VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

Fakulta elektrotechniky
a komunikačních technologií

DIPLOMOVÁ PRÁCE

Brno, 2021 Bc. Jakub Širjov

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

TESTOVACÍ POLYGON PRO KVANTOVOU DISTRIBUCI KLÍČŮ
QUANTUM KEY DISTRIBUTION TEST POLYGON

DIPLOMOVÁ PRÁCE
MASTER'S THESIS

AUTOR PRÁCE — **Bc. Jakub Širjov**
AUTHOR

VEDOUCÍ PRÁCE — **Ing. Michal Látal, DiS.**
SUPERVISOR

BRNO 2021

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

Diplomová práce

magisterský navazující studijní program **Telekomunikační a informační technika**

Ústav telekomunikací

Student: Bc. Jakub Širjov ***ID:*** 197644
Ročník: 2 ***Akademický rok:*** 2020/21

NÁZEV TÉMATU:

Testovací polygon pro kvantovou distribuci klíčů

POKYNY PRO VYPRACOVÁNÍ:

Cílem práce je detailní rozbor problematiky kvantové distribuce klíčů (QKD) a popis současného stavu. V rámci popisu současného stavu bude provedena rešerše komerčně nabízených řešení a bude provedeno jejich srovnání. V praktické části práce bude proveden návrh testovacího polygonu pro přenos QKD přes optickou datovou síť. Polygon bude navržen tak, aby na něm bylo možné testovat jak samotný přenos QKD, tak simultánní přenos s datovými službami a pro různé parametry (přenosové rychlosti 1-100 Gbit/s, rozestup mezi kvantovým a datovým kanálem 50-1000 GHz, výkony datového signálu v rozsahu 0-20 dBm). Návrh polygonu bude ověřen simulací ve vybraném simulačním SW (CVsim, OptiSystem, OMNeT++, NS-3).

DOPORUČENÁ LITERATURA:

[1] ISLAM, Nurul T. High-Rate, High-Dimensional Quantum Key Distribution Systems. Imprint: Springer, 2018. Springer Theses, Recognizing Outstanding Ph.D. Research. ISBN 978-3319989280.

[2] VAN METER, Rodney. Quantum networking. Hoboken, NJ: Wiley, 2014. Networks and telecommunications series. ISBN 978-1848215375.

Termín zadání: 1.2.2021 ***Termín odevzdání:*** 24.5.2021

Vedoucí práce: Ing. Michal Látal, DiS.

prof. Ing. Jiří Mišurec, CSc.
předseda rady studijního programu

ABSTRAKT

Diplomová práca je zameraná na objasnenie problematiky kvantovej distribúcie kľúčov (QKD) a vysvetlenie princípu fungovania samotného prenosu kvantového signálu. Následne sú porovnávaní komerční distribútori QKD a ich jednotlivé zariadenia. Praktická časť práce sa v prvej časti zaoberá prenosom kvantových kľúčov v simulačnom prostredí QKDNetsim. Druhá časť je zameraná na návrh a zostrojenie testovacieho polygónu, na ktorom bude možné testovať čo najviac možností zapojenia optickej siete s prenosom kvantového signálu s bežnými dátami v jednom vlákne. V poslednej časti sú vytvorené simulácie rôznych druhov filtrov pre potlačenie šumu v programe VPIphotonics a otestované možnosti simulátora QKDNetsim.

KĽÚČOVÉ SLOVÁ

distribúcia, DWDM, fotón, kľúč, kvantum, QKD, QKDN, QKDNetsim, Qubit, vlákno, VPIphotonics

ABSTRACT

The aim of this masters thesis is to explain quantum key distribution (QKD) and principle of signal transmission in the quantum channel. Further this thesis complains commercial distributors of QKD technologies and their individual appliances. Practical part of the thesis is separated to 3 parts. First part handles transmission of quantum keys in QKDNetsim simulator. Second part takes care of design and creation of a test polygon that allows for testing of many optical network configurations with quantum signal and normal data traffic being transmitted in a single fiber. Multiple simulations of use of various filter types to supress the signal noise in the program VPIphotonics and tested by QKDNetsim are shown in the last part of this thesis.

KEYWORDS

distribution, DWDM, fiber, key, photon, QKD, quantum, Qubit, QKDN, QKDNetsim, VPIphotonics

ŠIRJOV, Jakub. *Testovací polygon pro kvantovou distribuci klíčů*. Brno, 2021, 80 s. Diplomová práca. Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav telekomunikací. Vedúci práce: Ing. Michal Látal, DiS.

VYHLÁSENIE

Vyhlasujem, že svoju diplomovú prácu na tému „Testovací polygon pro kvantovou distribuci klíčů“ som vypracoval samostatne pod vedením vedúceho diplomovej práce, s využitím odbornej literatúry a ďalších informačných zdrojov, ktoré sú všetky citované v práci a uvedené v zozname literatúry na konci práce.

Ako autor uvedenej diplomovej práce ďalej vyhlasujem, že v súvislosti s vytvorením tejto diplomovej práce som neporušil autorské práva tretích osôb, najmä som nezasiahol nedovoleným spôsobom do cudzích autorských práv osobnostných a/alebo majetkových a som si plne vedomý následkov porušenia ustanovenia § 11 a nasledujúcich autorského zákona Českej republiky č. 121/2000 Sb., o práve autorskom, o právach súvisiacich s právom autorským a o zmene niektorých zákonov (autorský zákon), v znení neskorších predpisov, vrátane možných trestnoprávnych dôsledkov vyplývajúcich z ustanovenia časti druhej, hlavy VI. diel 4 Trestného zákonníka Českej republiky č. 40/2009 Sb.

Brno ....

podpis autora

POĎAKOVANIE

Rád bych poděkoval vedoucímu diplomové práce panu Ing. Michal Látal, DiS. za odborné vedení, konzultace, trpělivost a podnětné návrhy k práci.

Obsah

Zoznam obrázkov

Zoznam tabuliek

Úvod

Výber témy bol motivovaný rýchlo sa vyvíjajúcou technológiou a potrebou zachovať bezpečnú a tajnú komunikáciu. Nakoľko vývoj technológie vo všetkých smeroch ide dopredu, tak aktuálne bezpečnostné systémy už nie sú dostatočne bezpečné a sú napadnuteľné v reálnom čase. Smer, ktorý by mohol poskytnúť dostatočnú bezpečnosť je skrytý v technológiách zabezpečovacích systémov, postavených na princípoch kvantovej mechaniky, namiesto postupov využívajúcich zložité matematické operácie. Oblasti využitia týchto princípov sú ukryté v kvantovej kryptografii alebo pri využívaní technológií založených na kvantových počítačoch. Podstatnou časťou kvantovej kryptografie je kvantová distribúcia kľúčov, čo je aj hlavnou myšlienkou tejto práce. Táto popisuje problematiku kvantovej distribúcie kľúčov.

Teoretická časť práce začína úvodom do základov kryptografie, kde je kryptografia rozdelená do skupín, a kde sú vysvetlené jednotlivé princípy jej fungovania. Práca následne objasňuje základné princípy kvantovej mechaniky, ako Heisenbergov princíp neurčitosti a Bellova nerovnosť, ktoré kvantová distribúcia kľúčov využíva.

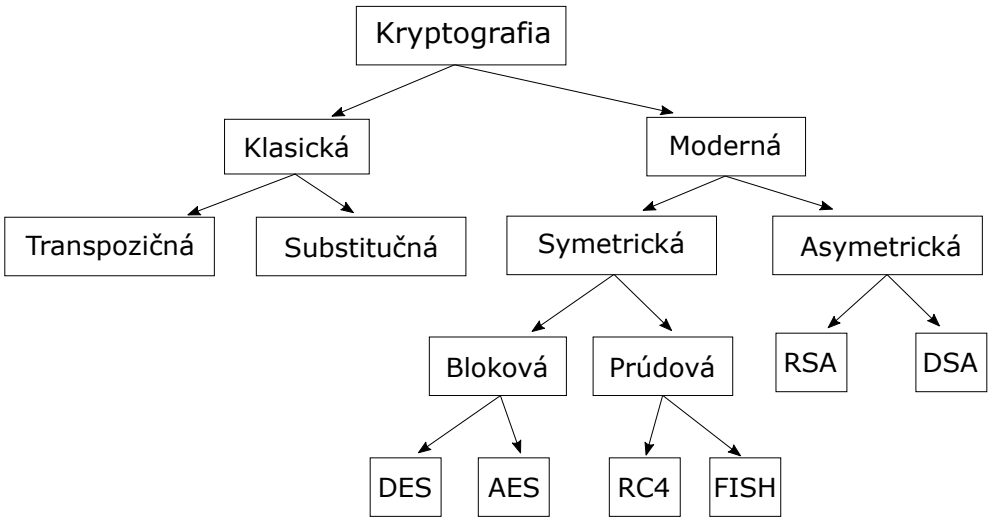
V ďalšej kapitole je popisovaný qubit (kvantový bit) ako základná jednotka kvantovej informácie. Ukazuje, ako sa táto jednotka môže merať, zdôrazňuje jej veľké výhody z pohľadu bezpečnosti a schopnosti ukladania informácií, ale tiež upriamuje pozornosť na nevýhody ako je zložitá manipulácia, ale aj jeho citlivosť na okolité vplyvy. Práca pokračuje úvodom do systémov kvantovej distribúcie kľúčov, princípmi fungovania a technológiou ich výmeny. Následne je predstavené fungovanie siete kvantovej distribúcie kľúčov a implementácie technológií, kde už boli tieto teórie využité. Ďalšia časť práce popisuje rozdelenie komunikačných protokolov využívaných v kvantovej distribúcii kľúčov a vysvetľuje princípy fungovania týchto protokolov. Koniec teoretickej časti obsahuje popis firiem, ktoré sa aktuálne venujú kvantovej distribúcii kľúčov a ponúkajú komerčné zariadenia.

Praktická časť sa zaoberá zadaným simulačným prostredím s nasimulovanou topológiou a prezentuje zistené možnosti využitia simulačného prostredia QKDNetsim. Následne sa práca venuje vytvoreniu testovacieho polygónu pre simulovanie prenosu používateľských dát súbežne s QKD v jednom vlákne v simulačnom prostredí VPIphotonics. Topológia polygónu je vytvorená tak, aby prenos bol čo najvariabilnejší a bolo možné testovanie čo najviac možností prenosu a zapojení.

1 Teoretická časť

1.1 Moderná kryptografia

Je každodennou súčasťou bežného človeka. Slúži na zabezpečenie elektronickej komunikácie pri prenose informácií na to, aby ich nezískala tretia strana. V prípade, ak by sa k informáciám dostala, kryptografia by sa mala zabezpečiť neschopnosť tretej strany dáta prečítať a následne zneužiť. Komunikácia môže byť drôtová (metalická, optická) alebo bezdrôtová (optická, rádiová, sonická). Komunikačný kanál



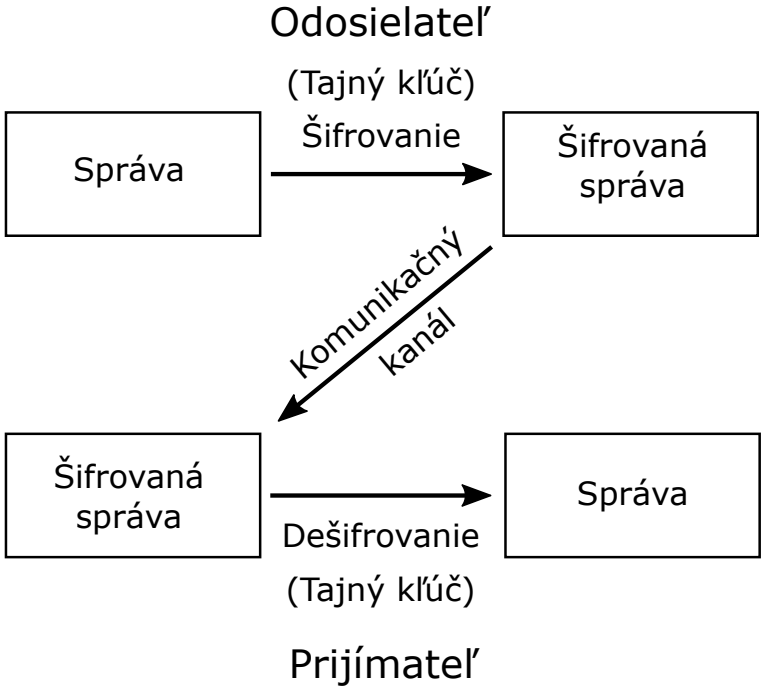
Obr. 1.1: Rozdelenie kryptografie

je jednoduché sledovať a následne odpočúvať, preto je nevyhnutné, aby boli údaje zabezpečené, teda zašifrované. Podstatou všetkých kryptografických prostriedkov je použitie rôznych zložitých matematických operácii pre zabezpečenie dát tak zložitých, aby ich nebolo možné v reálnom čase rozlúštiť. Kryptografiu sa delí podľa toho, akým spôsobom je použitá a rozdeľuje sa na symetrickú a asymetrickú, viď obr. 1.1 [1].

1.1.1 Symetrické šifry

Hlavným princípom symetrickej kryptografie je, že kľúč pre šifrovanie a dešifrovanie je rovnaký, respektíve je možné jeden od druhého jednoducho odvodiť viď obr. 1.2. Veľkou výhodou týchto šifier je, že nevyžadujú veľký výpočtový výkon, sú výpočtovo nenáročné a rýchle pri šifrovaní. Symetrické šifry sa delia na blokové a prúdové. Blokové šifry rozdeľujú informácie na rovnako veľké bloky bitov, ktoré sa následne zašifrujú. Prúdové zapracovávajú text po jednotlivých bitoch, tieto šifry boli inšpirované Vernamovou šifrou, tiež známou ako „one-time pads“ kde je každý znak správy

posunutý o náhodne zvolený počet miest, čo v konečnom dôsledku zmení originálnu správu na sled úplne náhodných znakov a v princípe je nerozlúštiteľná. Prúdové šifry sa delia na synchrónne a asynchrónne. Veľmi dôležité je, aby sa prijímateľ a odosielateľ na tomto tajnom kľúči dohodli vopred tak, aby nikto iný tento kľúč nezískal. Jednou z možností je manuálne (osobne) na oba konce spojenia doniesť bezpečne kľúč, čo je v dôsledku veľmi nepraktické alebo sa na to využije Asymetrické šifrovanie. Napríklad šifra AES (Advanced Encryption Standard), Triple DES (Data Encryption Standard), RC4 (Rivest Cipher 4) pre prenos symetrického kľúča alebo iný protokol, ktorý vytvorí bezpečné komunikačné spojenie cez nezabezpečený kanál (Diffie-Hellmanov algoritmus) [1], [2], [3], [4].

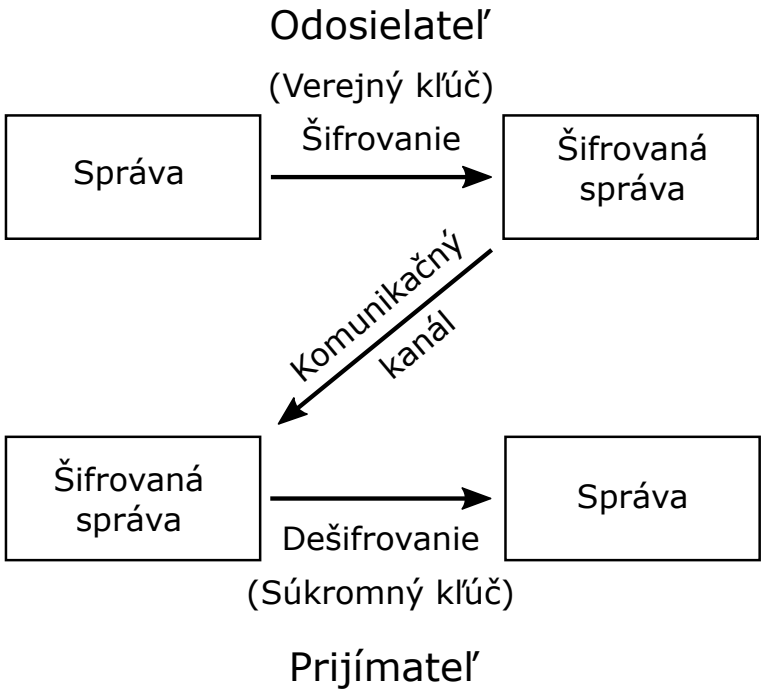


Obr. 1.2: Princíp šifrovania a dešifrovania pomocou symetrického kľúča

1.1.2 Asymetrické šifry

Na rozdiel od symetrického šifrovania podstatou asymetrického šifrovania je práve využitie dvojice kľúčov, teda rozdielne kľúče pre šifrovanie a dešifrovanie dát viď, obr. 1.3. Tieto kľúče sa volajú verejné kľúče (public key) a súkromné kľúče (private key), ktoré medzi sebou majú určitú matematickú spojitosť. Hlavnou myšlienkou je šifrovanie dát pomocou verejného kľúča, ktorý je voľne distribuovaný a nie je ním možné dešifrovať správu alebo následne odvodiť súkromný kľuč. Dešifrovanie je možné len pomocou súkromného kľúča, ktorý sa nikdy neposiela a zostáva v tajnosti. Pričom zo súkromného kľúča je jednoduché odvodiť verejný kľúč [1], [2], [3].

Asymetrická kryptografia rieši nedostatky, napríklad ako problém s dopredným bezpečným vymieňaním symetrických kľúčov. Komunikujúce strany nemusia mať obavy z toho, že by tajný kľuč získala tretia strana. Asymetrické kryptografia by mala zabezpečovať istotu identity odosielateľa a bezpečný prenos dát. Nevýhodou je, že vyžaduje vysoký výpočtový výkon a je pomalá pri šifrovaní dát. Z toho dôvodu sa väčšinou využíva pre bezpečný prenos symetrických kľúčov. Predstaviteľmi asymetrického šifrovania sú napríklad RSA (Rivest Shamir Adleman), DSA (Digital Signature Algorithm) alebo IDEA (International Data Encryption Algorithm). Najznámejšie RSA sa používa na podpisovanie dokumentov a jeho princíp stojí na časovej zložitosti rozdelenia veľkého čísla na súčin prvočísiel [2], [4].



Obr. 1.3: Princíp šifrovania a dešifrovania pomocou verejného a súkromného kľúča

1.1.3 Nasledujúci vývoj

V dôsledku neustále prudko narastajúceho výpočtového výkonu sa museli aj šifrovacie metódy zlepšovať, nakoľko sú založené na zložitých matematických operáciách a bolo ich už možné rozlúštiť v reálne krátkom čase. Preto technológie, ako umelá inteligencia alebo kvantové výpočty, môžu byť veľkou hrozbou bezpečnosti takéhoto druhu zabezpečenia, ale aj jej riešením. Kryptológia sa vyvíjala smermi, ako je šifrovanie chaosom, fraktálnym šifrovaním, kvantovými javmi alebo umelou inteligenciou. Práve kvantové javy sú využívané v kvantovej distribúcii kľúčov (Quantum Key Distribution, skrátene QKD), kde sa využívajú princípy kvantovej mechaniky.

Práve QKD je technológia, o ktorej sa dá povedať, že je bezpečná voči útokom s neobmedzeným výpočtovým výkonom [1].

1.2 Kvantová mechanika

Kvantová fyzika je hlavným odvetvím a kvantová mechanika je časťou kvantovej fyziky. Hlavný rozdiel medzi nimi je, že kvantová fyzika je odvetvie vedy, ktoré sa zameriava na kvantovú mechaniku a kvantová mechanika je súbor princípov, ktoré vysvetľujú správanie hmoty a energie. Kvantová fyzika opisuje vlastnosti fyzikálneho systému, zatiaľ čo kvantová mechanika popisuje správanie a vlastnosti častíc [5].

Teória štruktúry atómov popisuje správanie hmoty, vzájomne energetické ovplyvňovanie a veľa ďalších javov v mikroskopickom svete. Kvantová fyzika funguje na inom princípe a iných zákonoch ako fyzika makroskopických telies. Nakoľko vzdialenosti, prenosy energie a momenty hybnosti sú omnoho menšie ako hodnoty s ktorými majú ľudia skúsenosti z bežného života. Na konci 19. storočia boli objavené javy, ktoré nedokázala vysvetliť klasická fyzika, a to bol podnet pre vznik kvantovej fyziky. V kvantovej mechanike sa používajú matematické operátory, ktoré popisujú každú merateľnú veličinu. Hodnoty, ktoré dokáže meraná veličina nadobúdať, sú prevedené ako číslo daného operátora. Niektoré princípy kvantovej mechaniky môžu vyzerať nelogicky, pretože popisuje stavy a správanie, ktoré sú oproti bežnej fyzike iné. Existujú však určité spojitosti medzi kvantovou a klasickou fyzikou. Pokiaľ budeme prechádzať od častíc k makroskopickým telesám, budú sa vlnové dĺžky de Broglieových vĺn a Planckova konštanta $\hbar$ javiť nekonečne malé a zákony kvantovej fyziky sa budú meniť na zákony klasickej fyziky [6].

1.2.1 EPR paradox

Je to „myšlienkový experiment“, ktorý bol navrhnutý fyzikmi Einstein, Podolska a Rosen. Skratka EPR vznikla z počiatočných písmen uvedených mien. Podstatou je snaha dokázať, že vlnová funkcia nepopisuje správne fyzikálnu realitu, a tým vyvrátiť interpretáciu kvantovej mechaniky. Podľa tohto paradoxu existujú premenné, ktoré kvantová mechanika neobsahuje, a preto je nekompletná. Tento myšlienkový experiment je najznámejším príkladom kvantového zapletenia (quantum entanglement) [6], [7].

Myšlienkový experiment zahŕňa dvojicu zapletených častíc a bolo poukázané, že v ich stave, ak by bola zmeraná poloha prvej častice, je možné predpovedať polohu druhej častice. Pokiaľ by namiesto toho bola meraná hybnosť častice, potom by bolo možné predpovedať výsledok merania druhej častice. Snažili sa presadiť teóriu, že v prípade akéhokoľvek ovplyvnenia prvej častice sa nemôže zmeniť stav

druhej častice. Z toho predpokladu by vyplávalo, že by medzi týmito časticami bol skrytý prenos informácií rýchlejší, ako je rýchlosť svetla, čo je v rozpore s teóriou relativity [6], [7].

Odvolávali sa na princíp neskôr známy ako „EPR criterion of reality“, teda ak bez akéhokoľvek zásahu do systému vieme s istotou predpovedať hodnotu fyzikálnej hodnoty, tak musí existovať prvok reality, ktorý zodpovedá tejto hodnote. Z tejto teórie bolo usúdené, že častica má svoju hodnotu polohy a hybnosti ešte pred meraním, čo je v rozpore s názorom spojeným s Bohrom a Heisenbergom. Ich názor hovorí, že častica je v stave superpozície (nemá žiadnu konkrétnu hodnotu) pokiaľ ju nezmeriame [6], [7], [8].

1.2.2 Belova nerovnosť

John Bell publikoval článok skúmajúci záhadnú situáciu, a to paradox EPR, ktorý ukazoval nedostatky kvantovej mechaniky a navrhol, že tieto problémy by vedela vyriešiť teória skrytých premenných. Podľa zástancov skrytých premenných sú hodnoty previazaných (entaglovaných) častíc vopred dané, v prípade fotónov sú určené v okamihu emisie. Po zverejnení jeho článku sa vyvinul rad experimentov pre dokázanie alebo vyvrátenie skrytých premenných [7], [9].

Bellov experiment, sa snažil dokázať, že previazané častice si nesú svoje informácie stále, aj keď sú od seba vzdialené. Bellov teorém sa konkrétne zameriava na spin obidvoch častíc. Pretože spin má len jednu absolútnu hodnotu a mení sa len znamienko. Máme meracie osoby Boba a Alice, a pokiaľ budú mať obaja rovnakú os merania, tak jeden bude mať vždy zmerané opačné znamienko ako ten druhý. Problém vzniká, keď sa menia osi merania, pretože vtedy skryté premenné nevedia rozširovať svoje kvantovo mechanické korelácie. Tento rozdiel je vyjadrený pomocou Bellových nerovností. Pokiaľ sa chovanie páru častíc riadi lokálnou teóriou so skrytými premennými, musia byť splnené Bellove nerovnosti pre ľubovoľnú kombináciu uhlov. Vďaka Bellovym nerovnostiam je možné rozhodnúť medzi kvantovou mechanikou a teóriou skrytých premenných pomocou experimentu. Výsledok experimentu hovorí o neplatnosti teórií skrytých premenných. Ale ukázalo sa, že problém leží vpredpoklade lokalizácie, ktorá nezodpovedá skutočnosti. Experiment dokazuje, že existujú korelácie, ktoré porušujú predstavu o lokalizácií. Previazanie je podstatnou súčasťou všetkých procesov na kvantovej úrovni [7], [8], [9].

Všetky dosiaľ vykonané experimenty sú v súlade s kvantovou mechanikou [7].

1.2.3 Heisenbergov princíp neurčitosti

Haisebergov princíp je jedným zo základných postulátov kvantovej mechaniky. Princíp neurčitosti sa dá popísať ako súbor nerovníc, ktoré hovoria s akou presnosťou

sme schopní merať veličiny určitých párov častíc. Tieto veličiny sú napríklad poloha r, hybnosť p (vektorová veličina, ktorá charakterizuje pohybový účinok hmotnosti), energia E a čas t [10], [11], [12].

Princíp neistoty predstavil Werner Heisenberg, ktorý hovorí, že čím presnejšie je určená prvá veličina, tým je menej presné určenie druhej veličiny. To znamená, že pokiaľ zmeriame druhú veličinu a až potom prvú, dostaneme iné hodnoty ako v prvom meraní. Podľa princípu neurčitosti nie je možné, aby boli obe veličiny súčasne merané s vyššou presnosťou, než je horná hranica vyjadrená pomocou Planckovej konštanty [10], [12].

$$\Delta r \Delta \rho_x \geq h/4\pi \tag{1.1}$$

$$\Delta E \Delta t \geq h/4\pi \tag{1.2}$$

Rovnice 1.1 a 1.2 vyjadrujú, že súčin nepresnosti týchto veličín musí byť vždy väčší alebo rovný hodnote $h/4\pi$ [11].

Neurčitosť bola často zamieňaná s efektom pozorovateľa (v preklade Observer effect), ktorý hovorí o fakte, že nie je možné merať nejakú veličinu bez toho, aby sme ju nejakým spôsobom neovplyvnili, a tým nezmenili jej vnútorný stav [10].

Prvý princíp neurčitosti je vzťah medzi hybnosťou a pozíciou. Je možné si to predstaviť ako elektrón, ktorý obieha po nejakej kvantovej dráhe okolo jadra a je rozmazaný. V prípade, keď ho zastavíme, vieme kde je, ale nevieme zistiť, akú mal hybnosť, a to funguje aj opačne pre hybnosť. Inak povedané čim presnejšie meriame jednu veličinu tým je výsledok druhej nepresnejší. Tiež existuje relácia neurčitosti medzi energiou a časom, ktorá hovorí že buď vieme zmerať presne jeho časové alebo jeho energetické vlastnosti, a čím je vymedzený čas na pozorovanie kratší, tým nepresnejšie môžeme zmerať energiu tejto veličiny [11], [12].

1.2.4 Fotón

Je základná jednotka svetla a vo fyzike je známa ako stabilná elementárna častica, ktorá je popisovaná kvantom elektromagnetickej energie. Taktiež ju popisujú veličiny, ako sú vlnová dĺžka, frekvencia, energia a hybnosť. Fotón je častica, to bolo dokázané fotoelektrickým a Comptovým javom. Táto častica má súčasne vlastnosti vlny, čo bolo dokázané javom interferencie. Jav, že fotón má vlastnosti častice aj vlny sa nazýva vlnovo korpuskulárny dualizmus. Charakteristikou vlastnosťou tejto častice je nulový elektrický náboj a jeho pokojová hmotnosť je nulová. Taktiež patrí do skupiny bozónov a jeho spin je rovný 1, naproti tomu elektrón je fermiom a jeho spin je $-1/2$ (spin-up) alebo $+1/2$ (spin-down), pričom spin je vlastnosť častice

a nemá obdobu v našom makroskopickom svete. Je možné si ho predstaviť ako guličku, ktorá sa točí, ale nie je to guličkа a netočí sa. Tiež sa to dá predstaviť ako moment vnútornej hybnosti častice. O bozónoch je známe, že v jednom kvantovom stave sa môže nachádzať viac bozónov. To znamená, že v rámci jedného systému môžeme mať dva identické fotóny, naopak fermióny nemôžu existovať dve častice v tom istom kvantovom stave [13], [4].

Z praktického hľadiska sa pre zjednodušenie manipulácie používajú frekvencie v oblasti viditeľného svetla. Nevýhodou fotónov je obmedzená stredná vzdialenosť než častica zanikne, a tým pádom sú stratené aj informácie [15].

1.3 Qubit

V informačnej technike je základná jednotka bit, ktorej stav je vždy „0“ alebo „1“. Od tejto jednotky je odvodená jednotka kvantovej informácie a to je kvantový bit, skrátene qubit (quantum bit). Táto jednotka slúži ako elementárna jednotka informácie v kvantových počítačoch [15].

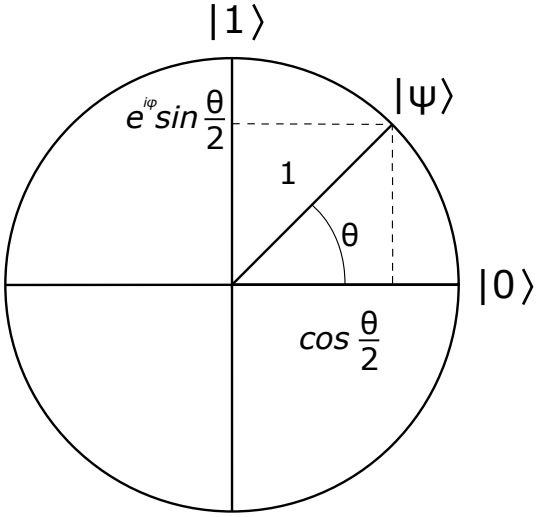
Jednotky qubity sú základné častice ako fotóny alebo elektróny, ktoré nesú informáciu. Pri elektróne to je spin, ktorý môže byť v smere hodinových ručičiek (spin-up) alebo v protismere (spin-down). V prípade fotónu, ktorý je pre túto prácu potrebné opísať podrobnejšie je to polarizácia, ktorá môže byť buď vodorovná alebo zvislá. Tento systém je schopný fungovať v superpozícií týchto stavov, teda môže byť polarizovaný diagonálne (šikmo posunutý o 45°), a to sa dá predstaviť ako kombinácia vodorovnej a zvislej polarizácie. Druhým spôsobom zakódovania informácie do fotónu je pomocou fázového posunu. Vtedy meriame interferenciu dvoch impulzov, z ktorých je jeden fázovo posunutý. Ak posielame impulzy rovnakou cestou tesne za sebou sa nazýva „time bin qubit“ [15], [16], [17].

Oproti klasickému bitu, ktorý nadobúda jeden z dvoch stavov, qubit môže nadobúdať vďaka kvantovej mechanike kombináciu týchto hodnôt. Preto stav qubitu je zobrazovaný symbolmi $|0\rangle$ a $|1\rangle$. Stav qubitu sa dá vysvetliť ako superpozícia pravdepodobností týchto stavov. To znamená, že s určitou pravdepodobnosťou α^2 stav $|1\rangle$ a s určitou pravdepodobnosťou β^2 stav $|0\rangle$ [15], [16].

1.3.1 Hilbertov priestor

Qubit je zobrazený a popísaný ako normovaný vektor (jednotkový vektor, ktorý má veľkosť 1) v dvojrozmernom Hilbertovom priestore kvantových stavov. Tento priestor je vektorový priestor so skalárnym súčinom. Tento priestor je vektorový priestor, ktorý je odvodený od skalárneho súčinu reálnych a komplexných čísiel. Skladá sa z normovaných bázových vektorov. Hilbertov priestor má ortogonálnu

bázu (vektory majú veľkosť 1 a sú vzájomne ortogonálne, teda pravouhlé) vektorov, ktoré sú označené ako $|0\rangle$ a $|1\rangle$, viď obr. 1.4. Ľubovoľná lineárna kombinácia týchto bázových vektorov je superpozícia. Z tohto dôvodu by sa výsledný vektor dal popísať ako lineárna kombinácia bázových vektorov „0“ a „1“, kde by koeficienty α^2 a β^2 výsledného vektoru hovorili, s akou pravdepodobnosťou qubit môže nadobudnúť buď stav „0“ alebo „1“. Uhol θ vyjadruje s akou pravdepodobnosťou je nameraný stav „0“ a „1“. Zmena uhlu φ vyjadruje zmenu fázového posunu, ale vo výsledku neovplyvní do akého stavu („0“ alebo „1“) qubit po zmeraní spadne [17], [18].



Obr. 1.4: Zobrazené bázové vektory na osiach X, Y a výsledný vektor ψ, ktorý je lineárnou kombináciou týchto bázových vektorov

Qubit matematicky môžme vyjadriť ako

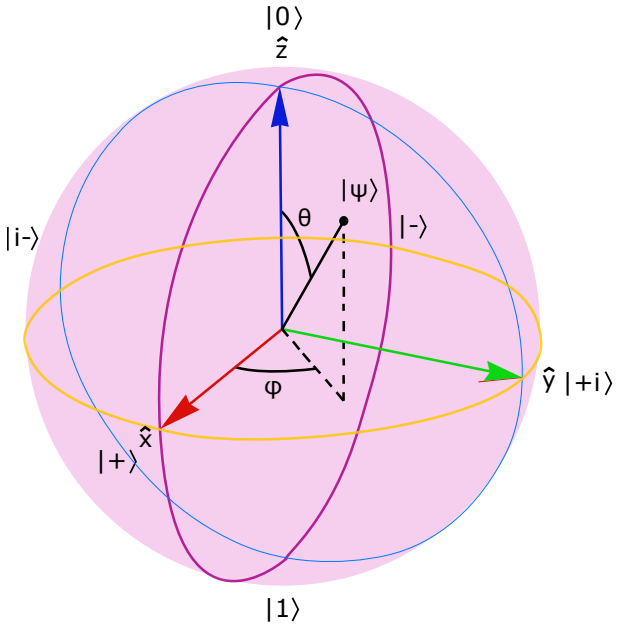
$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle. \tag{1.3}$$

ψ je výsledný stav qubitu a α, β sú amplitúdy a jedná sa o komplexné čísla pravdepodobnosti stavov $|0\rangle$ a $|1\rangle$, viď vzorec. 1.3. Pre tieto veličiny platí, že nakoľko súčet pravdepodobností musí byť vždy rovný 1. Hlavnou výhodou qubitu je, že je schopný uchovávať omnoho viac informácií, ako klasický bit. Pre počítačovú reprezentáciu qubitu sú potrebné 4 čísla typu double (dátový typ pre vyjadrenie kladných a záporných čísel na 20 desatinných miest), pre popísanie oboch komplexných amplitúd [17], [18].

Z kvantovej mechaniky vyplýva, že pokiaľ nie je qubit zmeraný a je v stave superpozície, tak stavy systému sú popísané pomocou amplitúdy pravdepodobnosti hodnoty a nie len pravdepodobnosťou hodnoty. Preto hodnoty môžu nadobúdať záporné aj komplexné čísla. [18].

1.3.2 Blochova sféra

Pre jednoduché zobrazenie pravdepodobností je možné použiť blochovú sféru. Blochová sféra zobrazuje dvojrozmerný Hilbertov priestor roztiahnutý do troch dimenzií [16].



Obr. 1.5: Blochova sféra s výsledným jednotkovým vektorom ψ, ktorý je kombináciou uhlov φ a θ.

$$|\psi\rangle = cos\left(\frac{\theta}{2}\right)|0\rangle + e^{i\varphi}sin\left(\frac{\theta}{2}\right)|1\rangle \tag{1.4}$$

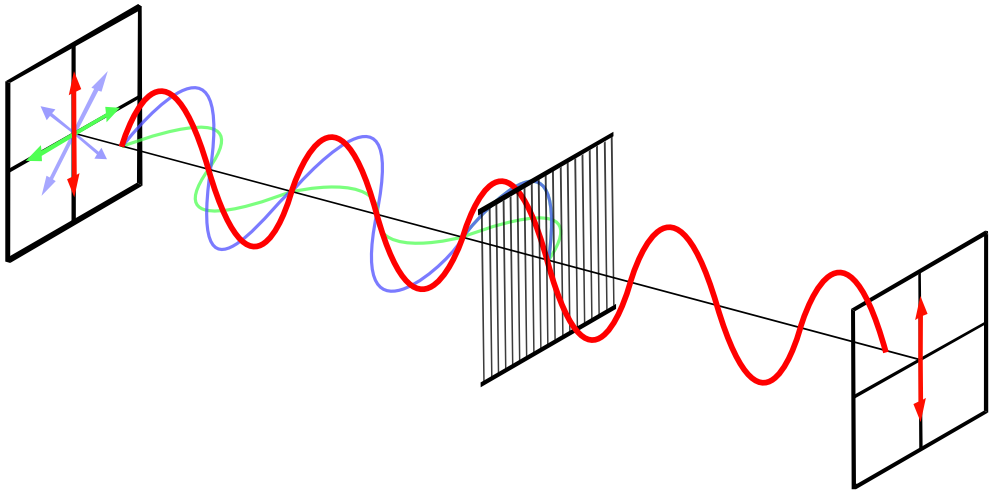
Pre vzťah 1.4 platí, že uhol θ môže nadobúdať hodnoty z intervalu $[0, \pi)$ a φ z $[0, 2\pi)$, tak dokážu pokryť celú blochovu plochu bez opakovania. Vďaka blochovej sfére sme schopní komplikovaný a abstraktný hilbertov priestor zobraziť o niečo jednoduchšie. Stav $|0\rangle$ ktorý, bol pôvodne na osi y sa presunul na os z hore a stav $|1\rangle$ dole. Výsledná pravdepodobnosť je zobrazená ako výsledný vektor ψ. Kombináciou uhlov θ a φ sme schopní vyjadriť akýkoľvek výstupný vektor ψ viď obr. 1.5, [16], [19].

1.4 Meranie qubitu

Ako je už známe, klasický bit je možné prečítať koľko krát chceme, ale qubit je zložitejší z pohľadu, že je na to len jeden pokus. Qubit môže byť reprezentovaný rôznymi časticami, ale pre túto prácu je dôležitý práve fotón [19].

Táto častica svetla reprezentuje qubit, napríklad prostredníctvom polarizácie. Z predchádzajúcich kapitol je známe, že qubit po zmeraní je v stave $|0\rangle$ alebo $|1\rangle$.

Prvý stav $|0\rangle$ bude prezentovaný ako horizontálna (vodorovná) polarizácia a druhý $|1\rangle$ ako vertikálna (zvislá). Polarizácia je vektorová fyzikálna veličina, ktorá hovorí, v akej osi (báze) a ktorým smerom vlna osciluje (kmitá). Jednotlivé fotóny budú prepúšťané cez polarizačný filter, čo je materiál, ktorý prepúšťa fotóny len s danou polarizáciu, viď obr. 1.6, v tomto prípade horizontálnou alebo vertikálnou. Ak je fotón mimo týchto bázových rovín, tak stav fotónu či prejde daným polarizačným filtrom je náhodný. Výsledok nie je úplne náhodný, ale závisí na jednotlivých výsledkoch pravdepodobností a tieto určujú amplitúdy pravdepodobností α a β, viď obr. 1.7.

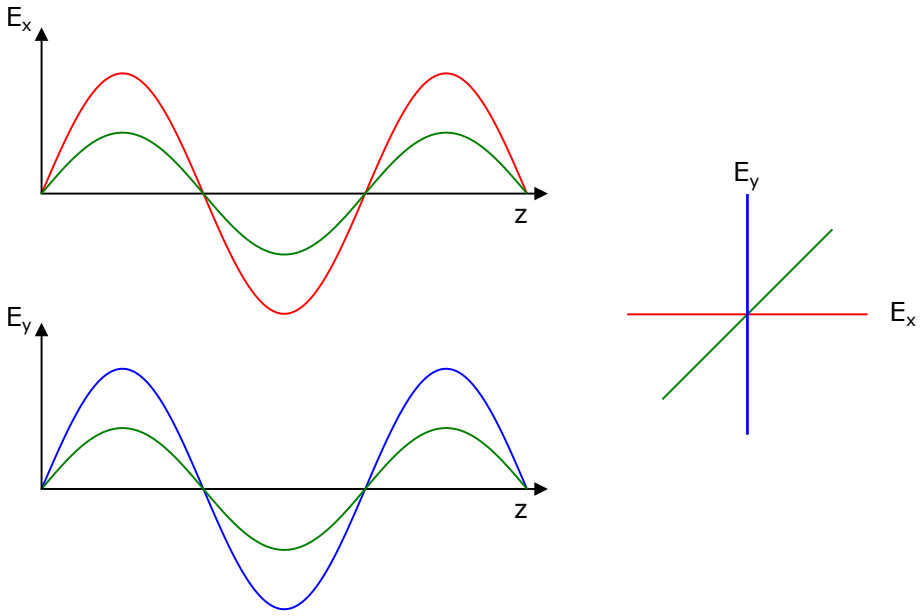


Obr. 1.6: Zobrazenie, funkcie polarizačného filtra ,kde prechádza lúč svetla len ten, ktorý má rovinu šírenia vlny rovnakú ako je rovina polarizačného filtra.

V tomto prípade, keď qubit nie je jednoznačne ani v jednej báze, tak spadne do jedného stavu, a to do stavu $|0\rangle$ s pravdepodobnosťou α^2 alebo do stavu $|1\rangle$ s+ pravdepodobnosťou β^2. Príkladom je, ak postavíme za sebou 2 polarizačné filtre v lineárnej báze rovín $\oplus$ a tieto sú voči sebe otočené o 90° (horizontálny a vertikálny) [19], [20], [23].

Napríklad, prvý filter bude horizontálny a odosielame fotón s horizontálnou polarizáciou. Tento fotón prejde so 100% pravdepodobnosťou, ale cez druhý polarizačný filter (vertikálny) určite nie. Ak by sme poradie filtrov vymenili, tak fotón cez prvý filter nikdy neprejde. Ale ak otočíme polarizáciu prvého polarizačného filtra o 45°(prvý filter je vertikálny otočený o 45° a druhý je horizontálny), tak fotón prvým filtrom niekedy prejde a niekedy nie, záleží na amplitúde pravdepodobnosti. Tým znáhodnil prechod cez druhý filter. Ak polarizovaný fotón dopadá na filter, ktorý nie je voči nemu ortogonálny, exituje pravdepodobnosť prechodu cez tento filter. Inak povedané, fotón polarizovaný v inej rovine ako je polarizačná sa bude chovať ako qubit v superpozícií, kde podľa uhlu natočenia od roviny filtra sa mení amplitúda

pravdepodobnosti. Čím je uhol od roviny väčší až do 90°, tým je pravdepodobnosť prechodu menšia [21], [22], [24].



Obr. 1.7: Zobrazená amplitúda pravdepodobnosti prechodu cez lineárny ⊕ polarizátor. Prevedenie diagonálnej vlny (zelenej) ako kombinácia vĺn vertikálnej E_y a horizontálnej E_x.

Druhá metóda reprezentácie qubitu je vykonávaná prostredníctvom fázového posunu fotónu. Pri meraní sa sleduje, či je interferencia konštruktívna alebo deštruktívna. Interferencia je merané pomocou dvojice detektorov (interferometrov) a tým vzniká bitová informácia. Sledovanie fázového posunu bolo zamýšľané pre entaglované qubity, ale túto metóduje možné využiť aj pre jednotlivé častice. Komunikačné strany využívajú mach zehnderov interferometer, medzi týmito stranami sú natiahnuté 2 optické vlákna a sú využívané fázové modulátory. Strany sa môžu rozhodnúť medzi dvomi fázovými posunmi a to 0 a π (odpovedá horizontálnej a vertikálnej báze) alebo $\pi/2$ a $3\pi/2$ (odpovedá diagonálnej báze). Hlavný problém je udržanie fázového posunu medzi dvomi qubitmi v dvoch dlhých vláknach [22].

Riešením tohto problému je na výstupe interferometru odosielateľa jeden z pulzov nechať prejsť kratšou dráhou (S) a ten druhý nechať prejsť dlhšou (L). Následne tieto dve vlny odoslať za sebou spoločným vláknom. Pre časový odstup vĺn v jednom vlákne sa qubit nazýva „time-bin qubit“. Po príchode k prijímateľovi pulzy rozdelíme, necháme ich prejsť obdobne krátkou a dlhou trasou. Vzniknú 4 pulzy a to SS, SL, LS, LL. SS a LL pulzy zahodíme, nakoľko nie sú podstatné, lebo navzájom neinterferujú. Ostávajúce dva prešli rovnako dlhú trasu a ich vzájomný fázový posun je daný Aliciným fázovým modulátorom. Vzniká buď konštruktívna alebo deštruktívna

interferencia a tým tvoria qubit [22].

Kvantový bit (qubit) je pomerne nestabilný a je náchylný k chybám a vydrží len určitý čas uchovávať svoje originálne nezmenené hodnoty. Tento čas sa nazýva koherenčný čas a ak tento čas uplynie, môže dôjsť k chybám a zmenám vnútorných hodnôt. Funkčnosť qubitu je založená hlavne na základných princípoch kvantovej fyziky a to superpozícia, previazanie (entaglement) a interferencia [19], [22].

1.4.1 Kvantové previazanie

V preklade quantum entaglement je druhom silnej korelácie medzi dvomi časticami (qubitmi), ktoré majú navzájom previazané svoje vlastnosti. O týchto dvoch časticiach hovoríme, že sú navzájom previazané, teda entaglované. Je to možné popísať ako komunikáciu medzi časticami, ktoré si navzájom vymieňajú informácie. Faktom je, že častice môžu byť od seba akokoľvek ďaleko aj tak sú stále previazané. V prípade zasiahnutia do stavu jednej z častíc sa zmenení jej stav a automaticky to ovplyvní aj druhú časticu. Kvantové previazanie si je možné predstaviť napríklad tak, že máme dve zatvorené krabice a v každej jednu guľu, ktorá je v stave modrá aj zelená súčasne. Keď otvoríme jednu krabicu a zmeriame stav jednej častice, tak vieme predpovedať stav druhej. Táto vlastnosť sa dá využiť napríklad pri samo opravných systémoch qubitu alebo sa využívajú ako základný princíp niektorých prenosových protokolov QKD [17], [20].

1.4.2 Interferencia

Tento jav je založený na podstate, že pravdepodobnosť musí byť nezáporná a môže sa s ostatnými len sčítať, naopak amplitúda môže nadobúdať aj záporné čísla, teda sa môže s ostatnými amplitúdami aj odčítať. To môže spôsobiť vzájomné vyrušenie týchto amplitúd (ak sú amplitúdy v proti fáze) a to sa nazýva deštruktívna interferencia. V prípade ak sa amplitúdy navzájom posilňujú, vzniká konštruktívna interferencia. Táto interferencia úzko súvisí so superpozíciou a meraním kvantového stavu. Keď sa uskutoční meranie qubitu, nastane deštruktívna interferencia a pokiaľ sa qubit nachádza v bázovom stave, je istý jeden zo stavov. Ak sa však v takomto stave nenachádza, tak stav je vybraný podľa pravdepodobnosti α^2 alebo β^2 [17], [25].

1.4.3 Neklonovací teorém

Tvrdí, že ľubovoľný kvantový stav nie je možné identicky skopírovať bez toho, aby sme poznali jeho stav už predtým. Napríklad základom pre jednofotónovú kryptografiu je práve tento teorém. Táto jednoduchá vlastnosť má veľký dopad v takýchto

systémoch. Z pohľadu bezpečnosti nie je možné skopírovať qubit alebo ho prečítať bez jeho zničenia. Tým pádom to druhá strana hneď zistí [22].

Nevýhodou tejto vlastnosti je napríklad to, že nie je možné si priebežne kontrolovať jeho stav. Taktiež možnosť uchovávať qubit v dočasnej pamäti alebo jednoduché opakovače (repeater), ktoré nemôžu kvôli tomuto teorému len tak zosilniť qubit a poslať ho ďalej [22].

1.4.4 Kvantová superpozícia

Superpozíciou môžme nazvať stavom, kde každý kvantový stav je možné vyjadriť ako kombinácia dvoch alebo viacerých odlišných stavov. Matematicky je princíp superpozície popísaný pomocou Schrödingerovej rovnice. Nakoľko je táto rovnica lineárna, jej riešenie bude tiež akákoľvek lineárna kombinácia jej riešení. Napríklad určitá častica sa nachádza vo viacerých stavoch súčasne, pokiaľ neprebehne jej meranie. To však neznamená, že bude nameraná priamo superpozícia, ale len stav častice. Pretože ak začneme meranie, častica bude narušená a následne spadne do jedného z možných stavov podľa pravdepodobnosti jednotlivých stavov. Z tohto dôvodu je potrebné systém zabezpečiť tak, aby čo najviac pôsobil proti vonkajším vplyvom tak, aby nenarušili superpozíciu. Aby bol udržaný a neovplyvnený kvantový stav je potrebné tento systém izolovať od okolia. V prípade ak systém nie je dostatočne izolovaný, vzniká dekoherencia. To znamená, že systém je v kontakte s vonkajšími vplyvmi a tým zanikajú kvantové vlastnosti. Kvantový stav môže dekoherovať okrem interakcie s okolím aj kvôli kolísavým zmenám teploty, vibráciám alebo okolitému elektromagnetickému vplyvu [4], [26].

1.5 Úvod do QKD

Skratka QKD znamená Quantum Key Distribution, v preklade kvantová distribúcia kľúčov. Taktiež je to jedno z odvetví kvantových sieti. Slovo kvantum pochádza z latinského slova quantus a má význam minimálneho množstva energie pri akejkoľvek interakcií. Hypotéza kvantovania pojednáva o tom, že akákoľvek fyzikálna vlastnosť môže nadobúdať len diskrétne celočíselné hodnoty v násobkoch jedného kvanta. V kvantovej fyzike sa namiesto determinizmu viac spolieha na pravdepodobnosť [28].

V QKD ako nositeľ informácie je používaná elementárna častica fotón. Technika pre generovanie kľúčov na kvantovej úrovni a ich prenos prostredníctvom fotónov sa označuje ako proces kvantovej distribúcie kľúčov. Niekedy je QKD nesprávne označované ako kvantová kryptografia, nakoľko QKD využíva kvantovú kryptografiu a je jej súčasťou. Kvantová distribúcia kľúčov je metóda generovania a distribuovania

kľúčov, ktorá využíva princípy kvantovej fyziky. Ako je známe, v základe existujú dve moderné základné metódy pre šifrovanie a to symetrické a asymetrické. Práve QKD poskytuje prostriedky pre distribúciu symetrických kľúčov [27], [28], [29].

Stručne povedané, že pri metóde QKD je kľúč pre zabezpečenie správy zaslaný pomocou individuálnych fotónov v stave kvantovej superpozície. Podstatou QKD je využitie kvantovej kryptografie pre bezpečné prenesenie kľúča, čo zaisťuje kvantová mechanika [29].

QKD je doplnková technológia a služba pre komunikačné siete. Pre jej funkciu sú nevyhnutne prenosové kanály, ako kvantový kanál typu bod-bod (point to point, skrátene P2P) pre prenos Qubitov. QKD sieť (QKD network, skrátene QKDN) je technológia, ktorá zvyšuje dosah a dostupnosť QKD. Zavedenie QKDN do už funkčných sieti nie je úplne jednoduché a prináša veľké výzvy z pohľadu návrhu architektúry a bezpečnosti. Preto je veľmi dôležité aby boli stanovené štandardy ako používať QKD v sieťach [27], [28], [29].

1.5.1 História

V prvej polovici 20. storočia Claude Shannon uverejnil informačno teoretickú bázu (myšlienku) pre zabezpečenie a utajenie správy. Tá je založená na tvrdení, že miera neistoty (entropia), ktorú je možné vložiť do správy, nesmie byť väčšia ako miera kryptografického kľúča použitého na jej zakódovanie. Pre úplne utajenie je nevyhnutné, aby kľúč bol minimálne taký dlhý, ako správa, ktorá má byť zabezpečená. Ďalšou podmienkou je, že tento kľúč sa nesmie opakovane používať. Preto je použitá Vernamova šifra. V praxi bezpečne distribuovať úplne náhodný kľuč je veľmi ťažké. Preto sa táto metóda neujala [30].

V 70. rokoch 20. storočia boli objavené kryptografické metódy, založené na výpočtovej zložitosti vedcami, ako napríklad Martin Hellman, Whitfield Diffie a ďalší. Tieto metódy sa spoliehajú na to, že útočníci nemajú neobmedzený matematický výpočtový výkon. Najznámejšia z týchto metód je algoritmus RSA, ktorý je založený na princípe faktorizácie čísel. Je jednoduché vynásobiť dve prvočísla, ale zistiť z výsledku čísla, ktorými bol výsledok vynásobený je veľmi náročné. Avšak nikto tieto predpoklady nepreukázal. Známa je taktiež Diffie-Hellmanova výmena kľúčov, ktorá slúži pre vytvorenie bezpečného spojenia pre výmenu kľúčov cez nezabezpečený kanál [30], [31].

Tieto techniky verejného kľúča sa využívajú veľmi často a fungujú na predpoklade, že niektoré matematické funkcie je jednoduché a možné vykonať jedným smerom, ale veľmi ťažké až nemožné je urobiť ich v opačnom smere a vrátiť späť v primeranom čase [30].

V roku 1984 Charles Bennet and Giles Brassard prišli s úplne inou myšlienkou

na metódu zabezpečenia. Bezpečnosť by mala mať radšej základy vo fyzikálnych zákonoch, ako v komplexných matematických výpočtoch. Myšlienka predstavovala zariadenie spolu so špeciálnym kryptografickým protokolom, ktoré dokáže vytvoriť tok náhodných bitov. Tieto bity zostanú tretej strane neznáme a v prípade útoku bude útočník rýchlo a jednoducho odhalený. Po úspešnom prenose tieto náhodné bity budú použité ako kľúč pre Vernamovu šifru na zabezpečenie správ. Týmto môžeme jednoducho dosiahnuť Shanonovu informačnú teóriu pre úplne zabezpečenie správy. Táto myšlienka je základ pre QKD, ktorá oproti konvenčným systémom, ktoré sa spoliehajú na zložité matematické výpočty, využíva fyzikálne zákony [30].

1.5.2 Princíp

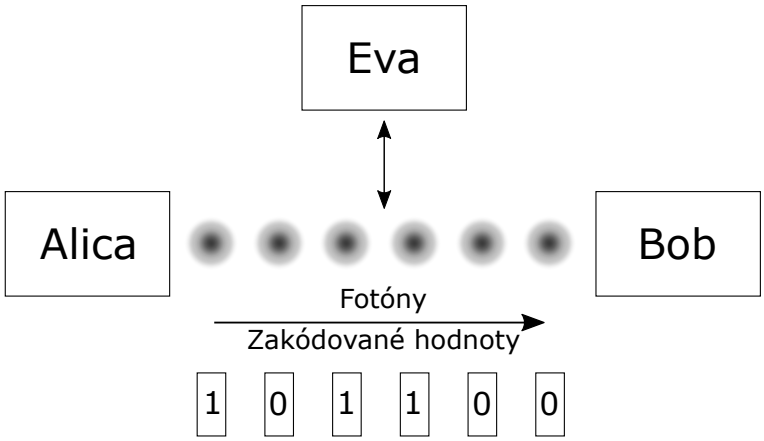
Prenos kvantovej informácie môže byť realizovaný dvomi spôsobmi. Jedným z nich je prenos prostredníctvom optického káblu. Tento druh prenosu je veľmi bežný pre prenos veľkého množstva používateľských dát, kde straty sú úplne bežné a čim je väčšia vzdialenosť, tým sú tie straty väčšie. V prípade QKD môže táto situácia spôsobiť problém, nakoľko samotné fotóny sú nositeľom informácie [14].

Druhou možnosťou je bezdrôtový prenos, ktorý využíva na bežný prenos mikrovlnné frekvencie. Problém je, že fotóny z mikrovlnných frekvencií majú menšiu energiu ako fotóny optické a dnešné technológie na to nie sú pripravené. Jeden z možných spôsobov využitia sú družice a pre toto spojenie je možné použiť optické fotóny. Nakoľko medzi povrchom zeme a družicou nie je veľké množstvo atmosféry, budúcnosť pre diaľkove prenosy by mohla smerovať práve týmto smerom [14].

QKD je riešením jedného z aktuálnych zabezpečovacích problémov, a to ako bezpečne preniesť šifrovací/dešifrovací kľúč tak, aby bola zaručená integrita s istotou, že ju nezíska tretia strana. Ďalšou jeho výhodou je, že pokiaľ je komunikácia odpočúvaná, je to jednoducho detegovateľné a je možné sa ochrániť príslušnými opatreniami. Pre tieto prípady je využívaná jeden z princípov kvantovej mechaniky, a to tá, že ak prebieha meranie, tak to nenávratne naruší systém. Každá technológia však má svoje nedostatky a metódy ako ju napadnúť [14].

QKD umožní dvom komunikačným stranám vytvoriť spoločný náhodný tajný šifrovací a dešifrovací kľúč. Komunikačné strany budú Alice, ktorá posiela tajnú správu a Bob, ktorý je prijímateľom tejto správy. Obe strany musia mať QKD modul. Posledná je Eva, ktorá je odpočúvajúcim útočníkom [30].

Ide o techniku dohody medzi Alicou a Bobom o zdieľaní náhodnej sekvencie bitov (tajného kľúču) medzi dvomi zariadeniami, kde odpočúvajúca Eva má veľmi malú pravdepodobnosť odpočúvať a úspešne získať tajný kľuč bez odhalenia. QKD nie je kryptosystém, ale je to bezpečná metóda výmeny kľúčov, ako napríklad Diffie-Hellman [30], [31].



Obr. 1.8: Základný princíp myšlienky fungovania QKD medzi Alicou a Bobom s odpočúvajúcou Evou

QKD je veľmi komplexná oblasť, kde existuje veľa prístupov a schém, ako môže daný systém fungovať.

Princíp QKD je zobrazený na obr. 1.8. Alica pošle Bobovi sériu fotónov, kde každý je modulovaný náhodnou hodnotou (qubity). Príkladom je, že Alica pošle Bobovi kartu, kde je náhodne na jednej strane „1“ a na druhej „0“. Ak si Bob prečíta rovnakú stranu ako Alica, tak majú obaja rovnakú hodnotu, ale ak si Bob vyberie druhú stranu, tak si náhodne vyberie „0“ alebo „1“ (náhodou sa môže trafiť do čísla, ktoré Alica posielala, ale na to sa nemožno vždy spoliehať) [30].

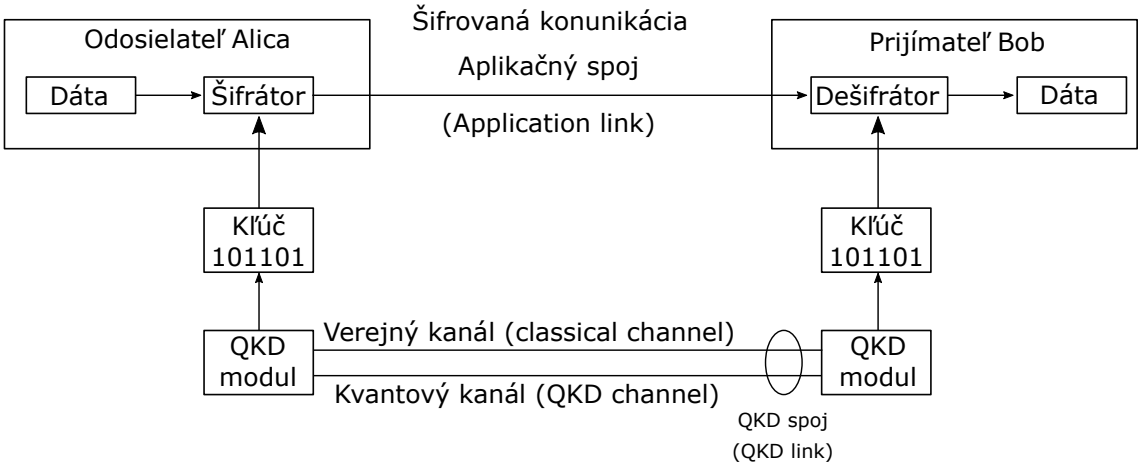
Keď Alica odošle všetky fotóny a Bob ich všetky prečíta, tak vykonajú takzvanú „Sifting transaction“ ako súčasť „Post processing“, kde si navzájom oznámia len informáciu, ktoré strany karty čítali (nie aké hodnoty prečítali). Zahodia všetky karty, ktoré neboli vybrané správne a zostávajúce karty tvoria sled jednotiek a núl, ktoré sa použijú ako surový kľuč. Všetky chyby a únik údajov sa odstránia počas fázy opravy chýb (error correction phase) a pri následných krokoch po spracovaní (post processing phase). Ďalším krokom po spracovaní je aj oneskorené zosilnenie súkromia (privacy amplification), a ten ktorý odstraňuje všetky pozostatky informácií o tajnom kľúči, ktoré by Eva mohla získať [30].

1.6 Technológia

Pre bežnú implementáciu QKD zahrňuje tri základné komponenty.

- Kvantový kanál (quantum channel) buď optický kábel alebo bezdrôtový prenos slúži pre odoslanie kvantových stavov fotónov (qubity), v ktorých sa prenáša náhodná sekvencia bitov od odosielateľa (Alica) k prijímateľovi (Bob). Tento kanál nemusí byť zabezpečený.

- Overený verejný komunikačný kanál (classical channel) medzi komunikačnými stranami. Jeho dôležitou úlohou je zabezpečiť synchronizáciu a výmenu dát medzi modulmi QKD. Aby mohli tieto strany uskutočniť „Post processing steps“ a mohli vygenerovať správny a tajný kľuč.
- Protokol pre výmenu kľúčov, ktorý využíva vlastnosti kvantovej mechaniky pre zaistenie bezpečnosti detegovaním odpočúvania alebo chýb a výpočtom množstva informácií, ktoré boli zachytené alebo stratené) [32].



Obr. 1.9: Základná schéma zostrojenia QKD medzi Alicou a Bobom

Obr. 1.9 znázorňuje zabezpečenie aplikačného (komunikačného) spojenia medzi koncovými stanicami. Moduly QKD generujú kľúče navzájom si ich vymieňajú a následne ich poskytujú pre zabezpečenie aplikačných správ (akékoľvek komunikačné spojenie). Na obr. 1.9 je vidieť, že QKD je doplnkovou technológiou pre bezpečnú výmenu kľúčov v sieti (existujúcej alebo budúcej) [33]. Pre kvantový kanál sú dôležité faktory ako straty kvôli vzdialenosti (distance loss), „galloping loss“ a straty pri prenose (connection loss), ktoré ovplyvňujú dôležitý parameter rýchlosť prenosu qubitov (qubit rate). Výkon klasického kanálu ovplyvňuje stabilita, hustota prenosu (data traffic) a metóda šifrovania (encryption method).

Aby mohol šifrátor, ktorý zašifruje/dešifruje správu pomocou tajného kľúča komunikovať s QKD modulom, musí obsahovať štandardizované rozhranie „key Delivery API“ od Európskeho inštitútu pre telekomunikačné normy (ETSI).

Toto rozhranie pre programovanie aplikácií (API) na doručovanie kľúčov (key delivery) je REST-API, a tým zabezpečuje komunikáciu jednoduchými volaniami a odpoveďami medzi kryptografickými aplikáciami a správou kľúčov (Key management, skrátene KM). Aplikácie požadujú od KM kľúče a KM ich dodáva. Volania API na KM sú majú byť realizované aplikáciami, pričom je potrebné, aby boli prítomné v rovnakej sieti ako KM, ku ktorému sa pripájajú. QKD sieť dokáže poskytovať

zdieľanie kľúča pre aplikácie v rôznych lokalitách. V prípade, ak sa nevyužíva toto rozhranie, môžu byť použité protokoly ako modbus a niekedy KMIP [35].

1.7 QKDN

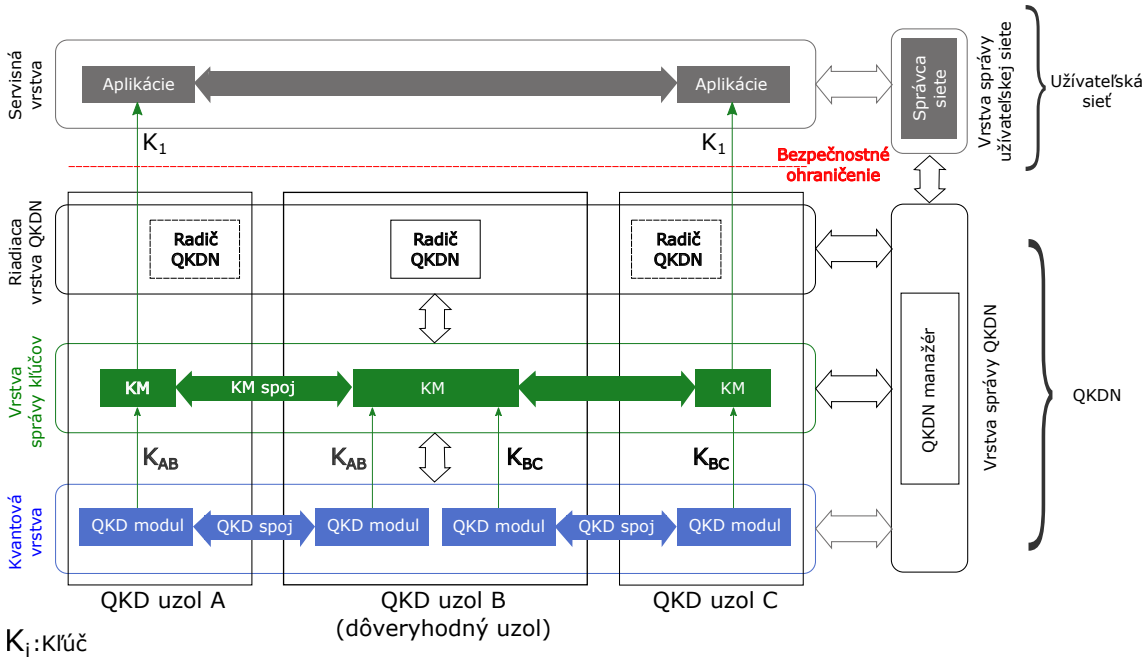
V čisto kvantovej sieti sa informácie uchovávajú v kvantovej podobe v QKD uzloch aj počas prenosu, čím sa zaisťuje ich ochrana. Kvantový opakovač distribuuje medzi stanicami previazanie (entaglované), a to by predstavovalo ideálne riešenie pre rozširovanie dosahu QKD bez potreby dôveryhodných uzlov. Technológia kvantového opakovača vyžaduje technológie kvantovej pamäte alebo kvantovej korekcie chýb, ktoré nie sú k dispozícii pre praktickú implementáciu so súčasnými technológiami.

Key relay je metóda na zdieľanie kľúčov medzi ľubovoľnými QKD uzlami cez pomocné QKD uzly. QKD link je tvorená z kvantového kanálu na prenos kvantových signálov a klasického kanálu na výmenu synchronizačných informácií a informácií použitých pri generovaní a overovaní kľúča [34].

Relay point ako QKD uzol slúži pre rozšírenie dosahu QKD, ale nemusí byť dôveryhodný(trusterd) ako QKD node. Tento relay point slúži ako detektor, ktorý využíva protokoly MDI, TF. Práve MDI QKD odstraňuje potrebu bezpečnej detekčnej stanice, ktorá je najväčšou zraniteľnosťou systému QKD [34].

QKDN vzniká prepojením viacerých QKD uzlov (QKD node), ktorý môže obsahovať viac QKD modulov, napríklad za účelom zvýšenia dosahu alebo spojením viacerých užívateľov v rámci rôznych topológií. Dôležité však je, že kvantové spojenie môže byť vždy len P2P (bod-bod), nakoľko Qubit nie je možné ukladať ani kopírovať. Hlavnou úlohou QKDN je zvýšenie bezpečnosti komunikácie. Jeden zo základných postupov je spájanie QKD liniek (QKD links) cez QKD uzly (QKD nodes), za účelom zdieľania bezpečných kľúčov medzi zvolenými QKD uzlami, aj keď nie sú priamo spojené QKD linkou, a tým dodávať kľúče kryptografickým aplikáciám používateľov, ktorí potrebujú zabezpečiť údaje pomocou kľúča v sieti používateľa. Za účelom realizácie bezpečného zdieľania kľúčov je potrebné, aby bol kľúč prenášaný od jedného uzla k ďalšiemu s vlastným kľúčom, pokiaľ je doručený do cieľového uzla. Kľúče by potom mali byť uložené v QKD uzle, použité pri prenose kľúčov (Key relay) a následne doručené kryptografickej aplikácii. Celá operácia je označovaná ako manažment kľúčov (Key Managment). Pre QKDN je kľúčové, že QKD uzle sú dôveryhodné v zmysle zabezpečenia proti vniknutiu a pred útokmi neoprávnených strán [34].

Obr. 1.10 zobrazuje štruktúru QKDN pripojenú k používateľskej sieti. V každom QKD uzle (QKD node) sa nachádza jeden alebo viac QKD modulov (QKD module), ale aj správa kľúčov (key managment). Pár QKD modulov je spojený pomocou QKD spoja (QKD link) a tieto spoje sú zreťazené pomocou QKD uzlov. Správy kľúčov



Obr. 1.10: Štruktúra QKDN a jej vrstvy

v QKD uzloch sú spojené pomocou KM spoja (KM link). Tento poskytuje funkcie pre správu kľúčov a schopnosť manipulovať s týmito kľúčmi a následne ich presúvať. Všetky tieto časti sú riadené pomocou QKDN radiča (QKDN controller) a taktiež dokáže ovládať trasy „kay relay“. Správa kľúčov poskytuje kľúče používateľom, ktorí ich potrebujú pre zabezpečenie komunikácie kryptografických aplikácií (aplications) medzi týmito používateľmi. KM tiež zahŕňa funkciu „key supply“, ktorá má na starosti poskytnutie kľúčov kryptografickým aplikáciám (aplications) [34].

Komunikácia začína požiadavkou kryptografických aplikácií používateľov o kľúče od správy kľúčov (KM). KM dodáva kľúče v presnom a bezpečnom formáte. Prenos dát medzi aplikáciami je zabezpečený kľúčami dodanými od KM a prebieha prostredníctvom aplikačného spoja (application link). Tieto kľúče môžu byt použité aj na overenie totožnosti, atď. Akonáhle aplikácie prevezmú kľúč, sú zaňho zodpovedné a QKDN ho zmaže alebo uchová podľa toho, ako je nastavený kľúčový manažment [34].

1.7.1 QKDN vrstvy

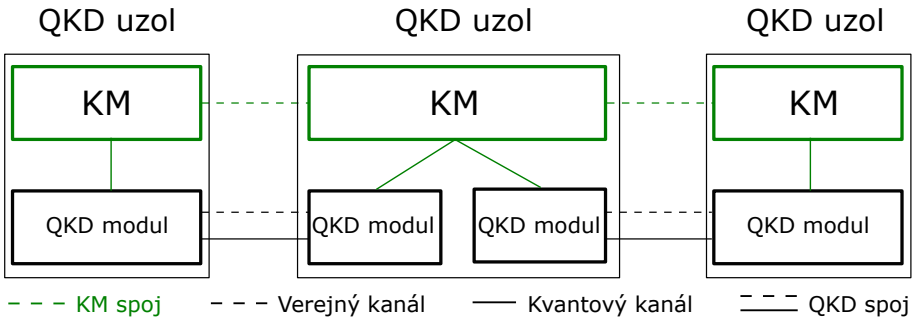
Na obr. 1.10 bola popísaná štruktúra QKDN, ktorá sa skladá z kvantovej vrstvy (quantum layer) (úplne dole), vrstvy správy kľúčov (key managment layer), riadiacej vrstvy QKDN (QKDN control layer) a správa vrstvy QKDN (QKDN management layer). Užívateľská sieť je popísaná vrstvou služieb (service layer) a vrstvou riadenia siete používateľov (user network management layer) [34].

Kvantová vrstva

Táto vrstva je umiestnená v modeli QKDN úplne dole. Na kvantovej vrstve QKD si moduly vymieňajú náhodný sled bitov (kľúče) prostredníctvom QKD spoja. QKD spoj obsahuje 2 kanály. Prvý kanál je fyzické optické spojenie nazývany kvantový kanál a druhý je logické spojenie nazývaný verejný kanál (classical channel), ktorý sa môže skladať z viacerých spojov slúžiacich pre synchronizáciu a triedenie kľúčov. Každý QKD modul prijatú bitovú sekvenciu zdieľa správe kľúčov, ktorá sa nachádza v rovnakom QKD uzle. Úlohou každého uzlu QKD je posielať svojmu správcovi QKDN (QKDN manager) parametre spojenia, ako je napríklad kvantová bitová chybovosť (QBER) [34].

Vrstva správy kľúčov

Na tejto vrstve je v každom uzle QKD umiestnený KM a sú navzájom prepojené KM spojom (KM link). KM vykonávajú správu kľúčov. Po prijatí náhodnej sekvencie bitov od QKD modulu v tom istom uzle, ich synchronizuje, formátuje a následne uloží ako kľúče, ktoré môže neskôr distribuovať. KM dostáva žiadosti o kľúče od kryptografických aplikácií a odosiela vo vhodnom formáte týmto aplikáciám žiadané množstvo kľúčov, ktoré sú synchronizované, autentizované vďaka KM spoju (KM link). KM spoje sú logické a existujú medzi ľubovolným párom QKD uzlov. V prípade, ak medzi komunikujúcimi stranami nie je priame spojenie KM, tak by mali zdieľať potrebné množstvo kľúčov prostredníctvom key relay. Vtedy KM požiada QKDN controler o vhodnú prenosovú trasu. KM má tiež na starosti sledovať životné cykly kľúčov.



Obr. 1.11: Štruktúra spojenia na kvantovej a kľúčovej vrstve cez dôveryhodný uzol.

KM má na starosti veľkosti kľúčov, ich formátovanie a ukladanie a získanie parametrov QKD spojov, ako je QBER, key rate, status spojenia, atď. Bezpečný prenos kľúčov cez KM spojenia má na starosti napríklad OTP (One Time Pad) šifrovanie, ktoré využíva iný kľúč pre zabezpečenie pôvodného kľúča.

Príkladom je obr. 1.10, kde je odosielaný kľúč z uzla A do uzla C. Kľúč K_1 je znázornený ako K_{ab} a je generovaný medzi uzlami A a B. V uzle B je K_{ab} zašifrovaný OTP pomocou K_{bc} a odoslaný do uzlu C.

Druhá možnosť je, že v A sa vytvorí náhodná bitová sekvencia K_{RN}, ktorá bude zakódovaná OTP pomocou K_{ab}. Následne rozšifrovaná v uzle B a znova zašifrovaná pomocou K_{bc} a odoslaná do uzlu C, kde bude znova dešifrovaná [34].

Riadiaca vrstva QKDN

Táto vrstva poskytuje kontrolné funkcie pre QKDN. Jedna z funkcií je riadenie smerovania key relay, riadenie QKD spojov a KM spojov riadenie autorizácie a autentizácie alebo kontrola politiky QoS [34].

Vrstva správy QKDN

Správca QKDN (QKDN manager) monitoruje a spravuje QKDN ako celok. Jeho úlohy sú napríklad správa chýb, konfigurácie, výkonu a bezpečnosti. Správca zbiera a monitoruje informácie o výkone QKD modulov a QKD spojov na kvantovej vrstve a taktiež informácie o správe kľúčov na vrstve správy kľúčov [34].

Servisná správa

V tejto vrstve sú umiestnené kryptografické aplikácie používateľov, ktoré dostávajú kľúče od KM a následné šifrujú alebo dešifrujú dáta. Tým zabezpečia bežnú komunikáciu medzi používateľmi prostredníctvom aplikačných spojov (application link) [34].

Vrstva správy užívateľskej siete

Funkcie v tejto vrstve spravujú manažment a riadenie virtualizovaných a nevirtualizovaných zdrojov v sieti používateľa [34].

1.7.2 Implementácie

QKD je jedna z kvantových technológií, ktoré boli už komercializované a sú dostupné na trhu. Obchodné spoločnosti, ktoré ich ponúkajú sú napríklad ID Quantique, Toshiba, QuintessenceLabs a MagiQ Technologies Inc. [36].

- **Quantum Xchange** v spolupráci s Toshiba vybudovali sieť medzi Wall Streetom a kanceláriami bankových inštitúcií v New Jersey
- **ID Quantique** implementoval QKD pre Ženevskú vládu pre potreby volieb medzi centrálnym dátovým centrom a centrálnym volebným systémom
- **SK Telecom** pracuje na implementácii QKD pre budúce 5G siete [29].

- V roku 2018 ponúkol **Quantum Xchange** 1000 km optického káblu a 19 colo centier a hub-ov na trase Boston, MA - Washington, D.C., čím spustil 1. kvantovú sieť v USA.
- Vo februári 2019 vydal **ETSI** štandard, ktorý poskytuje štandardné rozhranie pre zariadenia a aplikácie na prijímanie kvantových kľúčov, čím uľahčil zavádzanie nových QKD systémov [36].

Hlavnými výskumnými skupinami sú napríklad:

- **Quantum Technologies Group & Quantum Experiments and the Foundations of Physics Group**. V roku 1998 uskutočnili, ako prví na celom svete, kryptografický systém založený na previazaných fotónoch [37].
- **NIST Quantum Information Networks Group**. Skupina vykonáva vývoj a výskum v kvantovej komunikácii a v pridružených oblasti záujmu, s dôrazom na využitie v informačných technológiách. Skupina dokázala predviesť vysoko rýchlostný zabezpečovací systém, ktorý využíva OTP šifru a dokázali ho rozšíriť na sieť o troch QKD uzloch [37].
- **LMU Group**. Pracovná skupina sa venuje experimentálnej implementácii distribúcie kvantového kľúča protokolu typu Bennett-Brassard 1984 (BB84), cez 144 km bezdrôtovú linku, s využitím slabých koherentných pulzov laseru. Bezpečnosť bola zaistená využitím decoy-state analýzy. Daná implementácia umožnila distribuovať kľúč rýchlosťou 12,8 bps pri útlme cca. 35 dB [37].

1.8 Protokoly

Komunikačné protokoly predpokladajú, že komunikačné strany sú spojené dvomi komunikačnými kanálmi, a to klasickým kanálom, ktorý slúži na autentifikovanú komunikáciu o prenose qubitov a uzavretí dohody o zdieľanom tajnom kľúči. Druhý je kvantový kanál, ktorý je výhradne používaný na prenos qubitov [38]. Komunikácia v kvantovom kanále využíva princípy kvantovej mechaniky, ktoré vyžadujú vývoj nových komunikačných protokolov [3].

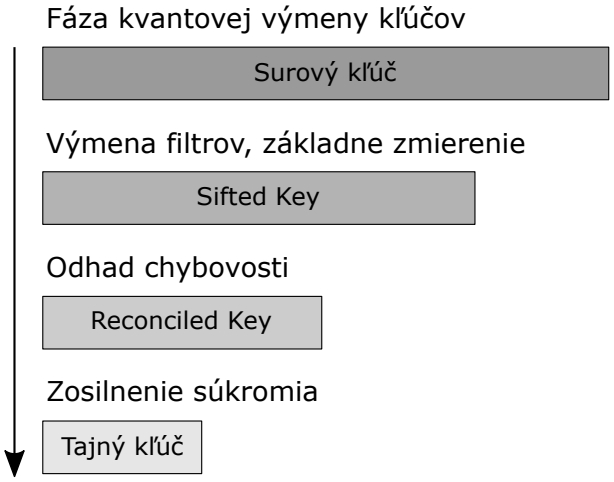
Kryptografické protokoly, využívané v QKD, umožňujú distribúciu náhodných symetrických reťazcov a bitov, ktoré vystupujú ako tajné zabezpečovacie kľúče. Je možné dokázať, že tieto kľúče sú bezpečné, a to aj v prípade, ak by mal útočník pri odpočúvaní neobmedzene veľký výpočtový výkon. Takáto úroveň bezpečnosti sa nazýva teoretická informačná bezpečnosť (information theoretic security). Protokoly QKD implementujú kľúče (qubity) generované QKD modulmi a môžu byť využité akoukoľvek kryptografickou aplikáciou, ktorá využíva symetrické kľúče. Takýmito aplikáciami sú napríklad šifra OTP, pokročilejší šifrovací štandard AES alebo autentifikácia pomocou hašovacieho autentifikačného kódu správy HMAC (keyed-Hash Message Authentication Code) [34].

Problematika sa dá opísať cestou komunikačných strán, ako odosielateľ Alica, prijímateľ Bob a odpočúvajúca Eva, ktorá má prístup k obom komunikačným kanálom. Typický protokol QKD má 8 stupňov.

1. Generovanie náhodných čísiel od Alice.
2. Kvantová komunikácia.
3. Preosievanie (Sifting) (základné zmierenie).
4. Zmierenie (Reconciliation).
5. Odhad či a koľko mohla Eva získať informácií.
6. Zosilnenie súkromia (Privacy amplification).
7. Autentifikácia verejných správ (Authentication of public messages).
8. Potvrdenie kľúča (Key confirmation).

Alica vygeneruje sled náhodných bitov buď z hardvérového alebo softvérového generátora náhodných čísiel. Krok 2 tieto bity zakóduje príslušným QKD protokolom do kvantových stavov (qubitov) a odošle ich Bobovi cez kvantový kanál, ako svetelný signál. Bob zmeria každý prijatý fotón a pridelí mu hodnotu [40].

Následne si Bob a Alica vymenia cez verejný kanál len informácie, v ktorých časových intervaloch detegovali fotóny a akým spôsobom ich merali. Tieto kľúče sú známe ako „raw keys“. Po výmene týchto informácii si vyberú svoje kľúče a prichádza „sifting phase“, kde si vymenia náhodne kľúče pre kontrolu odpočúvania, ktoré sa nazývajú „sifting key“. V ideálnom prípade by všetky odoslané kľúče perfektne korelovaný [40]. V praxi nie je možné, aby Alicin kľuč bol úplne kolorovaný



Obr. 1.12: Dĺžka kľúča pri jednotlivých krokoch spracovávania.

(totožný) s Bobovým. Počas prenosu vznikajú chyby, rôznymi druhmi útokov, pri čítaní, šum detektora alebo iné chyby pri čítaní qubitov. Chybovosť býva približne od 1 až 5 %. Tieto chyby musia byť lokalizované a opravené. Bob overí (reconcile) jeho kľuč s Aliciným pomocou „error correction method“ cez verejný kanál. Počas

overovania cez verejný kanál mohol útočník odpočúvať a zachytiť časť kľúču [40].

Z počtu chýb, ktoré Alica a Bob nájdu v Bobovom „sifting phase“ určia chybovosť, a ak chybovosť dosahuje určitú hodnotu, môžu z toho usúdiť, s akou pravdepodobnosťou bola konverzácia odpočúvaná Evou. Kvantová mechanika zaručuje, že Evine meranie bude tiež úplne náhodné, tzn. že zanesie chybovosť do prenosu, nakoľko je takmer nemožné, aby určila presne ten istý kľúč, ktorý bol odosielaný Alicou [40].

Potom sa vykoná „privacy amplification“, ktorá slúži pre odstránenie možnosti, že by Eva mohla zneužiť informácie, ktoré získala počas prenosu kľúčov cez verejný kanál. Eva má takmer nulovú vedomosť o výsledných bitoch kľúča, ktoré Alica a Bob používajú. Fáza „privacy amplification“ slúži na symetrické skracovanie kľúča, ktorý si Alica a Bob vymenili. Preto táto fáza pracuje s bitmi kľúča, ktorý sa postupne skracuje, aby znížila počet informácii, ktoré Eva odchytila a mohla by využiť. Samotný algoritmus je založený na hashovacich funkciách rodiny universal$_2$ a postupne skracuje kľúč, ktorý je zdieľaný medzi Alicou a Bobom [3] [41]. Týmto krokom sa získa posledná verzia zdieľaného, overeného a potvrdeného tajného kľúča medzi Alicou a Bobom. Na obr. 1.12 je znázornené skracovanie dĺžky kľúča od výmeny surového kľúča až po dohodnutý zdieľaný kľúč [40].

Kroky „sifting“, „reconciliation“ a „privacy amplification“ sa ako celok nazývajú „post-processing phase“, ktorého úlohou je hlavne legitimácia komunikujúcich strán, sledovanie odpočúvania a opravenie alebo potvrdenie tajného zdieľaného kľúča [3] [40].

1.8.1 Delenie protokolov

Poznáme dva spôsoby, ako je možné deliť protokoly. Hlavný spôsob je určený podľa toho, či je protokol založený na príprave a meraní (prepare and measure based) alebo je založený na kvantovom previazaní (Bellovom teoréme). Druhý spôsob delenia je podľa toho, či je informácia zakódovaná vo fotóne diskrétne (discrete) alebo spojito (continous) [38]. Do tejto skupiny patrí aj „Distributed Phase Reference“ skrátene DPR.

Spôsob merania

Protokol založený na **príprave a meraní** sa tak nazýva, pretože odosielateľ musí informácie pripraviť vo forme polarizácie fotónu a následne ho prijímateľ musí zmerať. Tieto QKD protokoly využívajú Heisenbergov princíp neurčitosti, kde sa spoliehajú, že nie je možne zmerať kvantový stav systému bez toho, aby sme ho nenarušili. Taktiež sa spoliehajú na neklonovací teorém, ktorý hovorí, že qubit nie je možné kopírovať alebo zosilniť. Tento mechanizmus umožňuje detegovať prítomnosť Evy

pomocou parametru chybovosti, ktorá vzniká počas prenosu. Sú to protokoly napríklad BB84, B92, Six State Protocol (SSP), SARG04, S13 [38].

Medzitým protokol založený na **previazaní** využíva na prenos tajného kľúča kvantové previazanie fotónov. Protokoly, ktoré využívajú tento princíp sú napríklad E91, BBM92, DPS, Coherent One Way (COW) [38].

Spôsob zakódovania premennej

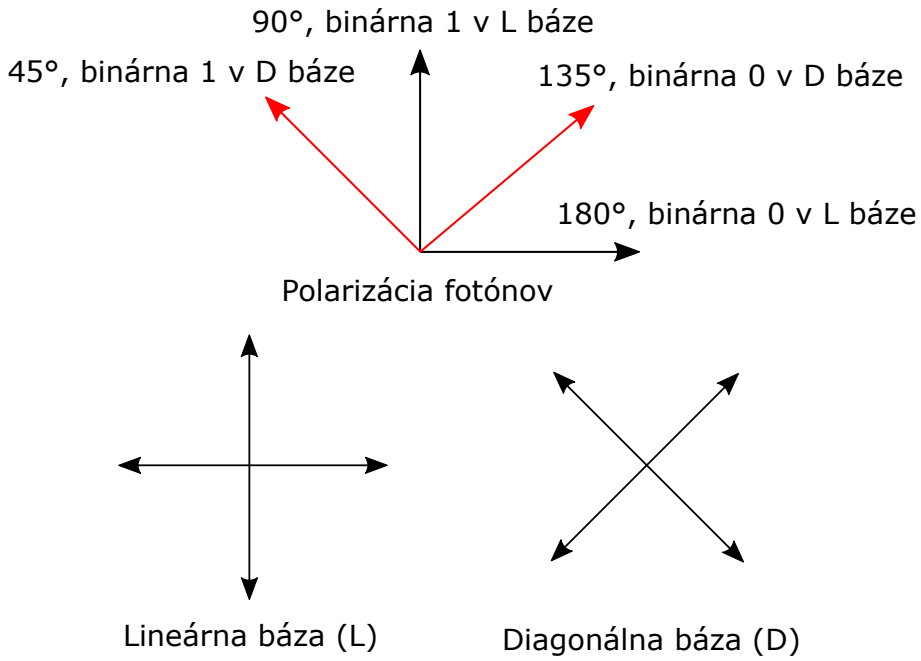
Základný rozdiel medzi **diskrétnymi premennými** (Discrete Variable skrátene DV) a **spojitými premennými** (Continuous Variable skrátene CV) je prirovnatelný k rozdielu medzi jedno fotónovým detektorom (single photon detector) a „Homodyne detector". Tieto protokoly pre prenos informácie využívajú buď vlastnosti častice alebo vlny fotónu.

- Single photon detector deteguje dopady alebo nedopady, keď fotón dopadne na detektor. Teda výsledok počtu je vždy diskrétny. Preto sú označované tieto protokoly, ktoré využívajú vlastnosti častice, ako QKD s diskrétnymi premennými „**DV-QKD**". Týmito protokolmi sú BB84, E91, atď. Informácia môže byť zakódovaná do vlastností jedného fotónu.
- „Homodyne detector" meria kvadratúry elektrického poľa dopadajúceho svetla. Výsledkom je zobrazenie fázy a amplitúdy elektrického poľa na osách kvadratúry. Výsledok je spojitý a využíva vlastnosti vlny, preto je nazývaný QKD so spojitými premennými „**CV-QKD**", kde informácia môže byť zakódovaná do amplitúdy a fázy kvadratúry laseru. Premenné tohto typu sú využívané v protokole GG02. [39].
- **„DPR"** protokoly sú založené na slabých koherentných impulzoch (weak coherent pulses) a patria medzi najpraktickejšie riešenia pre QKD na veľké vzdialenosti. Odlišujú sa od bežných schém QKD, pretože nekóduje na princípe výberu náhodných báz, ale kóduje informácie v čase a relatívnej fáze slabého koherentného pulzu. Protokoly, ktoré využívajú slabé koherentné pulzy sú napríklad COW alebo DPTS [42].

1.8.2 BB84

Ako bolo spomenuté, je to prvý QKD protokol navrhnutý vedcami Bennett a Brassard v roku 1984. Využíva Heisenbergov princíp neurčitosti, je z kategórie prípravy a merania a na prenos využíva diskrétne hodnoty. Pre kódovanie využíva bázu buď diagonálnu $\otimes$ alebo lineárnu $\oplus$. Ak je báza $\oplus$ a polarizácia vodorovná ($\rightarrow$), tak predstavuje hodnotu „0" a ak je vertikálna $\uparrow$, je to hodnota „1". U $\otimes$ báze to funguje rovnako, ak je polarizácia $\nearrow$ znamená „0" a $\nwarrow$ predstavuje „1". Alica posiela

fotóny podľa jednotlivých báz, v jednotlivých polarizáciách a tak dokáže reprezentovať hodnoty „0“ a „1“. Bob používa polarizačný delič zväzkov (Polarisation Beam Splitter skrátene PBS), ktorý má 2 detektory a každý fotón nameria v jednom z nich podľa toho akú bázu vyberie. Výber prebieha úplne náhodne. V prípade ak sa fotón



Obr. 1.13: Zobrazenie možných báz protokolu BB84 a hodnoty 0 a 1 v lineárnej a diagonálnej báze.

zakóduje v $\otimes$ báze a prečíta sa v $\oplus$, vtedy bude výsledok úplne náhodný. Pokiaľ by chcela Eva získať informácie z prenosu musí zmerať, čím qubity zničí. Taktiež musí vytvoriť náhodnú kombináciu filtrov a je nemožné, aby všetky báze trafila a vedela by presne zreplikovať všetky pôvodné hodnoty a poslať ich ďalej tak, aby si to Bob nevšimol. Alica a Bob sú v kontakte z dôvodu získania informácie o úplosti fotónov, ktoré mu posiela. Týmto vznikne „raw key“. Teraz si Alica a Bob verejne oznámia, u ktorého fotónu použili akú bázu a nechajú si bity, kde majú obaja rovnakú bázu. Tým vznikne „sifted key“. Z toho sledu bitov vyberú náhodné pár bitov a navzájom si ich vymenia cez verejný kanál a zistia hodnotu chybovosti. Tým overia či nebola komunikácia odpočúvaná a nesnažila sa Eve získať údaje. Ak je chybovosť pod určitou hodnotou, je tento kľuč bezpečný a môže byť použitý pre zabezpečenie komunikácie [19], [28], [45].

Tab. 1.1: Výmena zdielaného kľúča protokolu BB84.

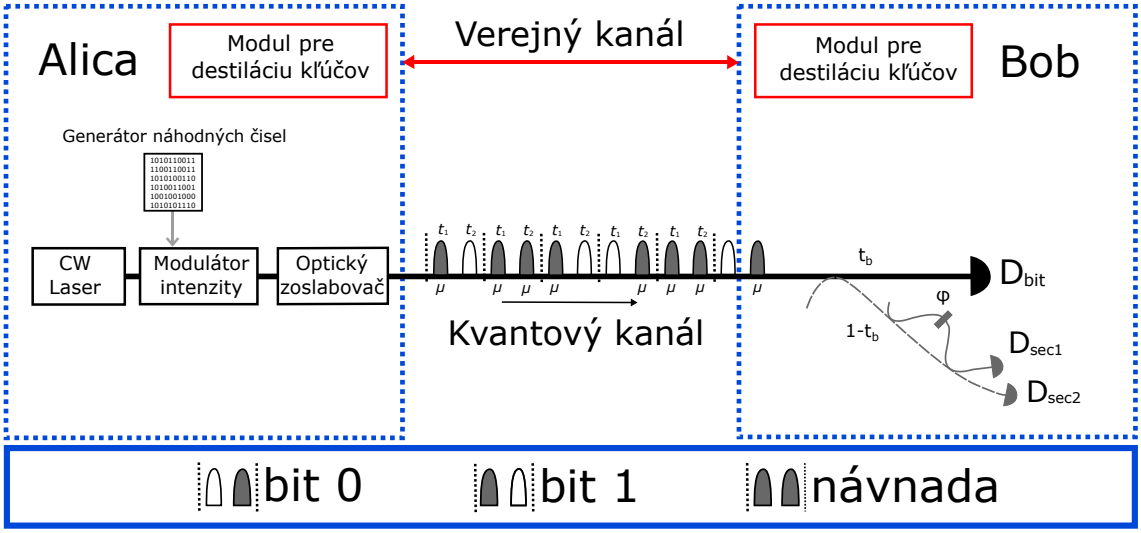
Kvantová výmena								
Alicine náhodné bity	1	1	0	0	1	1	0	0
A. vybrané náhodné báze	$\oplus$	$\otimes$	$\oplus$	$\oplus$	$\otimes$	$\otimes$	$\oplus$	$\otimes$
Bity zakódované do polarizácie	$\uparrow$	$\nwarrow$	$\rightarrow$	$\rightarrow$	$\nwarrow$	$\nwarrow$	$\rightarrow$	$\nearrow$
Bobové náhodne vybrané báze	$\otimes$	$\oplus$	$\oplus$	$\oplus$	$\otimes$	$\oplus$	$\oplus$	$\otimes$
B. zmerané hodnoty	0	1	0	0	1	0	0	0
Zhodné bity medzi A a B	Nie	Áno	Áno	Áno	Áno	Nie	Áno	Áno
Verejná komunikácia								
B. oznámi A. aké použil báze. A. potvrdí správne	$\times$	$\times$	✓	✓	✓	$\times$	✓	✓
Sifted key			0	0	1		0	0
B. výber niektorých bitov				0			0	
A. potvrdenie že bity sú rovnaké				✓			✓	
Výstup								
Výstupný zdieľaný kľúč			0		1			0

1.8.3 COW

Výhody tohto protokolu je, jednoduchosť implementácie v sieti a zostrojenie zariadenia v porovnaní s inými. Je tolerantný k zníženej interferencii viditeľnosti a je odolný voči útoku „Photon Number Splitting“ skrátene PNS. Tieto vlastnosti predpokladajú vysokú účinnosť, pokiaľ ide o generovanie bitov z qubitov [43].

Ďalšou výhodou protokolu COW je, že umožňuje implementáciu úplne pasívneho prijímača bez akéhokoľvek aktívneho prvku pre bázový výber. Taktiež nie je potrebná kontrola polarizácie ako u iných protokolov. Vyžaduje len dva detektory a v kombinácii s detektormi nízkeho hluku (low noise) je protokol COW obzvlášť výhodný pre diaľkové spoje alebo stratové vlákna [44].

Protokol patrí do skupiny využívajúcich previazanie a pre zakódovanie informácií používa DPR. Systém tohto protokolu je veľmi jednoduchý. Alica len potrebuje generovať sekvenciu kohenerentých impulzov. Na druhej strane Bob potrebuje na monitorovacom ramene len jednoduchý detektor pre rozpoznávanie impulzov a na zabezpečovacom zaisťuje bezpečnosť na princípoch kvantovej mechaniky [43], [45].



Obr. 1.14: Štruktúra protokolu COW.

Na obr. 1.14 je zobrazený systém protokolu COW. V tomto protokole je kódovanie zabezpečené modulátorom intenzity vysokej viditeľnosti (high-visibility intensity modulator), ktorý vytvára slabé impulzy v špecifických časových intervaloch „time bins“.*2 Informácia je kódovaná v čase. Informácia je zakódovaná do sekvencie dvoch impulzov v jednom časovom intervale s dvomi časovými oknami t_1 a t_2, kde aspoň v jednom okne musí byť impulz μ. „1“ je reprezentovaná ak je μ v t_1 a t_2 je prázdny. V prípade ak je μ v t_2 a t_1 je prázdny tak je definovaná „0“. Alica z bezpečnostného hľadiska môže odoslať μ v t_1 aj t_2. Tento stav sa nazýva návnadový (decoy state). Aby Bob získal kľuč (raw key), meria v čase príchodu impulzy na jeho dátovej linke

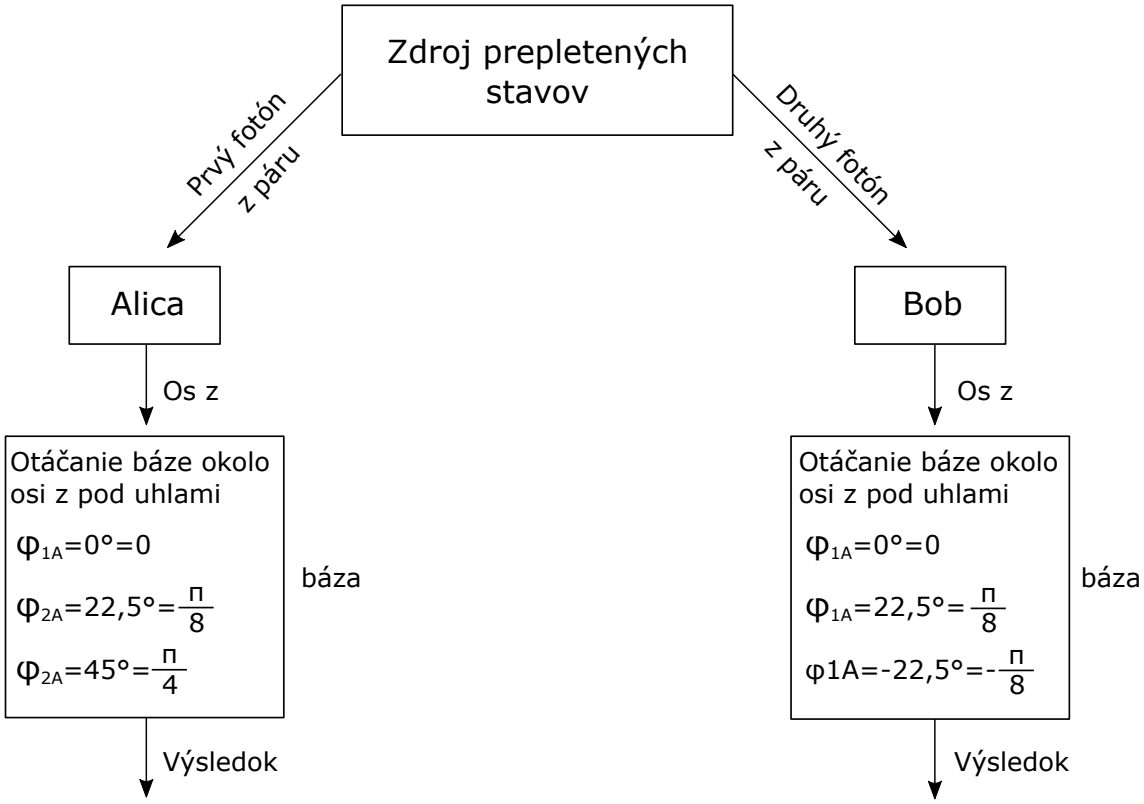
D_{bit}. Pre zaistenie bezpečnosti existuje druhá linka, kde Bob niekedy náhodne vyberie a zmeria spojitosť medzi po sebe idúcimi nie prázdnymi impulzmi ako sú „1“, „0“ a „decoy“. Na meranie sa používa interferometer a detektory D_{sec1} a D_{sec2}, v prípade, ak je vlnová dĺžka a fáza interferometra správne posunutá (nezmenná), tak všetky dopady sú na detektore D_{sec1}. Strata koherencie a tým aj zníženie viditeľnosti napovedá o tom, že komunikácia bola odpočúvaná a vtom prípade sa kľúč jednoducho zahodí [43], [44], [45].

Ak je zaistená bezpečnosť, Alica oznamuje Bobovi, ktoré bity z jeho surového kľúča má odstrániť, pretože inak zodpovedajú návnadovej sekvencií [43].

Následne Alica a Bob vytvoria zdieľaný tajný kľúč klasickým procesom, tak ako je oprava chýb a zosilnenie súkromia.

1.8.4 E91

Protokol bol navrhnutý v roku 1991 Arturom Ekert. Využíva princíp kvantového prepletenia fotónov a patria do skupiny DV QKD. Tento protokol je podobný spomínanému BB84, ale bol vytvorený bez jeho poznania. Vďaka previazaným (entaglovaným) párom, exituje medzi nimi kolorácia niektorých vlastností. Vďaka tomu dokážeme pár fotónov popísať jedným spoločným kvantovým stavom [4] [19]. Ko-



Obr. 1.15: Štruktúra komunikácie protokolu E91.

munikácia začína pri zdroji prepletených stavov, napríklad „spontaneous parametric down conversion“ skrátene SPDC, ktorý vytvorí pár previazaných fotónov, ktoré majú vzájomne kolorovanú ortogonálnu (pravouhlú) polarizáciu. Tento stav fotónov môžeme zapísať ako:

$$|\psi^-\rangle = \frac{1}{\sqrt{2}} \left(|\updownarrow\rangle |\leftrightarrow\rangle - |\leftrightarrow\rangle |\updownarrow\rangle \right). \tag{1.5}$$

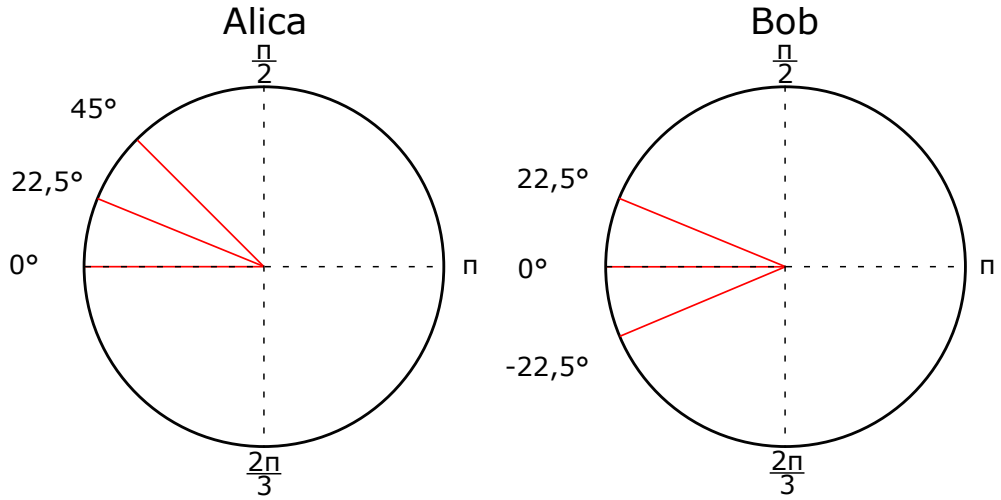
Jeden z páru letí k Alici a druhý k Bobovi, viď obr. 1.15. Obidve strany merajú pomocou báze $\oplus$, ktorá sa otáča okolo osi z. Táto os je pozdĺž smeru odkiaľ prelietavajú fotóny. Alica otáča bázu pod uhlami:

$$\varphi_{1A} = 0, \varphi_{2A} = \frac{\pi}{8} = 22,5°, \varphi_{3A} = \frac{\pi}{4} = 45°.$$

Na druhú strane, Bob otáča bázu pod uhlami:

$$\varphi_{1B} = 0, \varphi_{2B} = \frac{\pi}{8} = 22,5°, \varphi_{3B} = -\frac{\pi}{8} = -22,5°.$$

Tieto roviny sú vyberané v súlade s CHSH (nerovnica odvodená Clauser, Horne, Shimony a Holt z belových nerovníc) skúškou. Každá strana má vybrané tri posuny uhlov φ_i, každý medzi posunmi musí byť $22,5°$ a Alica a Bob musia mať dve z troch báz rovnaké. Meranie nadobúda, tak ako pri BB84 buď stav „0“ alebo „1“. Alica a Bob si neustále menia báze merania úplne náhodne a keď si namerajú dostatočné množstvo pomocou verejného kanálu, oznámia si aké uhly báze merali. Pokiaľ obaja zvolili rovnakú bázu, vedia určite, že namerali opačné hodnoty. Teda ak by Alica namerala „0 0 0 0“ Bob nameria určite „1 1 1 1“ [4] [19]. Pre merania kde použili



Obr. 1.16: Bázy Alice a Boba v protokolu E91.

rôzne bázy, si oznámia aj výsledok merania, kde testujú originálne Bellove nerovnosti alebo CHSH nerovnosti, aby skontrolovali existenciu Evi.

$$S = \langle \varphi_{1A}\varphi_{1B} \rangle - \langle \varphi_{1A}\varphi_{3B} \rangle + \langle \varphi_{3A}\varphi_{1B} \rangle + \langle \varphi_{3A}\varphi_{3B} \rangle. \tag{1.6}$$

Z týchto hodnôt spočítame hodnotu S, ktorá je zložená z koloračných koeficientov merania v rôznych bázach medzi Alicou a Bobom. Hodnota musí byť z intervalu $-2 \leq S \leq 2$ a taktiež môže nadobúdať maximálne $S = -2\sqrt{2}$ v CHSH nerovnosti. Teda, ak dôjdu k tomuto výsledku, tak namerané fotóny, kde mali Alica a Bob rovnakú bázu, sú použité ako tajný kľuč [45]. V prípade, ak by bolo S mimo intervalu, existuje pravdepodobnosť, že Eva odpočúvala, nakoľko množstvo previazaných častíc klesne a tým sa zníži hodnota S. Podľa veľkosti poklesu hodnoty S môže Alica a Bob dôjsť k záveru, že bola komunikácia odpočúvaná alebo sa vyskytla iná chyba v meracích zariadeniach [4], [19].

1.9 Výrobcovia QKD

QKD je aktuálna téma, ktorá má pred sebou ešte dlhú cestu. Najvýznamnejšie korporácie a organizácie sa venujú kvantovej bezpečnosti, kvantovým sieťam alebo aspoň ich častiam. Sú to tieto:

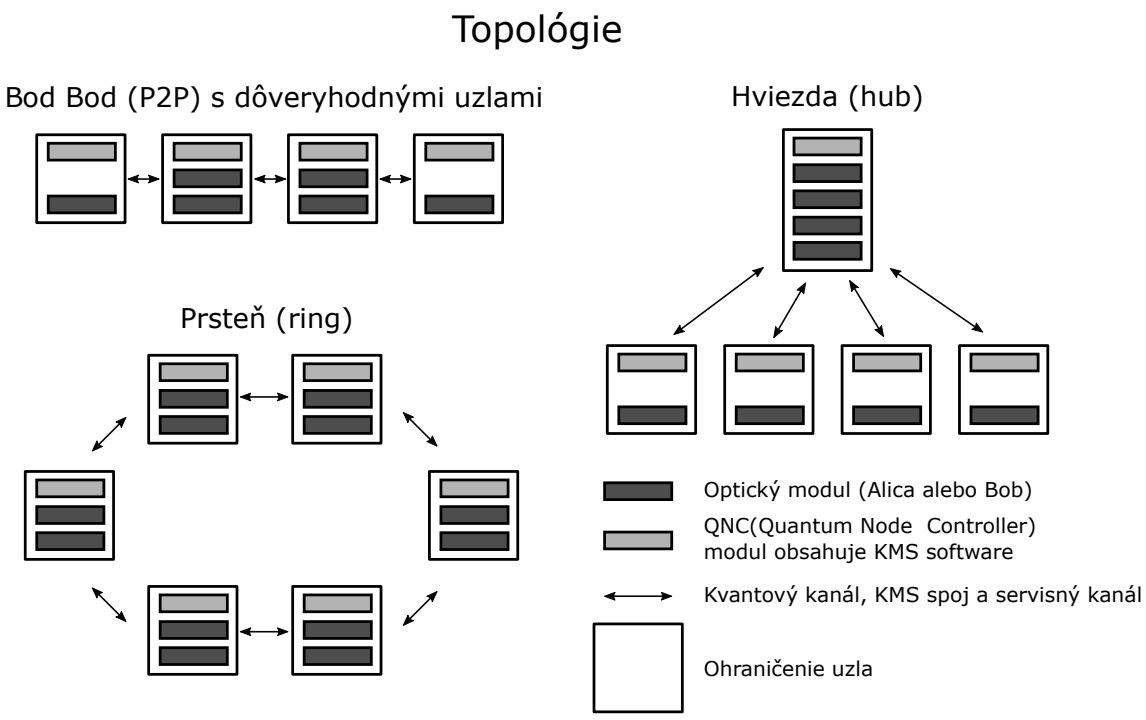
ID Quantique

ID Quantique sídli vo Švajčiarsku, a je jednou z prvých spoločností, ktoré poskytujú QKD, kvantovo bezpečné šifrovanie sieti (šifrátory v preklade Encryptor), bezpečné generovanie kvantových kľúčov a služby pre finančný priemysel a vládne organizácie po celom svete. Taktiež ponúkajú kvantový generátor náhodných čísel. ID Quantique sa aktívne podieľa na procesoch štandardizácie, najmä na ITU a ETSI, s cieľom zvýšiť interoperabilitu QKD a iných bezpečnostných systémov [46], [47].

- QKD systém
  - **Cerberis**[3] **QKD Systém** je ľahko integrovateľný v akomkoľvek dátovom centre. Môžu byť doňho vložené moduly „blades“ pre správu kľúčov, monitorovanie, administráciu a miesto pre jeden alebo dva QKD moduly pre kvantovú generáciu kľúčov a distribúciu cez kvantový kanál, ktoré obsahujú transmiter pre Alicu na jednom konci a pre Boba na druhom konci. Kvantová komunikácia prebieha cez klasické optické vlákna, čo vedie k ľahkej, lacnej a ľahko udržateľnej inštalácií. Všetky optické kanály su kompatibilné s ITU štandardmi pre „Dense Davelength Division Multiplexing“, skrátene DWDM.
    Pre maximalizáciu vzdialenosti medzi uzlami sa odporúča použiť pre kvantový kanál „dark fiber“. Pri využití multiplexovania komunikačného kanálu s kvantovým kanálom je možné zaistiť prenos v jednom vlákne na vlnovej dĺžke 1310 nm (pásmo O). Podporuje akýkoľvek druh sieťových topológií, ako sú siete typu point-to-point, ring a hub alebo prepojenie

Obr. 1.17: QKD systém Cerberis[3] od IDQ.

viacerých zariadení pre zväčšenie dosahu. V každom QKD uzle je KMS softvér na moduly „Quantum Node Controller“ (QND), ktorý rozhoduje o distribúcií kľúčov v uzle. QKD moduly môžu byť uložene v rovnakom šasi, záleží však od topológie [47].



Obr. 1.18: Topológie, ktoré Cerberis[3] podporuje s popísanými modulmi, ktoré potrebuje pri jednotlivých topológiach.

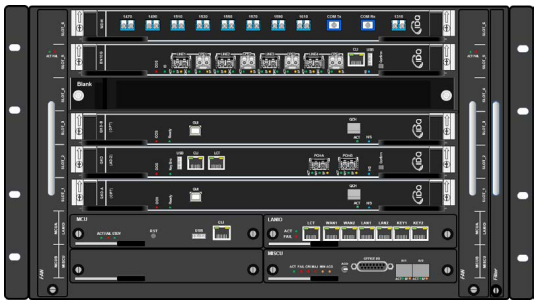
– **Clavis[3] QKD Platform** je výskumná platforma s automatizovanou alebo manuálnou prevádzkou. Používateľ tak môže experimentovať s rôznymi parametrami a študovať rôzne nastavenia. Clavis[3] platforma sa skladá z dvoch staníc, vysielacej jednotky Clavis[3]-A a prijímacej jednotky Clavis[3]-B. Každá stanica sa skladá z optickej a elektronickej platformy

riadenej externým počítačom, ktorý je so stanicou spojený prostredníctvom ethernetového spojenia.

Obr. 1.19: QKD systém Clavis^3 od IDQ.

Jednotky Clavis 3-A a Clavis 3-B sú spojené kvantovým kanálom, ktorý sa používa na prenos kľúčov. Tento kanál má výstupný konektor FC/APC a vlákno typu SMF-28. Servisný kanál je vyrobený z niekoľkých optických vlákien, ktoré sú k jednotkám pripojené pomocou SFP vysielačov a prijímačov s LC/UPC konektormi. Dve vlákna je možné redukovať na jediný pomocou SFP transceiverov podporujúcich obojsmerné prenosy [47].

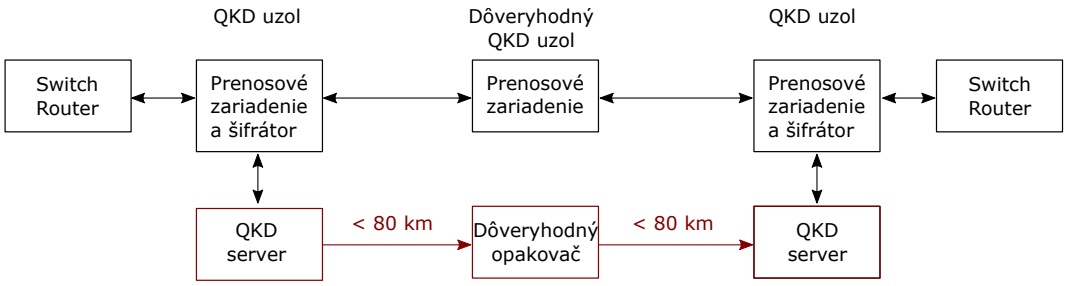
– **Clavis^{300} Quantum Cryptography Platform** je kompletné kryptografické riešenie, ktoré šifruje QKD s LEA (Light Encryption Algorithm). Clavis^{300} je jediné zariadenie od IDQ, ktoré poskytuje integrovaný šifrátor. Je ideálny pre testovanie kvantovej kryptografie a sieťových konfigurácií pre sieť P2P, viď obr. 1.22. Šifrátor je integrovaný a založený na



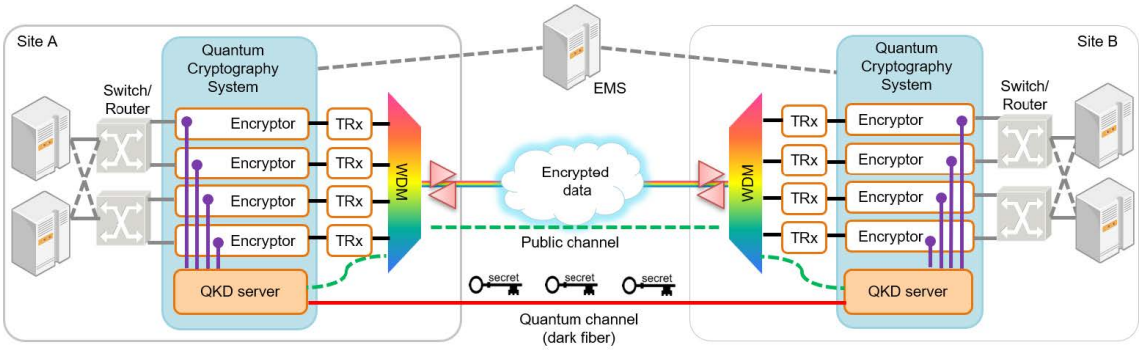
Obr. 1.20: QKD systém Clavis^{300} od IDQ.

Korean LEA. Pre vyšší výkon je odporúčaný „dark fiber“. Clavis^{300} je možné použiť aj ako prenosový uzol pre zväčšenie dosahu prenosu kľúčov viď obr. 1.21 [47].

- Šifrátory
  - Centauris CN9000 Series
  - Centauris CN8000
  - Centauris CN6000 Series
  - Centauris CN4000 Series
  - Centauris CV1000 Virtual Encryptor



Obr. 1.21: Clavis[300] použitý pre zvýšenie dosahu medzi komunikujúcimi stranami, ktorý využiva 2 QKD moduly (jeden pre príjem a druhý pre odosielanie kvantových informácii) sú zobrazené ako dôveryhodný opakovač.



Obr. 1.22: Zobrazené topológia P2P zariadenia Clavis[300], ktorá využíva vlnový multiplex (wavelength division multiplexing, skrátene WDM) pre prenos údajov.

- Generátor kvantových kľúčov
  - Quantis Appliance 2.0
  - Quantum Key Factory

Toshiba

Toshiba má svoje R & D centrum v Cambridge, ktoré sa zameriava aj na kvantovú oblasť. Výsledkom je kompletné riešenie pre QKD s už komerčným nasadením [46], [48].

- QKD systém
  - **Multiplexed QKD System** umožňuje prevádzku na vlákne prenášajúcom údaje, čím sa odstraňuje požiadavka na nákladné tmavé vlákno. Využíva kvantový kanál s vlnovou dĺžkou v telekomunikačnom O-pásme (od 1260 nm do 1360 nm), takže C-pásmo (od 1530 nm do 1565 nm) je voľné pre prenos používateľských dát. Môže pracovať v konvenčnom režime s dvojicou vlákien prenášajúcich jednosmerný prenos alebo s jedným vláknom prenášajúcim obojsmerné kvantové a klasické signály [48].

Tab. 1.2: Prehľad parametrov dostupných QKD systémov od IDQ

Názov	Cerberis^3	Clavis^3	Clavis^{300}
Protokol	COW	COW	T12
WDM	Áno	Áno	Áno
Rýchlosť generovania kľúčov [kb/s]	1,4	1,4	6
Prenosová stratovosť [dB]	12	12	12
Útlm [dB]	12-18	14-18	18-24
Chybovosť [%]	-	-	3
Podpora ETSI API	Áno	Áno	Áno
Dosah [km]	50-75	50-75	70
Vlastný šifrátor	Nie	Nie	Áno

Obr. 1.23: Multiplexovaný (MUX) systém QKD od Toshiba.

– **Long Distance QKD System** pracuje s kvantovým kanálom v telekomunikačnom C pásme pre čo najdlhší možný rozsah a najvyššiu možnú bezpečnú rýchlosť kľúča. Môže tolerovať obmedzenú šírku pásma multiplexovaných dát v pásme C [48].

Obr. 1.24: QKD systém na dlhé vzdialenosti (long distance) od Toshiba.

Qasky

Je čínska spoločnosť tiež nazývaná Anhui Qasky Science and Technology a zameriava sa na komercializáciu kvantovej kryptografie a elementov kvantových sietí z Čínskej akadémie vied. Ponúkajú produkty a služby vrátane koncových zariadení kvantovej

Tab. 1.3: Prehľad parametrov dostupných zariadení od Toshiba

Názov	MUX	Long Distance
Protokol	T12	
WDM	Áno	Nie
Rýchlosť generovania kľúčov [kb/s]	40	300
Prenosová stratovosť [dB]	10	
Útlm [dB]	16,8	28,8
Chybovosť	10	
Podpora ETSI API	Áno	
Dosah [km]	70	120
Vlastný šifrátor	Nie	
Počet vlákien	1/2	2

kryptografie, smerovacích a prepínacích zariadení siete, aplikačného a ovládacieho softvéru pre zabezpečenie sietí [46].

Quantum Xchange

Táto spoločnosť je dominantný poskytovateľ riešení pre kvantové siete a bezpečnosť v USA. Bola založená v roku 2016 v Marylande. Implementovali napríklad QKD systém, ktorý spája Wall Street a „back office“ rôznych finančných spoločnosti v New Jersey. Využívajú QKD službu Phio, ale nevyrábajú hardvér QKD. Integrujú hardvér QKD tretej strany s ich správou kľúčov (key managment), aby zabezpečili bezpečnú infraštruktúru distribúcie kľúčov. V súčasnej dobe pracujú s dodávateľmi QKD ako je ID Quantique a Toshiba. Spolupracujú tiež so Zayo Group, ktorý má k dispozícií „dark fiber“ a s výskumným ústavom Battelle, ktorý poskytuje zariadenia dôveryhodných uzlov [46].

MagiQ

Spoločnosť MagiQ sídli v Amerike a nachádza sa v štáte Massachusetts. Vyvíja vlastné riešenie pre QKD QPN-8606 a Q-Box. Ponúka tiež riešenie pre potlačenie elektromagnetických interferencií. Spomínané produkty nie sú už dlhšie štandardne ponúkané, ale bude vyvíjať a vytvárať riešenia na mieru, ktoré sú založené na týchto produktoch [46].

InfiniQuant

InfitnityQuant je nemecká spoločnosť, ktorá v spolupráci s Max Planck Institute vyvíja QKD riešenie pre satelity a optické vlákna. Sú v počiatočnej fáze vývoja QKD, ktoré využíva spojité premenné teda (CV-QKD) [46].

Qubitekk

Americká spoločnosť založená v roku 2012 v Kalifornií. Nedávno oznámila ako prvá generátor fotónov s technológiou „plug and play“ s naźvom QES1. Hlavnými produktami sú generátory kvantovo previazaných fotónov [46].

Quintessence Labs

Firma sídli v Austráli, ich hlavnými produktami sú generátory náhodných čísiel, QKD systémy, QKDN a kvantovo kryptografické zabezpečenie. Aktuálne majú vo vývoji druhú generáciu QKD, ktorá má umožniť využitie spojitých premenných prostredníctvom laserového lúča. Túto technológiu by mali byť schopné využiť bežné telekomunikačné zariadenia cez bežné optické vedenia [46].

2 Praktická časť

2.1 Simulátory

Sieťové simulátory umožňujú ušetriť pri uskutočňovaní projektov veľa peňazí a času. Simulačné prostredie ponúka vytvorenie zložitých sieťových topológii, vysoký stupeň kontroly, rôzne nastavenia parametrov siete a opakovanie experimentu.

2.1.1 QKDNetsim

Cieľom Quantum Key Distribution Network Simulation (QKDNetsim) nebolo vytvoriť samostatné simulačné prostredie, ale vývoj modulov QKD, ktoré bude možné implementovať do existujúcich a spoľahlivých simulátorov. V tomto prípade to bol NS-3. QKDNetsim podporuje simuláciu v rôznych sieťových topológii, bez ohľadu na QKD. Tento simulátor je voľne dostupný na internete. QKDNetsim sa zameriava na použitie kľúča a správu kľúčov, nepoužíva sa pre ich generáciu.

QKDNetsim obsahuje triedu QKDCrypto, ktorá využíva kryptografické algoritmy z knižnice Crypto++ a je napísaná v jazyku C++. Táto knižnica aktuálne podporuje kryptografické algoritmy ako AES, OTP, VMAC a veľa ďalších.

Tento implementačný model obsahuje sieťový modul QKD, kľúče QKD, vyrovnávaciu pamäť QKD, sieťové zariadenie QKD (QKD NetDevice) a „processing applications“. QKDNetsim bol vytvorený na Technickej univerzite v Ostrave a má ho v správe Katedra telekomunikácií Univerzity v Sarajeve a tím LIPTEL Technickej univerzity v Ostrave [49].

NS-3

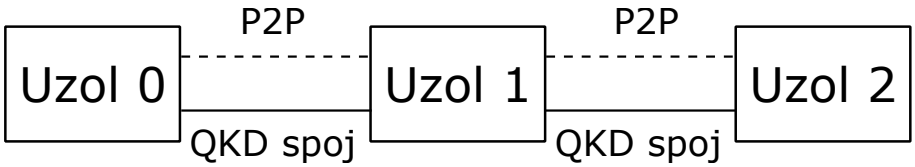
Network simulator 3rd version skrátene NS-3 je sieťové simulačné voľne dostupné prostredie a je licencované na základe NU GPLv2. NS-3 podporuje ako simulácie, tak aj emulácie a sú v ňom využívané hlavne jazyky C++ a Python. Simulátor umožňuje simulovať modely s realistickými podmienkami. Do NS-3 je možné implementovať veľa modulov, vďaka ktorým dokáže podporovať Wi-Fi, WiMAX, LTE a samozrejme siete využívajúce IP, ako aj siete bez IP. Podporuje smerovacie protokoly pre drátové aj bezdrôtové siete a veľa ďalších. NS-3 je v prevažnej väčšine využívané na výskumné a vzdelávacie účely [50].

2.2 Simulácie

Pre simuláciu QKD polygónu bolo zadané prostredie QKDNetsim. Podľa úvodnej stránky simulátora[1] bola zvolená inštalácia v prostredí Linux. Pre možné a očakávané problémy a jednoduchšiu správu bola inštalácia vykonaná prostredníctvom Virtualbox[2]. V prvom kroku bol nainštalovaný VirtualBox a následne Linux distribúcie Ubuntu verzie 20.04[3]. Po inštalácii bolo potrebné nainštalovať všetky potrebné balíčky (napr. python, g++, libcrypto++–dev, texlive a veľa ďalších) tak, aby QKDNetsim fungoval bez problémov.

V ďalšom kroku bola zrealizovaná samotná inštalácia simulačného prostredia NS-3, nakoľko QKDNetsim nie je samotný simulátor, ale len modul, ktorý NS-3 môže využiť. NS-3 je voľne dostupný z oficiálnej stránky a nainštalovaný podľa jeho návodu na predmetnej stránke[4]. Po úspešnej inštalácií bol stiahnutý modul QKDNetsim a bez vykonania ďalších krokov, by mal byť funkčný. Napriek niekoľkým opakovaným pokusom „build project“ aplikácia stále vypisovala chybu pri kompilácií. Z tohto dôvodu bola celá inštalácia opakovaná, pričom boli kontaktované osoby, ktoré sa podieľali na vytvorení tohto simulačného modulu. Po vzájomnej konzultácii bolo navrhnuté využiť zdieľané virtualizované zariadenie poskytované na webovej stránke simulátoru, na ktorom bol už nainštalovaný Linux s funkčným NS-3 a QKDNetsim.

V poskytnutom virtuálnom zariadení už ďalšie kroky po inštalácii fungovali a pre simuláciu bola vybraná jednoduchá topológia o 3 zariadeniach, viď obr. 2.1. Na tejto topológii boli zobrazené a otestované možnosti tohto simulačného prostredia. Po ďalšej komunikácii s jedným z tvorcov QKDNetsim bolo objasnené, že QKDNetsim nedokáže simulovať kvantovú úroveň QKD, teda, že sa nepoužíva na generovanie kľúča, ani pre žiadnu správu kvantového kanálu alebo odpočúvanie na kvantovej/fyzickej úrovni. Jeho činnosť je v prevažnej miere zameraná na použitie tajného kľúča a správu kľúčov na vyšších vrstvách.



Obr. 2.1: Topológia simulácie, kde komunikujú uzol 0 s uzlom 2 cez uzol 1. Uzly sú spojené P2P spojmi, cez ktoré prebieha komunikácia a tiež výmena kľúčov.

V simulátore boli nastavované parametre, ako rýchlosť generovania kľúčov medzi

[1] ttps://www.qkdnetsim.info/install/
[2] https://www.virtualbox.org/
[3] https://releases.ubuntu.com/20.04/
[4] https://www.nsnam.org/wiki/Installation

uzlami, rýchlosť premávky, smerovacie protokoly, čas začiatku a konca tvorby kľúčov, premávky a množstvo prenesených dát.

Taktiež bolo možné nastavovať parametre kvantového kanálu, ako parametre minimálneho množstva kľúčov (pod touto hodnotou, je v stave prázdny a kvantový spoj skolabuje), prahová hodnota (pod touto hodnotou je v stave nebezpečenstva), maximálna hodnota (maximálne množstvo kľúčov, ktoré môžu byť uložené) a počiatočná hodnota (množstvo kľúčov na začiatku simulácie). Ak je počiatočná hodnota na začiatku simulácie pod prahovou hodnotou je v stave dopĺňania. Skript so simulačným kódom obsahuje:

- importovanie používaných knižníc,
- výpis výstupu simulácie do konzoly,
- vytvorenie zariadení a linky medzi nimi,
- pridelenie parametrov komunikačnému kanálu,
- pridelenie IP adries zariadeniam,
- definícia QKD spojenia medzi zariadeniami a nastavenie parametrov,
- nastavenie premávky a jej parametre,
- určenie konca simulácie.

Výstupom simulátora boli smerovacie tabuľky, záznamy o prenose (.pcap) a graf vyrovnávacej pamäte kľúčov (množstvo tajných kľúčov medzi uzlami, ktoré sa dajú použiť pre šifrovanie premávky). Simulácie boli zamerané na zobrazenie vyrovnávacej pamäte počas priebehu komunikácie pri rôznych rýchlostiach generácie kľúčov (keyrate) a prenosových rýchlostiach premávky a porovnania poskytnutých komunikačných protokolov.

Tab. 2.1: Výstup z konzoly simulačného prostredia QKDNetsim pri vzorovej simulácií, kde existovalo dostatočné množstvo kľúčov pre zašifrovanie všetkých dát.

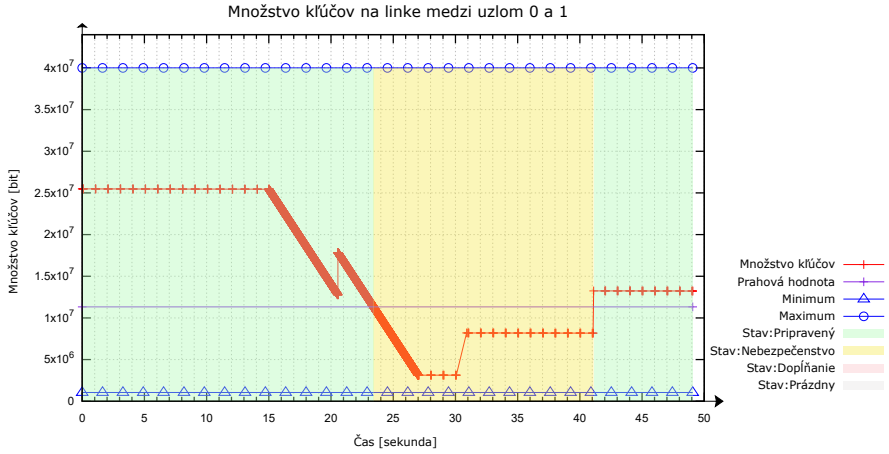
Zdrojová IP adresa		10.1.1.1	
Cieľová IP adresa		10.1.2.2	
Odoslané [bit]	750 000	Prijaté [bit]	750 000
Odoslané [paket]	1250	Prijaté [paket]	1250
Pomer [bit]	1	Pomer [paket]	1

Tab. 2.2: Prenosové parametre prvej simulácie

Spojenie	QKD spoj 1	QKD spoj 2	Premávka
Začiatok	10	3	15
Koniec	50	50	50
Keyrate [bit]	5 072 000	2 007 200	-
Prenosová rýchlosť [Mb/s]	-	-	2

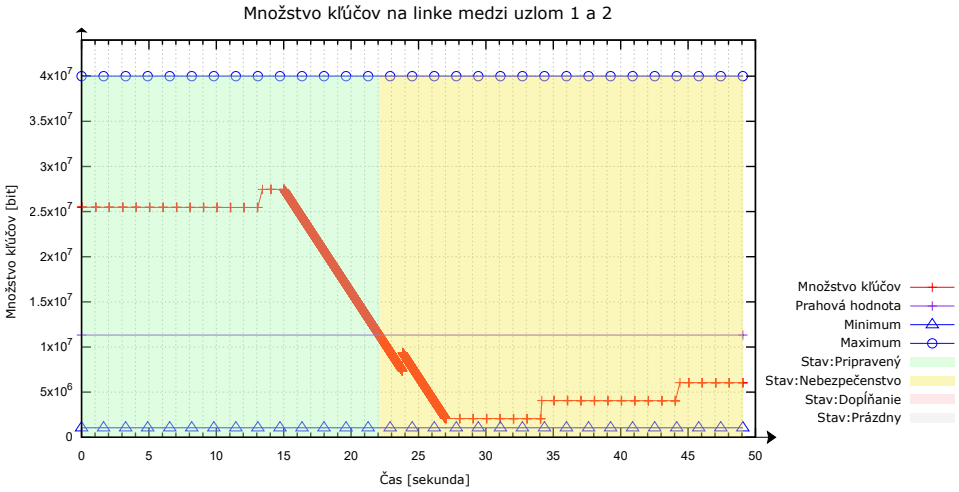
2.2.1 Prvá simulácia

Prvá a úvodná simulácia zobrazuje vplyv rýchlosti tvorenia kľúčov a rýchlosť premávky na vyrovnávaciu pamäť kľúčov. Taktiež boli vybrané rôzne časy začiatku tvorby kľúčov tak, aby na bol grafe viditeľný rozdiel.



Obr. 2.2: Priebeh zmeny množstva kľúčov medzi nultým a prvým uzlom so smerovacím protokolom DSDV.

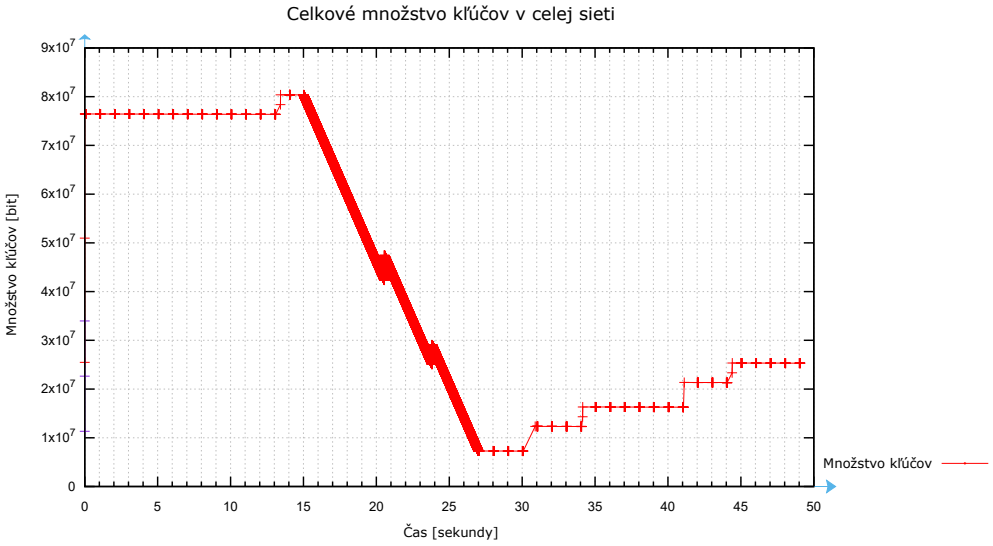
Premávka tvorila 3 000 000 bitov, jeden paket mal nastavenú veľkosť 60 bitov a ostatné parametre boli nastavené, viď. tab. 2.2. Z grafov je zjavné, že od definovaného začiatku tvorby kľúčov vždy prebehne 10 sekúnd a až potom sa odošle nastavené množstvo kľúčov a táto situácia sa opakuje.



Obr. 2.3: Priebeh zmeny množstva kľúčov medzi prvým a druhým uzlom so smerovacím protokolom DSDV.

Pri spustení premávky je zjavné znižovanie množstva kľúčov vo vyrovnávacej pamäti. V prípade keď množstvo kľúčov klesne pod prahovú úroveň (treshold), a táto

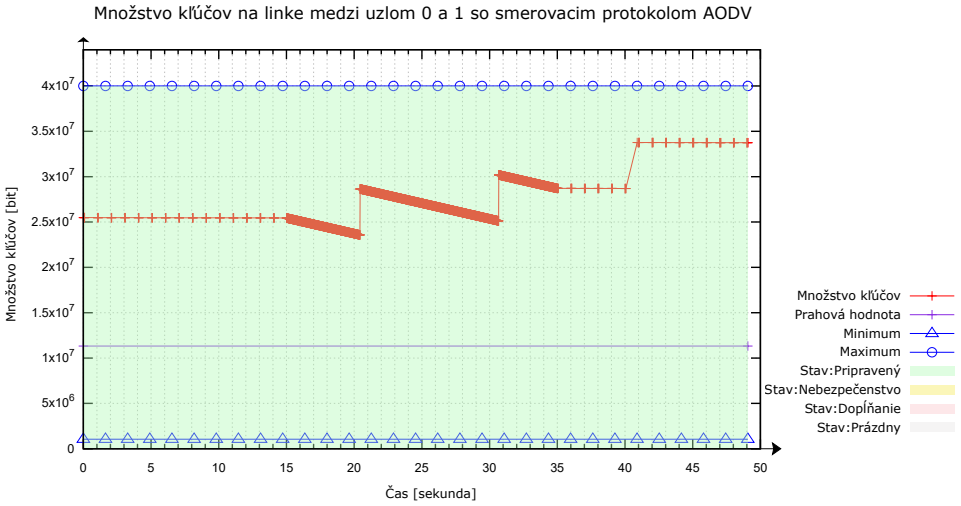
pamäť sa dostane do stavu nebezpečne nízkeho množstva kľúčov (prezentované žltou častou grafu).



Obr. 2.4: Priebeh zmeny množstva kľúčov v celej sieti so smerovacím protokolom DSDV.

2.2.2 Druhá simulácia

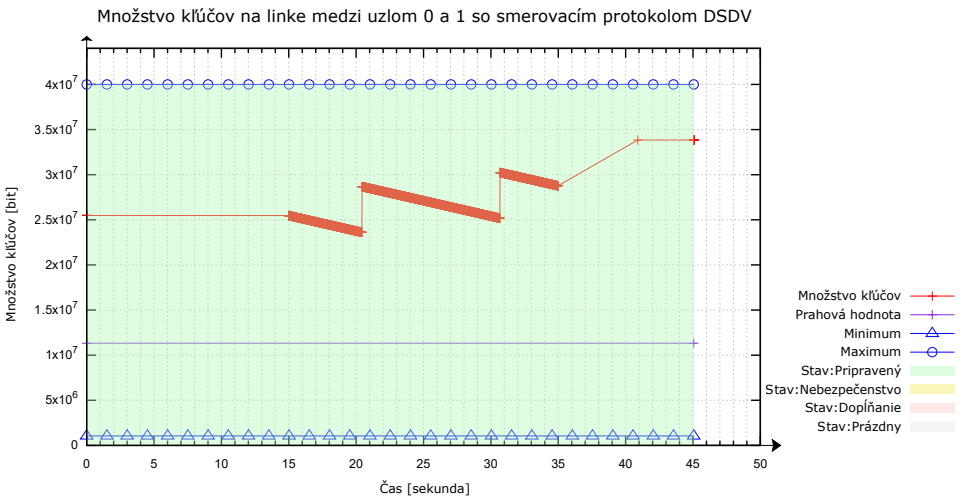
Druhá simulácia zobrazuje je vplyv smerovacích protokolov na vyrovnávaciu pamäť kľúčov. V simulátore boli základné protokoly:



Obr. 2.5: Zobrazenie vplyvu smerovacieho protokolu AODV na priebeh zmeny množstva kľúčov medi uzlami 0 a 1.

Ad hoc On-demand Distance Vector skrátene AODV je smerovací protokol pre mobilné a bezdrôtové siete. Ad hoc je pomenovanie pre sieť, kde sú dva rovnocenné prvky, ktoré komunikujú priamo bez použitia prístupového bodu. AODV dokáže smerovať unicast aj multicast. Tento protokol je reakčný, teda smerovanie začína až keď príde požiadavka pre spojenie, dovtedy neprebieha žiadna komunikácia. Protokol pre zistenie vhodnej cesty zisťuje dĺžku vektora, využíva algoritmus Distance Vector (vektor je označený ako skok na určitý smerovač (next hop) a vzdialenosť k nemu (metric)) [51].

Destination-Sequenced Distance Vector Protocol, skrátene DSDV funguje ako proaktívny protokol, sleduje aktuálne dianie siete a nadväzuje spojenie ešte predtým, ako príde požiadavka na spojenie kvôli komunikácií. Využíva Bellman Ford algoritmus a jeho hlavným prínosom je, že rieši problém so smerovacími slučkami (routing loop). Informácie o smerovacích tabuľkách sú distribuované medzi účastníkmi častým odosielaním výpisov a aktualizácií. DSDV je optimalizovaný pre mobilné a bezdrôtové ad hoc siete [51].



Obr. 2.6: Zobrazenie vplyvu smerovacieho protokolu DSDV na priebeh zmeny množstva kľúčov medzi nultým a prvým.

Optimized Link-State Routing Protocol, skrátene OLSR. Smeruje informácie na základe optimalizovaných stavov liniek. Je to proaktívny smerovací protokol a je definovaný ako čisto smerovací protokol. Smerovanie vždy začína v uzle a porovnáva cieľovú adresu a smerovacie tabuľky. Informácie sú posielané z uzlu na uzol, až kým nedorazia k cieľu, pričom je vždy hľadaná najkratšia cesta k cieľu. Tiež je používaný v mobilných ad hoc sieťach a tiež je ho možné použiť aj v iných bezdrôtových sieťach [51].

Pre simuláciu boli vybrané protokoly AODV a DSDV. Počas simulácie boli rozdielne len smerovacie protokoly, ostatné parametre boli rovnaké.

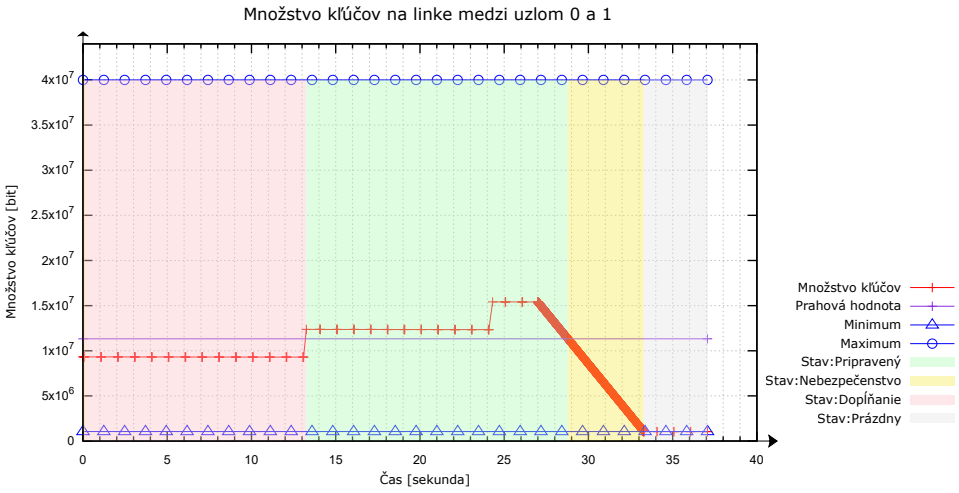
Vo výsledných grafoch sú len mierne rozdiely, avšak najvýraznejší rozdiel je pri protokole DSDV, kde strany komunikovali pravidelne a kde priebeh viac spĺňa očakávané pravidelnosti spojenia a opakované dodávania kľúčov. Pri protokole AODV je spojenie naviazané až keď začne prenos dát alebo výmena kľúčov.

2.2.3 Tretia simulácia

V tejto simulácii bolo sledované, ako sa bude sieť správať, ak bude nastavená príliš vysoká premávka, nedostatočné generovanie kľúčov a počiatočná hodnota bude nastavená pod prahovou hodnotou. Z grafu je zjavné, že v prípade ak v pamäti nie je dostatočné množstvo kľúčov, je na začiatku v stave dopĺňanie a po čase sa dostala do stavu pripravená a po spustení premávky množstvo kľúčov klesne pod minimálnu hodnotu, komunikácia skolabuje a už sa neobnoví.

Tab. 2.3: Výstup z konzoly simulačného prostredia QKDNetsim pri simulácií vysokého toku dát, kde nebolo dostatočné množstvo kľúčov, ani dostatočné rýchla regenerácia kľúčov.

Zdrojová IP adresa		10.1.1.1	
Cieľová IP adresa		10.1.2.2	
Odoslané [bit]	4 000 200	Prijaté [bit]	3 112 200
Odoslané [paket]	6 667	Prijaté [paket]	5 187
Pomer [bit]	0,778011	Pomer [paket]	0,778011



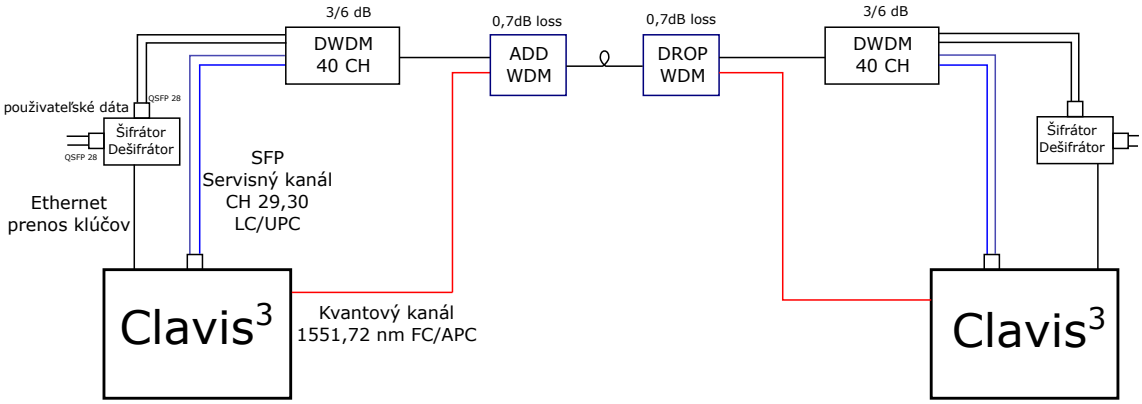
Obr. 2.7: Priebeh zmeny množstva kľúčov medzi nultým a prvým uzlom pri vysokom prenose dát.

2.3 Návrh testovacieho polygónu

Testovací polygón slúži pre testovanie prenosu s variabilnými možnosťami nastavenia jednotlivých komponentov a parametrov tak, aby bolo možné obsiahnuť čo najviac druhov zapojení, a tým umožniť variabilitu čo najväčšieho množstva zapojení optických sietí.

2.3.1 Topológia polygónu

Topológia je navrhnutá tak, aby sa mohol simulovať vplyv prenosu bežných používateľských dát na kvantový kanál. Kvantový kanál a servisný kanál je prenášaný súbežne s používateľskými dátami. Parametre prenosu sú nastavované tak, aby kvantový kanál dosiahol čo najväčší dosah a jednotlivé komponenty mu spôsobili čo najmenší útlm. Základom topológie sú dva QKD moduly, viď obr. 2.8, v kvantovom kanále prebieha jednosmerná komunikácia, kde sa odosielajú jednotlivé fotóny a následné dve vlákna pre obojsmernú komunikáciu servisného spojenia medzi modulmi. Dáta sú odosielané do šifrátora, kde sú uložené kľúče pre zabezpečenie dát, ale toto zariadenie nie je súčasťou práce a v práci sa bude uvažovať, že dáta sú už zašifrované. V poslednej časti sú zariadenia multiplexory, ktoré slúžia pre spojenie viacerých prenosov do jedného optického vlákna. Avšak DWDM má vstupný útlm vyše 3 dB, čo je pre kvantový kanál veľmi obmedzujúce, a preto bolo potrebné nájsť alternatívne zariadenie, s ktorým bude možné naviazať kvantový kanál do optického vedenia, a tým zariadením je práve Add/Drop multiplexor, pretože najlimitujúcejšou časťou topológie je práve kvantový prenos, ktorého úroveň signálu je pevne nastavená a nie je ju možné žiadnym spôsobom zosilniť.



Obr. 2.8: Topológia testovacieho polygónu pre simultánny prenos QKD a používateľských dát.

2.3.2 Komponenty

Topológia sa zakladá na vysielacích zariadeniach, ako sú SFP a jeho variácie alebo QKD pre kvantový kanál. QKD je zdrojom pre kvantový signál, servisnú komunikáciu a odosielanie kľúčov do šifrátora. Dáta z QKD pokračujú do DWDM, ktoré slúži pre spojenie viacerých prenosov do jedného vlákna. Pre naviazanie kvantového kanála do vlákna je použitý Add/Drop multiplexor.

SFP

Form-factor pluggable je optický modulárny transreceiver, ktorý slúži pre odosielanie aj prijímanie optického signálu. Sú nástupcami GBIC a podporujú štandardy ako SONET, Gigabit Ethernet, Fibre Channel a ďalšie. Toto zariadenie je použité ako komunikačný modul v QKD pre servisné spojenie. Pre komunikáciu používateľských dát je odhadovaná rýchlosť 100 Gb/s a pre túto rýchlosť je uvažované QSFP28 s vysielacím výkonom 5 dBm.

QKD

Na základe rešeršu dostupných zariadení, ich aktuálnej ceny a dostupnosti bolo vybrané zariadenie Clavis[3], viď obr. 1.19. Jednotlivé špecifikácie zariadenia boli konzultované vedúcim práce priamo s IDQ. Kvantový kanál je prenášaný iba jedným smerom na vlnovej dĺžke 1551,72 nm. Je to 32. kanál ITU štandardu so šírkou pásma 1,25 GHz. Signálová úroveň kvantového kanálu bola vypočítaná na -89 dBm ($1{,}258 \cdot 10^{-12}$ W) a jeho dynamika je 14 dB. Táto je kľúčovým parametrom pri návrhu topológie. Servisný kanál, kde prebieha komunikácia obojsmerne, využíva kanály ITU 29., 30., a to pre vlnové dĺžky 1554,13 nm a 1553,33 nm. Vysielacia úroveň je 4 dBm ($2{,}512 \cdot 10^{-3}$ W) a prijímacia -28 dBm ($1{,}584 \cdot 10^{-6}$ W). Vstupné SFP pre servisný kanál je FWLF1632xx od firmy Finisar. Pre odosielanie aj prijímanie je samostatné vlákno a prenosová rýchlosť až do 2,7 Gb/s. Má malú disperziu vďaka DFB (Distributed FeedBack) laseru a môže dosiahnuť vzdialenosti až do 120 km.

Šifrátor

Šifrátor nie je súčasťou diplomovej práce a je v tejto práci zanedbaný. Toto zariadenie má mať 100 Gb/s optický vstup pre nešifrované dáta, druhý vstup je sieťový konektor 8P8C s prenosovou technológiou ethernet, ktorý slúži pre prijímanie šifrovacích kľúčov od Clavis[3]. Optický výstup šifrátora je 100 Gb/s QSFP 28 pre odosielanie zašifrovaných používateľských dát.

DWDM

Systém DWDM (Dense Wavelength Division Multiplexing) je systém s hustým vlnovým multiplexom. DWDM využíva hlavne pásmo C, ktoré je v rozsahu od 1530 nm do 1565 nm a predstavuje konvenčné pásmo. Vláknová optika vykazuje najmenšiu stratu práve v pásme C a má významnú výhodu v prenosových systémoch na veľké vzdialenosti. Nebolo vybrané žiadne špecifické DWDM, ale je očakávané štyridsať kanálové so vstupným útlmom 3 dB.

Add/Drop WDM

Add/Drop WDM je zvolené pre nízky vstupný útlm len 0,7 dB, a to práve pre naviazanie kvantového kanálu do vlákna k servisnému kanálu a šifrovaným dátam. Pre naviazanie kvantového kanálu bolo vybrané iné zariadenie z dôvodu, že DWDM má vysoký vstupný útlm a dosah prenosu je obmedzený práve kvantovým kanálom. Tento kanál nie je možné zosilovať a má dovolenú maximálnu stratu počas prenosu 14 dB.

Optické vlákno

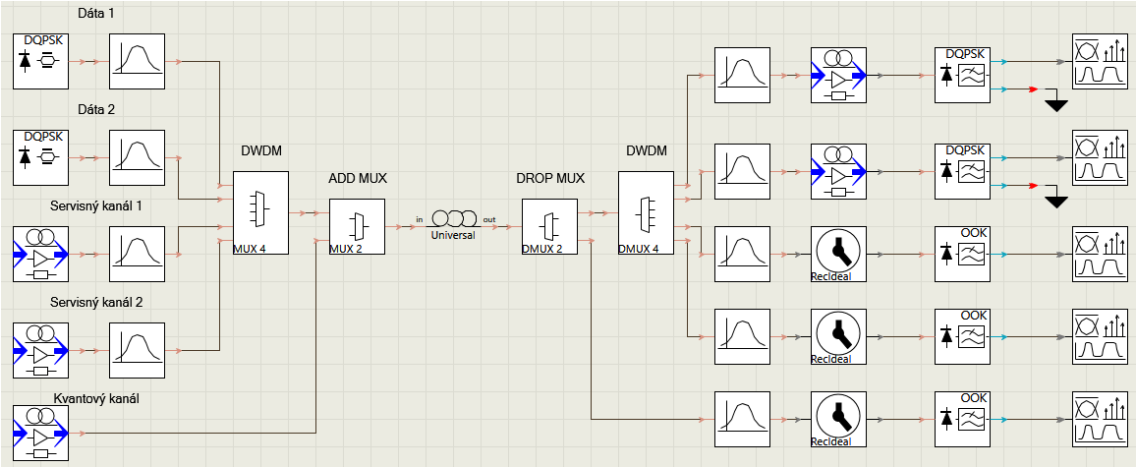
Prenosové optické vlákno má nastavené parametre podľa vlákna G.652D. Jeho útlm je 0,2 dB/km. Toto vlákno má posunutú disperziu a pri simuláciách kvôli nepresnosti nastavenia tohto parametru bude táto hodnota zanedbávaná a nastavená na nulu [52].

Dosah je možné vypočítať ako dvakrát Add/Drop multiplexor, čo je v súčte 1,4 dB a následne optické vlákno, ktorého útlm je 0,2 dB/m a to vychádza na 63 km. Tento výpočet je čisto teoretický a nepočíta sa pri ňom so žiadnymi uzlami, zvarmi, konektormi ani inými útlmami, ktoré v praxi reálne vznikajú.

2.4 Simulačné scenáre

Topológia je navrhnutá podľa topológie testovacieho polygónu, ale nie je tam zapojený šifrátor. Prvé dve vedenia sú dátové pre prenos dát, kde prebieha komunikácia o rýchlosti 100 Gb/s pomocou DQPSK modulácie na kanáloch 20. a 21.. Ďalšie sú dva servisné kanály na kanáloch 29., 30. o rýchlosti 3 Gb/s a posledný je jednosmerný prenos kvantového signálu na kanály 32., viď obr. 2.9.

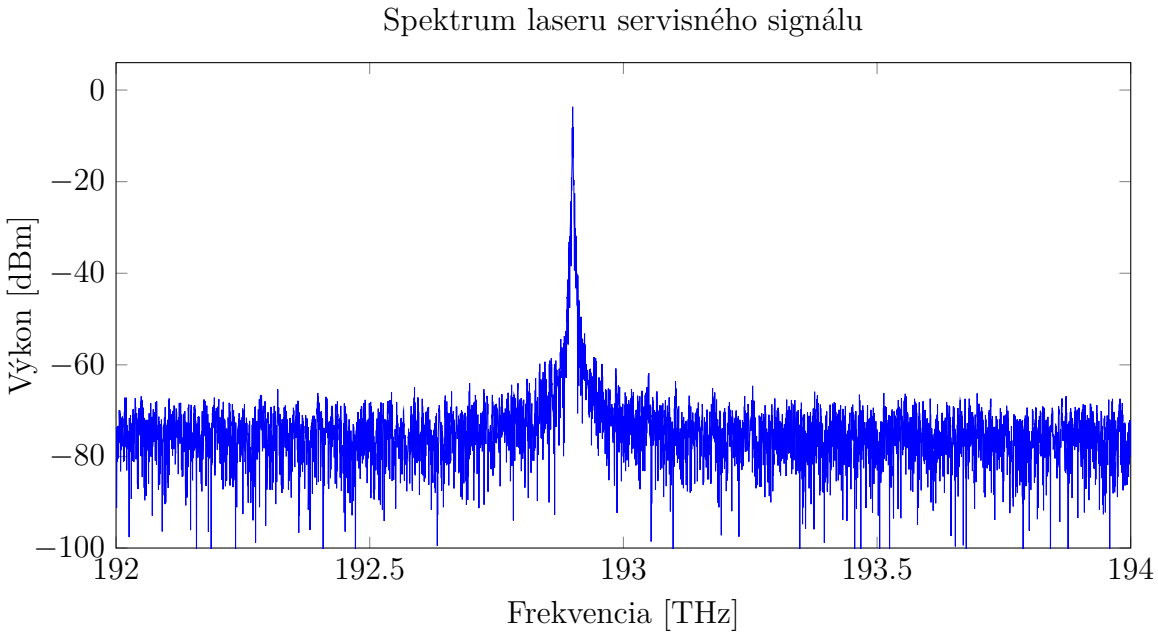
Simulačné scenáre obsahujú porovnania filtrov a ich prenosové funkcie ako Gaussova, Besselova a Butterworthova [53]. Niektoré filtre nie sú ideálne, a preto je potrebné ich niekedy sériovo zapojiť tak, aby potlačili šum na takú úroveň, aby neprekryl kvantový kanál, ale pritom príliš neznehodnotili pôvodný signál. Hlavnou úlohou



Obr. 2.9: Testovacia topológia v programe VPIphotonics pre simuláciu prenosu kvantového signálu spolu s bežnými dátami.

bolo porovnať filtračné vlastnosti filtrov a zvoliť taký, ktorého vlastnosti sa budú podobať čo najviac reálnym WDM filtrom a zistiť, ktoré filtre sú najvhodnejšie.

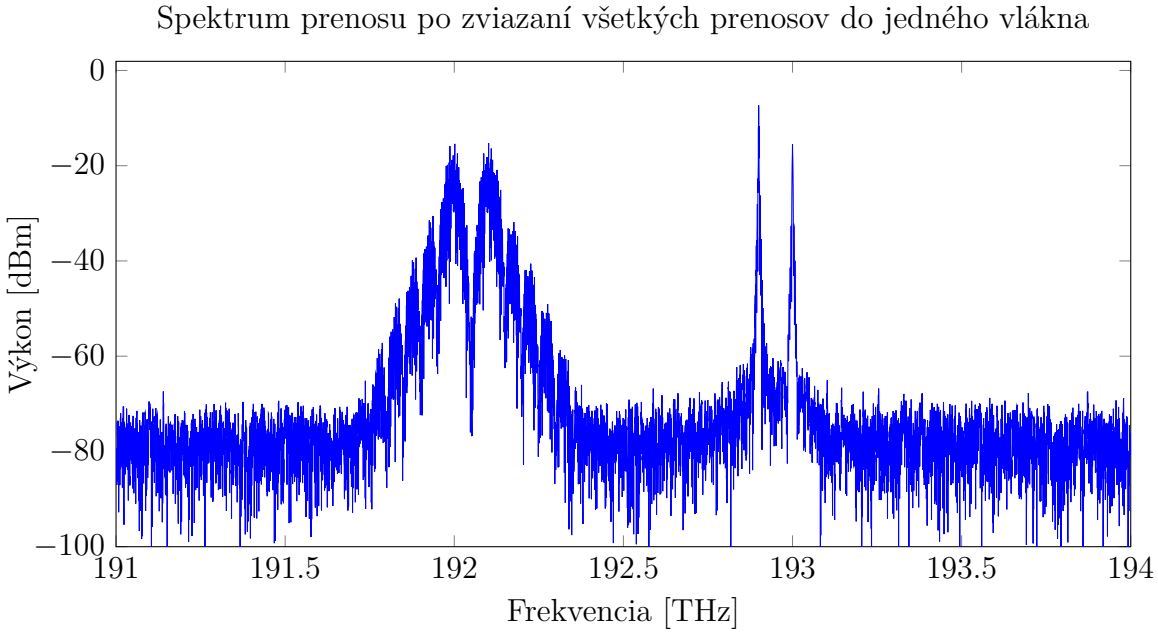
2.4.1 Simulácia bez pridaných filtrov



Obr. 2.10: Spektrálna charakteristika zdroju servisného kanálu bez filtrácie na vlnovej dĺžke 1554,13 nm (kanál 29.) s hodnotou šumu RIN −120 dB/Hz.

V prvej fáze bol simulovaný prenos dátového, servisného a kvantového kanálu súbežne bez akýchkoľvek filtrov. Najvýkonnejšie signály sú dátové a servisné kanály,

viď. obr. 2.11, ale kvantový kanál je úplne utopený v šume. Z toho dôvodu je potrebné vybrať filter tak, aby dokázal preniesť kvantový signál spolu s ostatnými, ale pritom neznehodnotiť pôvodné signály.

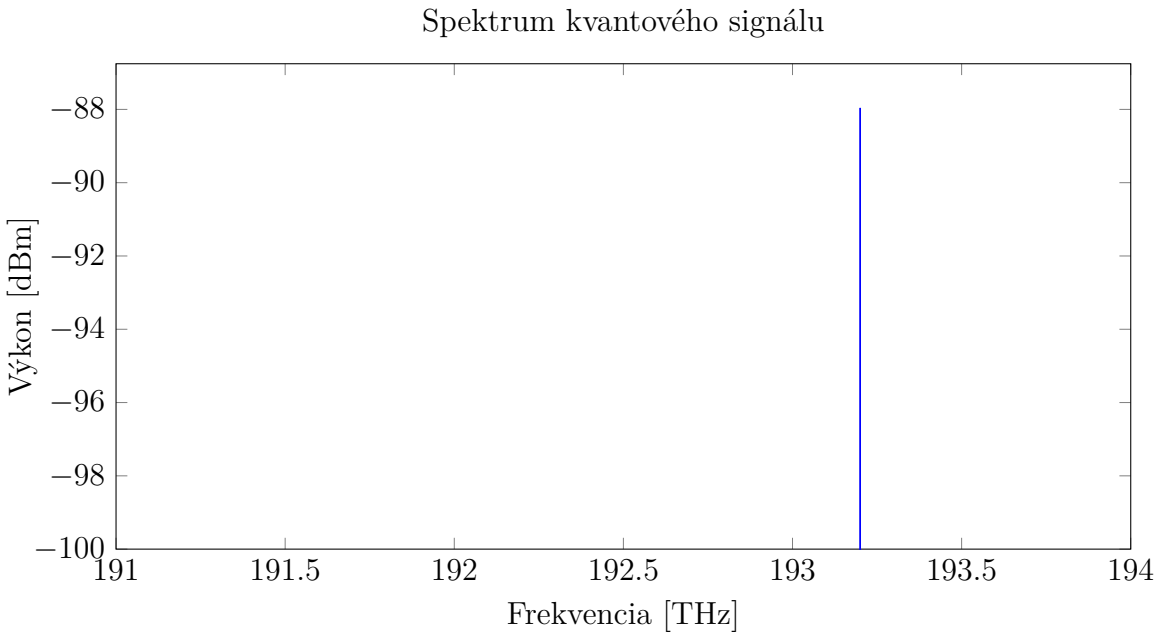


Obr. 2.11: Prvé dva signály zľava sú prenosové dátové o rýchlosti 100 Gb/s a následne sú dva servisné kanály. Kvantový kanál ma úroveň −89 dBm a šum je na úrovni približne −75 dBm, preto ho nie je možné vidieť.

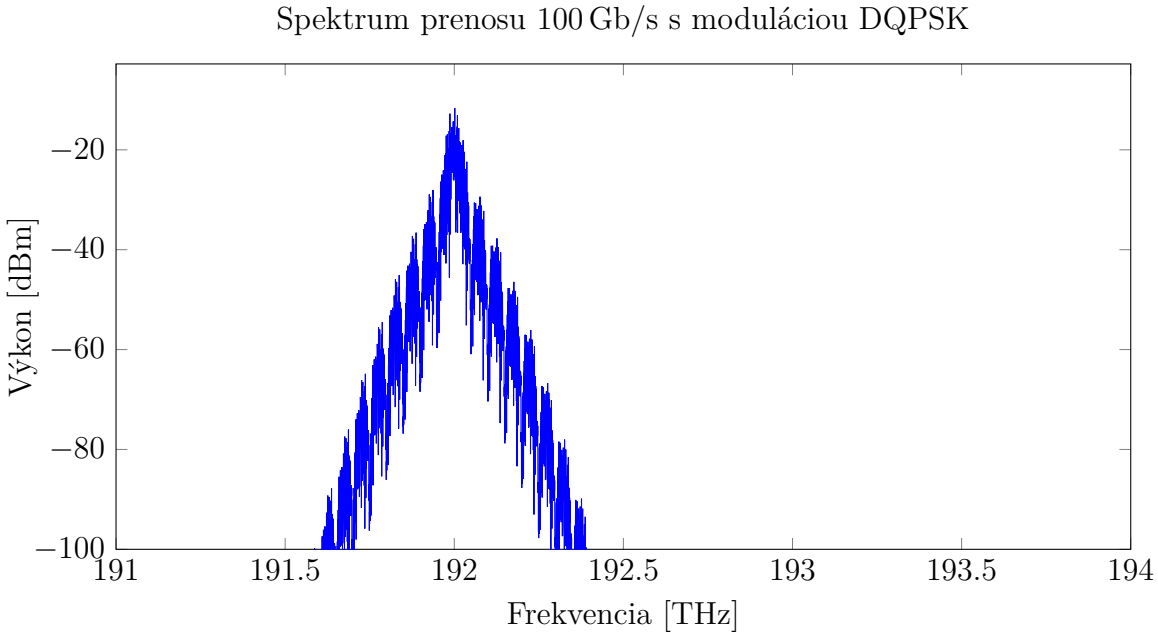
Kvantový signál bol spočítaný ako energia fotónu na vlnovej dĺžke 1551,72 nm, ktorá bola vynásobená frekvenciou prenosu, teda 1,25 GHz a následne redukovaný, keďže každý impulz neobsahuje fotón. Výsledok je −89,208 dBm a jeho spektrum je ideálny impulz, viď. obr. 2.12.

Úroveň zdrojového signálu pre servisný signál je nižšia, ako nastavená hodnota, viď. obr. 2.10, a to kvôli nastaveným reálnym vlastnostiam laseru (šum, fotónový drift, bočný signál zdroja atď.). Spektrum prenosu sa podobá reálnemu spektru laseru. Hodnota šumu sa počas celého spektra drží na hodnote −65 dbm až −70 dBm, čo je vysoko nad prahovou hodnotou kvantového signálu.

Zdrojový signál dátového signálu je podstatne širší ako servisný signál, čo zapríčinila DQPSK modulácia a vysoká prenosová rýchlosti 100 Gb/s, viď obr. 2.13. Spektrum sa postupne rozširuje a je ho potrebné orezať tak, aby nezasahoval do susedných prenosových kanálov a tým nerušil susedné prenosy.



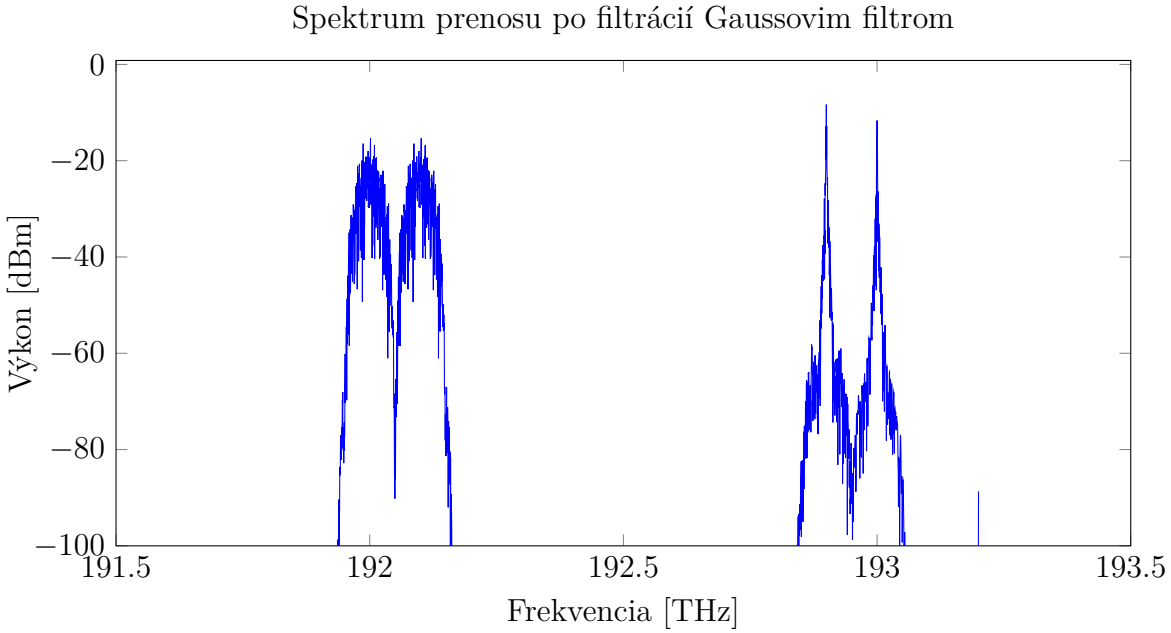
Obr. 2.12: Kvantový signál vysielaný na kanále 32. je podstatne nižšie než komunikácia v bežných optických sieťach, preto je potrebné nastaviť parametre siete tak, aby šum z ostatných vedení neovplyvnil veľmi citlivý prenos kvantového kanálu.



Obr. 2.13: Zdrojový signál dátového prenosu DQPSK na kanále 20. a vlnovej dĺžke 1561,42 nm.

2.4.2 Simulácia Gaussovho filtra

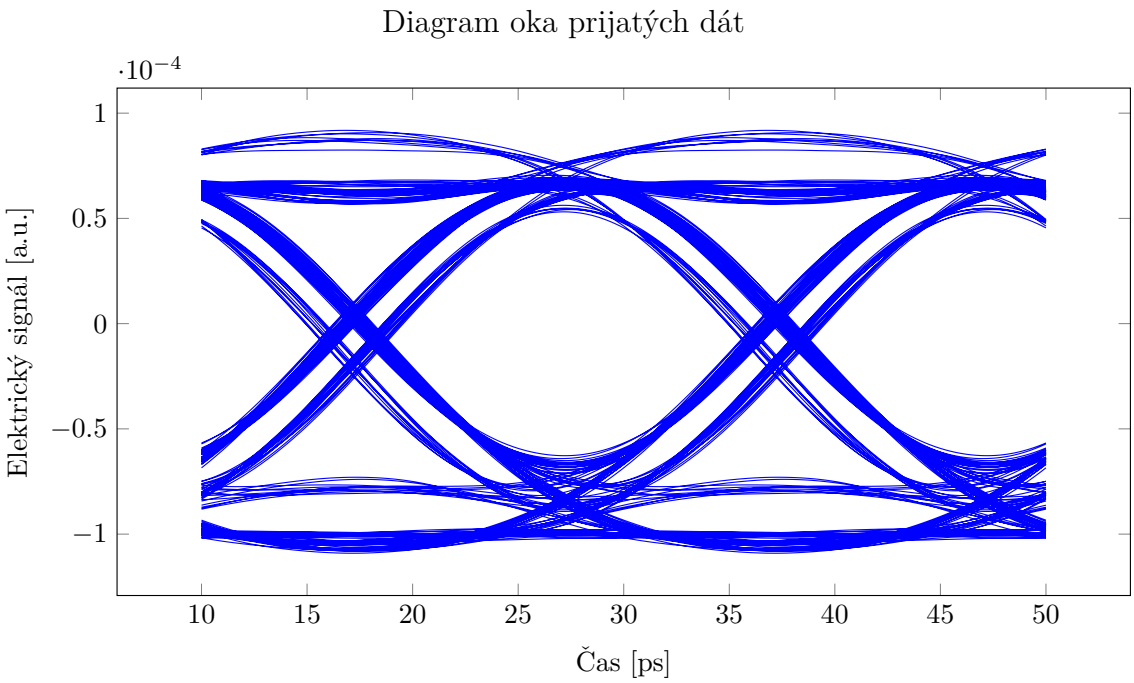
Pre prvú simuláciu bol vybraný Gaussov filter s nastaveným pásmovým priepustom, ktorý sa správa ideálne a potlačí postranný šum úplne dole a je viditeľný dostatočný rozostup (izolácia) medzi dátovými, servisnými a kvantovým kanálom, kde sa jednotlivé signály neovplyvňujú, viď. obr. 2.14. Pri prenose bola nastavená šírka pásma na 75 GHz a stupeň filtrácie 3.



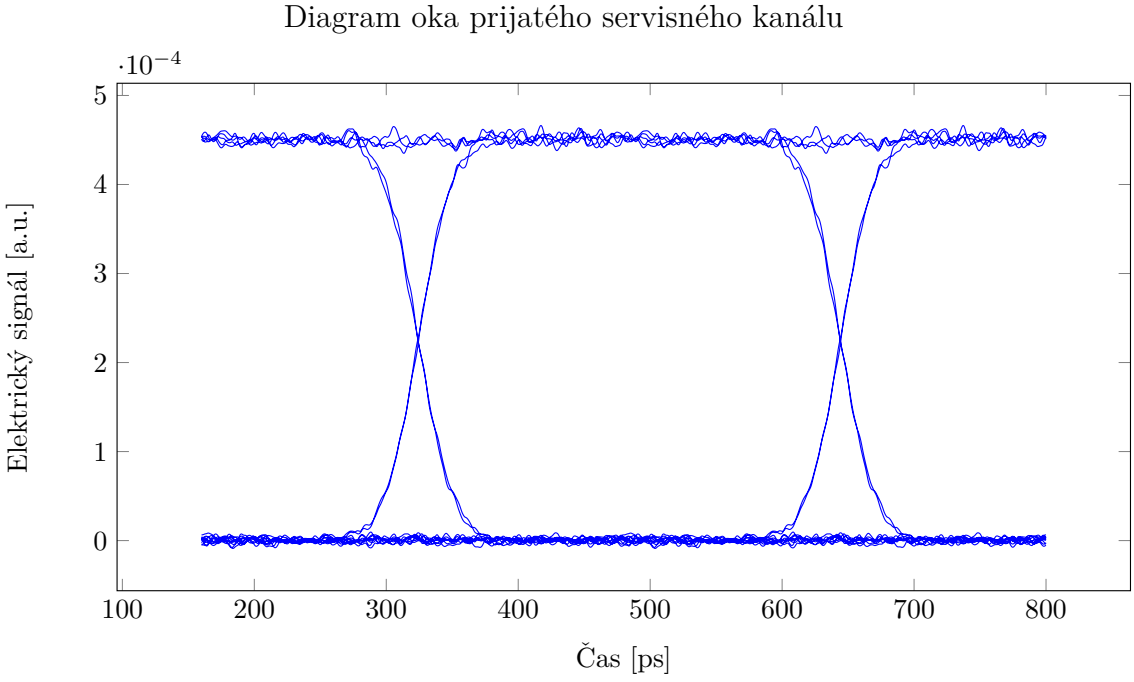
Obr. 2.14: Gaussov filter potlačil šum ideálne a to úplne dole. Pri 100 GHz kanáloch nevnikajú žiadne vzájomné ovplyvnenia medzi jednotlivými kanálmi.

Výstupný diagram oka významne napovie a zhodnotí kvalitatívne parametre prenášaného signálu. S diagramom oka súvisia parametre ako chybovosť, odstup signálu od šumu, premenlivé oneskorenie, medzisymbolová interferencia, atď.. Výstupný diagram prenosu používateľských dát napovedá, že prenos prebehol úspešne s minimálnymi stratami viď. obr. 2.15.

Podobne výstupný diagram oka servisného kanálu má ideálny tvar, kde nie sú viditeľné žiadne nedokonalosti, okrem mierneho zvlnenia v oblasti logickej jednotky, viď. obr. 2.16.



Obr. 2.15: Výstupný signál dátového signálu o rýchlosti 100 Gb/s, filtrovaný cez Gaussov filter so šírkou pásma 75 GHz.

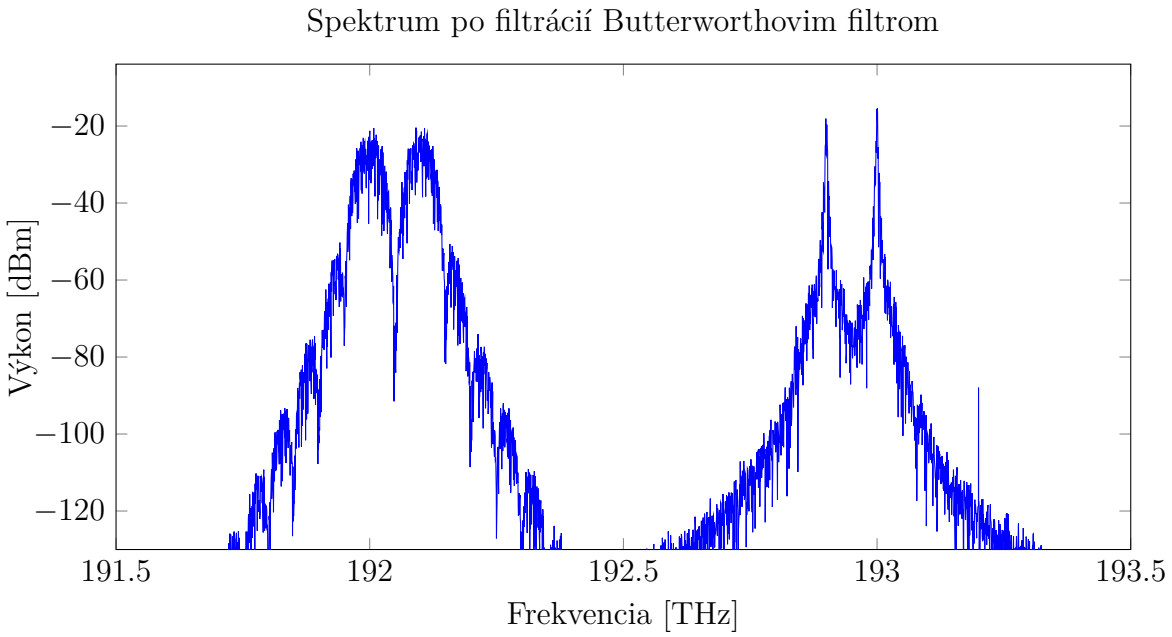


Obr. 2.16: Výstupný signál servisného kanálu, filtrovaný cez Gaussov filter so šírkou pásma 75 GHz.

2.4.3 Simulácia Butterworthovho filtra

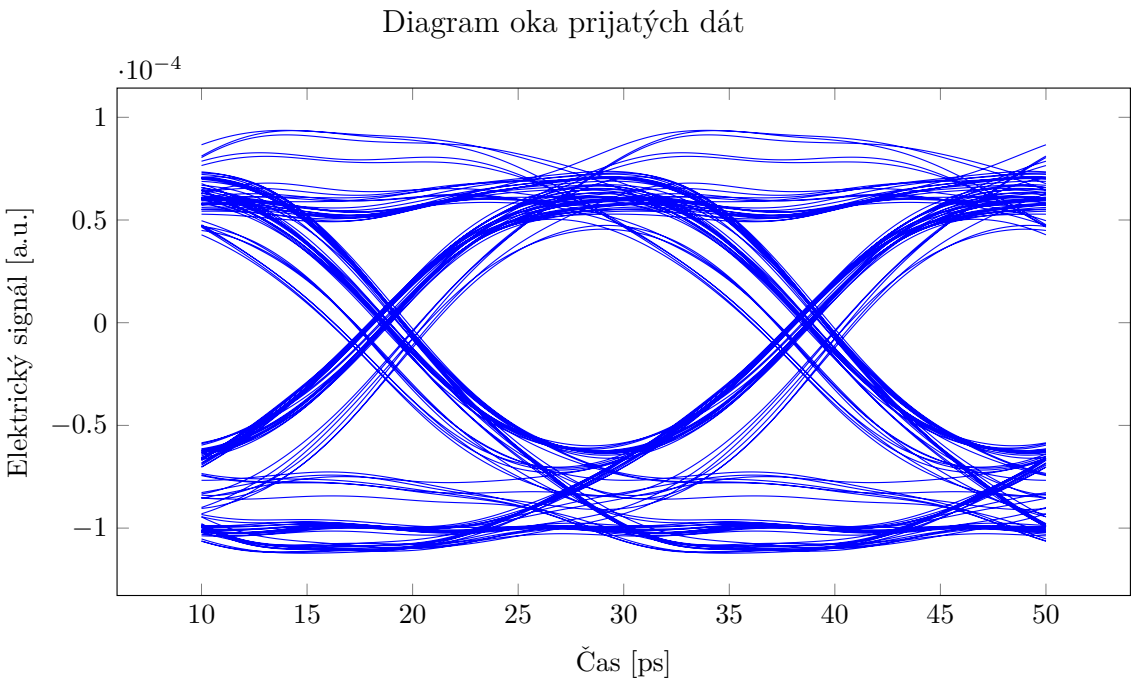
Charakteristika tohoto filtra nie je vôbec ideálna a stále je v bočných pásmach viditeľný šum. Pripomína reálne správanie filtrov, s vytvorením dostatočne veľkej izolácie medzi kanálmi tak, aby bol kvantový signál dostatočne vysoko nad úrovňou šumu, viď. obr. 2.17.

Na filtroch bol nastavený stupeň filtrácie 3 so šírkou pásma filtrácie 75 GHz, aby sa jeho parametre čo najviac priblížili k reálnym vlastnostiam filtrov a potlačili šum na takú úroveň tak, aby vytvoril dostatočnú izoláciu kvantového signálnu.

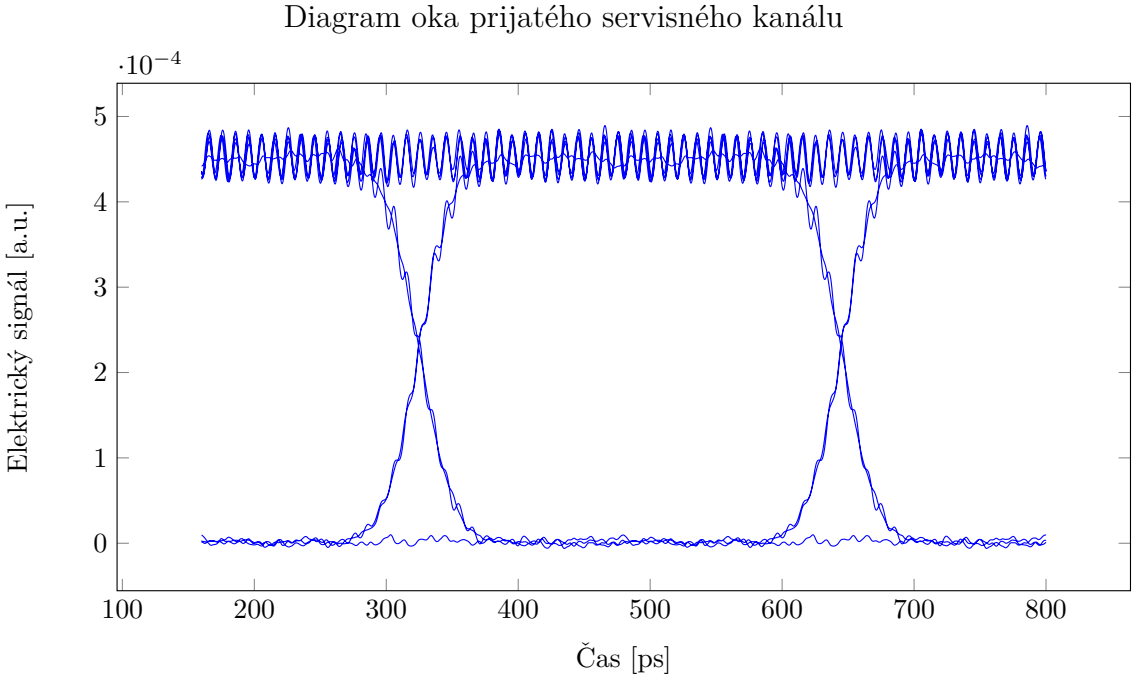


Obr. 2.17: Jeden Butterworthov filter tretieho stupňa bol postačujúci na potlačenie šumu a vytvoril dostatočné veľkú izoláciu kvantového kanála.

Kvantový kanál je nad úrovňou šumu približne −30 dBm, čo by malo zabezpečiť postačujúci odstup od šumu pre bezproblémové spracovanie signálu. Šírka pásma bola nastavená pre všetky filtre rovnako tak, aby sa simuloval ich priebeh a mohlo sa uvažovať, ako blízko pri kvantovom signáli by sa jednotlivé signály mohli vysielať. Ako je z grafov zreteľné, viď. obr. 2.17, vždy je ideálne, aby medzi vysielaním a kvantovým signálom bola medzera, aspoň o šírke jedného kanála. V prípade ak, by vysielací kanál bol hneď vedľa kvantového kanálu filtrácia by musela byť podstatne silnejšia, aby šum nezasahoval do kvantového kanálu.



Obr. 2.18: Výstupný signál dátového signálu o rýchlosti 100 Gb/s, filtrovaný cez Butterworth filter so šírkou pásma 75 GHz.



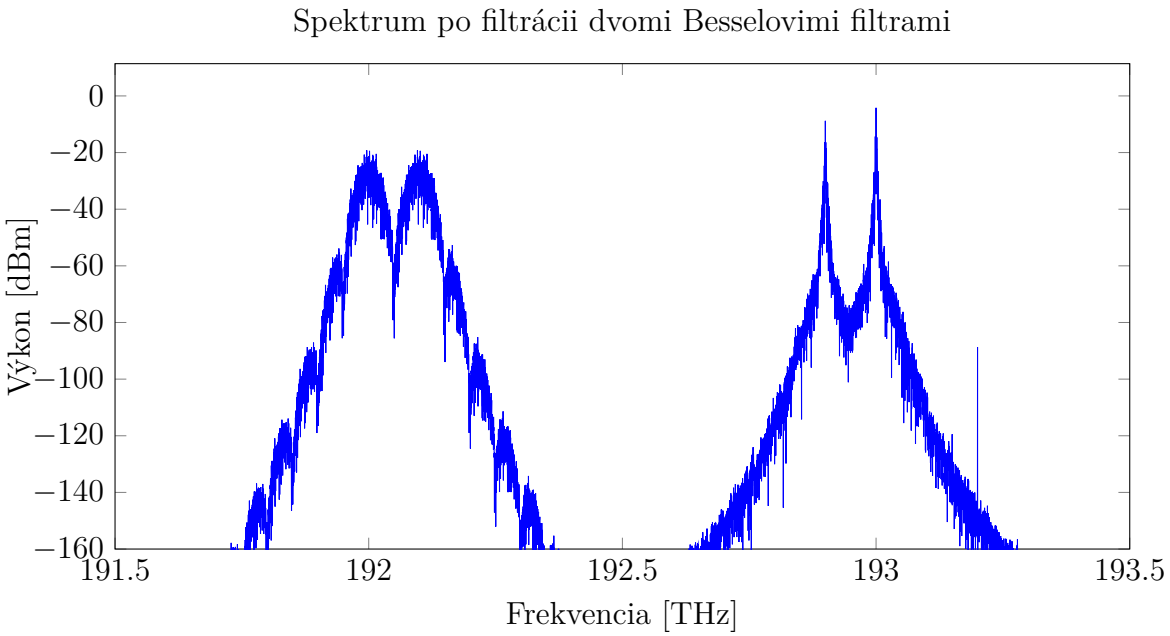
Obr. 2.19: Výstupný signál servisného kanálu, filtrovaný cez Butterworth filter so šírkou pásma 75 GHz.

Diagram oka prenosu dátového prenosu, viď. obr. 2.18, je podstatne rozptýlenejší, než po filtrácií Gaussovým filtrom. Najväčší vplyv na kvalitu signálu malo použitie filtra s nastavenou šírkou pásma na 75 GHz, ale bežné optické prenosy nie je problém obnovovať a zosilovať, čo sa ale nedá povedať o kvantovom signáli.

Na rozdiel od Gaussovho filtra prenos servisného kanála má nedokonale odfiltrovaný signál a do prenášaného 29. kanála zasahuje 30. kanál, čo je vidieť na diagrame oka ako zvlnenie v hornej časti grafu, viď. obr. 2.19. Ale ani takýto vplyv susedného signálu nemá v konečnom dôsledku žiadny dopad na bitovú chybovosť servisného signálu, viď. obr. 2.5.

2.4.4 Simulácia Besselovho filtru

Následne bol zvolený Besselov filter, ktorý má podobnú charakteristiku ako Butterworth filter. Taktiež ako pri všetkých filtroch bol nastavený pásmový priepust o šírke pásma 75 GHz a stupeň filtrácie 3. Nakoľko jeden filter odfiltroval kvantový kanál iba s izoláciou približne −15 dBm, boli použité dva sériovo zapojené filtre. Pri zapojení dvoch filtrov je šum potlačený až na úroveň −150 dBm, viď. obr. 2.20.



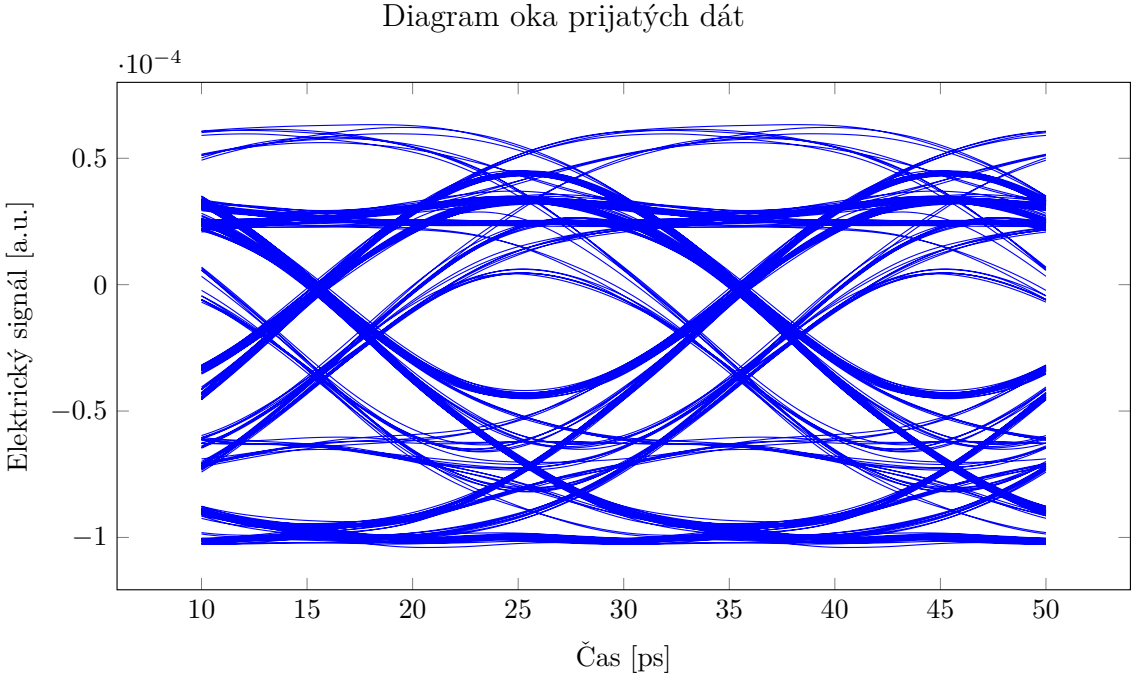
Obr. 2.20: Spektrum prenosu po filtrácií každého prenosu dvomi Besselovými filtrami.

Filtre spôsobili značné poškodenie prenášaného dátového prenosu, viď. obr. 2.21. V porovnaní s ostatnými filtrami, Besselov najvýznamnejšie ovplyvňuje dátový prenos, viď. tab. 2.4. Na druhej strane tento druh filtra ovplyvňuje hlavne vysoko rýchlostné prenosy a nemá takmer žiadny viditeľný vplyv na prenos servisného signálu,

viď. obr. 2.22.

Výstupom všetkých simulácií a porovnaním ich výsledkov je, že Gaussov filter dokázal obsiahnuť všetky vlastnosti filtra, ktoré by na danú komunikáciu boli vyžadované. Následne pre odfiltrovanie kvantového signálu by bol vhodnejší Butterworthov filter ako Besselov. Z dôvodu šetrnosti k prenosu dát je vhodnejší Butterworthov filter.

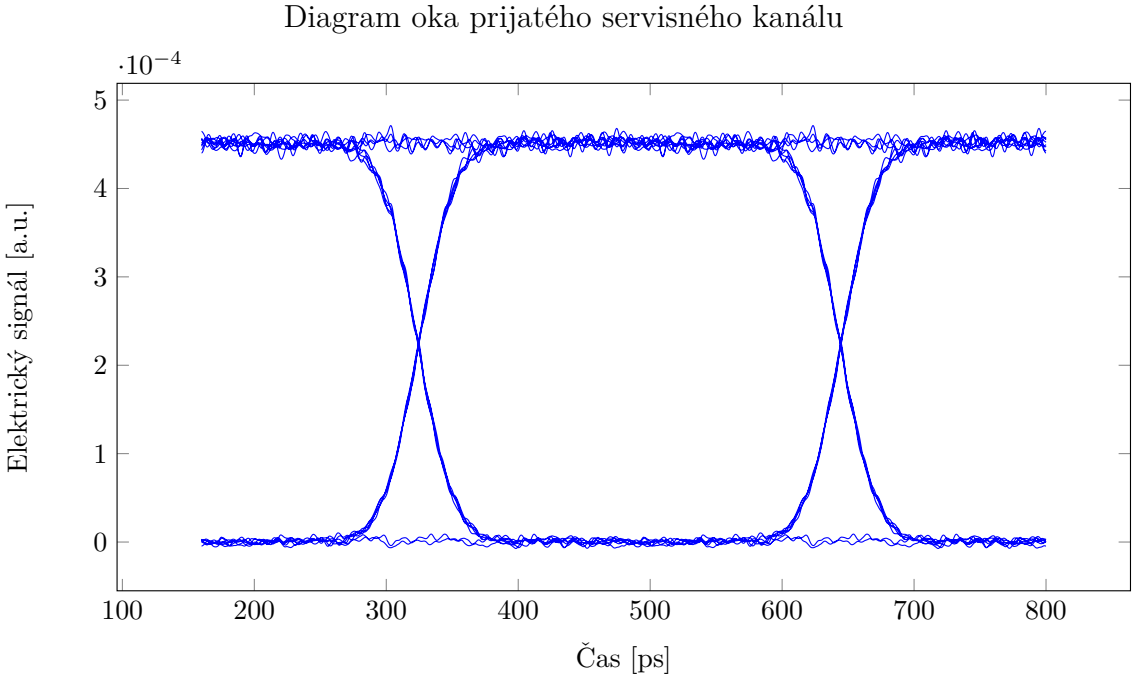
V ďalšej časti bola porovnávaná bitová chybovosť, v závislosti na vzdialenosti prenosu. Simulovaná a testovacia vzdialenosť bola zvolená 250 m a skoro maximálna dovolená teoretická vzdialenosť 60 km. Závislosť filtra na vzdialenosti ukázala vzrast bitovej chybovosti pri vzdialenosti 60 km, ktorá bola predovšetkým spôsobená útlmom optického vlákna. Filter sa správa veľmi podobne pri 250 m, tak aj pri 60 km a nie je viditeľný vplyv druhu filtra na prenosovú vzdialenosť, viď. tab. 2.5.



Obr. 2.21: Výstupný diagram oka dátového signálu o rýchlosti 100 Gb/s, filtrovaný cez dva Besselove filtre so šírkou pásma 75 GHz.

2.4.5 Simulácia reálneho filtru

Po rešerši reálnych filtrov a porovnaniach ich parametrov nie je možné úplne napodobniť správanie reálnych filtrov v prostredí VPIphotonics a nastaviť im reálne parametre. Reálne DWDM a Add/Drop WDM využívajú napríklad TFF (Thin Film Filter). Charakteristickou vlastnosťou takéhoto filtra je pasívny charakter a nízka



Obr. 2.22: Výstupný diagram oka servisného kanála, filtrovaný cez dva Besselove filtre so šírkou pásma 75 GHz.

Tab. 2.4: Porovnanie filtrov a ich závislosť na bitovej chybovosti (BER) prenosov vo vzdialenosti 250 m.

Filter	Sevisný kanál	Dátový prenos
Chybovosť	BER [-]	BER [-]
Gaussov	0	$1{,}3125 \cdot 10^{-11}$
Butterworthov	0	$1{,}2719 \cdot 10^{-5}$
Besselov	0	$4{,}1625 \cdot 10^{-4}$

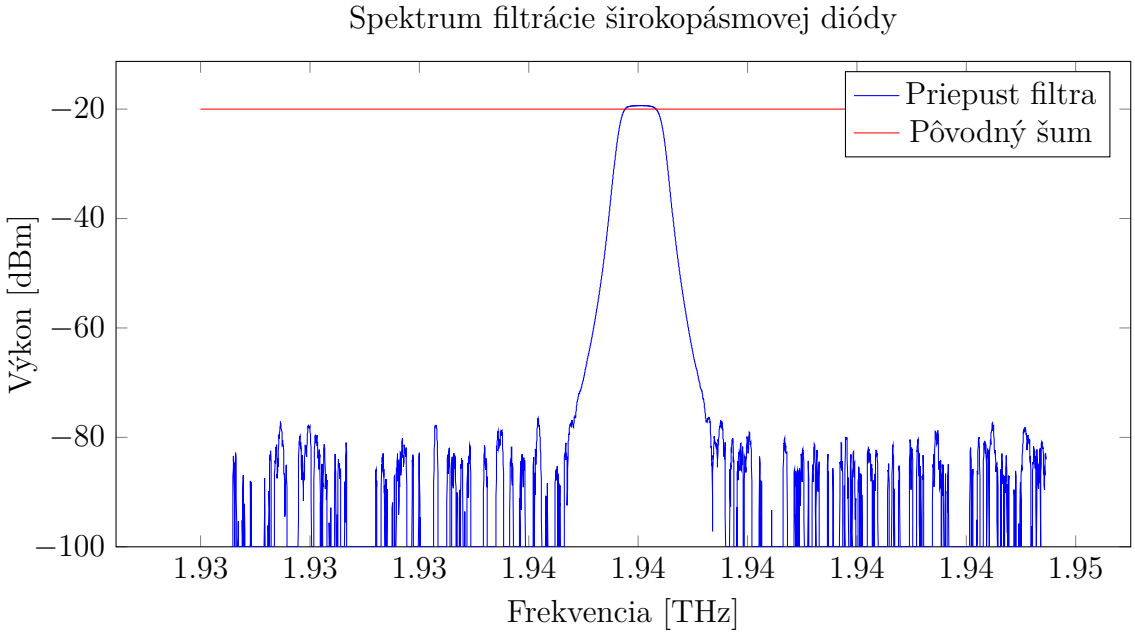
cena. Práve pre takýto filter bola meraná filtračná charakteristika na široko pásmovej dióde, viď. obr. 2.23.

Charakteristika reálneho filtra bola overená praktickým meraním v laboratóriu. Do vybraného filtra „100G CH38 DWDM“ svietila širokopásmová dióda, ktorej spektrum bolo zobrazené ako pôvodný šum a výstupná charakteristika je zobrazená v grafe, viď. obr. 2.23. Tento filter potlačil spektrum okolo kanála do hĺbky −80 dBm, čo zodpovedá potlačeniu signálu približne o 55 dBm. Tvar filtra sa podobá najviac na Gaussov filter, na ktorom nebolo možné nastaviť reálne vlastnosti, ako je napríklad potlačenie šumu do určitej hĺbky. V simulátore vysielací signál servisných kanálov má nastavené reálne vlastnosti z datasheetu a nastavenú hodnotu relatívneho šumu RIN (Relative Intensity Noise) na −120 dB/Hz, viď. obr. 2.10. Úroveň šumu tohto signálu je okolo −65 dBm.

Tab. 2.5: Porovnanie filtrov a ich závislosť na bitovej chybovosti (BER) prenosov vo vzdialenosti 60 km.

Filter	Sevisný kanál	Dátový prenos
Chybovosť	BER [-]	BER [-]
Gaussov	$2{,}1833 \cdot 10^{-7}$	0,0754
Butterworthov	$2{,}0870 \cdot 10^{-7}$	0,0942
Besselov	$2{,}0290 \cdot 10^{-7}$	0,1431

Z toho sa dá predpokladať, že ak by sme mali testovanú topológiu reálnu a pripojili ju do reálneho filtra, ktorého charakteristika je známa, tak hodnota šumu bude potlačená a klesne na −120 dBm, čo je dostatočne nízka úroveň na bezproblémový prenos kvantového kanálu. Z charakteristiky Gaussovho filtra je vidieť, že sa rozširuje veľmi pomaly. Z toho sa dá usúdiť, že by reálny signál neprekonal vzdialenosť celého kanála, čo je v skúmanej simulácií vzdialenosť medzi druhým servisným a kvantovým kanálom.



Obr. 2.23: Zobrazené spektrum použitia reálneho DWDM filtra na široko pásmovú diódu na kanále 38..

Záver

K splneniu cieľa diplomovej práce bolo potrebné naštudovať si problematiku kvantovej distribúcie kľúčov, na ktorej princípe je založený prenos informácií, ktorý zabezpečuje podmienky ich utajenia pred tretími stranami. Na objasnenie tejto problematiky bolo potrebné sa zaoberať oblasťami, ktoré priamo súvisia s procesmi zabezpečujúcimi bezpečný prenos informácií. V práci boli popísané základy kryptografie a kvantovej mechaniky. Podrobne bola vysvetlená problematika qubitu ako základnej jednotky kvantovej informácie a jej meranie. Boli taktiež objasnené potreby vývoja kvantovej kryptografie založenej na QKD ako účinného nástroja na stále sa zvyšujúce kritériá zabezpečenia prenosu informácií s ohľadom na rýchlo sa vyvíjajúce technológie, ktoré v súčasnosti používané technológie na zabezpečenie informácií ohrozujú.

V časti zaoberajúcej sa qubitom boli ukázané jeho možnosti, jeho výhody a nevýhody ako nositeľa informácie a spôsoby jeho merania. Vysvetlený bol princíp fungovania QKD a využitie QKD so znázorneným priebehom výmeny kľúčov.

V ďalšej časti bola vysvetlená štruktúra QKDN podľa štandardov, podstata dôveryhodného uzla a jeho fungovanie. Následne boli vysvetlené delenia protokolov, ich výhody, možnosti použitia a samotný princíp fungovania.

Po prieskume trhu boli preverení a popísaní aktuálni výrobcovia a firmy zaoberajúce sa QKD a boli zistené dostupné komerčné QKD systémy na trhu. Tieto zariadenia boli popísané a vypísané ich parametre. Najvhodnejšími kandidátmi, ktorí komunikovali a mali najlepšiu zverejnenú ponuku zariadení sú Toshiba a ID Quantique.

Praktická časť predstavila využitie zadaného simulačného prostredia QKDNetsim v NS-3 pre simulovanie prenosu QKD. QKDNetsim je primárne smerovaný pre správu kľúčov a ich distribúciu, a nie je zameraný na ich generáciu alebo pre správu kvantového kanála. Boli vytvorené tri druhy simulácii a boli otestované možnosti simulátora.

V ďalšej časti bol vytvorený návrh testovacieho polygónu tak, aby bolo možné simulovanie prenosu používateľských dát súbežne s QKD. Tento polygón bol simulovaný vo VPIphotonics, kde bol simulovaný simultánny prenos dát spoločne s QKD. Hodnoty šumu boli príliš vysoké a prehlušili kvantový signál, preto boli porovnané rôzne filtre tak, aby odfiltrovali šum a neprekryli kvantový kanál. Ideálne dopadol Gaussov, následne Butterworthov a posledný simulovaný Besselov.

Následne bol porovnaný BER v závislosti na vzdialenosti prenosu s použitými filtrami a v poslednej časti bol zobrazený reálny nameraný filter, ktorý bol porovnávaný s nasimulovanými filtrami. Z týchto simulovaných údajov vyplýva, že by pri použití zdrojového signálu, ako bol nastavený v simulácií a potlačení šumu pomo-

cou reálneho filtra, by bol šum dostatočne potlačený tak, aby bol kvantový signál izolovaný od šumu.

Dielčie výsledky práce boli prezentované na študentskej konferencii EEICT 2021.

Literatúra

[1] PETROVSKÝ, Bc. Peter. *Formální analýza kryptografických protokolů*. Brno, 2015. Diplomová práca. VUT Brno. Vedoucí práce Ing. Vlastimil Člupek.

[2] Súčasnosť šifrovania - symetrické a asymetrické šifry, DES, IDEA, RSA, PGP. *Encyklopediapoznania* [online]. Slovensko: Wesline [cit. 2020-11-23]. Dostupné z: https://encyklopediapoznania.sk/clanok/445/sucasnost-sifrovania-symetricke-a-asymetricke-sifry-des-idea-rsa-pgp

[3] JACAK, Monika, Janusz JACAK, Piotr J-ŹWIAK a Ireneusz J-ŹWIAK. Quantum cryptography: Theoretical protocols for quantum key distribution and tests of selected commercial QKD systems in commercial fiber networks.

International Journal of Quantum Information [online]. 2016, **14**(2), -1 [cit. 2020-11-26]. ISSN 02197499. Dostupné z: doi:10.1142/S0219749916300023

[4] ŠEDIVÁ, Kateřina. *Kvantová komunikace*. Zlín, 2017. Bakalárska práca. Univerzita Tomáše Bati ve Zlíne.

[5] Rozdiel medzi kvantovou fyzikou a kvantovou mechanikou. *Mort-sure* [online]. 2020 [cit. 2020-11-24]. Dostupné z: https://sk.mort-sure.com/blog/difference-between-quantum-physics-and-quantum-mechanics/

[6] PIŠÚT, Ján, Ladislav GOMOLČÁK a Vladimír ČERNÝ. *Úvod do kvantovej mechaniky*. Bratislava: Knižničné a edičné centrum FMFI UK, 2008, 376 s. ISBN 978-80-89186-33-4.

[7] *Paradox EPR - EPR paradox Paradox EPR* [online]. Česko: Wikimedia Foundation, 2020 [cit. 2020-11-24]. Dostupné z: https://cs.qaz.wiki/wiki/EPR_paradox

[8] CEJNAR, Pavel a Miloslav DUŠEK. Kvantové hlavolamy IV. *Vesmír* [online]. Česko: VESMÍR, 1998 [cit. 2020-11-24]. Dostupné z: https://vesmir.cz/cz/casopis/archiv-casopisu/1998/cislo-6/kvantove-hlavolamy-iv.html

[9] SVRŠEK, Jiří. EPR paradox a Bellův teorém. *Natura* [online]. Česko: Natura, 1996 [cit. 2020-11-24]. Dostupné z: http://natura.baf.cz/natura/1998/12/9812-8.html

[10] *Princip nejistoty - Uncertainty principle Princip nejistoty* [online]. Česko: Wikimedia Foundation, Inc. Princip nejistoty, 2020 [cit. 2020-11-24]. Dostupné z: https://cs.qaz.wiki/wiki/Uncertainty_principle

[11] Heisebergove vzťahy neurčitosti. *EFyzika* // [online]. Bratislava: Slovenská technická univerzita v Bratislave [cit. 2020-11-24]. Dostupné z: http://kf-lin.elf.stuba.sk/ ballo/STU_online/Fyzika%20II/13%20kapitola/13.4/kvantF4-3.htm

[12] MOKRÁŇ, Michal, Filip VARHANÍK, Boris BALHEIN a Samuel Ján PLESNÍK. Heisenbergov princíp neurčitosti. *Podivný Mikrosvet* [online]. Slovensko: 1sg, 2016 [cit. 2020-11-24]. Dostupné z: http://www.1sg.sk/www/data/01/projekty/2016_2017/elks/Mikrosvet/-neurcitost.html

[13] *Zav_prace_soubor_verejne* [online]. Brno: vutbr, 2016 [cit. 2020-11-24]. Dostupné z: https://www.vutbr.cz/www_base/zav_prace_soubor_verejne.php?-file_id=7676

[14] KŘELINA, Michal. Kvantový seriál — díl 7. — Kvantové sítě — Úvod. *Qubits* [online]. Česko: Quantum Phi, 2020 [cit. 2020-11-24]. Dostupné z: https://qubits.cz/serialy/kvantovy-serial-dil-7-kvantove-site-uvod/

[15] Co je Qubit? *Netinbag* [online]. Amerika: Netinbag, 2020 [cit. 2020-11-24]. Dostupné z: https://www.netinbag.com/cs/internet/what-is-a-qubit.html

[16] What is a qubit? *Quantum-inspire* [online]. Holandsko: QuTech, 2020 [cit. 2020-11-24]. Dostupné z: https://www.quantum-inspire.com/kbase/what-is-a-qubit/

[17] VOJÁČEK, Antonín. Kvantový počítač — princip, funkce, možné použití. *Vyvoj.hw.cz* [online]. Česko: HW server, 2012 [cit. 2020-11-24]. Dostupné z: https://vyvoj.hw.cz/teorie-a-praxe/trendy/kvantovy-pocitac-princip-funkce-mozne-pouziti.html

[18] *Hilbertove priestory*. Slovensko, 2014. Dostupné také z: http://zeus.elf.stuba.sk/Katedry/KM/predmety/ufa/ufa2.pdf

[19] HOVANOVÁ, Bc. Tatiana. *Kvantově bezpečná kryptografie*. Brno, 2019. Bakalárska práca. VUT Brno. Vedoucí práce Prof. Ing. Jiří Mišurec, CSc.

[20] *Kvantový seriál — díl 2. — Kvantové počítače — Qubit* [online]. Česko: Quantum Phi, 2020 [cit. 2020-11-24]. Dostupné z: https://qubits.cz/serialy/kvantovy-serial-dil-2-kvantove-pocitace-qubit/?fbclid=IwAR0qsFmpVSNPbEgDuMEPLkoQhptd_OPOJYxHepsp6t-ToYZfNa5klL7gD8FI

[21] ŠIBÍK, Juraj. *Kvantové výpočty*. Praha, 2008. Bakalárska práca. Univerzita Karlova v Prahe. Vedoucí práce Prof. RNDr. Lubomír Skála, DrSc.

[22] STRÁSKÝ, Josef. *Kvantová kryptografie*. Praha, 2008. Bakalárska práca. Univerzita Karlova v Prahe. Vedoucí práce Prof. RNDr. Lubomír Skála, DrSc.

[23] REICHL, Jaroslav. Polarizace světla. *Jreichl* [online]. Česko: SPŠST Panská v Praze, 2017 [cit. 2020-11-24]. Dostupné z: http://fyzika.jreichl.com/main.article/view/462-polarizace-svetla

[24] Polarizace světla. *WikiSkripta* [online]. Praha: Univerzita Karlova, 2020 [cit. 2020-11-24]. Dostupné z: https://www.wikiskripta.eu/w/Polarizace_sv%C4%9Btla

[25] *Svet kvantovej fyziky III* [online]. Česko: Quark, 2005 [cit. 2020-11-24]. Dostupné z: http://www.quantum.physics.sk/rcqi/docs/popular/quark_qm3.pdf

[26] *Kvantová superpozice - Quantum superposition* [online]. Česko: Wikimedia Foundation, 2020 [cit. 2020-11-24]. Dostupné z: https://cs.qaz.wiki/wiki/Quantum_superposition

[27] KOTHARI, Abhishek. Qubit By Qubit. *Medium* [online]. Amerika: medium, 2018 [cit. 2020-11-24]. Dostupné z: https://medium.com/@abhishekkothari/qubit-by-qubit-104139024edc

[28] RUSSELL, J. Application of Quantum Key Distribution. *MILCOM 2008 - 2008 IEEE Military Communications Conference* [online]. 2008, **2008**(1), 1-6 [cit. 2020-11-24]. Dostupné z: doi:10.1109/MILCOM.2008.4753169

[29] *Kvantový seriál — díl 9. — Kvantové sítě — Současná situace* [online]. Česko: Quantum Phi, 2020 [cit. 2020-11-24]. Dostupné z: https://qubits.cz/serialy/kvantovy-serial-dil-9-kvantove-site-soucasna-situace/

[30] ELLIOTT, C. Quantum cryptography. *IEEE Security Privacy* [online]. 2004, **2004**(2), 57-61 [cit. 2020-11-24]. Dostupné z: doi:10.1109/MSP.2004.54

[31] JAKUBÍČEK, Michal. *Návrh zabezpečení systému dálkového měření kvality dodávky elektrické energie*. Brno, 2013. Bakalárska práca. VUT Brno. Vedoucí práce Ing. Petr Mlýnek, Ph.D.

[32] What is Quantum Key Distribution? *Quintessencelabs* [online]. Amerika: cloudsecurityalliance.org, 2015 [cit. 2021-5-5]. Dostupné z: https://www.quintessencelabs.com/wp-content/uploads/2015/08/CSA-What-is-Quantum-Key-Distribution-QKD-1.pdf

[33] *What is Quantum Key Distribution?*. Singapur, 2020. Dostupné také z: https://www.quintessencelabs.com/wp-content/uploads/2015/08/CSA-What-is-Quantum-Key-Distribution-QKD-1.pdf

[34] Y.3800. *Overview on networks supporting quantum key distribution*. 1. Geneva, Switzerland: ITU, 2019.

[35] *Protocol and data format of REST-based key delivery API*. GS QKD 014. Sophia Antipolis Cedex - FRANCE: ETSI, 2019.

[36] ROUSE, Margaret. Quantum key distribution (QKD). *SearchsScurity* [online]. Amerika: TechTarget, 2020 [cit. 2020-11-25]. Dostupné z: https://searchsecurity.techtarget.com/definition/quantum-key-distribution-QKD

[37] ELBOUKHARI, M., A. AZIZI a M. AZIZI. Quantum Key Distribution in practice: The state of art. *2010 5th International Symposium On I/V Communications and Mobile Network* [online]. 2010, **2010**(1), 1-4 [cit. 2020-11-25]. Dostupné z: doi:10.1109/ISVC.2010.5656421

[38] NURHADI, A. I. a N. R. SYAMBAS. Quantum Key Distribution (QKD) Protocols: A Survey. *2018 4th International Conference on Wireless and Telematics (ICWT)* [online]. 2018, **2018**(1), 1-5 [cit. 2020-11-27]. Dostupné z: doi:10.1109/ICWT.2018.8527822

[39] TUTORIAL: CONTINUOUS-VARIABLE QUANTUM COMMUNICATION. *Infiniquant* [online]. Germany: infiniquant, 2020 [cit. 2020-11-27]. Dostupné z: http://infiniquant.com/tutorial-continuous-variable-quantum-communication/

[40] LOPES, Minal a Nisha SARWADE. Cryptography from Quantum Mechanical Viewpoint. *International Journal on Cryptography and Information Security* [online]. 2014, **2014**(4), 1-25 [cit. 2020-11-27]. Dostupné z: doi:10.5121/ijcis.2014.4202

[41] CALVER, Timothy I. *AN EMPIRICAL ANALYSIS OF THE CASCADE SECRET KEY RECONCILIATION PROTOCOL FOR QUANTUM KEY DISTRIBUTION*. Ohio, 2011. THESIS. Wright-Patterson Air Force Base.

[42] YIN, Zhen-Qiang, Shuang WANG, Wei CHEN, Yun-Guang HAN, Rong WANG, Guang-Can GUO a Zheng-Fu HAN. Improved security bound for the round-robin-differential-phase-shift quantum key distribution. *Nature Communications*. 2018, **9**(1), 457. ISSN 2041-1723. Dostupné z: doi:10.1038/s41467-017-02211-x

[43] STUCKI, Damien, Sylvain FASEL, Nicolas GISIN, Yann THOMA a Hugo ZBINDEN. Coherent one-way quantum key distribution. *Proc SPIE*. 2007/05/04. Dostupné z: doi:10.1117/12.722952

[44] *Components and Internal Interfaces*. GR QKD 003 V2.1.1. France: ETSI, 2018.

[45] PIRANDOLA, S., U. L. ANDERSEN, L. BANCHI, et al. Advances in Quantum Cryptography. *ArXiv*. 2020.

[46] Private/Startup Companies. *Quantum Computing Report* [online]. Amerika: Quantum Computing Report, 2020 [cit. 2020-12-06]. Dostupné z: https://quantumcomputingreport.com/privatestartup/

[47] *ID Quantique* [online]. Switzerland: ID Quantique, 2020 [cit. 2020-12-06]. Dostupné z: https://www.idquantique.com/

[48] *Quantum Key Distribution* [online]. Japan: Toshiba, 2020 [cit. 2020-12-06]. Dostupné z: https://www.toshiba.co.jp/qkd/en/index.htm

[49] *QKDNETSIM* [online]. Česko, Bosnia and Herzegovina: QKDNetSim Team, 2020 [cit. 2020-12-10]. Dostupné z: https://www.qkdnetsim.info/

[50] *Ns-3 Network Simulator* [online]. CC BY-SA 4.0, 2020 [cit. 2020-12-10]. Dostupné z: https://www.nsnam.org/

[51] KLOBUŠICKÝ, Ivan. *Smerovanie v mobilných ad hoc sieťach*. Bratislava, 2010. Bakalárska práca. FIIT STU. Vedoucí práce Ing. Peter Magula.

[52] G.652. *SERIES G: TRANSMISSION SYSTEMS AND MEDIA, DIGITAL SYSTEMS AND NETWORKS: Transmission media and optical systems characteristics — Optical fibre cables*. 11/2016. Geneva, Switzerland: ITU, 2016.

[53] CHEN, X., P. R. HORCHE a A. M. MINGUEZ. Analysis of signal impairment and crosstalk penalty induced by different types of optical filters in 100 Gbps PM-DQPSK based systems. In: *2014 19th European Conference on Networks and Optical Communications - (NOC)*. 2014, s. 35-40. Dostupné z: doi:10.1109/NOC.2014.6996824

Zoznam symbolov, veličín a skratiek

AES Advanced Encryption Standard

AODV Ad hoc On-demand Distance Vector

API

BER Bit Error Rate Application programming interface

COW Coherent One Way

CV Continuous Variable

DV Discrete Variable

DPR Distributed Phase Reference

DPS Differential Phase Shift

DES Data Encryption Standard

DSDV Destination-Sequenced Distance Vector Protocol

DFB Distributed Feedback Laser

DSA Digital Signature Algorithm

DWDM Dense Wavelength Division Multiplexing

DQPSK Differential Quadrature PhaseShift Keying

ETSI European Telecommunications Standards Institute

HMAC keyed-Hash Message Authentication Code

ITU International Telecommunication Union

IDEA International Data Encryption Algorithm

IP Internet Protocol

KM Key Mnagment

KMIP Key Management Interoperability Protocol

KM Key management

LEA Light Encryption Algorithm

LTE	Long Term Evolution
NS-3	Network Simulator 3
OLSR	Optimized Link-State Routing Protocol
OTP	One Time Pad
PBS	Polarisation Beam Splitter
P2P	Point to Point
QBER	Quantum Bit Error Rate
QKD	Quantum Key Distribution
QKDN	Quantum Key Distribution Network
Qubit	Quantum bit
QoS	Quality of Service
QSFP	Quad Small Form-factor Pluggable
RSA	Rivest, Shamir, Adleman
RIN	Relative Intensity Noise
RC4	Rivest Cipher 4
SPDC	Spontaneous Parametric Down Conversion
SFP	Small Form-factor Pluggable
Wi-Fi	Wireless Fidelity
WiMAX	World Interoprability For Microwave Access
WDM	Wavelength Division Multiplexing
km	Kilometer
dB	DeciBell
dBm	DeciBell na milliWatt
kb/s	Kilobit za sekundu
W	Watt

Mb/s	Megabit za sekundu
Gb/s	Gigabit za sekundu
nm	Nanometer
dB/m	DeciBell na meter