [cit. 2023-11-27].

[16] PIRANDOLA, S.; ANDERSEN, U. L.; BANCHI, L.; BERTA, M.; BUNANDAR, D. et al. Advances in quantum cryptography. Online. *Advances in Optics and Photonics*. 2020, roč. 12, č. 4. ISSN 1943-8206. Dostupné z: https://doi.org/10.1364/AOP.361502. [cit. 2023-11-11].

[17] KUPČA, Vojtěch. *Teorie a perspektiva kvantových počítačů*. Online, Diplomová práce, vedoucí Ing. Tomáš Rosa. Praha: České vysokého učení technické v Praze, Fakulta elektrotechnická, 2001. Dostupné z: https://www.karlin.mff.cuni.cz/~holub/soubory/qc/qc.html. [cit. 2023-11-12].

[18] KOUPILOVÁ, Zdeňka a KÁCOVSKÝ, Petr. *Kapitola 2: Základní postuláty kvantové mechaniky*. Online. Kvantová fyzika (nejen) pro budoucí učitele.

Praha: Katedra didaktiky fyziky Matematicko-fyzikální fakulty Univerzity Karlovy, 2020. Dostupné z: https://kdf.mff.cuni.cz/vyuka/kvantovka/QM02-KoupilovaKacovsky.pdf. [cit. 2023-11-28].

[19] VISWANATH, Pranav. Quantum States And The Bloch Sphere. Online. *Medium*. 2021. Dostupné z: https://medium.com/quantum-untangled/quantum-states-and-the-bloch-sphere-9f3c0c445ea3. [cit. 2023-11-28].

[20] NEMA, Prashant a NENE, Manisha J. Pauli Matrix based Quantum Communication Protocol. Online. In: *2020 IEEE International Conference on Advent Trends in Multidisciplinary Research and Innovation (ICATMRI)*. IEEE, 2020, s. 1-6. ISBN 978-1-7281-7734-2. Dostupné z: https://doi.org/10.1109/ICATMRI51801.2020.9398393. [cit. 2023-11-28].

[21] KYRILLIDIS, Anastasios. Introduction to quantum computing: Bloch sphere. Online. *Tasos' posts*. Dostupné z: https://akyrillidis.github.io/notes/quant_post_7. [cit. 2023-11-28].

[22] NEWMAN, Marcus R.A. Bloch sphere. Online. Dostupné z: https://prefetch.eu/know/concept/bloch-sphere/. [cit. 2023-12-03].

[23] 05. Polarization (Jones vectors and matrices, partial polarization, Stokes parameters). Online. *YouTube*. 2018. Dostupné z: https://www.youtube.com/watch?v=RowMxWt4mVE&t=370. [cit. 2023-12-08].

[24] GAMEL, Omar a JAMES, Daniel F. V. Measures of quantum state purity and classical degree of polarization. Online. *Physical Review A*. 2012, roč. 86, č. 3. ISSN 1050-2947. Dostupné z: https://doi.org/10.1103/PhysRevA.86.033830. [cit. 2023-12-08].

[25] DIAMANTI, Eleni; LO, Hoi-Kwong; QI, Bing a YUAN, Zhiliang. Practical challenges in quantum key distribution. Online. *Npj Quantum Information*. 2016, roč. 2, č. 1. ISSN 2056-6387. Dostupné z: https://doi.org/10.1038/npjqi.2016.25. [cit. 2023-10-31].

[26] PAJTINOVÁ, Mária. *Metody kvantové kryptografie*. Online, Bakalářská práce, vedoucí doc. Ing. Václav Zeman, Ph.D. Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav telekomunikací, 2009. Dostupné z: https://www.vut.cz/www_base/zav_prace_soubor_verejne.php?file_id=18607. [cit. 2023-11-01].

[27] ALLÉAUME, R.; BRANCIARD, C.; BOUDA, J.; DEBUISSCHERT, T.; DIANATI, M. et al. Using quantum key distribution for cryptographic purposes:

A survey. Online. *Theoretical Computer Science*. 2014, roč. 560, s. 62-81. ISSN 03043975. Dostupné z: https://doi.org/10.1016/j.tcs.2014.09.018. [cit. 2023-11-03].

[28] NURHADI, Ali Ibnun a SYAMBAS, Nana Rachmana. Quantum Key Distribution (QKD) Protocols: A Survey. Online. In: *2018 4th International Conference on Wireless and Telematics (ICWT)*. IEEE, 2018, s. 1-5. ISBN 978-1-5386-6161-1. Dostupné z: https://doi.org/10.1109/ICWT.2018.8527822. [cit. 2023-11-03].

[29] MUKHERJEE, Arka. Quantum Key Distribution: The Future Of Secure Communication. Online. In: *Electronics For You*. 2022. Dostupné z: https://www.electronicsforu.com/technology-trends/quantum-key-distribution-future-secure-communication. [cit. 2023-11-03].

[30] ARCHANA, B. a KRITHIKA, S. Implementation of BB84 quantum key distribution using OptSim. Online. In: *2015 2nd International Conference on Electronics and Communication Systems (ICECS)*. IEEE, 2015, s. 457-460. ISBN 978-1-4799-7225-8. Dostupné z: https://doi.org/10.1109/ECS.2015.7124946. [cit. 2023-11-15].

[31] KE CUI; JIAN WANG; HONG-FEI ZHANG; CHUN-LI LUO; GE JIN et al. A Real-Time Design Based on FPGA for Expeditious Error Reconciliation in QKD System. Online. *IEEE Transactions on Information Forensics and Security*. 2013, roč. 8, č. 1, s. 184-190. ISSN 1556-6013. Dostupné z: https://doi.org/10.1109/TIFS.2012.2228855. [cit. 2023-11-15].

[32] BISWAS, Chitra; HAQUE, Md. Mokammel a DAS GUPTA, Udayan. A Modified Key Sifting Scheme With Artificial Neural Network Based Key Reconciliation Analysis in Quantum Cryptography. Online. *IEEE Access*. 2022, roč. 10, s. 72743-72757. ISSN 2169-3536. Dostupné z: https://doi.org/10.1109/ACCESS.2022.3188798. [cit. 2023-11-15].

[33] STRNKA, Libor. *Kvantová kryptologie*. Online, Bakalářská práce, vedoucí Ing. Roman Šenkeřík, PhD. Zlín: Univerzita Tomáše Bati ve Zlíně, Fakulta aplikované informatiky, 2010. Dostupné z: https://digilib.k.utb.cz/bitstream/handle/10563/12638/strnka_2010_bp.pdf?sequence=1&isAllowed=y. [cit. 2023-11-13].

[34] ITU-T D2.3. Quantum key distribution network protocols: Quantum layer. Online. 2021. Dostupné z: https://www.itu.int/en/ITU-T/focusgroups/qit4n/Documents/D2.3%20part%201.pdf. [cit. 2023-11-11].

[35] *Kvantová hrozba a kvantově odolná kryptografie*. Online. Brno: NÚKIB, 2023. Dostupné z: https://www.nukib.cz/download/uredni_deska/Priloha%20-%20Minimalni%20pozadavky%20na%20kryptograficke%20algoritmy.pdf. [cit. 2023-11-06].

[36] ANSSI views on the Post-Quantum Cryptography transition. Online. 2022. Dostupné z: https://www.ssi.gouv.fr/uploads/2022/01/anssi-technical_position_papers-post_quantum_cryptography_transition.pdf. [cit. 2023-11-06].

[37] LOVIC, Victor. Quantum Key Distribution: Advantages, Challenges and Policy. Online. *Cambridge Journal of Science and Policy*. 2020. Dostupné z: https://doi.org/10.17863/CAM.58622. [cit. 2023-11-07].

[38] KŘELINA, Michal. Kvantově odolné šifrování: Otázky a odpovědi pro vás!. Online. *Qubits.cz*. 2020. Dostupné z: https://qubits.cz/clanky/kvantove-odolne-sifrovani-otazky-a-odpovedi-pro-vas/. [cit. 2023-11-04].

[39] PUŽMANOVÁ, Rita. *Kvantová kryptografie pro bezpečnou distribuci klíčů*. Online. 2004. Dostupné z: https://www.lupa.cz/clanky/kvantova-kryptografie-pro-bezpecnou-distribuci-klicu/. [cit. 2023-11-01].

[40] HÁLA, Vojtěch. Kvantová kryptografie. Online. *Aldebaran bulletin*. 2005, roč. 3, č. 14. ISSN 1214-1674. Dostupné z: https://www.aldebaran.cz/bulletin/2005_14_kry.php. [cit. 2023-11-12].

[41] BENNETT, Charles H. a BRASSARD, Gilles. Quantum cryptography: Public key distribution and coin tossing. Online. *Theoretical Computer Science*. 2014, roč. 560, s. 7-11. ISSN 03043975. Dostupné z: https://doi.org/10.1016/j.tcs.2014.05.025. [cit. 2023-11-12].

[42] KLÍČNÍK, Ondřej. *Kvantová distribuce klíčů přes optickou vláknovou infrastrukturu*. Online, Bakalářská práce, vedoucí doc. Ing. Petr Münster, Ph.D. Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav telekomunikací, 2021. Dostupné z: https://www.vut.cz/www_base/zav_prace_soubor_verejne.php?file_id=227549. [cit. 2024-05-07].

[43] *QuEST: Activities - B92 Protocol*. Online. Quantum communication. Roman Research Institue, 2019. Dostupné z: https://www.rri.res.in/quic/qkdactivities.php. [cit. 2023-11-22].

[44] LUCAMARINI, M.; PATEL, K. A.; DYNES, J. F.; FRÖHLICH, B.; SHARPE, A. W. et al. Efficient decoy-state quantum key distribution with quantified security. Online. *Optics Express*. 2013, roč. 21, č. 21. ISSN 1094-4087. Dostupné z: https://doi.org/10.1364/OE.21.024550. [cit. 2023-11-29].

[45] LO, Hoi-Kwong; MA, Xiongfeng a CHEN, Kai. Decoy State Quantum Key Distribution. Online. *Physical Review Letters*. 2005, roč. 94, č. 23. ISSN 0031-9007. Dostupné z: https://doi.org/10.1103/PhysRevLett.94.230504. [cit. 2023-11-30].

[46] STANLEY, M; GUI, Y; UNNIKRISHNAN, D; HALL, S.R.G a FATADIN, I. Recent Progress in Quantum Key Distribution Network Deployments and Standards. Online. *Journal of Physics: Conference Series*. 2022, roč. 2416, č. 1. ISSN 1742-6588. Dostupné z: https://doi.org/10.1088/1742-6596/2416/1/012001. [cit. 2024-05-01].

[47] GRAMEGNA, Marco; TRAINA, Paolo; BERNARDI, ETTORE a MOREVA, EKATERINA. *Standardization Roadmap on Quantum Technologies written by the CEN-CENELEC Focus Group on Quantum Technologies (FGQT)*. Online. FGQT, 2023. Dostupné z: https://www.cencenelec.eu/media/CEN-CENELEC/AreasOfWork/CEN-CENELEC_Topics/Quantum%20technologies/Documentation%20and%20Materials/fgqt_q04_standardizationroadmapquantumtechnologies_release1.pdf. [cit. 2024-05-03].

[48] *ETSI: European Telecommunications Standards Institute*. Online. Sofia Antipolis: ETSI, 2024. Dostupné z: https://www.etsi.org/. [cit. 2024-05-03].

[49] *ITU-T: International Telecommunication Union Telecommunication Standardization Sector*. Online. Ženeva: ITU-T, 2024. Dostupné z: https://www.itu.int. [cit. 2024-05-04].

[50] *IEEE: Institute of Electrical and Electronics Engineers*. Online. New Jersey: IEEE, 2024. Dostupné z: https://www.ieee.org/. [cit. 2024-05-03].

[51] *ISO: International Organization for Standardization*. Online. Ženeva: ISO, 2024. Dostupné z: https://www.iso.org/home.html. [cit. 2024-05-03].

[52] *IEC: International Electrotechnical Commission*. Online. Ženeva: IEC, 2024. Dostupné z: https://www.iec.ch/homepage. [cit. 2024-05-03].

[53] ČSN EN 60825-1 ED. 3. (367750), *Bezpečnost laserových zařízení - Část 1: Klasifikace zařízení a požadavky*. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2015. [cit. 2024-05-05].

[54] RIND, Pavel. *Vliv laserového útoku na práci pilota*. Online, Diplomová práce, vedoucí Ing. Jiří Chlebek, Ph.D. Brno: Vysoké učení technické v Brně, Fakulta strojního inženýrství, Letecký ústav, 2011. Dostupné z: `https://www.vut.cz/www_base/zav_prace_soubor_verejne.php?file_id=40608`. [cit. 2024-05-05].

Seznam symbolů a zkratek

B92	Bennett - protokol vytvořený v 1992
BB84	Bennett, Brassard - protokol vytvořený v 1984
CV-QKD	Continuous-Variable Quantum Key Distribution
dB	Decibel
dBm	Decibel-miliwatt
DOP	Degree of polarization
DV-QKD	Discrete-Variable Quantum Key Distribution
EB	Entanglement-Based
ETSI	European Telecommunications Standards Institute
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
ISO	International Organization for Standardization
ITU	International Telecommunication Union
ITU-T	International Telecommunication Union Telecommunication Standardization Sector
LHP	Lineární horizontální polarizace
LVP	Lineární vertikální polarizace
PM	Prepare and Measure
PNS	Photon Number Splitting
PQC	Post-Quantum Cryptography
QBER	Quantum Bit Error Rate
QKD	Quantum Key Distribution
QKDN	Quantum Key Distribution Network
QSC	Quantum-Safe Cryptography

SARG04 Scarani, Acin, Ribordy, Gisin - protokol vytvořený v roce 2004

SDN Software Defined Networks

SSP Six State Protocol

T12 Toshiba 2012, protokol

Matematické veličiny

$\sigma_x, \sigma_y, \sigma_z$	Pauliho matice
$\vec{B}$	vektor magnetického pole
$\vec{E}$	vektor elektrického pole
$\vec{J}$	Jonesův vektor
$\boldsymbol{J}$	Jonesova matice
$\boldsymbol{M}$	Muellerova matice
S_0, S_1, S_2, S_3	Stokesovy parametry
$\|\psi\rangle$	Kvantový stav zapsaný pomocí „ket“ vektoru
$\oplus$	Vertikálně-horizontální báze
$\otimes$	Diagonální báze

Seznam příloh

A Aktuálně platné standardy

V této příloze je obsažen seznam aktuálně platných standardů od organizací ETSI, ITU-T, IEEE a ISO/IEC, a také dokumenty, které jsou v současné době ve vývoji.

A.1 ETSI

Tab. A.1: Seznam aktuálně platných standardů ETSI [48].

Dokument	**Verze**	**Datum publikace**	**Obsah**
ETSI GS QKD 016	V2.1.1	2024-01	Profil ochrany pro systémy QKD.
ETSI GS QKD 018	V1.1.1	2022-04	Rozhraní orchestrace pro softwarově definované sítě (SDN).
ETSI GS QKD 015	V2.1.1	2022-04	Řídící rozhraní SDN.
ETSI GS QKD 004	V2.1.1	2020-08	Aplikační rozhraní.
ETSI GS QKD 012	V1.1.1	2019-02	Specifikace parametrů zařízení a komunikačních kanálů.
ETSI GS QKD 014	V1.1.1	2019-02	Protokoly a formáty dat rozhraní REST API pro doručení klíčů.
ETSI GR QKD 007	V1.1.1	2018-12	Slovník shromažďující definice a zkratky používané ve spojitosti s QKD.
ETSI GR QKD 003	V2.1.1	2018-03	Definování vlastností komponent a interních rozhraní.
ETSI GS QKD 011	V1.1.1	2016-05	Charakterizace optických komponent.
ETSI GS QKD 008	V1.1.1	2010-12	Bezpečnostní požadavky pro moduly QKD.
ETSI GS QKD 005	V1.1.1	2010-12	Bezpečnostní důkazy.
ETSI GS QKD 002	V1.1.1	2010-06	Případy použití QKD.

Tab. A.2: Seznam standardů ETSI ve vývoji [48].

Dokument	**Obsah**
ETSI GS QKD 010	Zaměřuje se na zabezpečení implementace QKD v jednosměrných systémech proti útokům trojským koněm.
ETSI GS QKD 013	Charakteristika optického výstupu vysílacích modulů QKD.
ETSI GR QKD 017	Analýza síťových architektur.
ETSI GR QKD 019	Návrh rozhraní QKD s autentizací.
ETSI GS QKD 020	Protokoly a formáty dat rozhraní REST API pro interoperabilní systém správy klíčů.
ETSI GS QKD 021	Rozhraní orchestrace SDN pro interoperabilní systém správy klíčů.
ETSI GS QKD 022	Architektura sítě.
ETSI GS QKD 023	Rozhraní pro monitorování a datový model.

A.2 ITU-T

Tab. A.3: Seznam aktuálně platných standardů ITU-T série Q [49].

Dokument	**Datum schválení**	**Obsah**
ITU-T Q.4160	2023-12	QKDN – Framework protokolu.
ITU-T Q.4161	2023-12	Protokoly pro rozhraní Ak pro QKDN.
ITU-T Q.4162	2023-12	Protokoly pro rozhraní Kq-1 pro QKDN.
ITU-T Q.4163	2023-12	Protokoly pro rozhraní Kx pro QKDN.
ITU-T Q.4164	2023-12	Protokoly pro rozhraní Ck pro QKDN.

Tab. A.4: Seznam standardů ITU-T série Q ve vývoji [49].

Dokument	**Obsah**
ITU-T Q.QKDN_Mk	Protokoly pro rozhraní správce QKDN.
ITU-T Q.QKDNi_KM	Protokoly pro rozhraní mezi správci klíčů pro propojení QKDN.
ITU-T Q.QKDNi_profr	Propojení QKDN - Framework protokolu.

Tab. A.5: Seznam aktuálně platných standardů ITU-T série X [49].

Dokument	**Datum schválení**	**Obsah**
ITU-T X.1702	2019-11	Architektura generátoru náhodných čísel s kvantovým šumem.
ITU-T X.1710	2020-10	Bezpečnostní framework pro QKDN.
ITU-T X.1712	2021-10	Bezpečnostní požadavky a opatření pro QKDN – Správa klíčů.
ITU-T X.1713	2024-04	Bezpečnostní požadavky na ochranu QKD uzlů.
ITU-T X.1714	2020-10	Kombinace klíčů a poskytování důvěrných klíčů pro QKDN.
ITU-T X.1715	2022-07	Bezpečnostní požadavky a opatření pro integraci QKDN a sítě pro bezpečné ukládání dat.
ITU-T X.1811	2021-04	Bezpečnostní pokyny pro použití kvantově bezpečných algoritmů v systémech IMT-2020.

Tab. A.6: Seznam standardů ITU-T série X ve vývoji [49].

Dokument	**Obsah**
ITU-T X.sec_QKD_profr	Framework protokolů pro kvantovou distribuci klíčů v QKDN.
ITU-T X.sec_QKDN_AA	Autentizace a autorizace v QKDN.
ITU-T X.sec_QKDN_CM	Bezpečnostní požadavky a opatření QKDN – kontrola a správa.
ITU-T X.sec_QKDNi	Bezpečnostní požadavky na propojení QKDN (QKDNi).

Tab. A.7: Seznam aktuálně platných standardů ITU-T série Y [49].

Dokument	**Datum schválení**	**Obsah**
ITU-T Y.3800	2019-10	Přehled sítí podporujících QKD.
ITU-T Y.3801	2020-04	Funkční požadavky na sítě pro QKD.
ITU-T Y.3802	2020-12	QKDN – Funkční architektura.
ITU-T Y.3803	2020-12	QKDN – Správa klíčů.
ITU-T Y.3804	2020-09	QKDN – Kontrola a správa.
ITU-T Y.3805	2021-12	QKDN – Kontrola SDN.
ITU-T Y.3806	2021-09	QKDN – Požadavky na zajištění kvality služeb.
ITU-T Y.3807	2022-02	QKDN – Parametry kvality služeb.
ITU-T Y.3808	2022-02	Framework pro integraci QKDN a sítě pro bezpečné ukládání dat.
ITU-T Y.3809	2022-02	Model založený na rolích při nasazení QKDN.
ITU-T Y.3810	2022-09	QKDN – Framework.
ITU-T Y.3811	2022-09	QKDN – Funkční architektura pro zajištění kvality služby.
ITU-T Y.3812	2022-09	QKDN – Požadavky na zajištění kvality služeb založené na strojovém učení.
ITU-T Y.3813	2023-01	QKDN – Funkční požadavky.
ITU-T Y.3814	2023-01	QKDN – Funkční požadavky a architektura pro podporu strojového učení.
ITU-T Y.3815	2023-09	QKDN – Přehled odolnosti.
ITU-T Y.3816	2023-09	QKDN – Vylepšení funkční architektury pro zajištění kvality služeb na základě strojového učení.
ITU-T Y.3817	2023-09	Propojení QKDN – Požadavky na zajištění kvality služby.
ITU-T Y.3818	2023-09	Propojení QKDN – Architektura.
ITU-T Y.3819	2023-12	QKDN – Požadavky a model pro autonomní správu a kontrolu.
ITU-T Y.3820	2024-04	Propojení QKDN – Řízení SDN.
ITU-T Y.3821	2024-04	QKDN – Požadavky na odolnost.

Tab. A.8: Doplňující dokumenty série ITU-T Y.3800 [49].

Dokument	**Datum schválení**	**Obsah**
ITU-T Y.Sup70	2021-07	QKDN – Využití strojového učení.
ITU-T Y.Sup75	2023-03	QKDN – Budoucí sítě s podporou kvantových technologií.
ITU-T Y.Sup79	2023-11	QKDN – Role v end-to-end kryptografických službách s nekvantovou kryptografií.
ITU-T Y.Sup80	2023-11	Případové studie QKDN.

Tab. A.9: Seznam standardů ITU-T série Y ve vývoji [49].

Dokument	**Obsah**
ITU-T Y.QKDN-da	QKDN – Hodnocení spolehlivosti.
ITU-T Y.QKDNi-qos-fa	Propojení QKDN – Funkční architektura pro zajištění kvality služeb.
ITU-T Y.QKDN-nq-qos-rf	Požadavky a framework zajištění kvality služeb pro integrované služby QKDN a nekvantové uživatelské sítě.
ITU-T Y.QKDN-qos-auto-fa	QKDN – Vylepšení funkční architektury pro autonomní zajištění kvality služeb.
ITU-T Y.QKDN-qos-auto-rq	QKDN – Požadavky na autonomní zajištění kvality služeb.
ITU-T Y.QKDN-qos-mmq	QKDN – Metodika měření parametrů QoS.
ITU-T Y.QKD-IPSec-fr	Framework pro integraci QKD a IPSec.
ITU-T Y.QKDNf-fr	Framework federace QKDN.
ITU-T Y.QKDN-nq-rf	Požadavky a framework pro integrované služby QKDN a nekvantové uživatelské sítě.
ITU-T Y.QKDN-orfr	Framework pro orchestraci sítě pro distribuci kvantových klíčů.
ITU-T Y.QKDN-rsff	QKDN – Funkční framework odolnosti.
ITU-T Y.QKDN-safr	QKDN – Framework pro povědomí o službách
ITU-T Y.QKDN-TSNfr	Framework pro integraci QKDN a časově citlivé sítě.

A.3 IEEE

Tab. A.10: Seznam standardů IEEE ve vývoji [50].

Dokument	**Obsah**
IEEE P7130	Definice a terminologie používaná v kvantových technologiích.
IEEE P1913	Softwarově definovaná kvantová komunikace.

A.4 ISO/IEC

Tab. A.11: Seznam aktuálně platných standardů ISO/IEC [51, 52].

Dokument	**Datum publikace**	**Obsah**
ISO/IEC 23837-1	2023-08	Bezpečnostní požadavky, metody testování a vyhodnocení pro distribuci kvantových klíčů – Část 1: Požadavky
ISO/IEC 23837-2	2023-09	Bezpečnostní požadavky, metody testování a hodnocení pro distribuci kvantových klíčů – Část 2: Metody hodnocení a testování

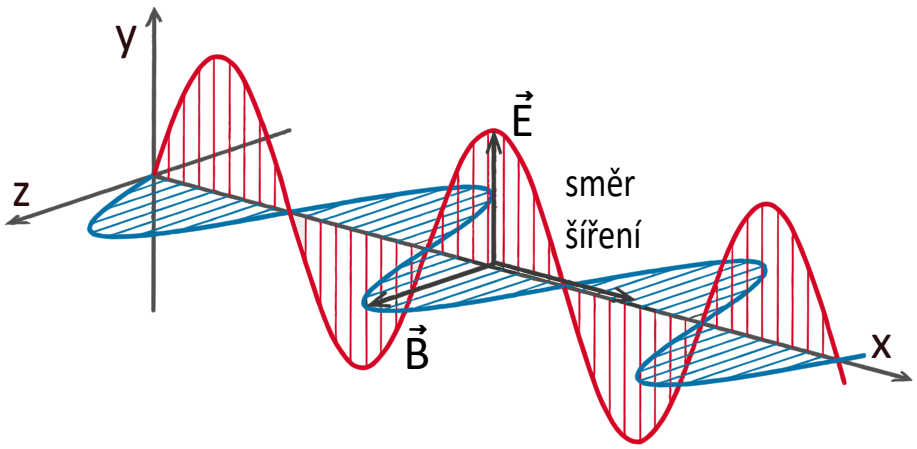
B Laboratorní úloha

B.1 Cíl úlohy

Cílem této laboratorní úlohy je poskytnout praktické porozumění klíčovým principům polarizace světla a jejich aplikaci v kvantové distribuci klíčů (QKD). Úloha je zásadní pro pochopení, jak polarizace světla může být využita pro bezpečný přenos informací v oblasti současné kryptografické praxe.

B.2 Teoretický úvod

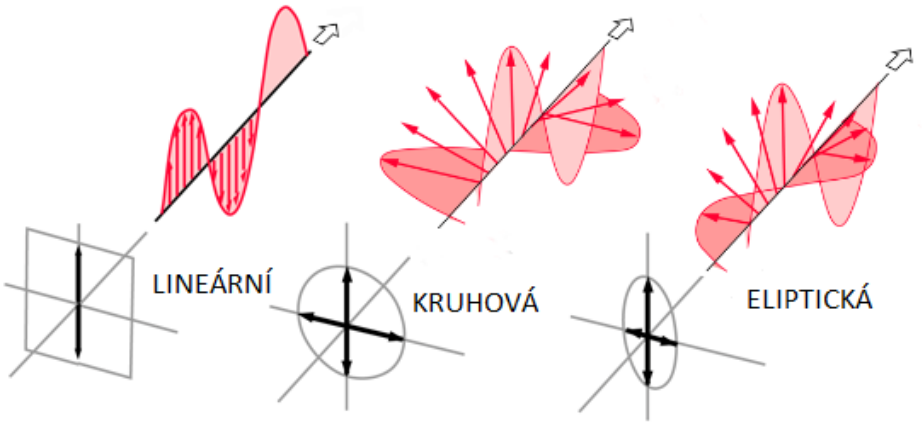
Základy polarizace světla
Polarizace je fyzikální vlastnost elektromagnetického vlnění, jako je světlo, při které se oscilace elektromagnetického vlnění omezuje nebo orientuje do určitého směru. Elektromagnetická vlna se skládá ze dvou vektorů: vektoru elektrického pole $\vec{E}$ a vektoru magnetického pole $\vec{B}$. Vektory $\vec{E}$ i $\vec{B}$ jsou navzájem kolmé a zároveň leží v rovině, která je kolmá ke směru šíření vlnění.



Obr. B.1: Elektromagnetická vlna a její složky.

Podle orientace oscilace elektrického pole $\vec{E}$ se rozlišují tři základní typy polarizace:

- **Lineární polarizace** – Vektor $\vec{E}$ kmitá stále v jednom směru. Lineární polarizace může být horizontální, vertikální nebo nakloněná pod určitým úhlem vzhledem k ose.
- **Kruhová polarizace** – Vektor $\vec{E}$ opisuje kruh.
- **Eliptická polarizace** – Vektor $\vec{E}$ opisuje elipsu. Eliptická polarizace je kombinací lineární a kruhové polarizace.



Obr. B.2: Druhy polarizace.

Pokud vektor elektrického pole $\vec{E}$ náhodně osciluje ve všech směrech bez preferované orientace, jedná se o nepolarizované světlo (typické pro běžné světlo jako je sluneční záření nebo žárovka).

Kvantová distribuce klíčů

Kvantová distribuce klíčů (QKD) je metoda bezpečné komunikace umožňující dvěma stranám (obvykle nazývaným jako Alice a Bob) sdílet společný tajný klíč, který je možné použít pro šifrování či dešifrování zpráv. QKD je považována za vysoce bezpečnou z toho důvodu, že je založena na fyzikálních zákonech, konkrétně na principech kvantové mechaniky. To zaručuje, že jakákoli informace přenášená pomocí fotonů (částice světla) se při pokusu o odposlech třetí stranou nevratně změní. Komunikující strany tak mohou zjistit, že došlo k narušení.

V rámci kvantové distribuce klíčů je polarizace důležitým nástrojem. Polarizace fotonů se používá k zakódování a přenosu informací. Konkrétním příkladem je protokol BB84, který používá polarizaci fotonů k vytvoření bezpečného kvantového komunikačního kanálu.

Protokol BB84

Protokol BB84 je jeden z prvních a nejznámějších protokolů QKD. Základním principem tohoto protokolu je použití čtyř specifických stavů polarizace, které umožňují zakódování binárních informací do fotonů:

- **Horizontální polarizace** – Foton je polarizován pod úhlem 0°. Tento stav může reprezentovat bit 0.
- **Vertikální polarizace** – Foton je polarizován pod úhlem 90°. Tento stav může reprezentovat bit 1.

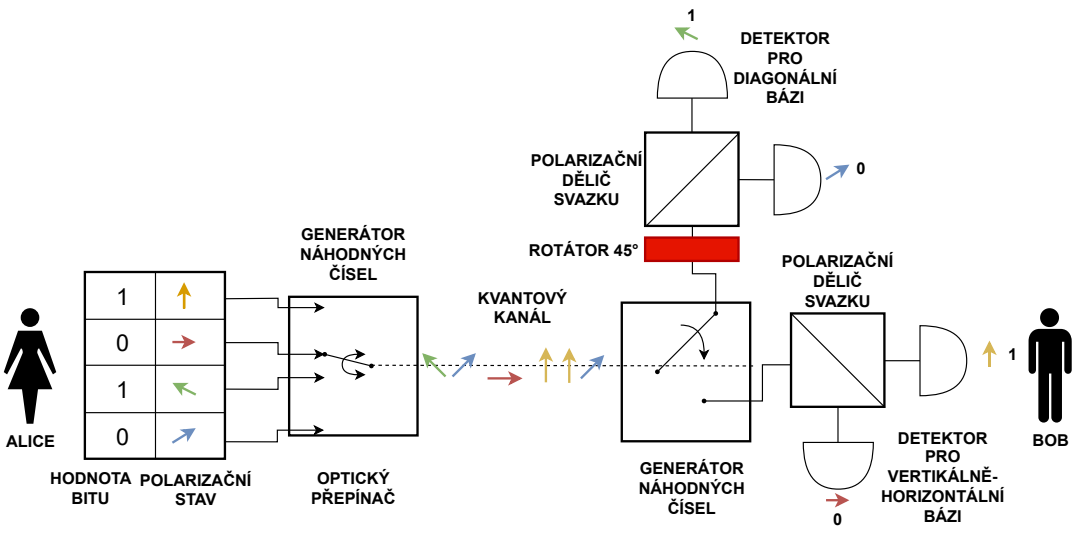
- **Diagonální polarizace** – Foton je polarizován pod úhlem 45°. Tento stav může reprezentovat bit 0.
- **Antidiagonální polarizace** – Foton je polarizován pod úhlem 135°. Tento stav může reprezentovat bit 1.

Pro měření stavů polarizace se používají dvě základní báze:

- **Vertikálně-horizontální báze** – Měření v této bázi umožňuje detekovat stavy fotonů polarizovaných horizontálně nebo vertikálně.
- **Diagonální báze** – Měření v této bázi umožňuje detekovat stavy fotonů polarizovaných diagonálně nebo antidiagonálně.

Výměna klíče probíhá následovně:

- **Příprava a odeslání fotonů Alicí** – Alice náhodně vygeneruje sekvenci bitů a náhodně volí báze, ve kterých tak zakóduje každý bit do stavu jednoho fotonu. Poté odesílá tuto sérií fotonů Bobovi.
- **Příjem a měření fotonů Bobem** – Bob fotony přijímá na své straně a provádí měření v náhodně vybraných bázích.
- **Sdělení výsledků** – Bob sdělí Alici své výsledky, a to konkrétně kterou bázi použil pro každý foton. Alice a Bob porovnají své báze, a ponechají si jen ty bity, kde použili stejnou bázi. Shodná série bitů tak tvoří klíč, ostatní bity jsou zahozeny.



Obr. B.3: Obecné schéma protokolu BB84.

B.3 Seznam přístrojů a pomůcek

- HeNe laser – Hélium-neonový laser vyzařuje lineárně polarizovaný paprsek s vlnovou délkou 632,8 nm. Laser patří do bezpečnostní třídy 3B, proto je potřeba mít nasazené ochranné brýle.
- Lineární polarizátor – Slouží k propouštění světla s kmitáním elektrického pole v určitém směru, zatímco světlo polarizované v jiném směru blokuje nebo snižuje jeho intenzitu.
- Polarizační dělič svazku – Propouští světlo polarizované v jednom směru a odráží světlo polarizované kolmo k tomuto směru.
- Výkonový dělič svazku – Výkonový dělič svazku s poměrem 50:50 rovnoměrně rozdělí vstupní paprsek na dvě části a každá z nich obdrží polovinu původní intenzity světla.
- Polarizační rotátor 45° – Otáčí polarizační rovinu světla o 45°.
- Kolimátor – Slouží k usměrnění rozbíhavých nebo sbíhavých světelných paprsků do paralelního svazku.
- Montážní základny, sloupky, držáky sloupků, optická vlákna, čistící pero, měřič optického výkonu, šedý filtr, ochranné brýle

B.4 Bezpečnostní pokyny

Manipulace s laserem

Laser v laboratoři patří do bezpečnostní třídy 3B, je tedy **povinné mít nasazené ochranné brýle**. Nikdy nenechávejte zapnutý laser bez dozoru, vždy jej mějte pod kontrolou. Vyvarujte se pohledu do výstupního otvoru laseru. Přímý i odražený paprsek laseru může způsobit vážné poškození očí. V žádném případě nesměřujte laserový paprsek na lidi.

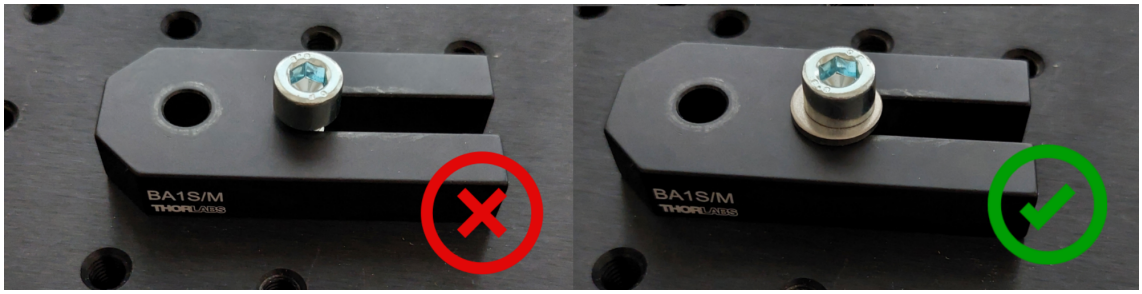
B.5 Pokyny pro práci

Uchycení optických komponent

Optické komponenty (lineární polarizátor, polarizační a výkonový dělič svazku, polarizační rotátor, kolimátor) jsou již nachystány v příslušných ochranných držácích. V průběhu práce je nevyjímejte z držáků, aby nedošlo k jejich poškození neodborným zacházením. Ujistěte se, že při manipulaci s komponentami v držácích se nedotýkáte prstů skleněných částí povrchu. Mohlo by dojít k jejich znečištění a zkreslení výsledků měření. Zajistěte, aby všechny držáky byly pevně uchyceny na optickém stole.

Montážní základna

Montážní základna je základní prvek, který poskytuje stabilní platformu pro další části. Montuje se přímo do optického stolu. Aby při dotahování šroubu nedošlo k poškození základny, je nutné vložit pod hlavičku šroubu podložku.



Držák sloupku

Držák sloupku slouží k udržení a přesnému nastavení výšky a polohy sloupků pomocí bočních nastavitelných šroubů. Držák se našroubuje na montážní základnu skrz prodlužovací matici.

Sloupek

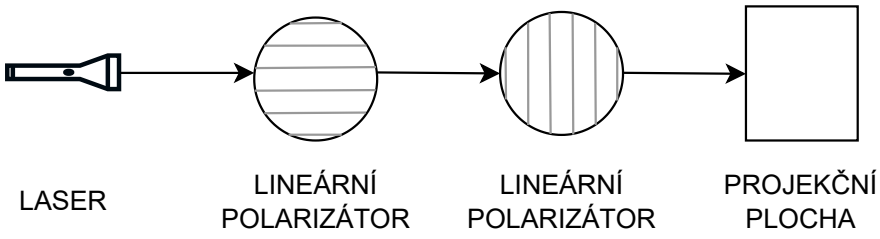
Sloupky se vsunou do držáku a slouží jako podpůrné struktury pro další optické komponenty.

B.6 Zadání laboratorní úlohy

B.6.1 Pozorování změny intenzity světla se dvěma polarizátory

V této části budete pozorovat světlo procházející lineárními polarizátory a analyzovat, k jakým změnám intenzity světla dochází při různých úhlech polarizátorů.

Schéma aparatury



Obr. B.4: Schéma zapojení se dvěma polarizátory.

Postup

1. Na jednom konci optického stolu se nachází již upevněný laser. Na druhý konec stolu, naproti laseru, umístěte stojan s papírem, na kterém budete pozorovat intenzitu paprsku.
2. Laser zapněte otočením klíče na napájecím zdroji. Paprsek musí směřovat na projekční plochu.
3. Lineární polarizátory se již nachází v rotačních držácích. Dbejte na to, abyste se skla nedotkli prsty, a našroubujte polarizátory s držáky na sloupky, které pak vložíte do držáku sloupků.
4. První polarizátor umístěte mezi zdroj světla a projekční plochu tak, aby světlo z laseru procházelo jeho středem.
5. Nastavte na prvním polarizátoru 0°. Nyní je jeho polarizační rovina horizontální a rovnoběžná s polarizací laseru.
6. Obdobným způsobem umístěte druhý polarizátor podle schématu. Ujistěte se, že paprsek prochází středem obou polarizátorů a dopadá na projekční plochu.
7. Zachovejte první polarizátor na 0°, druhým polarizátorem otáčejte a pozorujte změny intenzity světla.
8. Otáčejte druhý polarizátor o úhly 0°, 45°, 90° a 135° a výsledky zapisujte do tabulky B.1 (například silná, poloviční, žádná atd.).

Tab. B.1: Pozorování změn intenzity světla při různých úhlech polarizace.

Úhel druhého polarizátoru	**Pozorovaná intenzita světla**
0°	silná
45°	poloviční
90°	žádná
135°	poloviční

Kontrolní otázky

Kdy byla zaznamenána nejvyšší intenzita světla na projekční desce v průběhu otáčení druhého polarizátoru? Vysvětlete.

Nejvyšší intenzita světla byla zaznamenána, když polarizační osy obou polarizátorů byly nastaveny rovnoběžně, tedy když byl druhý polarizátor nastaven také na úhel 0°. V takovém případě není žádná část světla blokována, světlo prochází skrz oba dva polarizátory v maximální intenzitě.

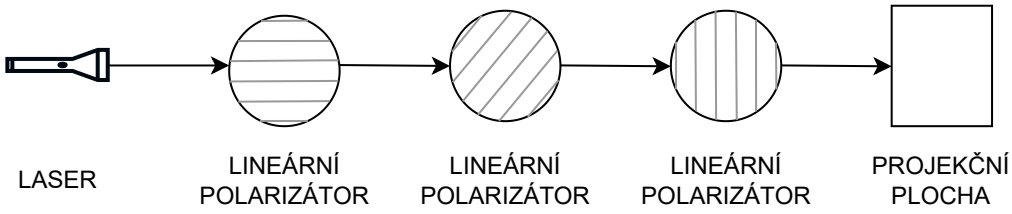
Kdy byla pozorována nejnižší intenzita? Vysvětlete.

Nejnižší (žádná) intenzita světla byla pozorována, když byly polarizační osy na sebe kolmé, což odpovídá úhlu 90° pro druhý polarizátor. První polarizátor propouští světlo, které je polarizované ve směru 0°. Toto světlo vstupuje do druhého polarizátoru, který je nastavený na 90°. Vzhledem k tomu, že světlo polarizované ve směru 0° je kolmé na osu druhého polarizátoru, je toto světlo druhým polarizátorem zcela blokováno.

B.6.2 Pozorování změny intenzity světla se třemi polarizátory

Záměrem je pozorování stavu, kdy vkládání třetího polarizátoru mezi dva vzájemně ortogonálně (kolmo) orientované polarizátory může znovu umožnit průchod světla, který by jinak byl blokován.

Schéma aparatury



Obr. B.5: Schéma zapojení se třemi polarizátory.

Postup

- Vraťte se k uspořádání, kdy neprocházelo žádné světlo a polarizační roviny byly kolmé (první polarizátor nastavte na úhel 0° a druhý na 90°).
- Přidejte třetí lineární polarizátor mezi původní dva.
- Začněte otáčet prostředním polarizátorem a pozorujte, zda dojde k opětovnému průchodu světla na projekční ploše.
- Postupně prostředním polarizátorem otáčejte o úhly 0°, 45°, 90° a 135° a výsledky si zapisujte do tabulky B.2.

Tab. B.2: Pozorování intenzity světla při různých úhlech prostředního polarizátoru.

Úhel prostředního polarizátoru	**Viditelnost světla**
0°	ne
45°	ano
90°	ne
135°	ano

Kontrolní otázky

Vysvětlete, jakým způsobem vložení třetího polarizátoru umožnilo průchod světla, které bylo původně blokováno prvními dvěma polarizátory.

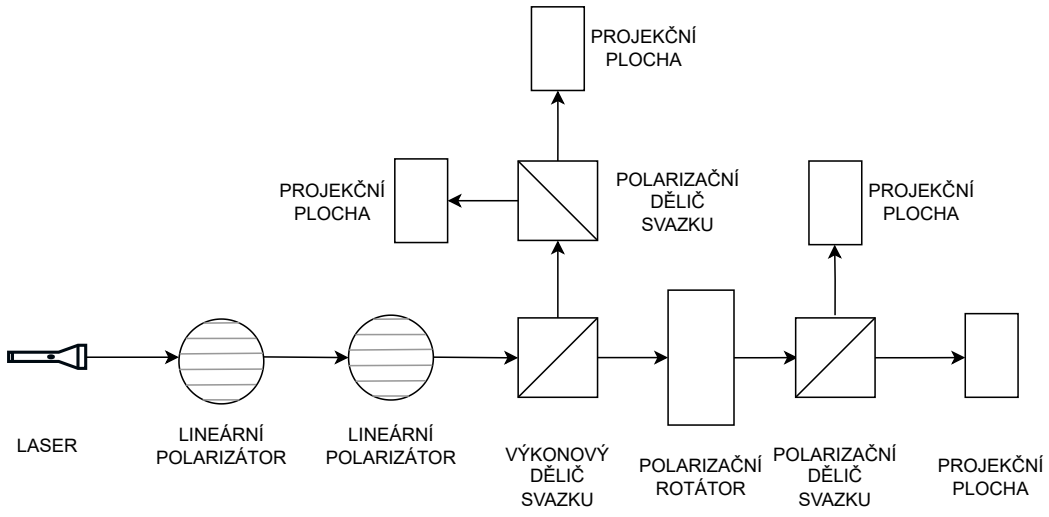
Vložením dalšího polarizátoru mezi původní dva, například se směrem polarizační osy na 45°, dochází k následujícímu:

- **První polarizátor (0°):** Světlo, které prochází tímto polarizátorem, se stává lineárně polarizovaným ve směru 0°.
- **Prostřední polarizátor (45°):** Po průchodu prostředním polarizátorem světlo není čistě polarizované ve směru 0° nebo 90°, ale ve směru 45°, což znamená, že se skládá ze dvou složek: jedna ve směru 0° a druhá ve směru 90°.
- **Poslední polarizátor (90°):** Když světlo polarizované ve směru 45° prochází posledním polarizátorem nastaveným na 90°, složka světla ve směru 90° projde.

B.6.3 Praktická simulace protokolu BB84

Budete provádět praktickou simulaci protokolu BB84, který se řadí mezi nejznámější protokoly pro kvantovou distribuci klíčů. V protokolu BB84 jsou informace zakódovány v polarizaci fotonů. Pozorováním světla na každém výstupu při různých úhlech polarizace získáte základní představu o tom, jak polarizační stavy ovlivňují měření. Tato úloha nepředstavuje plně funkční implementaci protokolu BB84, je pouze jeho zjednodušenou simulací. Laser v laboratoři má vyšší výkon než je obvyklé pro kvantovou distribuci klíčů, kde se pracuje s jednotlivými fotony nebo slabými světelnými pulzy.

Schéma aparatury



Obr. B.6: Schéma zapojení praktické simulace protokolu BB84.

Postup

1. Z předchozí úlohy ponechejte první dva lineární polarizátory a stojan s papírem na konci optického stolu naproti laseru. Pokud jsou polarizátory příliš daleko od sebe, přesuňte je k sobě blíže, aby se celá aparatura vešla na optický stůl. První polarizátor bude pevně nastaven na 0°, druhým polarizátorem budete v průběhu úlohy otáčet.
2. Podle schématu aparatury umístěte zbylé stojánky s papírem, které budou sloužit jako projekční plochy na výstupy z polarizačních děličů svazku.
3. Výkonový dělič svazku (označení 20 mm) umístěte za druhý lineární polarizátor tak, aby oba jeho výstupy dopadaly na projekční plochy.

4. Na jeden výstup výkonového děliče svazků umístěte polarizační dělič svazku (označení 15 mm). Oba jeho výstupy musí opět dopadat na stojany s papírem.
5. Na druhý výstup výkonového děliče svazku umístěte polarizační rotátor a za něj druhý polarizační dělič svazku. Opět zajistěte, aby oba výstupy dopadaly na stojany s papírem.
6. Ujistěte se, že máte všechny komponenty pevně zafixované, a že laserový paprsek prochází všemi komponentami.
7. Postupně otáčejte polarizátor o úhly 0°, 45°, 90° a 135° a pozorujte, co se děje se světlem na každém výstupu.

Souvislost experimentu a protokolu BB84

V protokolu BB84 Alice zakóduje binární hodnoty (0 a 1) do fotonů pomocí čtyř různých polarizačních stavů (0°, 45°, 90° a 135°), a to odpovídá dvěma bázím: vertikálně-horizontální a diagonální. Alice je v úloze reprezentována lineárním polarizátorem, kterým otáčíte o různé úhly (0°, 45°, 90° a 135°).

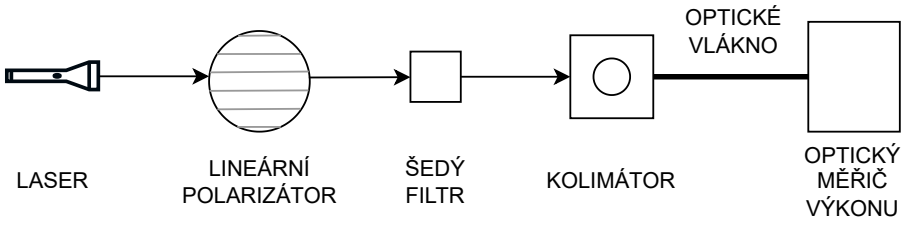
Výkonový dělič svazku rozdělí paprsek do dvou cest, což simuluje situaci, kdy foton má 50% šanci, že půjde jednou cestou a 50% šanci, že půjde druhou cestou. Každá cesta reprezentuje měření v jiné bázi. Na jednom výstupu výkonového děliče svazku se nachází polarizační dělič svazku, který rozděluje fotony podle polarizace (horizontální nebo vertikální), a to odpovídá měření ve vertikálně-horizontální bázi.

Na druhém výstupu je umístěn polarizační rotátor následovaný dalším polarizačním děličem svazku, který opět rozděluje fotony podle jejich polarizace, což odpovídá měření v diagonální bázi. Když pozorujete, kam dopadá světlo na projekční plochy, simulujete Boba který měří přicházející fotony v různých polarizačních stavech.

B.6.4 Vliv různých typů optických vláken na polarizaci světla

V poslední části úlohy budete pozorovat vliv různých typů vláken na polarizaci světla. Konkrétně budete porovnávat běžné jednovidové (SM) vlákno a vlákno uchovávající polarizaci (PM).

Schéma aparatury



Obr. B.7: Schéma zapojení s optickým vláknem.

Postup

1. Za laserem ponechejte pouze lineární polarizátor nastavený na 0°.
2. Nastavte šedý filtr do cesty paprsku, aby intenzita paprsku nebyla příliš silná a nedošlo k poškození měřicího zařízení.
3. Umístěte kolimátor tak, aby světelný paprsek vstupoval do jeho čočky.
4. Před měřením vždy očistěte oba konce optického vlákna čistícím perem. Připojte výstup kolimátoru k běžnému SM vláknu. Druhý konec vlákna připojte k měřiči optického výkonu.
5. Pomocí tří šroubů na držáku kolimátoru upravte pozici tak, aby detektor ukazoval co největší intenzitu světla.
6. Pomalu hýbejte vláknem a pozorujte změny intenzity světla na detektoru. Stupňujte postupně rozsah pohybů od jemných až po větší ohyby, abyste mohli sledovat, jak různé typy pohybů ovlivňují intenzitu světla.
7. Vyměňte běžné SM vlákno za PM vlákno.
8. Opět pomalu hýbejte vláknem a pozorujte změny intenzity světla na detektoru. Stupňujte pohyby vlákna stejným způsobem jako u předchozího vlákna.

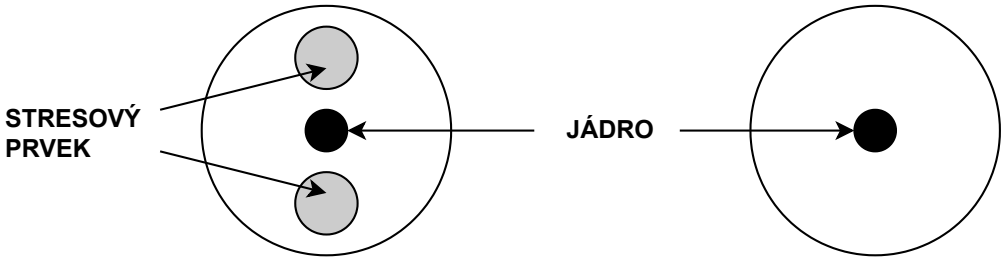
Kontrolní otázky

Jak se liší chování světla v PM vláknu a obyčejném SM vláknu při ohýbání?

PM vlákno lépe zachovává polarizaci světla, to znamená, že změny intenzity světla při pohybu vlákna byly menší a stabilnější. Naopak v obyčejném SM vláknu se projevovaly mnohem větší změny intenzity světla v důsledku narušení polarizace.

Vysvětlení

V běžném optickém vlákně dochází ke změně polarizace v důsledku změn v jeho geometrii. Proměnlivá geometrie znamená, že tvar optického vlákna se mění, například když se ohýbá, natahuje nebo stlačuje. Tyto změny tvaru ovlivňují cestu, kterou se světlo ve vlákně pohybuje, což může změnit jeho směr kmitání (polarizaci). Na rozdíl od toho, PM vlákno má speciální struktury, jako jsou stresující prvky, které pomáhají tyto změny kompenzovat a udržovat stabilní polarizaci světla.



Obr. B.8: Vlevo: PM vlákno typu PANDA, vpravo: SM vlákno.

C Simulace úlohy v aplikaci Virtual Lab od Quantum Flytrap

Virtual Lab od společnosti Quantum Flytrap je interaktivní webová aplikace, která umožňuje v reálném čase simulovat kvantové experimenty. Tento nástroj využívá intuitivní uživatelské rozhraní založené na metodě drag-and-drop (táhni a pusť), což umožňuje uživatelům bez potřeby znalosti programování sestavovat složité kvantové experimenty snadno a rychle.

Tato příloha obsahuje vizualizace schémat, která byla implementována v rámci laboratorní úlohy. Pro každý experiment jsou přiloženy snímky obrazovky, na nichž je znázorněno jak zapojení, tak zaznamenané výsledky. To umožňuje lepší představení jednotlivých kroků v návrhu laboratorní úlohy, která byla popsána v předchozí příloze B.

C.1 Pozorování změny intenzity světla se dvěma polarizátory

Zde dochází k simulaci světelného paprsku procházejícího dvěma lineárními polarizátory. Postupně se otáčí druhým polarizátorem o předem definované úhly a pozorují se změny v intenzitě světla na projekční ploše (ve Virtual Labu znázorněno pomocí detektoru).

Obr. C.1: Pozorování změny intenzity světla se dvěma polarizátory: 2. polarizátor otočen o 0°.

Obr. C.2: Pozorování změny intenzity světla se dvěma polarizátory: 2. polarizátor otočen o 90°.

C.2 Pozorování změny intenzity světla se třemi polarizátory

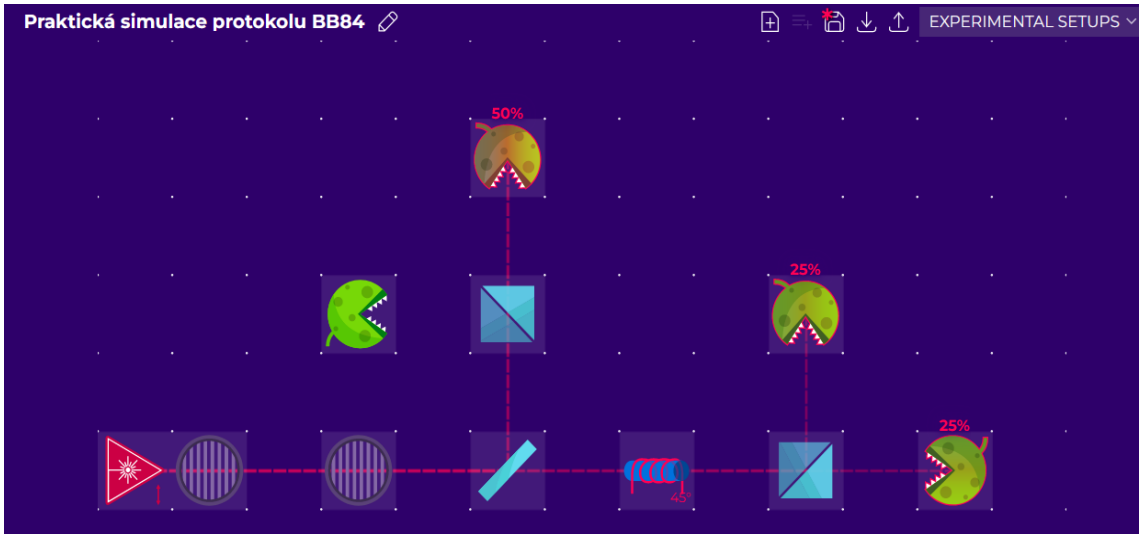
Nejdříve se nastaví původní dva polarizátory tak, aby jejich polarizační osy byly navzájem kolmé. Poté se mezi ně vloží další lineární polarizátor a pozoruje se, jak se obnovuje průchod světla pří otáčení o specifické úhly.

Obr. C.3: Pozorování změny intenzity světla se třemi polarizátory: prostřední polarizátor otočen o 0°.

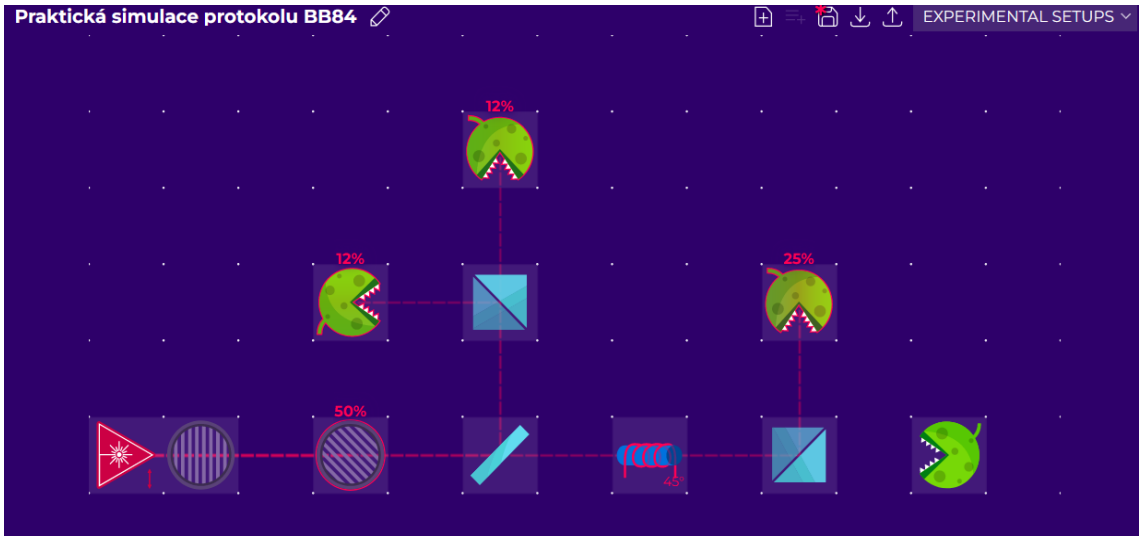
Obr. C.4: Pozorování změny intenzity světla se třemi polarizátory: prostřední polarizátor otočen o 45°.

C.3 Praktická simulace protokolu BB84

V této úloze se sestaví aparatura pro praktickou ukázku funkčnosti protokolu BB84. Polarizátorem se otáčí o předem definované úhly a pozorují se změny intenzity světla na všech výstupech.



Obr. C.5: Praktická simulace protokolu BB84: polarizátor otočen o 0°.



Obr. C.6: Praktická simulace protokolu BB84: polarizátor otočen o 45°.