



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

KVANTOVÁ DISTRIBUCE KLÍČŮ

QUANTUM KEY DISTRIBUTION

DIPLOMOVÁ PRÁCE

MASTER'S THESIS

AUTOR PRÁCE

AUTHOR

Bc. Ondřej Klíčník

VEDOUCÍ PRÁCE

SUPERVISOR

doc. Ing. Petr Münster, Ph.D.

BRNO 2023

Diplomová práce

magisterský navazující studijní program **Informační bezpečnost**

Ústav telekomunikací

Student: Bc. Ondřej Klíčnický

ID: 211259

Ročník: 2

Akademický rok: 2022/23

NÁZEV TÉMATU:

Kvantová distribuce klíčů

POKYNY PRO VYPRACOVÁNÍ:

Cílem diplomové práce je detailní rozbor problematiky kvantové distribuce klíčů (QKD) a popis současného stavu. Bližší zaměření práce bude na bezpečnost kvantových přenosů a rovněž možnost sdílení vlákna kvantovým a datovými signály současně. V rámci praktické části práce budou provedena experimentální měření simulující vybrané útoky na kvantovou infrastrukturu s cílem odepření služby. Současně bude navrženo a připraveno pracoviště pro experimentální ověření možnosti sdílení optického vlákna kvantovým a datovými signály současně.

DOPORUČENÁ LITERATURA:

- [1] I. B. Djordjevic, Physical-Layer Security and Quantum Key Distribution. Springer, 2019.
- [2] M. Filka, Optoelektronika pro telekomunikace a informatiku, Druhé, rozšířené vydání. Brno: Prof. Ing. Miloslav Filka, Csc. a kol., 2017.

Termín zadání: 6.2.2023

Termín odevzdání: 19.5.2023

Vedoucí práce: doc. Ing. Petr Münster, Ph.D.

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

UPOZORNĚNÍ:

Autor diplomové práce nesmí při vytváření diplomové práce porušit autorská práva třetích osob, zejména nesmí zasahovat nedovoleným způsobem do cizích autorských práv osobnostních a musí si být plně vědom následků porušení ustanovení § 11 a následujících autorského zákona č. 121/2000 Sb., včetně možných trestněprávních důsledků vyplývajících z ustanovení části druhé, hlavy VI. díl 4 Trestního zákoníku č.40/2009 Sb.

ABSTRAKT

Tato diplomová práce nepřímo navazuje na bakalářskou práci Kvantová distribuce klíčů přes optickou vláknovou infrastrukturu [1]. Na rozdíl od předchozího dokumentu bude pozornost zaměřena zejména na praktické použití QKD (Quantum key distribution) systému Clavis³. Z tohoto důvodu jsou v teoretické části stručně vysvětleny fyzikální jevy vztahující se k v praxi používaným QKD protokolům, které jsou většinou založeny na fázovém kódování. Speciální pozornost je věnována zejména protokolu COW (Coherent one-way protocol) implementovaném v zařízeních Clavis³. Tento protokol je rovněž srovnán s praktickými implementacemi protokolu BB84. Dále jsou nastíněny principy dalších pokročilých QKD technik a rozebrány jevy v optickém vlákně, které mohou mít vliv na kvantový kanál. Samostatná kapitola je také věnována standardizaci a topologiím QKD sítí. V neposlední řadě se pak práce věnuje tématu útoků proti praktickým implementacím QKD protokolů.

V praktické části jsou provedena měření zacílená na praktické nasazení zařízení Clavis³ v běžné komunikační síti. Jedná se zejména o možnost sloučení kvantového kanálu do jednoho vlákna spolu s klasickými kanály pomocí WDM (Wavelength-division multiplex) a analýzu vlivu Ramanova šumu na maximální komunikační vzdálenost. Současně je ověřena odolnost systému proti změnám polarizace a manipulaci s vláknem. V neposlední řadě je srovnán výkon systému při použití třístavové a čtyřstavové verze protokolu COW a otestován přípravek pro simulaci odposlechu.

KLÍČOVÁ SLOVA

Clavis³, COW protokol, destilace, Grafana, hacking, kvantová distribuce klíčů (QKD), kvantová mechanika, nelineární jevy, QKD síť (QKDN), QKD polygon, standardizace, Ubuntu, vlnový multiplex (WDM)

ABSTRACT

This thesis is indirectly related to the bachelor thesis Quantum key distribution over optical fiber infrastructure [1]. Unlike the previous paper, the focus will be mainly on the practical application of the QKD (Quantum key distribution) system Clavis³. For this reason, physical phenomena related to practically used QKD protocols are briefly explained in the theoretical part. These are mostly based on phase coding. In particular, special attention is paid to the Coherent one-way protocol (COW) implemented in Clavis³ devices. This protocol is also compared with practical implementations of the BB84 protocol. Furthermore, the principles of other advanced QKD techniques are outlined and the phenomena in the optical fiber that may affect the quantum channel are discussed. A separate chapter is also devoted to standardization and topologies of QKD networks. Last but not least, the thesis addresses the topic of attacks against practical implementations of QKD protocols.

In the practical part, measurements aimed at practical deployment of Clavis³ devices in a common communication network are performed. These include the possibility of combining a quantum channel into a single fiber together with classical channels using Wavelength-division multiplexing (WDM) and the analysis of the effect of Raman noise on the maximum communication distance. At the same time, the robustness of the system against polarization changes and fiber manipulation is verified. Finally, the performance of the system using three-state and four-state versions of the COW protocol is compared and the eavesdropping simulation module is tested.

KEYWORDS

Clavis³, COW protocol, distillation, Grafana, hacking, quantum key distribution (QKD), quantum mechanics, nonlinear phenomena, QKD network (QKDN), QKD polygon, standardization, Ubuntu, WDM (wavelength-division multiplex)

KLÍČNÍK, Ondřej. *Kvantová distribuce klíčů*. Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav telekomunikací, 2023, 185 s. Semestrální práce. Vedoucí práce: doc. Ing. Petr Münster, Ph.D.

Prohlášení autora o původnosti díla

Jméno a příjmení autora: Bc. Ondřej Klíčnick
VUT ID autora: 211259
Typ práce: Semestrální práce
Akademický rok: 2022/23
Téma závěrečné práce: Kvantová distribuce klíčů

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

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

Brno

.....
podpis autora*

*Autor podepisuje pouze v tištěné verzi.

PODĚKOVÁNÍ

Rád bych poděkoval vedoucímu diplomové práce panu doc. Ing. Petru Münsterovi, Ph.D. za odborné vedení, konzultace, trpělivost a podnětné návrhy k práci. Dále pak své rodině, která mě v průběhu studia podporovala.

Obsah

| | |
|---|-----------|
| Úvod | 23 |
| 1 Fyzikální základ | 25 |
| 1.1 Foton | 25 |
| 1.2 Fáze a polarizace | 26 |
| 1.2.1 Polarizátory | 27 |
| 1.3 Interference a koherence | 28 |
| 1.3.1 Machův-Zehnderův interferometr | 29 |
| 1.4 Qubit | 31 |
| 1.5 Rozlišení kvantových stavů | 32 |
| 2 Cesta k COW protokolu | 33 |
| 2.1 BB84: Bennett & Brassard (1984) | 33 |
| 2.1.1 BB84 – Polarizační kódování | 34 |
| 2.1.2 BB84 – Fázové kódování | 35 |
| 2.2 COW protokol | 37 |
| 2.3 Sledované parametry COW protokolu | 39 |
| 2.3.1 Útoky na COW protokol | 41 |
| 3 Destilace klíče | 43 |
| 3.1 Oprava chyb (Error correction) | 43 |
| 3.1.1 LDPC algoritmus pro QKD | 44 |
| 3.2 Zesílení bezpečnosti (Privacy amplification) | 46 |
| 3.2.1 Kompresní poměr | 46 |
| 3.3 Autentizace (Authentication) | 47 |
| 4 Kvantový hacking | 49 |
| 4.1 Útok dělením počtu fotonů (PNS attack) | 51 |
| 4.2 Útok dělením paprsku (Beam splitting attack) | 52 |
| 4.3 Útoky založené na USD | 52 |
| 4.4 Muž uprostřed (Man in the middle attack) | 53 |
| 4.5 Trojský kůň (Trojan horse attack) | 54 |
| 4.6 Útok na neaktivní detektor (Dead-time attack) | 55 |
| 4.7 Útok falešnými stavy (Faked states attack) | 56 |
| 4.8 Útok časovým posunem (Time-shift attack) | 57 |
| 4.9 Ostatní významné útoky | 57 |

| | | |
|----------|---|-----------|
| 5 | Kontrafaktuální definitivnost | 59 |
| 5.1 | Elitzurův-Vaidmanův tester bomb | 59 |
| 5.2 | Kontrafaktuální kvantová kryptografie (CQC) | 60 |
| 6 | Techniky prodloužení dosahu QKD | 63 |
| 6.1 | Důvěryhodný opakovač (Trusted repeater) | 63 |
| 6.2 | QKD nezávislé na měřicím zařízení (MDI-QKD) | 63 |
| 6.3 | Kvantový opakovač | 64 |
| 7 | Nežádoucí jevy ve vlákne | 65 |
| 7.1 | Útlum | 65 |
| 7.1.1 | Lineární útlum | 66 |
| 7.1.2 | Nelineární útlum | 66 |
| 7.1.3 | Logaritmické jednotky | 67 |
| 7.1.4 | Útlum a ztráty | 68 |
| 7.1.5 | Složky celkového útlumu trasy | 69 |
| 7.1.6 | Útlumové články | 71 |
| 7.1.7 | Zesilovače a opakovače klasických signálů | 71 |
| 7.2 | Disperze | 73 |
| 7.2.1 | Vidová disperze | 73 |
| 7.2.2 | Chromatická disperze | 73 |
| 7.2.3 | Polarizační vidová disperze (PMD) | 74 |
| 7.3 | Šum a přeslech | 75 |
| 7.3.1 | Spontánní a stimulovaná emise | 75 |
| 7.3.2 | Zesílená spontánní emise (ASE) | 75 |
| 7.3.3 | Kerrův jev | 76 |
| 7.4 | Rozptyl | 78 |
| 7.4.1 | Elastický rozptyl | 78 |
| 7.4.2 | Neelastický rozptyl | 80 |
| 7.4.3 | Brillouinův rozptyl | 83 |
| 8 | Topologie a standardizace | 85 |
| 8.1 | Referenční model | 86 |
| 8.1.1 | QKD modul (QKDE) | 89 |
| 8.1.2 | Systém pro správu klíčů (KME) | 90 |
| 8.1.3 | QKDN/SDN kontrolér | 91 |
| 8.1.4 | Softwarově definované sítě (SDN) | 92 |
| 8.2 | Reálné zapojení | 93 |
| 8.2.1 | Postkvantová kryptografie | 93 |
| 8.2.2 | Příklad kvantově chráněné sítě | 94 |

| | | |
|-----------|---|------------|
| 9 | Zařízení Clavis³ | 97 |
| 9.1 | Popis systému | 97 |
| 9.2 | Parametry systému | 98 |
| 9.3 | Eva | 99 |
| 9.4 | Současná topologie systému | 100 |
| 9.4.1 | Prvky systému | 100 |
| 9.4.2 | Správa a monitorování | 102 |
| 9.4.3 | Vlastní monitorování | 102 |
| 9.5 | Analýza bezpečnosti | 103 |
| 9.5.1 | Klasické algoritmy v QKD systému | 103 |
| 9.5.2 | Správa systému | 103 |
| 9.5.3 | Klasický kanál | 105 |
| 10 | Měření na mezifakultní optické trase | 107 |
| 10.1 | Trasa FEKT–FIT v Brně | 107 |
| 10.2 | Třístavový a čtyřstavový COW protokol | 108 |
| 10.2.1 | Srovnání | 108 |
| 10.2.2 | Výsledky měření | 110 |
| 10.3 | Vliv změn polarizace | 111 |
| 10.3.1 | Výsledky měření | 113 |
| 10.4 | Vliv manipulace s vláknem | 114 |
| 10.4.1 | Výsledky měření | 115 |
| 10.5 | Vliv zpoždění části pulzů | 116 |
| 10.5.1 | Výsledky měření | 117 |
| 11 | Sloučení kvantového a servisních kanálů | 119 |
| 11.1 | Fáze I: Návrh a ověření bezpečnosti prvotní trasy | 120 |
| 11.2 | Fáze 2: Tlumení servisních kanálů | 122 |
| 11.2.1 | Přeslech nebo šum? | 125 |
| 11.2.2 | Ramanův šum | 126 |
| 11.3 | Fáze 3: Sestavení a ladění finální trasy | 127 |
| 11.3.1 | Snižování délky trasy | 131 |
| 11.4 | Výsledky měření | 133 |
| | Závěr | 135 |
| | Literatura | 137 |
| | Seznam symbolů a zkratk | 151 |
| | Seznam příloh | 159 |

| | | |
|----------|---|------------|
| A | Srovnání kvality 100GHz filtrů | 161 |
| A.1 | Výkon laseru | 162 |
| A.2 | Směr PASS → COM | 163 |
| A.3 | Směr PASS → REF | 166 |
| A.4 | Směr REF → COM | 169 |
| A.5 | Kvalita provedení filtrů | 172 |
| A.6 | Vložný útlum a izolace filtrů | 174 |
| A.6.1 | Vložný útlum | 174 |
| A.6.2 | Izolace sousedních kanálů | 175 |
| B | Výpočet Ramanova rozptylu | 177 |
| C | Standardy pro QKD | 179 |
| C.1 | ETSI | 179 |
| C.2 | ITU-T | 182 |
| C.3 | IEEE | 185 |
| C.4 | ISO/IEC | 185 |

Seznam obrázků

| | | |
|-----|--|----|
| 1.1 | Elektromagnetické spektrum [6]. | 25 |
| 1.2 | Přibližná útlumová křivka optických vláken [7]. | 26 |
| 1.3 | Příklad využití polarizátorů [13]. | 28 |
| 1.4 | Konstruktivní (vlevo) a destruktivní interference (vpravo) [14, 15]. . . | 28 |
| 1.5 | Průchod světla k detektorům A a B horní a spodní větvi [16, 17]. . . | 29 |
| 1.6 | Zleva téměř 100% viditelnost, 50% viditelnost a téměř nulová viditelnost [18]. | 30 |
| 1.7 | Blochova koule [20]. | 31 |
| 1.8 | Rozdíl mezi MESD a USD měřením [22]. | 32 |
| 2.1 | Polarizační kódování. | 34 |
| 2.2 | Možná implementace protokolu BB84 s polarizačním kódováním [24]. | 34 |
| 2.3 | Fázové kódování. | 35 |
| 2.4 | Možná implementace protokolu BB84 s fázovým kódováním [27]. . . . | 35 |
| 2.5 | Možné výstupy vzniklé interferencí prostředních pulzů [28]. | 36 |
| 2.6 | Možná implementace třístavového protokolu COW. Žluté pulzy obsahují foton. Šedě jsou vyznačeny prázdné vakuové pulzy [30]. | 38 |
| 2.7 | Redukce klíče v průběhu QKD procesu. | 40 |
| 3.1 | Tannerův graf znázorňující výše uvedenou Gallagerovu matici. | 44 |
| 3.2 | Průběh algoritmu pro opravu přeneseného klíče [41]. | 45 |
| 4.1 | Porovnání ideálního a reálného QKD kryptosystému [44]. | 49 |
| 4.2 | PNS útok na nechráněný protokol a návnadové stavy [45]. | 51 |
| 4.3 | Průběh BS útoku [48]. | 52 |
| 4.4 | Průběh útoku typu Muž uprostřed [53]. | 53 |
| 4.5 | Trojský kůň využívající OFDR ke zjištění vnitřního stavu kodéru [54]. | 54 |
| 4.6 | Úspěšně provedený útok na neaktivní detektory (černé) pomocí oslepení náhodným pulzem [56]. | 55 |
| 4.7 | Útok na nedokonalosti detektorů pomocí oslepení (černé detektory) a falešného stavu [58]. | 56 |
| 4.8 | Srovnání času účinnosti jednotlivých detektorů v čase [59]. | 57 |
| 5.1 | Test funkčnosti bomby pomocí měření bez interakce. | 59 |
| 5.2 | Možná implementace protokolu CQC [66]. | 60 |
| 6.1 | Podstata MDI-QKD protokolů. | 63 |
| 6.2 | Kvantová distribuce klíčů postavená na dvou kvantových opakovačích [79]. | 64 |
| 7.1 | Srovnání makrohybů a mikrohybů [67]. | 69 |
| 7.2 | Příčiny vzniku ztrát [67]. | 70 |
| 7.3 | Rozdíl mezi optickým zesilovačem a opakovačem [72]. | 71 |

| | | |
|-------|--|-----|
| 7.4 | Zkreslení pulzu dané vidovou disperzí v optickém vlákne [67]. | 73 |
| 7.5 | Zkreslení pulzu dané chromatickou disperzí v optickém vlákne [67]. | 74 |
| 7.6 | Změna polarizace zapříčiněná PMD v optickém vlákne [67]. | 74 |
| 7.7 | Spontánní a stimulovaná emise [90]. | 75 |
| 7.8 | Vhodné umístění zesilovače EDFA [94]. | 76 |
| 7.9 | Rozložení původních a nových frekvencí vzniklých důsledkem FWM [98]. | 77 |
| 7.10 | Rayleighův rozptyl [106]. | 79 |
| 7.11 | Mieův rozptyl [106]. | 79 |
| 7.12 | Optický rozptyl [106]. | 79 |
| 7.13 | Srovnání Rayleighova a Ramanova rozptylu [109]. | 81 |
| 7.14 | Stokesův a Anti-Stokesův rozptyl. Grafy převzaty z článku [100]. | 81 |
| 7.15 | Příklad časové filtrace. | 82 |
| 8.1 | Základní referenční model tak, jak byl popsán ve standardu ITU-T Y.3800. | 87 |
| 8.2 | Funkce QKD modulu tak, jak byly popsány ve standardu ITU-T Y.3802. | 89 |
| 8.3 | Funkce KMS tak, jak byly popsány ve standardu ITU-T Y.3803. | 90 |
| 8.4 | Funkce QKDN kontroléru, SDN modulu a SDN orchestrátoru tak, jak byly popsány ve standardech ITU-T Y.3804 a ITU-T Y.3805. | 91 |
| 8.5 | Základní princip SDN systému [117] [122]. | 92 |
| 8.6 | Příklad QKD sítě. Kontrolní a správní vrstva jsou zjednodušeny. | 95 |
| 9.1 | Rozdíl mezi QKD servery Alicí a Bobem. | 97 |
| 9.2 | Zařízení Eva sloužící k odposlechu na kvantovém kanále. | 99 |
| 9.3 | Princip zařízení Eva. | 99 |
| 9.4 | Současný stav logické topologie QKD polygonu. | 101 |
| 9.5 | Výpis souboru obsahující informace o uživatelích a QKD serverech. | 104 |
| 9.6 | Maximální povolený rozdíl mezi jednotlivými kanály QKD systému. | 105 |
| 10.1 | Optická trasa mezi VUT FEKT a VUT FIT v Brně. | 107 |
| 10.2 | Rozdíl v rychlosti mezi třístavovým a čtyřstavovým COW. | 108 |
| 10.3 | Rozdíl v chybovosti (QBER) mezi třístavovým a čtyřstavovým COW. | 109 |
| 10.4 | Rozdíl ve viditelnosti mezi třístavovým a čtyřstavovým COW. | 109 |
| 10.5 | Zapojení pro testování vlivu polarizace. | 111 |
| 10.6 | Polarizační kontrolér. | 111 |
| 10.7 | Rychlost při vypnutém scrambleru a různých nastaveních kontroléru. | 112 |
| 10.8 | Rychlost při zapnutém scrambleru a různých nastaveních kontroléru. | 112 |
| 10.9 | Zapojení trasy s robotickou rukou. | 114 |
| 10.10 | Pohyby robotické ruky s vlákem. | 114 |
| 10.11 | Rychlost při různé manipulaci s optickým kabelem. | 115 |
| 10.12 | Zapojení pro simulaci útoku pomocí modulu Eva. | 116 |

| | | |
|-------|---|-----|
| 11.1 | Prvotní navržené zapojení QKD polygonu. | 120 |
| 11.2 | Testování tolerance kvantového kanálu. | 122 |
| 11.3 | Výpočet Ramanova šumu. | 126 |
| 11.4 | Výsledná funkční trasa s provedenými změnami. | 127 |
| 11.5 | Postupná změna výkonu servisních kanálů při průchodu trasou. | 127 |
| 11.6 | Graf výkonu servisních kanálů u zdroje. | 128 |
| 11.7 | Graf výkonu servisních kanálů po průchodu multiplexorem a zatlu- mení. | 129 |
| 11.8 | Graf výkonu servisních kanálů po průchodu cirkulátory a sdílenou trasou. | 129 |
| 11.9 | Schéma použitých zesilovačů. | 130 |
| 11.10 | Graf výkonu servisních kanálů po zesílení EDFA zesilovačem o 15 dB. | 130 |
| 11.11 | Graf výkonu servisních kanálů po oříznutí signálu pomocí CWDM filtru. | 131 |
| 11.12 | Problematika tlumení servisních kanálů. | 131 |
| A.1 | Princip funkce DWDM filtrů. | 161 |
| A.2 | Zapojení trasy. | 162 |
| A.3 | Zapojení trasy. | 163 |
| A.4 | Charakteristika filtru 1 pro zapojení PASS → COM. | 163 |
| A.5 | Charakteristika filtru 2 pro zapojení PASS → COM. | 164 |
| A.6 | Charakteristika filtru 3 pro zapojení PASS → COM. | 164 |
| A.7 | Charakteristika filtru 4 pro zapojení PASS → COM. | 165 |
| A.8 | Charakteristika filtru 5 pro zapojení PASS → COM. | 165 |
| A.9 | Zapojení trasy. | 166 |
| A.10 | Charakteristika filtru 1 pro zapojení PASS → REF. | 166 |
| A.11 | Charakteristika filtru 2 pro zapojení PASS → REF. | 167 |
| A.12 | Charakteristika filtru 3 pro zapojení PASS → REF. | 167 |
| A.13 | Charakteristika filtru 4 pro zapojení PASS → REF. | 168 |
| A.14 | Charakteristika filtru 5 pro zapojení PASS → REF. | 168 |
| A.15 | Zapojení trasy. | 169 |
| A.16 | Charakteristika filtru 1 pro zapojení REF → COM. | 169 |
| A.17 | Charakteristika filtru 2 pro zapojení REF → COM. | 170 |
| A.18 | Charakteristika filtru 3 pro zapojení REF → COM. | 170 |
| A.19 | Charakteristika filtru 4 pro zapojení REF → COM. | 171 |
| A.20 | Charakteristika filtru 5 pro zapojení REF → COM. | 171 |

Seznam tabulek

| | | |
|------|--|-----|
| 1.1 | Polarizace elektromagnetických vln [8]. | 27 |
| 1.2 | Důkaz zachování energie v MZI [16, 17]. | 29 |
| 2.1 | Time-bin kódování. Monitorovací báze obsahuje pouze návnadové stavy nikoli data. | 37 |
| 7.1 | Převod na logaritmické jednotky. | 67 |
| 8.1 | Nejdůležitější ETSI rozhraní pro prvky QKDN [117]. | 85 |
| 8.2 | Nejdůležitější ITU-T standardy definující architekturu QKDN [116]. | 86 |
| 8.3 | Srovnání PQC a QKD [123]. | 93 |
| 9.1 | Znamé parametry systému Clavis ³ | 98 |
| 9.2 | Vypočtené parametry systému Clavis ³ | 99 |
| 9.3 | Parametry SFP modulů Finisar a Skylane [121, 124]. | 105 |
| 10.1 | Průměrná rychlost u třístavového a čtyřstavového COW. | 110 |
| 10.2 | Průměrná chybovost (QBER) u třístavového a čtyřstavového COW. | 110 |
| 10.3 | Průměrná viditelnost u třístavového a čtyřstavového COW. | 110 |
| 10.4 | Průměrná rychlost doručování klíčů, pro různá nastavení úhlu destiček. | 113 |
| 10.5 | Průměrná rychlost, chybovost a viditelnost při manipulaci s vláknem. | 115 |
| 10.6 | Vliv útoku na QKD systém Clavis ³ | 116 |
| 11.1 | Výkon kvantového kanálu při sloučení s oběma servisními kanály. | 123 |
| 11.2 | Výkon kvantového kanálu při sloučení s kanálem CH30. | 124 |
| 11.3 | Výkon kvantového kanálu při sloučení s kanálem CH29. | 124 |
| 11.4 | Výkon kvantového kanálu při sloučení s oběma servisními kanály. | 125 |
| 11.5 | Výkon kvantového kanálu při sloučení s oběma servisními kanály. | 125 |
| 11.6 | Konečné výsledky měření. | 132 |
| A.1 | Srovnání sousedních kanálů. | 162 |
| A.2 | Referenční hodnoty kanálů naměřené přímo na výstupu laseru | 172 |
| A.3 | Srovnání měřených filtrů pro směr PASS → COM. | 172 |
| A.4 | Srovnání měřených filtrů pro směr PASS → REF. | 172 |
| A.5 | Srovnání měřených filtrů pro směr REF → COM. | 173 |
| A.6 | Hodnoty výkonu při výstupu z laseru a filtrů pro výpočet vložného útlumu. | 174 |
| A.7 | Vypočtený vložný útlum. | 174 |
| A.8 | Hodnoty výkonu při výstupu z laseru a filtrů pro výpočet izolace. | 175 |
| A.9 | Vypočtená izolace sousedních kanálů. | 175 |
| B.1 | Výkon SRS u obou servisních kanálů. | 178 |
| C.1 | Typy ETSI dokumentů. | 179 |
| C.2 | Kompletní seznam ETSI dokumentů vztahujících se ke QKD. | 180 |
| C.3 | Kompletní seznam ETSI dokumentů vztahujících se k PQC. | 181 |

| | | |
|-----|--|-----|
| C.4 | Typy ITU-T dokumentů. | 182 |
| C.5 | Kompletní seznam ITU-T dokumentů vztahujících se ke QKD kategorie X. | 183 |
| C.6 | Kompletní seznam ITU-T dokumentů vztahujících se ke QKD kategorie Y. | 184 |
| C.7 | Kompletní seznam IEEE dokumentů vztahujících se ke QKD. | 185 |
| C.8 | Kompletní seznam ISO/IEC dokumentů vztahujících se ke QKD. | 185 |

Úvod

Roku 1984 byl americko-kanadskou dvojicí vědců, Gillem Brassardem a Charlesem Bennettem, navržen první protokol kvantové distribuce klíčů a do dnešní doby se jedná o nejrozšířenější aplikaci kvantové kryptografie. Spolu s postkvantovou kryptografií se jedná o technologie, které budou v následujících letech schopné vzdorovat hrozbě spočívající v útocích pomocí kvantových počítačů. V současnosti existuje nepřehledné množství QKD protokolů založených na různých jevech kvantové mechaniky a v různých fázích vývoje a praktické implementace. Tato práce se věnuje jak v praxi používaným protokolům, tak potenciálně zajímavým experimentálním schémátům jako je kontrafaktuální kvantová kryptografie nebo teorie kvantových opakovačů.

Ačkoliv je QKD často považováno za bezpodmínečně bezpečnou technologii (tzn. není možné na ni účinně útočit), reálné implementace zařízení oplývají mnoha nedokonalostmi, které je možné zneužít k útoku. Současně je kvantový signál velmi náchylný vůči jakémukoliv rušení, zejména pak nelineárním jevům. Z tohoto důvodu se tato práce věnuje i těmto tématům. Další kapitoly se věnují popisu reálného systému Clavis³ a standardizaci topologie QKD sítí, která se v posledních letech rychle rozvíjí. Normalizovány však nejsou samotné QKD protokoly, hlavní pozornost je naopak upřena na systémy správy klíčů a síťové kontroléry.

Praktická část se věnuje pokusům se zařízením Clavis³. Jedná se zejména o testování odolnosti systému vůči změnám vybraných parametrů. Příkladem může být změna polarizace, geometrie vlákna a podobně. Takové slabiny je následně možné použít k útokům s cílem odepření služby. Vzhledem k nutnosti integrace QKD do běžných konvergovaných sítí je hlavní část měření věnována zejména sloučení kvantového signálu do jednoho vlákna s ostatními kanály pomocí vlnového multiplexu.

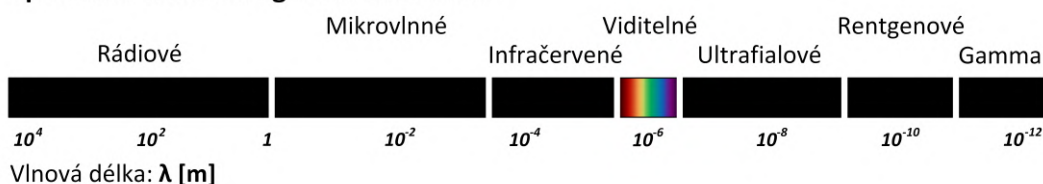
1 Fyzikální základ

1.1 Foton

Foton je elementární nehmotná stabilní intermediální částice popisující kvantum elektromagnetické energie. Tedy nejmenší možnou nedělitelnou jednotku elektromagnetického záření. V případě optických vláknových přenosů (včetně QKD) se, z důvodu nízkého útlumu, nejčastěji využívají oblasti infračerveného spektra. Tedy asi 186 THz až 235 THz. Respektive 1276 nm až 1612 nm [2, 3, 4, 5, 6].

- **Elementární částice** – Není známa její vnitřní struktura, tedy zda se skládá z dalších subčástic.
- **Nehmotná částice** – Její klidová hmotnost je nulová.
- **Stabilní částice** – Má nekonečný poločas rozpadu, tedy životnost. Vzniká a zaniká při různých interakcích.
- **Intermediální částice** – Zprostředkovává základní interakce (silná, slabá, elektromagnetická a gravitační). Tyto interakce popisují všechny známé způsoby vzájemného silového působení částic a pole.

Spektrum elektromagnetického záření



Obr. 1.1: Elektromagnetické spektrum [6].

Foton může existovat pouze v pohybu. Ve vakuu se foton pohybuje vždy rychlostí světla. To ovšem neplatí pro pohyb v materiálech, kde dochází ke snížení rychlosti. Toho se využívá například pro změnu polarizace na eliptickou či kruhovou [2, 3, 4, 5].

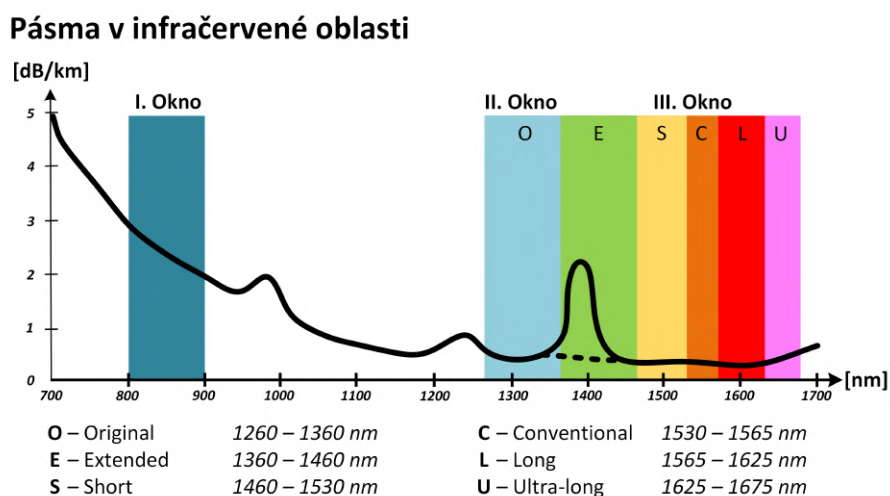
$$E = h\nu = \frac{hc}{\lambda} \quad (1.1)$$

- $E = [J]$ – Energie fotonu
- $h = [J \cdot s]$ – Planckova konstanta ($6,62607015 \cdot 10^{-34} J \cdot s$)
- $\nu = [Hz]$ – Frekvence
- $c = [m/s]$ – Rychlost světla ($299\,792\,458 m/s$)
- $\lambda = [m]$ – Vlnová délka

Ze vzorce je zřejmé, že energie fotonu závisí výhradně na vlnové délce respektive frekvenci. Čím je vlnová délka kratší a frekvence vyšší, tím vyšší je jeho energie. Je zřejmé, že vztah mezi těmito veličinami je:

$$\lambda = c \cdot \nu \quad (1.2)$$

V optických vláknech platí závislost měrného útlumu na vlnové délce světla tak, jak je popsáno na obrázku 1.2. Standardně se pro optické přenosy využívala tři okna a to v oblasti 850, 1300 a 1550 nm. Novější dělení zavádí šest nových pásem, pojmenovaných O, E, S, C, L a U [7].



Obr. 1.2: Přibližná útlumová křivka optických vláken [7].

1.2 Fáze a polarizace

Foton je elektromagnetická vlna. To znamená, že se skládá z vektoru elektrického pole \vec{E} a z vektoru pole magnetického \vec{B} . Směr šíření je potom dán Poyntingovým vektorem \vec{v} . Protože jsou na sebe všechny vektory kolmé, stačí uvažovat směr šíření a pouze jeden z vektorů \vec{E} a \vec{B} . Většinou se tak využívá pouze vektor \vec{E} [8, 9]. To, jakým způsobem elektrické (a magnetické) pole osciluje, popisuje polarizace.

Libovolnou elektromagnetickou vlnu (včetně fotonu) lze vnímat jako superpozici dvou jiných vln. Bude-li dále uvažován pouze vektor \vec{E} , je možné jej rozložit na dvě vzájemně ortogonální (kolmé) složky popisované vektory \vec{E}_x a \vec{E}_y . Amplituda a vzájemná fáze těchto složek následně určuje o jakou polarizaci se jedná [8, 9].

V případě, že vektor \vec{E} rotuje kolem osy z náhodně (vždy je na ni ale kolmý), jedná se o světlo nepolarizované. Pokud osciluje pouze v jediné rovině, jedná se

o světlo lineárně polarizované. Za předpokladu, že dojde mezi oběma složkami k fázovému posunu vzniká kruhová (90°) nebo eliptická (jiný úhel) polarizace. Podmínky jsou stručně popsány v tabulce 1.1 [8, 9].

Tab. 1.1: Polarizace elektromagnetických vln [8].

| Světlo | Charakteristika |
|------------------------|---|
| Nepolarizované | Různé amplitudy, fáze a frekvence |
| Lineárně polarizované | Stejná frekvence a fáze, amplituda se může lišit |
| Kruhově polarizované | Stejná frekvence a amplituda, fázový posun 90° |
| Elipticky polarizované | Stejná frekvence, liší se amplituda nebo fázový posun |

1.2.1 Polarizátory

Změna polarizace světla se provádí pomocí zařízení zvaného polarizátor. Nejčastěji se používají dichroické a fázové retardační polarizátory [10].

- **Dichroické polarizátory** – Jedná se o absorpční polarizátory, to znamená, že je pohlceno světlo kmitající v určitých směrech. Z tohoto důvodu se používají jako lineární polarizátory. Jsou schopny lineárně polarizovat i nepolarizované světlo v takovém případě dochází k 50% snížení intenzity. V případě, že jsou za sebou postaveny dva zkřížené polarizátory (horizontální + vertikální) je pohlceno 100 % světla. Rovněž se používají pojmy polaroid nebo polarizační filtr.
- **Fázové retardační destičky** – Ovlivňují polarizaci změnou fáze mezi složkami \vec{E}_x a \vec{E}_y . Fázový posun může být libovolný, nejčastěji se ale používá posun o 90° nebo 180° . Využívají polarizaci dvojlomem.
 - **Půlvlňná destička** – Fázový posun $\pi = 180^\circ$ – mění směr lineární polarizace o 90° . Tedy z horizontální na vertikální a opačně. Označuje se jako rotátor. U nepolarizovaného světla ke změně nedochází.
 - **Čtvrtvlňná destička** – Fázový posun $\pi/2 = 90^\circ$ – mění polarizované světlo na kruhově polarizované světlo a opačně. U nepolarizovaného světla ke změně nedochází.

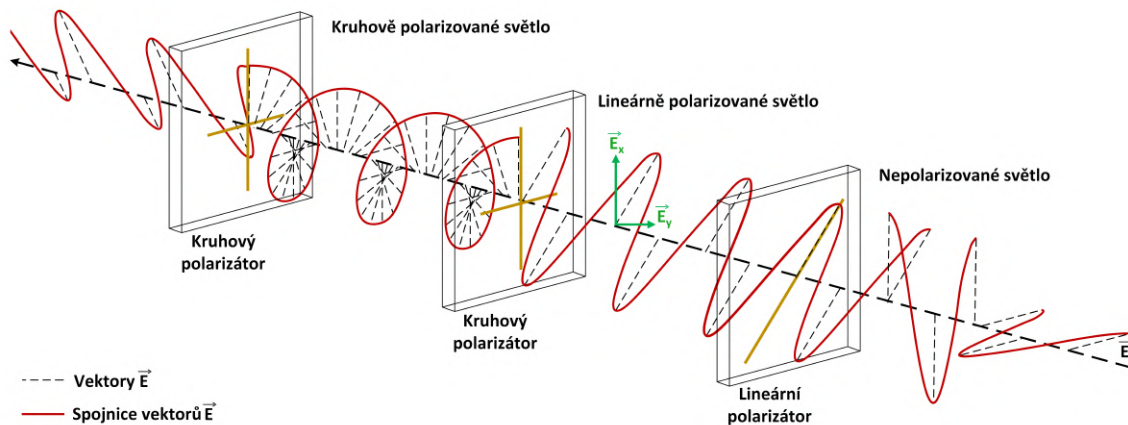
Příklad průchodu světla různými polarizátory je uveden na obrázku 1.3 níže. Průběh je popisován ve směru zprava doleva [11, 12].

1. Nepolarizované světlo prochází vertikálně postaveným lineárním polarizátorem. Polovina jeho intenzity je pohlcena (není zohledněno na obrázku). Zbytek je polarizován s náklonem 45° a prochází dál.
2. Následuje čtvrtvlňná destička pootočená o 45° stupňů vůči prvnímu polarizátoru tak, aby obě složky \vec{E}_x a \vec{E}_y (zeleně) měly stejnou intenzitu. Zde dochází

mezi oběma složkami k fázovému posunu 90° a vzniká kruhově polarizované světlo. Pokud by byl zvolen jiný úhel náklonu destičky, lišila by se amplituda obou složek a vznikla by polarizace eliptická.

3. Pokud je navíc umístěna další, stejně natočená čtyřvláková destička, dochází k dodatečnému fázovému posunu o 90° . Celkem se tedy jedna ze složek zpozdí o 180° , což je ekvivalentem půlplnné destičky (rotátor). Tímto vzniká opět lineárně polarizované světlo, nyní ovšem s opačnou polarizací než původně.

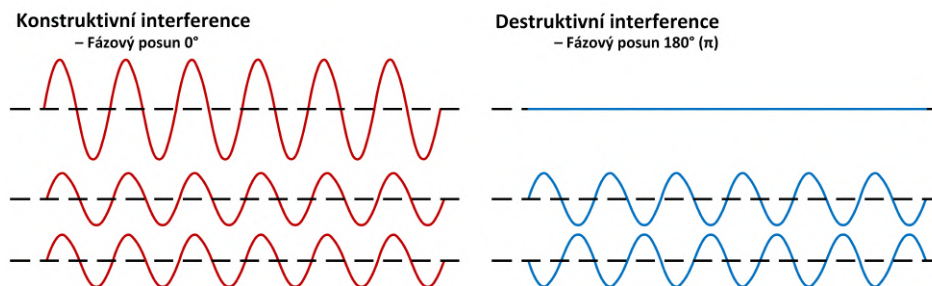
Lineárně polarizované světlo



Obr. 1.3: Příklad využití polarizátorů [13].

1.3 Interference a koherence

Koherence je vzájemná souvislost fáze a amplitudy vlnění. To může vycházet buď ze dvou různých míst (prostorová), nebo z místa stejného, avšak s určitým časovým posunem (časová). Za koherentní je světlo považováno, má-li stejnou frekvenci, směr a fázi. Koherence dvou vln má vliv na výsledek jejich vzájemné interference. To je demonstrováno na obrázku 1.4 [14, 15].

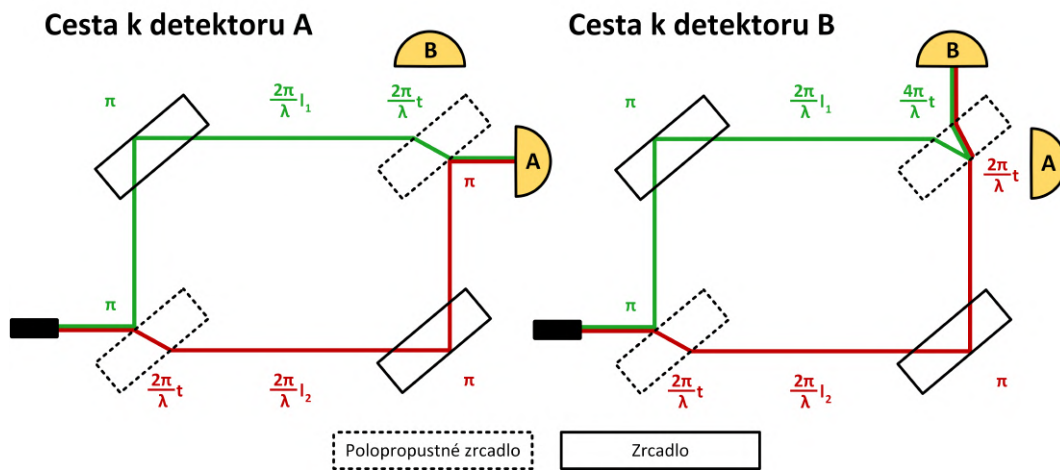


Obr. 1.4: Konstruktivní (vlevo) a destruktivní interference (vpravo) [14, 15].

1.3.1 Machův-Zehnderův interferometr

MZI (Machův-Zehnderův interferometr) je zařízení sloužící k určení fázového rozdílu dvou interferujících paprsků světla. Způsob fungování MZI je znázorněn na obrázku 1.5. Zde jsou hodnoty fázového posunu označeny zeleně pro horní cestu a červeně pro cestu dolní. Proměnné v obrázku značí:

- l_1 – Délka horní cesty
- l_2 – Délka spodní cesty
- t – Délka cesty v děliči svazků



Obr. 1.5: Průchod světla k detektorům A a B horní a spodní větvi [16, 17].

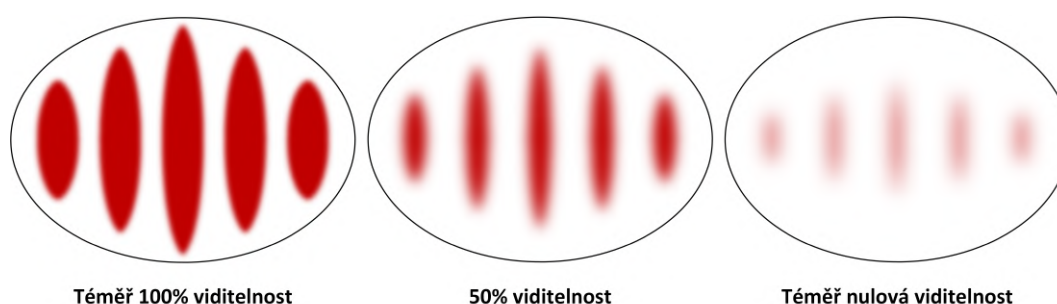
Celkový fázový posun světla procházejícího jednou větví se určí součtem všech v obrázku vyznačených hodnot. V případě, že dochází k odrazu, obrací se fáze. Z toho plyne nárůst posunu o π . Dále je započtena změna fáze daná délkou trasy vláknem (l_1 , l_2) a délkou trasy v děliči (t). Děliče jsou natočeny o 45° stupňů k přímce dané laserem. Tabulka 1.2 ukazuje vztah mezi světlem, které v daný okamžik dorazí na detektor A a na detektor B [16, 17].

Tab. 1.2: Důkaz zachování energie v MZI [16, 17].

| Detektor A | Detektor B |
|--|--|
| Získaný fázový posun vlny jdoucí přes horní větev | |
| $\varphi_{HA} = 2\pi + 2\pi \left(\frac{l_1+t}{\lambda} \right)$ | $\varphi_{HB} = 2\pi + 2\pi \left(\frac{l_1+2t}{\lambda} \right)$ |
| Získaný fázový posun vlny jdoucí přes dolní větev | |
| $\varphi_{DA} = 2\pi + 2\pi \left(\frac{l_2+t}{\lambda} \right)$ | $\varphi_{DB} = \pi + 2\pi \left(\frac{l_2+2t}{\lambda} \right)$ |
| Fázový rozdíl obou vln | |
| $\varphi_A = \varphi_{HA} - \varphi_{DA} = 2\pi \left(\frac{l_1-l_2}{\lambda} \right) = \delta$ | $\varphi_B = \varphi_{HB} - \varphi_{DB} = \pi + 2\pi \left(\frac{l_1-l_2}{\lambda} \right) = \delta + \pi$ |

Z daných výpočtů plyne, že u detektoru A je vztah mezi oběma větvemi vždy o π posunutý oproti detektoru B. Bude-li tedy u detektoru A fázový rozdíl mezi světlem procházejícím dolní a horní větví roven 0, bude u detektoru B v protifázi, tedy posunut o π . Tímto vznikne na detektoru A plná konstruktivní interference (dopadne sem veškeré světlo) a u detektoru B destruktivní interference (nedopadne sem nic). Tímto je dodržen zákon zachování energie. Poměr dopadajícího světla je možné upravit změnou délky trasy [16, 17].

Čím je tento poměr vyrovnanější, tím více dochází k rozostření interferenčního obrazce. Tak jako na obrázku 1.6. Veličina, která tento jev popisuje se nazývá interferometrická viditelnost. Ta se pohybuje v rozmezí 0–1, případně ji lze vyjádřit rovněž v procentech [16, 17].



Obr. 1.6: Zleva téměř 100% viditelnost, 50% viditelnost a téměř nulová viditelnost [18].

U některých QKD protokolů (např. COW) bývá trasa navržena tak, aby byla na detektoru A v ideálním případě 100% viditelnost. V případě manipulace na trase dochází k narušení koherence a část intenzity je přeorientována na detektor B. Rovněž v případě, kdy k interferenci nedochází, je výběr detektoru náhodný. V případě, že jsou na konci umístěny detektory, je možné určit viditelnost na detektoru A jako poměr kliknutí na detektoru A ku celkovému počtu detekcí. Např. dorazí-li 100 pulzů a detekci 5 z nich provede detektor B, potom je viditelnost 95 %. Lze spočítat pomocí vzorce níže [19].

$$V = \frac{P - P_B}{P} = \frac{P_A}{P} \cdot 100 \quad (1.3)$$

- $V = [\%]$ – Viditelnost
- P – Celkový počet dorazivších pulzů
- P_A – Pulzy detekované na detektoru A
- P_B – Pulzy detekované na detektoru B

1.4 Qubit

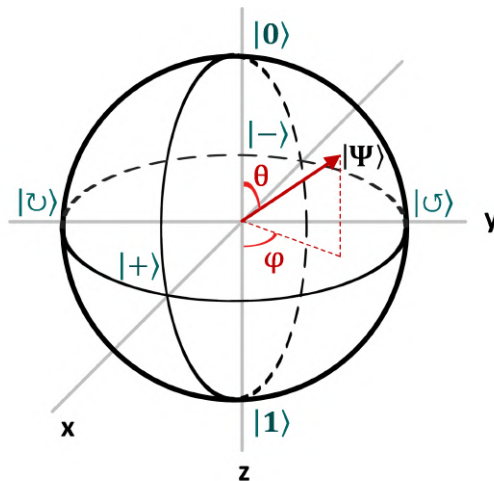
Zatímco klasický bit může nabývat pouze hodnot 0 a 1, qubit může nabývat jak stavů $|0\rangle$ a $|1\rangle$, tak jejich libovolné kombinace – superpozice. Samotný qubit je definován matematicky pomocí vektorů a lze jej implementovat pomocí různých fyzikálních jevů. Vektory $|0\rangle$ a $|1\rangle$ jsou ortogonální (kolmé; v Blochově kouli svírají 180°) a nazývají se bázovými vektory. Pomocí nich je možné vyjádřit libovolný jiný stav (vektor) qubitu snadno podle vzorce níže [20].

$$|\Psi\rangle = \alpha |0\rangle + \beta |1\rangle \quad (1.4)$$

Qubit bývá často zobrazen v tzv. Blochově kouli podobně jako na obrázku 1.7. Zde je možné vidět tři báze. A to $X = \{|0\rangle, |1\rangle\}$, $Y = \{| \odot \rangle, | \ominus \rangle\}$ a $Z = \{|+\rangle, |-\rangle\}$. Samotné značení se může lišit. Jednotlivé stavy se nacházejí na povrchu koule a jsou tak definovány pomocí úhlů θ a φ . Z toho plyne, že koeficienty α a β jsou komplexní čísla [20].

$$|\Psi\rangle = \cos \frac{\theta}{2} |0\rangle + e^{i\varphi} \sin \frac{\theta}{2} |1\rangle \quad (1.5)$$

K vyjádření stavu qubitu postačí jedna báze. Dále uvedené QKD protokoly jsou postaveny na střídání bází, kterými je qubit vyjádřen. Pokud je tak využívána báze X spolu s bází Z, není ze stavu qubitu možné určit, která báze byla použita pro jeho vytvoření [20].



Obr. 1.7: Blochova koule [20].

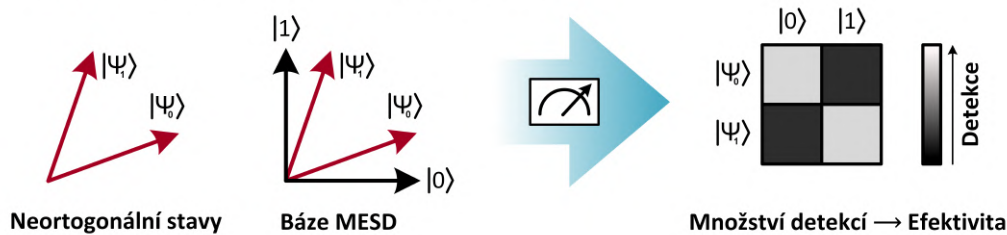
1.5 Rozlišení kvantových stavů

Pojem souhrnně označuje techniky, pomocí kterých je možné po provedení malého množství měření určit kvantový stav objektu. Důležitou roli hraje ortogonalita daných stavů. Jsou-li stavy vzájemně ortogonální, je jejich rozlišení snadné a zcela spolehlivé. Naopak stavy neortogonální spolehlivě rozlišit nelze. Existují ovšem dvě strategie zaměřené na získání co nejpřesnějších výsledků [21, 22].

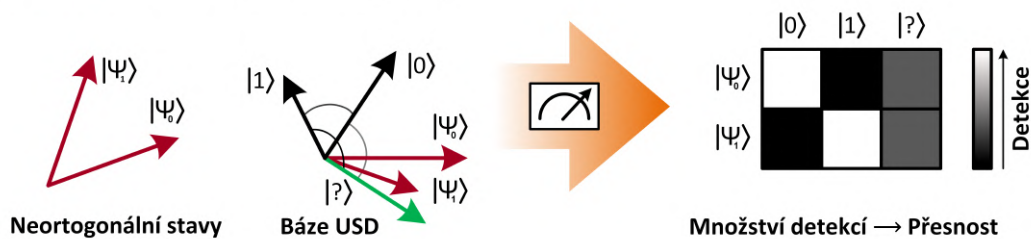
- **Rozlišení stavů s minimální chybou**
 - **MESD** – Minimum error state discrimination
 - Metoda spočívá v provedení měření tak, aby byla minimalizována chyba výsledku. Výstupem je tedy vždy jeden ze vstupních stavů. Tento výsledek ovšem může být chybný.
- **Jednoznačné rozlišení stavů**
 - **USD** – Unambiguous state discrimination
 - Metoda spočívá v provedení měření tak, aby byla minimalizována neprůkaznost výsledku. Výhodou je, že stavy jsou vždy určeny bezchybně. V některých případech je ovšem výsledek považován za neprůkazný. To znamená, že o něm není známa žádná informace.

Rozdíl obou technik je zřejmý z obrázku 1.8. Zatímco MESD určí kvantové stavy v některých případech špatně (tmavě šedé čtverce), v případě USD je stav určen vždy správně (bílé čtverce). V opačném případě je stav označen za neprůkazný $\rightarrow |?\rangle$.

Rozlišení stavů s minimální chybou (MESD)



Jednoznačné rozlišení stavů (USD)



Obr. 1.8: Rozdíl mezi MESD a USD měřením [22].

2 Cesta k COW protokolu

První návrh protokolu kvantové distribuce klíčů představili roku 1984 Američan Charles Bennet a Kanadan Gilles Brassard. Podle jejich jmen a roku publikování byl tak protokol nazván BB84. Tento zvyk se v oboru ujal a proto je mnoho protokolů pojmenováno podobným způsobem (SARG04, B92, E91, BBM92, LM05...). V současnou chvíli existuje ohromné množství protokolů s nespočtem modifikací v různých fázích vývoje a praktické, případně komerční implementace. Zařízení Clavis³ využívá tzv. COW (Coherent one-way) protokol. Z tohoto důvodu se práce bude věnovat zejména jemu. K lepšímu pochopení je srovnán s protokolem BB84 [23].

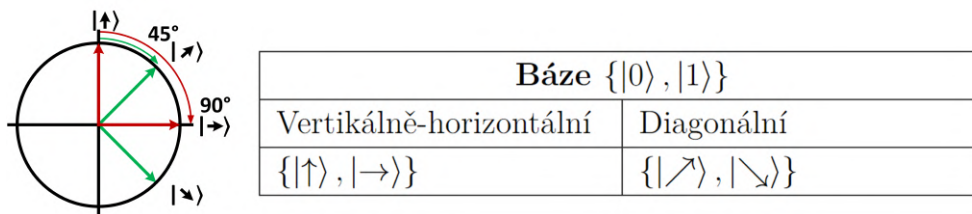
2.1 BB84: Bennett & Brassard (1984)

Nyní bude popsáno obecné schéma protokolu BB84. Jedná se o matematický model, který může být založen na různých fyzikálních jevech. Nejčastěji se uvádí původní polarizační kódování. V praxi se ale nejčastěji vyskytuje kódování fázové. Rovněž existuje v mnoha dalších modifikacích (SARG04, SSP, T12, B92...) Obecný postup je následující [23].

1. **Výměna hrubého klíče** – Necht jsou dva uzly Alice a Bob, mezi kterými dochází k výměně klíčů pomocí qubitů. Protokol využívá dvou ortogonálních bází (způsobů kódování). Dohromady tedy čtyř stavů. Alice si vygeneruje náhodnou sekvenci bitů s hodnotami 0 a 1. Dále náhodně střídá báze (50:50), kterými daný bit kóduje. Vše následně odesílá Bobovi, který pro přijatý qubit rovněž náhodně vybere bázi (50:50) pro měření. Je-li báze stejná jako u Alice bude výsledek měření správný. Pokud ne, bude správný v 50 % případů.
2. **Prosévání klíče** – Bob odešle Alici po veřejném kanále pořadí bází, které použil. Alice je porovná se svými bity. Ty, u kterých byla použita stejná báze, jsou použity k sestavení tzv. hrubého klíče. Zbytek je zahozen. Dále Alice i Bob použijí (obětují) část hrubého klíče k detekci odposlouchávající Evy. Hodnoty daného bitu na obou stranách jsou porovnány a odhaleny případné chyby. Tímto se odhadne tzv. QBER (Quantum-bit error rate). Eva je svými měřeními nucena dělat chyby, které by se zde projeví. Chyby ovšem mohou být způsobeny i dalšími faktory např. nelineárními jevy ve vlákně. Z tohoto důvodu je určena hranice, po kterou je výměna považována za bezpečnou. V případě BB84 se uvádí QBER nižší než 11 %.
3. **Destilace klíče** – Má tři fáze: Opravu chyb, zesílení bezpečnosti kompresí a autentizaci k vyloučení MITM (Man in the middle) útoku. Není přímo závislá na konkrétním QKD protokolu.

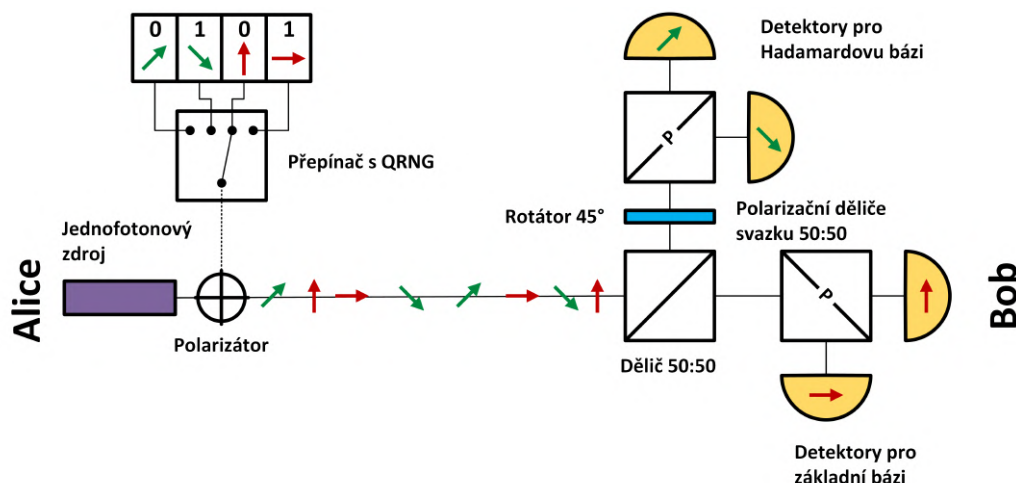
2.1.1 BB84 – Polarizační kódování

Jedná se o původní návrh protokolu BB84, který využívá lineární polarizace fotonu. Základní schéma se nachází na obrázku 2.2 níže. Zde je náhodným způsobem vybrána hodnota pro zakódování (0 nebo 1) a báze. Základní tj. vertikálně-horizontální (červená) a Hadamardova tj. diagonální (zelená). Polarizací světla je tak vytvořen jeden ze čtyř stavů. Hodnoty 0 a 1 jsou kódovány podle tabulky na obrázku 2.1 [24, 25].



Obr. 2.1: Polarizační kódování.

U Boba se pak foton dostane náhodným způsobem k detektorům jedné z bází. Například pokud Bob změří qubit ve stavu $|\rightarrow\rangle$ pomocí báze $\{|\uparrow\rangle, |\rightarrow\rangle\}$ získá správný výsledek. Pokud by použil Hadamardovu bázi bude výsledek zcela náhodný [24, 25].

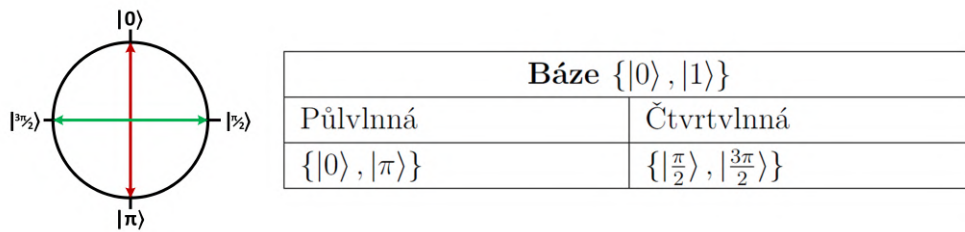


Obr. 2.2: Možná implementace protokolu BB84 s polarizačním kódováním [24].

V praxi se místo jednofotonových zdrojů používají slabé koherentní lasery. Ty produkují tzv. slabé koherentní pulzy (WCP – Weak coherent pulses). Důsledkem je, že zdroj světla není schopen vždy vygenerovat pouze jeden foton, jak by bylo záhodno. Místo toho generuje pulzy o průměrně velmi malém počtu fotonů. Toto množství je dáno tzv. **fotonovým číslem**. Počet pulzů obsahující foton je určen pomocí Poissonova rozložení. WCP lze zneužít pomocí tzv. PNS (Photon-number splitting) útoku. Z tohoto důvodu se v tomto případě používají tzv. návnadové stavy, které PNS útoku zabraňují. Jejich podstata je uvedena v předchozí práci [24, 25, 26].

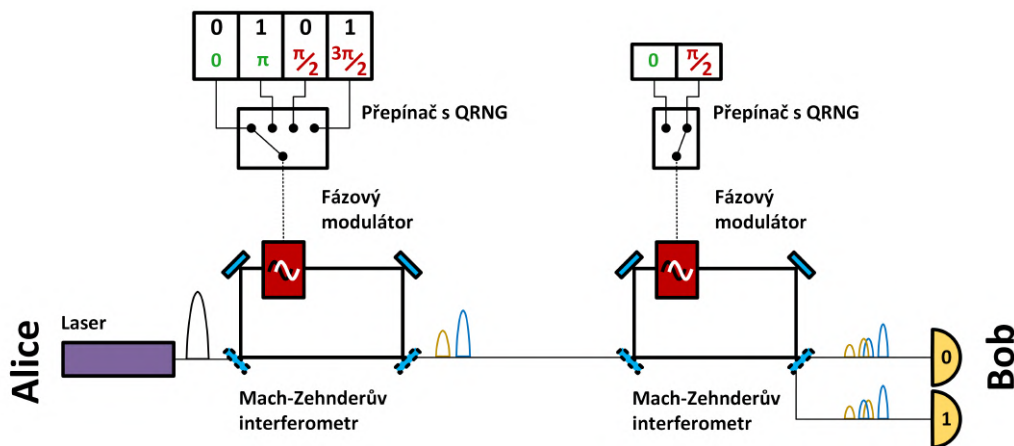
2.1.2 BB84 – Fázové kódování

Druhou a v praxi častěji se vyskytující možností je použití fázového kódování. Laser produkuje slabé koherentní pulzy, které se následně rozdělí na dva pomocí asymetrického Machova-Zehnderova interferometru. Delší větev obsahuje ztrátový fázový modulátor, pomocí kterého může Alice zakódovat hodnoty 0 a 1 ve dvou bázích tak, jak je uvedeno na obrázku 2.3. To provede posunutím fáze pulzu o vybraný úhel. Obě trasy interferometru následně ústí do jednoho společného vlákna. Vzdálenost obou pulzů je tak dána rozdílnou délkou tras a uděleným fázovým posunem [27, 28, 29].



Obr. 2.3: Fázové kódování.

Bob disponuje identickým MZI, kde pomocí fázového modulátoru vybírá měřící báze. Zde se každý pulz rozdělí na další dva. První (modrý) a poslední (žlutý) pulz neinterferují a nejsou tedy použity. Druhému (modrému) pulzu je průchodem horní větví uděleno stejné zpoždění jako třetímu (žlutému). Z tohoto důvodu mezi nimi dochází k interferenci. Její výsledek je dán Bobovým výběrem báze. Veškeré možnosti jsou uvedeny na obrázku 2.5 [27, 28, 29].



Obr. 2.4: Možná implementace protokolu BB84 s fázovým kódováním [27].

Na MZI jsou připojeny dva detektory, kliknutí na jednom z nich určuje, zda byla změřena hodnota 0 nebo 1. Interferometr je seřízen tak, aby viditelnost na detektoru nuly byla 100 %. Ve chvíli, kdy dochází ke konstruktivní interferenci, je

tedy naměřena 0. V případě destruktivní interference na detektoru nuly musí být konstruktivní interference zaznamenána na detektoru jedničky. V dalších případech je kliknutí detektorů náhodné a tyto bity jsou zahozeny [27, 28, 29].

| H | Výběr Alice | Výběr Boba | D | Výběr Boba | D |
|---|-------------|------------|---|------------|---|
| 0 | 0 → | 0 | 0 | → π/2 | ? |
| 1 | π → | 0 | 1 | → π/2 | ? |
| 0 | π/2 → | 0 | ? | → π/2 | 0 |
| 1 | 3π/2 → | 0 | ? | → π/2 | 1 |

H – Hodnota D – Detektor, který klikne

Obr. 2.5: Možné výstupy vzniklé interferencí prostředních pulzů [28].

2.2 COW protokol

COW patří do kategorie protokolů distribuované fázové reference (DPR – Distributed phase reference). Rovněž na něj lze nahlížet jako na zjednodušenou verzi protokolu BB84 s fázovým kódováním. V případě COW se většinou používá spíše výraz time-bin kódování. Báze z protokolu BB84 jsou nahrazeny bázi datovou a monitorovací. Ačkoliv byl protokol vyvinut za účelem snadné implementace, jeho pochopení je mírně složitější než v případě protokolů typu BB84. Rovněž zatím nebyla prokázána odolnost proti veškerým typům útoků tak jako u BB84 [30, 31].

Tab. 2.1: Time-bin kódování. Monitorovací báze obsahuje pouze návnadové stavy nikoli data.

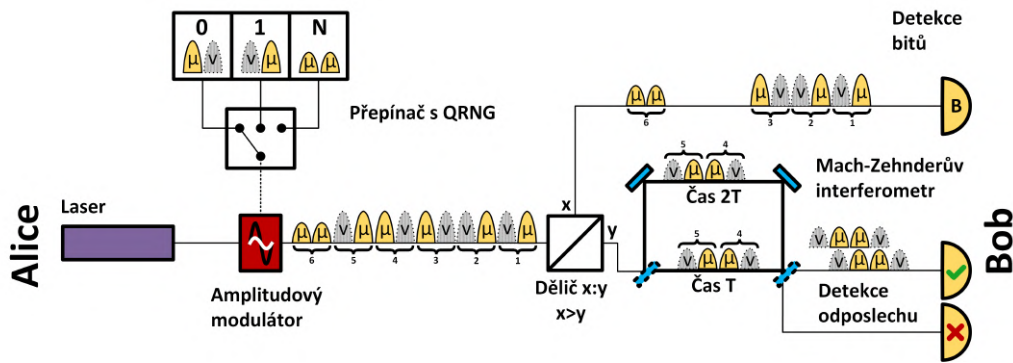
| Báze $\{ 0\rangle, 1\rangle\}$ a $\{ N\rangle\}$ | |
|---|-----------------------|
| Datová | Monitorovací |
| $\{ \mu-v\rangle, v-\mu\rangle\}$ | $\{ \mu-\mu\rangle\}$ |

Protokol je založen výhradně na technologii slabých koherentních pulzů (WCP) a využívá dvou datových a jednoho návnadového stavu. Použitím WCP je dána neortogonalita obou datových stavů. Z tohoto důvodu nelze rovněž mluvit o qubitech, které ortogonalitu vyžadují. Důvodem je výskyt vakuového pulzu. Oba stavy se tak částečně překrývají (obsahují stejný prvek) z čehož vyplývají závažné důsledky pro jejich vzájemné rozlišení od stavů návnadových. Tedy, že není možné s určitostí říct v jakém pulzu se foton nachází. I mezi sebou lze oba stavy správně rozlišit pouze pomocí USD měření s určitou pravděpodobností (měření času detekce fotonu). V ostatních případech není foton detekován (stav je nejednoznačný). Pravděpodobnost správné detekce se vypočte následovně [30, 31].

$$P_{USD} = 1 - P_{Překryv} \quad (2.1)$$

V případě prostého nahrazení WCP za jednofotonový zdroj by ovšem byly všechny stavy vzájemně ortogonální a bylo by je tak možné od sebe odlišit (tedy odlišit datové stavy od návnadových). Stejně jako u jiných QKD protokolů je bezpečnost kvantového spoje průběžně vyhodnocována. Na rozdíl od protokolů rodiny BB84 je úroveň celkové bezpečnosti kanálu vypočítávána nejen na základě chybovosti (QBER), ale i interferometrické viditelnosti a dalších parametrů [30, 31].

Základní myšlenka protokolu je následující. Alice náhodně vybírá ze tří možných stavů, které kóduje umístěním fotonu do jedné ze dvou pozic v časovém okně. Kromě datových hodnot 0 a 1, které slouží k vytvoření klíče má k dispozici ještě tzv. návnadový stav. Ten je základem celého protokolu a obsahuje jeden foton, který se může vyskytovat na libovolné pozici v časovém okně [30, 31].



Obr. 2.6: Možná implementace třístavového protokolu COW. Žluté pulzy obsahují foton. Šedě jsou vyznačeny prázdné vakuové pulzy [30].

Dále je přítomen dělič (pasivní prvek, může být použit i aktivní přepínač), který většinu pulzů odrazí do horní datové větve, kde dochází k měření bitů. Menší část pak prochází do monitorovací větve k ověření vzájemné koherence [30, 31].

- **Datová linka** – Většina pulzů je přeměřována sem. Zde dochází k měření bitů. Podle času, kdy detektor v časovém okně klikne, je tak bit určen jako 1 nebo 0, a to s minimální chybovostí (jedná se o USD). V případě návnadového stavu je naměřená hodnota náhodná a v průběhu destilace je zahozena. Výstupem je potom bitová posloupnost pro tvorbu klíče a počáteční odhad QBER. Jednoduchost Bobovy datové větve má praktické výhody. Nejsou zde žádné ztrátové a aktivní prvky a lze tak zvýšit vzdálenost přenosu. Rovněž není potřeba žádný generátor náhodných čísel [30, 31].
- **Monitorovací linka** – Pulzy přeměřované sem jsou použity k ověření vzájemné koherence pomocí Machova-Zehnderova interferometru. K tomuto účelu mohou posloužit dva slabé koherentní pulzy a to jak mezi dvěma okny (posloupnost 0-1) tak v rámci návnadového stavu. Výstupním údajem o stavu systému je interferometrická viditelnost tak, jak byla popsána výše v kapitole 1.3.1 [30, 31].

Na konci výměny oznámí Bob Alici, ve kterých oknech došlo k detekci na datové lince a kdy došlo k detekci destruktivní interference (druhý detektor). Alice naopak pošle Bobovi informace o tom, kdy byla použita jaká báze, tzn. kdy byly zaslány návnadové stavy. Bob následně tyto bity odstraní ze svého hrubého klíče. Dále pokračují odhadem chybovosti a destilací. Na základě QBER, viditelnosti a dalších parametrů je odhadnuta hodnota zabezpečení kvantového spoje. Pokud klesne pod stanovený práh, není klíč použit [30, 31].

2.3 Sledované parametry COW protokolu

Z výše uvedeného textu plyne, že v případě QKD protokolů je bezpečnost i výkon systému sledován pomocí určitých parametrů. V případě COW protokolu se jedná zejména o rychlost doručování klíčů, která se určuje po destilaci, QBER a viditelnost. Tyto parametry lze vyjádřit následovně:

- **Rychlost doručování klíčů**

$$v_{Kl\acute{c}\acute{h}} = v_{Bob} - v_{Pros\acute{e}v\acute{a}n\acute{i}} - v_{QBER} - v_{Oprava} - v_{Kompresa} \text{ [bit/s]} \quad (2.2)$$

- **Kvantová bitová chybovost (QBER)**

$$QBER = \frac{v_{Chyby}}{v_{Bob}} \cdot 100 \text{ [%]} \quad (2.3)$$

- **Interferometrická viditelnost**

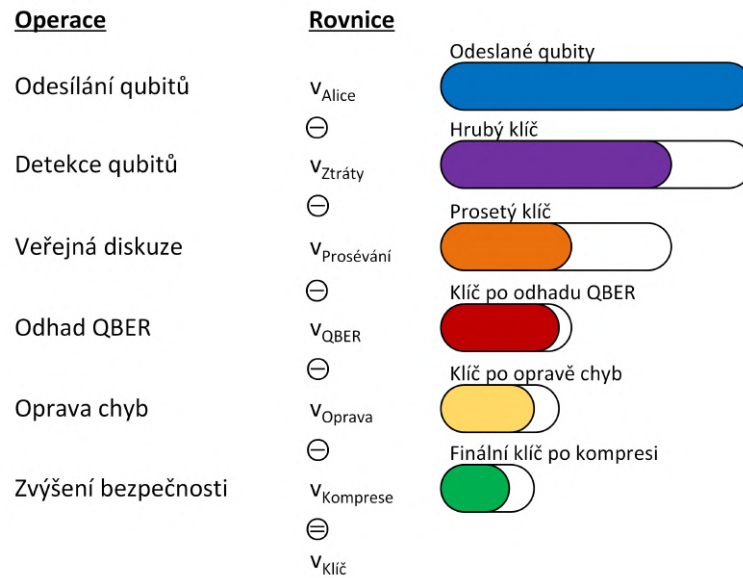
$$V = \frac{v_{Konstruktivn\acute{i}}}{v_{Celkem}} \cdot 100 \text{ [%]} \quad (2.4)$$

Výše použité proměnné jsou popsány níže. Zatímco rychlost doručování klíčů a QBER jsou měřeny na datové lince (první čtyři proměnné). Viditelnost je měřena na lince monitorovací (poslední dvě proměnné). Rovnice číslo 2.2 je rovněž graficky zpracována na obrázku 2.7. Pro výše uvedené rovnice dále platí následující:

$$v_{Bob} = v_{Alice} - v_{Ztr\acute{a}ty} \text{ [bit/s]} \quad (2.5)$$

- v_{Alice} = [bit/s] – Množství vygenerovaných bitů u Alice
- v_{Bob} = [bit/s] – Množství změřených bitů u Boba
- $v_{Ztr\acute{a}ty}$ = [bit/s] – Množství na trase ztracených bitů
- $v_{Pros\acute{e}v\acute{a}n\acute{i}}$ = [bit/s] – Množství bitů, u kterých byla zvolena nesprávná báze
- v_{QBER} = [bit/s] – Množství bitů obětovaných k odhadu QBER
- v_{Oprava} = [bit/s] – Množství neúspěšně opravených a zahozených klíčů
- $v_{Kompresa}$ = [bit/s] – Množství bitů ztracených při kompresi
- v_{Chyby} = [bit/s] – Množství nesprávně přenesených bitů
- $v_{Konstruktivn\acute{i}}$ = [bit/s] – Množství bitů, které konstruktivně interferovaly
- v_{Celkem} = [bit/s] – Celkové množství bitů, které dorazily na monitorovací linku

Postupná redukce klíče tak, jak byla popsána rovnicemi 2.2 a 2.5 je naznačena na obrázku 2.7. Z Alicí odeslaných qubitů dorazí k Bobovi jen jejich určitá část, která následně vytvoří hrubý klíč. Po veřejné diskuzi je další část (polovina u BB84) bitů zahozena. Část bitů je následně zveřejněna k odhadu QBER. Následně dochází k samotné opravě chyb, která však nemusí být vždy úspěšná a neopravené klíče jsou zahozeny. Opravené klíče jsou následně naopak komprimovány, čímž se naposledy sníží jejich velikost a získá finální sdílený klíč.



Obr. 2.7: Redukce klíče v průběhu QKD procesu.

2.3.1 Útoky na COW protokol

Nejjednodušším způsobem, jak se může Eva pokusit o odposlech, je prosté měření od Alice přicházejících pulzů. V případě datových pulzů $|\mu-v\rangle$ a $|v-\mu\rangle$ není měření problematické. Foton se nachází pouze v pulzu na dané pozici a je tak nesprávně rozlišen jen v zanedbatelném množství případů (viz překrytí výše). Evě tak nic nebrání dané stavy zkopírovat a poslat dále nicnetušícímu Bobovi [30, 31].

Bezpečnost je tak postavena právě na návnadových stavech. V jejich případě není Eva schopna určit, na které pozici se foton nachází. Návnady jsou ve skutečnosti superpozičním stavem a foton se na určité pozici vyskytuje pouze s určitou pravděpodobností. Stejně tak není Eva schopna určit, zda se jedná o jeden z datových stavů, nebo stav návnadový [30, 31].

Pokud Alice odešle návnadový stav a zachytí ho Eva, ve většině případů je odeslán do datové větve, kde je náhodně prohlášen za jeden z bitů a následně zahozen. Stejná situace nastane i v případě, že Eva odešle místo něj jeden z datových pulzů. QBER tak není ovlivněna a tímto způsobem Bob odposlech nepozná. Pokud by se takový falešný pulz dostal do monitorovací větve, nebudou mít některé pulzy s čím interferovat a výběr detektoru tak bude zcela náhodný. Tímto způsobem je snížena viditelnost a Bob získá informace o odposlechu [30, 31].

Další techniky odposlechu jsou dále popsány v kapitole 4 Kvantový hacking. Tyto útoky jsou zaměřeny jak na praktické slabiny reálných implementací, tak na samotné návrhy některých protokolů. Na rozdíl od protokolů typu BB84 nebyla u COW dosud prokázána odolnost proti veškerým známým útokům. Obecně je COW protokol bezpečný proti individuálním útokům pomocí přeposílání, jako například PNS útok, BS útok a některým útokům s nulovou chybou, které jsou založeny na USD. Specifický útok postavený na USD existuje i pro COW protokol. Řešením může být modifikace protokolu takovým způsobem, aby obsahoval ještě čtvrtý stav. Jedná se další návnadový pulz, složený ze dvou po sobě jdoucích vakuových pulzů. Aby byl protokol chráněn i proti některým kolektivním útokům, je nutné přidat další modifikace. Otázka odolnosti proti koherentním a kolektivním útokům však zatím není zcela vyřešena [32, 33, 34].

3 Destilace klíče

Za předpokladu, že během přenosu nebyl přítomen žádný útočník a použité přístroje jsou ideální, měl by být hrubý klíč bez chyb. V praxi ale odposlech není jedinou příčinou chyb v klíči. Veškerá praktická kvantová kryptografie se vyznačuje chybovostí způsobenou nedokonalostmi nebo poruchami kvantového kanálu [35].

Aby nebyla ohrožena bezpečnost, jsou všechny chyby přičítány útočníkovi. Hrubý klíč tak musí být dále zpracován (Post-processing). Tato fáze je známá také jako destilace klíče. Skládá se ze tří hlavních kroků [35].

- **Oprava chyb** (Error correction) – První krok, ve kterém se opraví všechny chyby v klíči pomocí klasického protokolu pro opravu chyb. Tento krok rovněž umožňuje přesně odhadnout skutečnou chybovost (QBER). Díky ní je možné přesně vypočítat množství informací, které může mít útočník o klíči k dispozici.
- **Zesílení bezpečnosti** (Privacy amplification) – Druhý krok spočívá ve vhodné komprimaci klíče tak, aby se snížila informovanost útočníka. Čím více informací útočník zná, tím více musí být klíč komprimován, aby byl bezpečný.
- **Autentizace** (Authentication) – Tento krok se někdy do destilace nezapočítává. Jelikož však samotná kvantová distribuce není schopná čelit útokům může uprostřed, je nutné autentizovat servisní kanál.

3.1 Oprava chyb (Error correction)

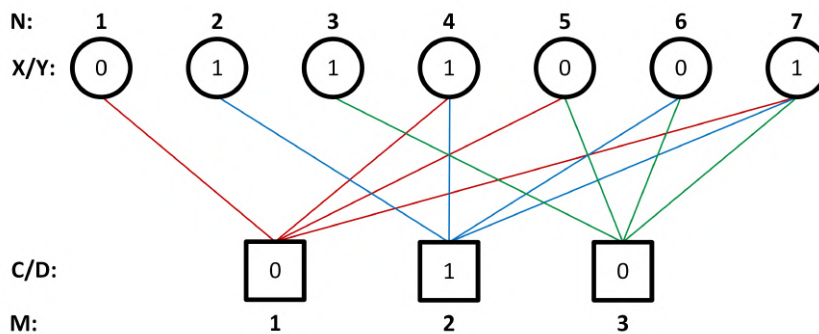
Oprava chyb u QKD protokolů bývá založena na nízkohustotních kódech s kontrolou parity (LDPC – Low-density parity check). Z tohoto důvodu bude jejich princip stručně nastíněn. Proměnné použité v tomto textu jsou popsány níže [36, 39]

- G – Gallagerova matice
- $H(Z)$ – Otisk bitové posloupnosti
- M/N – Počet kontrolních / informačních bitů
- C/D – Vektor kontrolních bitů u Alice / Boba o velikosti M
- X/Y – Vektor prosetých bitů u Alice / Boba o velikosti N

Jedná se o kódy definované řídkou, předem náhodně vygenerovanou, kontrolní maticí G s M řádky a N sloupci. Tato matice se rovněž označuje jako Gallagerova. Zde řádky udávají počet kontrolních bitů ($M = 3$) a sloupce počet přenášených informačních bitů ($N = 7$). Danou matici je rovněž možné překreslit do tzv. Tannerova grafu, kde 1 v matici značí společnou hranu. Propojení vrcholů hranami je náhodné a ne všechny informační bity jsou tak kontrolovány všemi paritními bity. Tato řídkost zajišťuje dostatečnou rychlost kódu v kombinaci se statisticky vysokou šancí na úspěšnou opravu [39, 40].

Příklad Gallagerovy matice se nachází níže s odpovídajícím Tannerovým grafem na obrázku 3.2. Je-li množství informačních bitů X nebo Y sudé je odpovídající paritní bit C nebo D roven 0 (červeně a zeleně). Pokud je počet informačních bitů lichý, je paritní bit roven 1 (modře) [39, 40].

$$G = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix}$$



Obr. 3.1: Tannerův graf znázorňující výše uvedenou Gallagerovu matici.

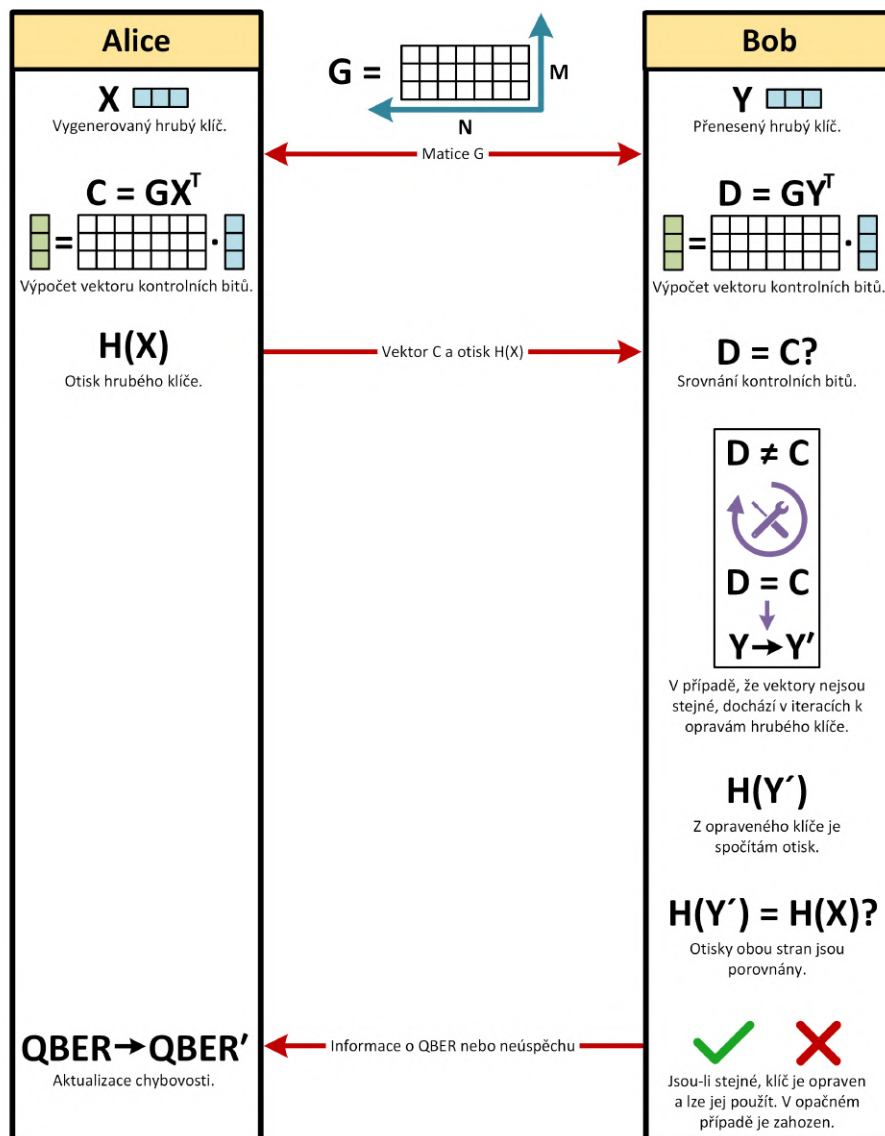
Na LDPC kód lze nahlížet jako na množinu samostatných nezávislých paritních kódů (SPC – Single parity check), kde každý paritní bit LDPC kódu reprezentuje jeden SPC kód. Každý SPC kód je dekódován zvlášť. Informace o pravděpodobnosti, zda je každý přenášený bit 0 nebo 1 každého dekodéru je porovnávána a aktualizována podle ostatních redundantních SPC dekódování stejného informačního bitu. Každý SPC kód je pak na základě aktualizovaných informací znovu dekódován. Tento proces se opakuje, dokud se nezíská platné kódové slovo nebo se nevyčerpají všechny možnosti [39, 40].

3.1.1 LDPC algoritmus pro QKD

Po prosévání získají Alice i Bob sekvenci N bitů, které slouží jako základ pro sdílený klíč. Tento hrubý klíč stále obsahuje chyby, které jsou v následujícím kroku odstraněny pomocí dalšího dialogu. V průběhu opravy chyb ovšem dochází k úniku informací, který musí být vykompenzován v dalším kroku. Postup je následující [41].

1. Alice a Bob si na základě počáteční QBER určí společnou Gallagerovu paritní matici G s rozměry $M \cdot N$. Čím je QBER vyšší, tím je matice hustší.
2. Alice si následně vypočítá vektor všech kontrolních bitů jako $C = GX^T$ (v modulu 2). Spolu s ním si pomocí hašovací funkce vypočítá otisk $H(X)$.

- Bob rovněž vypočte vektor kontrolních bitů $D = GY^T$ a svůj výsledek porovná s výsledkem Alice. Pokud $C \neq D$, je na hrubý klíč ($Y \rightarrow Y'$) v iteracích aplikován LDPC opravný algoritmus do doby, než jsou oba vektory shodné ($C = D$), nebo nebylo vyčerpáno maximum iterací.
- Bob vypočítá $H(Y')$ a srovná jej s $H(X)$. Pokud oprava proběhla úspěšně, budou se obě hodnoty s vysokou pravděpodobností rovnat. Takový klíč je možné použít v dalším kroku. Bob rovněž pošle Alici informace o chybách, které jsou následně použity ke zpřesnění odhadu QBER. V opačném případě odešle Bob Alici zprávu o neúspěchu a klíč je zahozen.



Obr. 3.2: Průběh algoritmu pro opravu přeneseného klíče [41].

3.2 Zesílení bezpečnosti (Privacy amplification)

Předchozí procesy vyžadují vzájemnou komunikaci mezi Alicí a Bobem po klasickém kanálu. Tímto způsobem ovšem dochází k určitému úniku informací. K zachování vysoké úrovně bezpečnosti je nutné provést její zesílení pomocí hašovací funkce dohodnuté pomocí veřejné diskuze po klasickém kanálu [36].

K zesílení bezpečnosti klíče se používá například tzv. **Toeplitzův hašovací algoritmus**, jehož základem je Toeplitzova matice T . Ta má počet sloupců S , počet řádků R a obsahuje konstantní, zleva doprava sestupné diagonály. To umožňuje snížit nutné množství náhodných bitů. Tato matice není tajná a přenáší se veřejným kanálem po tom, co byl celý základ pro klíč přenesen a opraven. Matice je dále vynásobena vektorem obsahujícím přenesené a opravené bity B . Dochází tak k nastavitelnému zhašování a kompresi bitů. Tímto vzniká finální klíč K [36].

Níže je uveden příklad s maticí T o rozměrech $R = 3$ a $S = 4$. Předpokladem pro úspěšné násobení matic je použit vektor B s počtem prvků $S = 4$. Výstupem je následně komprimovaný vektor K o velikosti $R = 3$, obsahující finální sdílený klíč [36].

$$K = T \cdot B = \begin{pmatrix} t_1 & t_2 & t_3 & t_4 \\ t_5 & t_1 & t_2 & t_3 \\ t_6 & t_5 & t_1 & t_2 \end{pmatrix} \cdot \begin{pmatrix} b_1 \\ b_2 \\ b_3 \\ b_4 \end{pmatrix} = \begin{pmatrix} k_1 \\ k_2 \\ k_3 \end{pmatrix}$$

Z důvodů eliminace nežádoucích efektů daných omezenou velikostí bloku je vhodné, aby byla velikost vektoru T co největší. Naopak je ovšem omezena velikostí operační paměti. Prakticky se velikost pohybuje kolem $S = 10^6$ bitů [36].

3.2.1 Kompresní poměr

Sledovatelným parametrem je tzv. kompresní poměr (compression ratio). Jedná se o poměr mezi délkou výsledného zkomprimovaného klíče a vstupujícího opraveného klíče. V případě použití Toeplitzova algoritmu, lze vypočítat rovněž jako poměr počtu řádků a sloupců matice [37, 38].

$$KP = \frac{d_{\text{Komprimovaný}}}{d_{\text{Opravený}}} \cdot 100 = \frac{R}{S} \cdot 100 [\%] \quad (3.1)$$

3.3 Autentizace (Authentication)

Jedním z problémů, který samotná kvantová distribuce klíčů není schopná řešit sama, je obrana proti útokům muže uprostřed. Z tohoto důvodu musí dojít k autentizaci obou komunikujících stran. Základem je obousměrná autentizace servisního kanálu. Ta je založena na sadách předsdílených inicializačních klíčů (ISK – Initialization shared key). Z bezpečnostních důvodů musejí být tyto klíče nahrány na zařízení předem. Následně se postupně obnovují z přenášené kvantové komunikace [36].

Samotný přenos může být založen na různých kryptografických prostředcích. Nejčastěji se využívá hašovacích funkcí. Z každé zprávy přenášené servisním kanálem je spočítán otisk, který je následně zašifrován pomocí ISK a odeslán protistraně. Druhá strana otisk dešifruje pomocí svého shodného ISK a rovněž spočítá otisk z přenesené zprávy. Následně oba otisky porovná. Jsou-li oba otisky stejné, ví, že zpráva byla odeslána ze správného zdroje. Odesílatel zprávy se tak vůči příjemci autentizoval [36].

Ačkoliv kvantový kanál může být napaden mužem uprostřed, samotný je bez funkčního servisního kanálu nepoužitelný. Bezpečnost je tak závislá na zvoleném šifrovacím algoritmu. Autentizační protokol může být založen i na jiném principu. Příkladem může být tzv. postkvantová kryptografie (PQC – Post-quantum cryptography) [36, 42].

4 Kvantový hacking

Kvantová distribuce klíčů je často považována za bezpodmínečně bezpečnou. Praktické implementace libovolného QKD protokolu se však značně liší od svých teoretických modelů a obsahují řadu nedokonalostí, kterých je možné využít k tzv. kvantovému hackingu. Srovnání lze najít na obrázku 4.1 níže. Při hodnocení bezpečnosti se předpokládá, že má útočník libovolnou technologii a neomezený výpočetní výkon (kvantovou paměť, kvantový počítač atp.), zatímco uživatelé používají reálná nedokonalá zařízení. Tyto předpoklady jsou nutné, neboť kvantová distribuce klíčů má být prokazatelně bezpečná proti jakémukoli útoku. Tedy i takovému, který není se současným stavem technologií realizovatelný [43, 44].

Srovnání ideálního a reálného QKD systému



Obr. 4.1: Porovnání ideálního a reálného QKD kryptosystému [44].

Jednotlivé útoky lze rozdělit podle různých kritérií tak, jak je uvedeno ve výčtu níže. Vybrané útoky jsou dále detailněji popsány [44].

- **Podle místa zranitelnosti:**

- **Zdroj** – Útoky jsou vedeny proti zranitelnostem v reálném zdroji. Jsou měřeny např. proti zdroji slabých koherentních pulzů nebo modulátorům.
- **Kódování** – Na kódování se útočí zejména v případě specifických QKD schémat jako Plug-and-play a Sagnacovo QKD.
- **Detektor** – Nejčastěji se útočí na zranitelnosti v reálných detektorech. K tomuto účelu se používá lavinová dioda (APD – Avalanche photodiode).

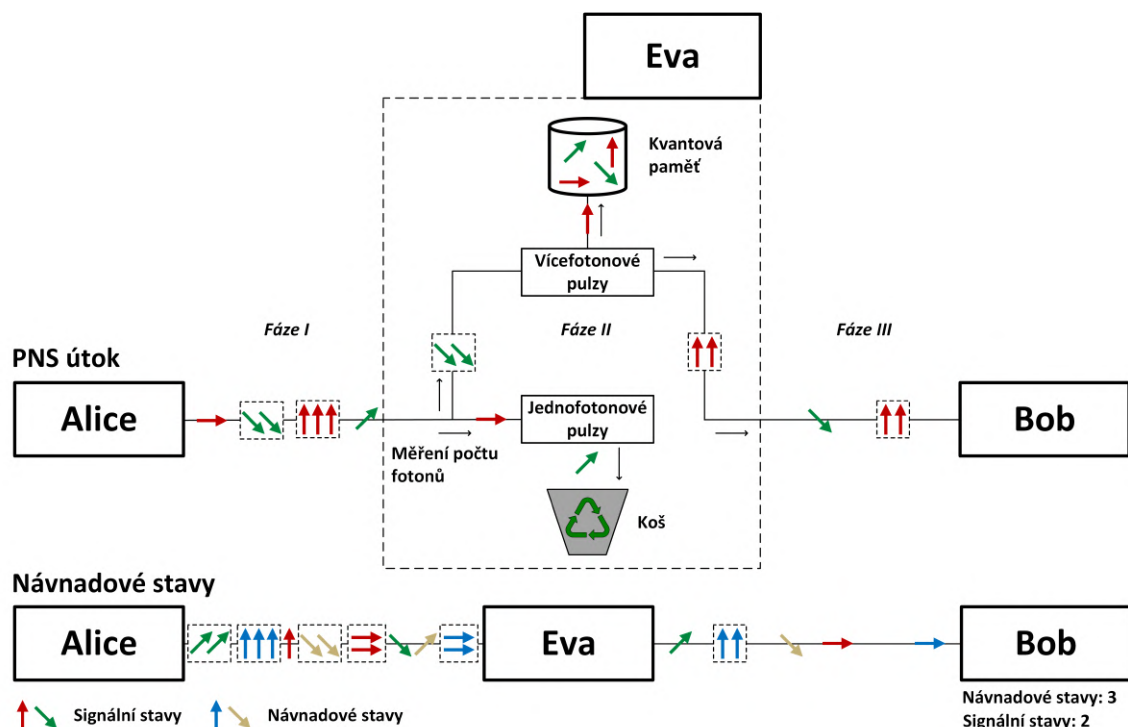
- **Podle rozsahu:**

- **Individuální útok** (Individual-particle attack) – Útoky jsou vedeny postupně proti jednotlivým částicím. Jsou obecně považovány za slabší.
- **Společný útok** (Joint attack) – Útok je veden nad skupinou částic současně. Důvodem může být snaha o dodržení koherence. Nejsilnější skupinou těchto útoků jsou tzv. kolektivní útoky (Collective attack).

- **Další pojmy:**
 - **Útok odepřením služby** (Denial of service attack) – Jednodušší útoky, které neslouží k získání přenášeného klíče. Jejich cílem je QKD proces přerušit, nikoliv získat klíč. Jelikož jsou v současnosti používány zejména přímé linky, je nejjednodušším způsobem přerušování trasy. Další možností je pak například oslepit Bobovy detektory.
 - **Útok přeosláním** (Intercept-resend attack) – Útočník zachytí Aliciny signály a provede nad nimi určitou operaci. Následně tyto signály, většinou upravené nebo falešné, přešle Bobovi.
 - **Útok oslepením** (Blinding attack) – Jedná se o různé útoky zaměřené na nedokonalosti APD detektorů. Ty lze různými technikami oslepit a tímto způsobem ovlivnit výsledek měření. Dostupný tak v danou chvíli může být například jen jeden z detektorů.
 - **Trojský kůň** (Trojan-horse attack) – Odvozeno od pověstného způsobu překonání hradby do zabezpečeného prostoru. Jedná se o útoky na zdroj, kdy Eva vyšle k Alici světelný pulz. Ten vnikne do kodéru Alice a je tak kódován stejně jako Alicin qubit. Část pulzu se následně odrazí zpět, čímž Eva získá informace o Alicině qbitu.
 - **Útok s nulovou chybou** (Zero-error attack) – Různé útoky, které ovšem negenerují chyby v přenosu. Pokročilejší techniky jsou založeny na jednoznačném rozlišení stavů (USD).
 - **Koherentní útok** (Coherent attack) – Jedná se o různé útoky, jejichž společnou vlastností je, že nenarušují koherenci přenosu. Problematické jsou zejména v případě fázově orientovaných protokolů typu COW.

4.1 Útok dělením počtu fotonů (PNS attack)

Anglicky Photon-number splitting attack. Jedná se o útok na nedokonalý zdroj, vysílající slabé koherentní pulzy. V případě použití takového zdroje je množství fotonů v pulzech dáno Poissonovým rozložením. Ačkoliv je průměrné množství fotonů na pulz vždy menší než 1, mohou nastat případy, kdy jeden z pulzů obsahuje dva a více fotonů. Ačkoliv jsou tyto případy vzácné, představují příležitost pro Evu, která si jeden foton ponechá a zbytek pošle dále Bobovi. Pulzy obsahující jen jeden foton Eva zahodí a Bob se k nim tak nikdy nedostane. Jakmile začne Bob s Alicí zveřejňovat informace o bázích k ustanovení hrubého klíče, získá Eva informace, podle kterých si je schopna klíč sama odvodit [45, 46].

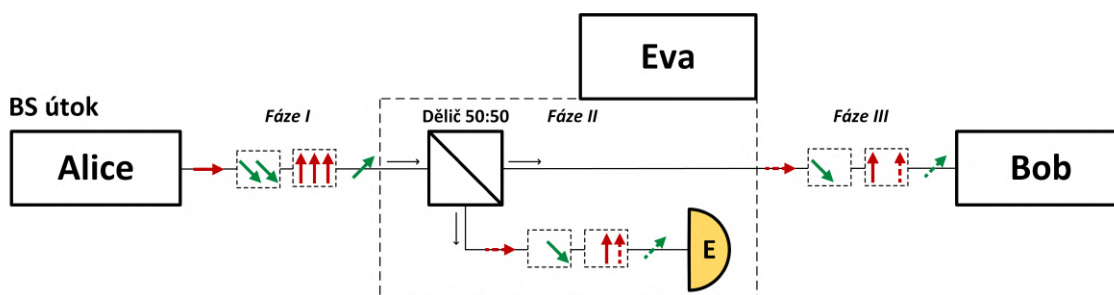


Obr. 4.2: PNS útok na nechráněný protokol a návnadové stavy [45].

V případě protokolu BB84 lze k obraně před PNS útokem použít tzv. návnadové stavy (decoy states), které Evu detekují. Princip je takový, že Alice posílá Evě kromě běžných stavů i stavy návnadové, s vyšším průměrným množstvím fotonů na pulz. Eva je ovšem nedokáže rozlišit od klasických datových pulzů, a tak útočí na každý pulz s vyšším počtem fotonů. U obou stavů zahazuje pulzy jednofotonové. Pokud by byla ztráta jednofotonových pulzů zapříčiněna ztrátovostí přenosového kanálu, bude počet ztracených návnadových stavů odpovídat počtu ztracených stavů signálních. Pokud je ovšem přítomna Eva, přijme Bob mnohem více stavů návnadových než signálních [45, 46].

4.2 Útok dělením paprsku (Beam splitting attack)

Jedná se o další útok zaměřený na WCP zdroj. Zatímco PNS útok vyžaduje v současnosti nedostupné technologie, BS útok je o mnoho méně sofistikovaný. V tomto případě disponuje Eva pouze děličem svazku 50:50 a detektory. Je-li vyslán pulz obsahující dva (nebo více) fotonů, je jeden foton odražen k Eviným detektorům, zatímco druhý pokračuje dál přímo k Bobovi. Odražené fotony může Eva měřit průběžně, případně je může uložit do kvantové paměti a měřit až po zveřejnění měřícíchází. Tímto způsobem získá Eva částečně stejné výsledky jako Bob. Řešením jsou opět návnadové stavy [47, 48].



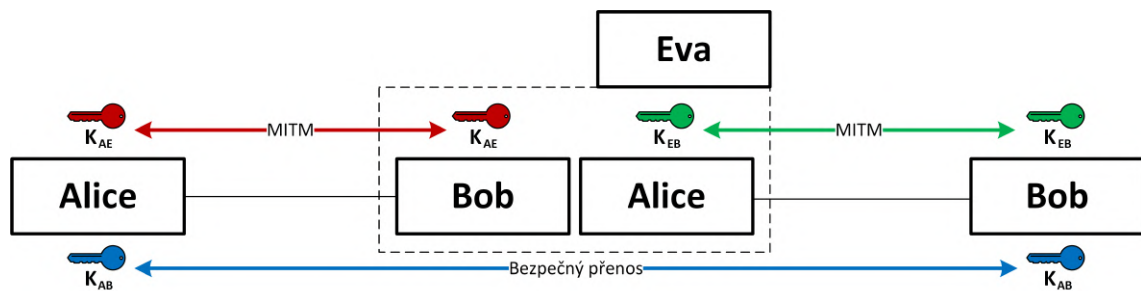
Obr. 4.3: Průběh BS útoku [48].

4.3 Útoky založené na USD

Jedná se o skupinu útoků založených na technikách jednoznačného rozlišení kvantových stavů. Jak bylo zmíněno v kapitole 1.5, základem této techniky je bezchybnost měření. To ji činí výhodnou (i když složitě realizovatelnou) pro útoky proti QKD systémům. Je zřejmé, že se jedná o ideální volbu pro útoky s nulovou chybovostí. Značně zjednodušeným příkladem může být měření všech Alicí odeslaných signálů, které následně přepošle Bobovi. Výsledek je vždy správný, případně je měření prohlášeno za neprůkazné. V takovém případě Eva signál zahodí, respektive k Bobovi odešle vakuový pulz. Detailnější popis těchto útoků a možné obrany je však nad rámec tohoto textu [49, 50, 51, 52].

4.4 Muž uprostřed (Man in the middle attack)

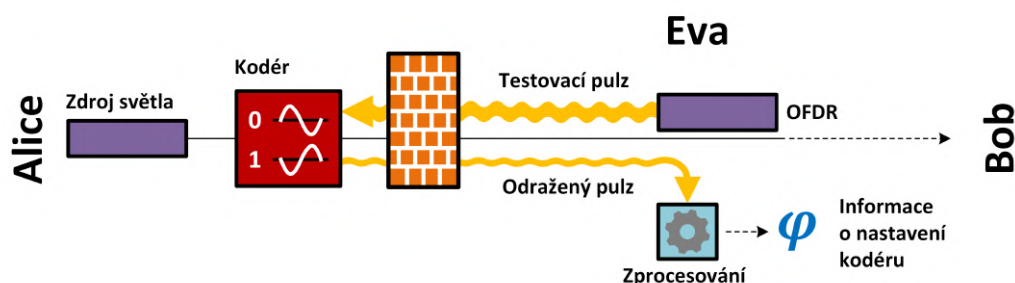
Ačkoli je v teoretické rovině kvantová distribuce klíčů považována za bezpodmínečně bezpečnou, samotná optická část nedisponuje žádnou ochranou proti útoku muže uprostřed. Útok probíhá podobně jako v případě klasických protokolů. Na rozdíl od ostatních útoků založených na odposlechu, neoperuje MITM pouze na kvantovém kanálu. Místo toho spočívá útok v nastrčení kompletního Evina škodlivého zařízení mezi Alicí a Bobem. Jsou tak ustanovena dvě oddělená spojení mezi Alicí a Evou a mezi Evou a Bobem. Z tohoto důvodu je nutné zajistit autentizaci obou protistran. To se v praxi zajišťuje ruční distribucí společného předsdíleného klíče [53].



Obr. 4.4: Průběh útoku typu Muž uprostřed [53].

4.5 Trojský kůň (Trojan horse attack)

Jedná se útoky založené na nedokonalostech kódovacích optických prvků v Alici a Bobovi. Jméno je odvozeno od analogie otevřených vrat, která symbolizují časové okno pro zaslání testovacího signálu. Útoky se liší podle používaného QKD protokolu, základem je analýza odraženého světla (reflektometrie). Příkladem může být Eva, která založí svůj útok na optické frekvenční reflektometrii (OFDR – Optical frequency domain reflectometry). Použije tak svůj koherentní zdroj k prozkoumání stavu fázového nebo polarizačního modulátoru. Toho docílí tak, že v okamžiku, kdy je Alicino zařízení aktivní, odešle testovací pulz a následně provede analýzu odrazu. Různá nastavení modulátoru se mohou projevit odlišnými vlnovými délkami odraženého světla. Tímto způsobem lze určit jaký stav Alice odeslala [54, 55].



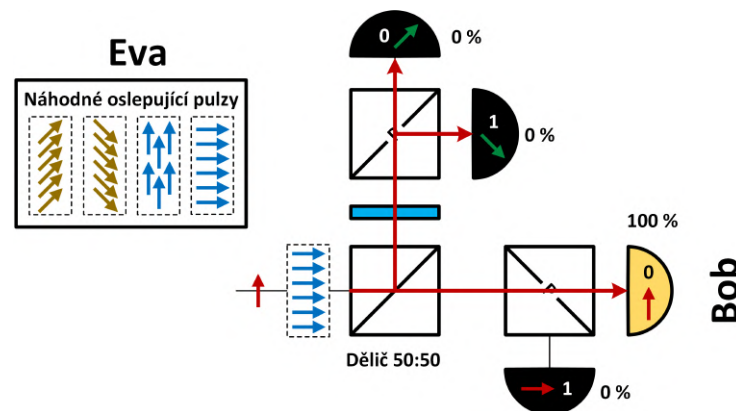
Obr. 4.5: Trojský kůň využívající OFDR ke zjištění vnitřního stavu kodéru [54].

Obrana proti těmto typům útoků je založena na co nejkratší délce časového okna a na co nejpřesnější možné filtraci propuštěných vlnových délek (ideálně pouze vlnová délka kvantového kanálu) [54, 55].

4.6 Útok na neaktivní detektor (Dead-time attack)

Jedná se o útok na lavinové detektory (APD), které slouží k detekci jednofotonových pulzů. Využívá jejich vlastností, kdy APD není po detekci fotonu schopna po určitý čas detekovat fotony další. Tento interval se označuje jako tzv. dead-time a umožňuje útočnickovy oslepit daný detektor. Útok probíhá tak, že Eva čeká, než Alice odešle svůj jednofotonový pulz. Krátce před něj vyšle silnější pulz s libovolně zvolenou polarizací tak, aby dorazil na detektor v čase jeho neaktivity. Např. Eva vyšle vícefotonový pulz $|\rightarrow\rangle$, který oslepí vše, kromě detektoru pro stav $|\uparrow\rangle$. V závislosti na Alicí odeslaném stavu si tak Eva vynutí detekci tímto detektorem nebo zahození pulzu. Jedná se o jednoduchý útok oslepením [56].

Jednou z možností je použít APD detektor disponující jakousi bránou (Gated detector). To v praxi znamená, že je fotodioda v Geigerově módu¹ pouze v časech, kdy se očekává příjem kvantového signálu. Ani to však není řešením proti sofistikovanějším osleповacím útokům [57].

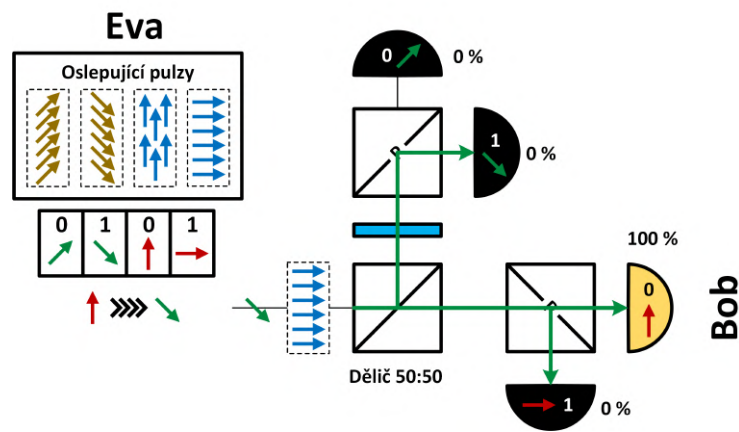


Obr. 4.6: Úspěšně provedený útok na neaktivní detektory (černé) pomocí oslepení náhodným pulzem [56].

¹Geigerův mód se používá pro extrémní zvýšení zisků a je nutný pro detekci jednotlivých fotonů

4.7 Útok falešnými stavy (Faked states attack)

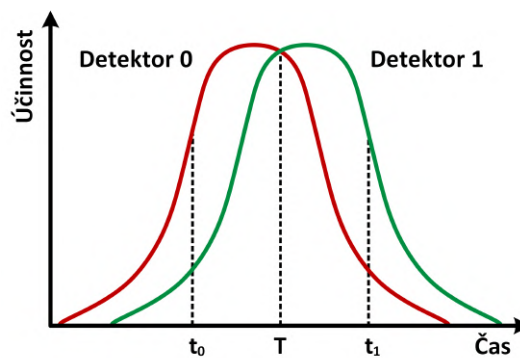
Opět se jedná se o útok na APD. Základ je stejný. V případě, že je na detektor upřen spojitý paprsek světla, dojde k saturaci a detektor není dále schopen detekovat fotony. Využitím této techniky může Eva ovlivnit způsob, jakým Bob vybírá měřící báze. Toto lze demonstrovat např. na protokolu BB84. Eva změří Alicí odeslaný stav a sama si připraví opačný stav v opačné bázi, tzv. falešný stav. Například pokud změří foton s polarizací $|\uparrow\rangle$ (0 v bázi X), připraví si stav $|\searrow\rangle$ (1 v bázi Z). Současně s odesláním falešného stavu se ale pokusí oslepit oba detektory bitu 1 pomocí pulzu s polarizací $|\rightarrow\rangle$. Jelikož je před detektorem bitu $|\nearrow\rangle$ (0 v bázi Z) polarizační dělič, ke kliknutí falešného stavu zde nemůže nikdy dojít. Jak vyplývá z obrázku 4.7 níže, jedinou možností je tak stejný detektor, kterým měřila Eva. Je zřejmé, že většina fotonů není detekována [58].



Obr. 4.7: Útok na nedokonalosti detektorů pomocí oslepení (černé detektory) a falešného stavu [58].

4.8 Útok časovým posunem (Time-shift attack)

Technika je podobná předchozímu útoku a opět spoléhá na nedokonalosti Bobových detektorů. Základní myšlenkou je, že jednotlivé detektory se od sebe mírně liší v časech své účinnosti. To znamená, že v danou chvíli je jeden z detektorů citlivější než druhý a má proto větší šanci zachytit světelný signál. V ideálním případě může nastat i chvíle, kdy je aktivní jen jeden z detektorů, zatímco ostatní jsou zcela mimo provoz. Příklad porovnání dvou detektorů je vidět na obrázku 4.8 níže. Je zřejmé, že v čase t_0 je citlivost detektoru 0 znatelně vyšší. K demonstraci útoku lze opět použít schéma z obrázku 4.7. Eva si tedy stejně jako v předchozím případě připraví falešné stavy v opačné bázi a s opačnou hodnotou. Dále odešle tento stav tak, aby na Bobův detektor dorazil v čase maximálního rozdílu mezi účinnostmi detektoru Evou zachyceného stavu (co nejvyšší účinnost) a ostatních detektorů (co nejnižší účinnost). Tímto způsobem se sníží QBER, a Eva získá část přenášeného klíče. V ideálním případě je chybovost nulová a Eva získá celý klíč [59, 60].



Obr. 4.8: Srovnání času účinnosti jednotlivých detektorů v čase [59].

4.9 Ostatní významné útoky

Kromě výše popsaných, existuje i velké množství dalších útoků. Ty mohou využívat různé zranitelnosti a jsou mnohdy specifické pro konkrétní protokol, případně jeho modifikaci. Příkladem může být útok přemapováním fáze (Phase-remapping attack) mířící na dvoucestná QKD schémata jako Plug&Play QKD. Dalším příkladem útoku oslepením je útok po uzavření brány (After-gate attack). Případně též útoky cílící na části praktického QKD systému pracujícími s klíčem v klasické podobě. Rovněž zde nebyly detailněji rozepsány konkrétní příklady kolektivních útoků [61, 62, 63].

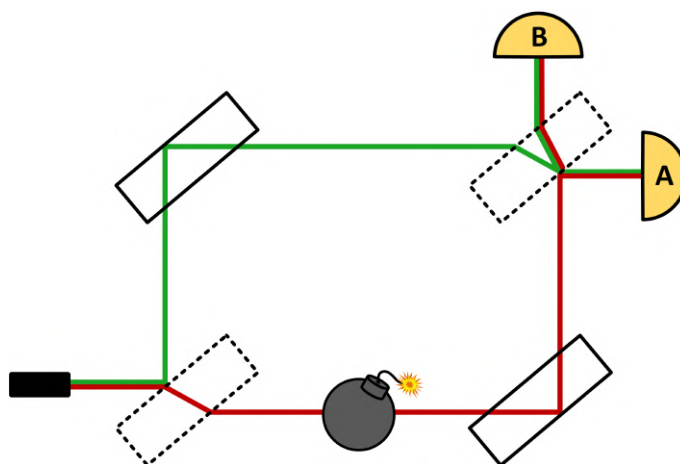
5 Kontrafaktuální definitivnost

Pojem označuje jednoznačnost výsledků měření, která ovšem nebyla ve skutečnosti provedena. Tedy schopnost určit existenci objektů a jejich vlastnosti, i když nebyly změřeny. V takovém případě se hovoří o tzv. měření bez interakce (Interaction-free measurement). Jinak řečeno, necht' je měření, které může vrátit pouze x možných výsledků. Je-li provedeno standardní měření pro $x - 1$ možností a není vrácen validní výsledek, pak výsledkem musí být x -tá možnost [64].

5.1 Elitzurův-Vaidmanův tester bomb

Jedná se o myšlenkový experiment, který využívá měření bez interakce k ověření funkčnosti bomby. Tzn. snaží se získat informace o předmětu bez interakce s ním. Princip experimentu je následující:

K dispozici je určité množství na světlo citlivých bomb. Tedy takových, které disponují světelným detektorem. To znamená, že je-li foton tímto detektorem absorbován, dojde k výbuchu. Některé z těchto bomb ovšem nejsou funkční a foton tak projde skrz ně dále. Cílem je určit, které bomby jsou funkční bez toho, aby byly všechny odpáleny [65].



Obr. 5.1: Test funkčnosti bomby pomocí měření bez interakce.

Testovaná bomba je umístěna do jedné z tras Machova-Zehnderova interferometru tak, jak je znázorněno na obrázku 5.1 výše. Ze zdroje jsou vysílány jednofotonové pulzy, které jsou následně rozděleny na dva. MZI je nastaven tak, aby veškeré světlo dopadalo na detektor A (konstruktivní interference). Ve chvíli, kdy je jeden z pulzů zablokovan a nedojde tak k interferenci, je výběr detektoru náhodný. V závislosti na funkčnosti se budou výsledky lišit [65].

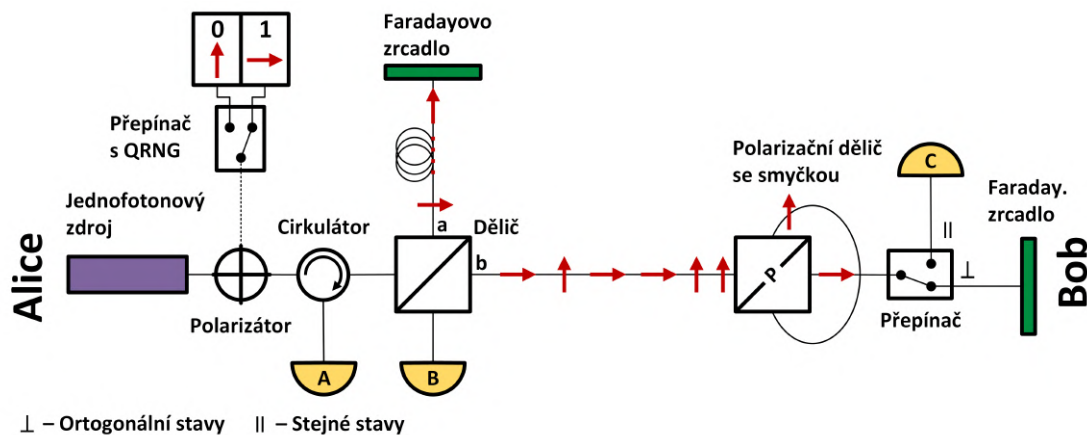
- **Nefunkční bomba** – Je-li bomba nefunkční, nedochází k interakci s fotonem. Pulz tak prochází dál a nakonec interferuje s pulzem, který prošel horní větví. V tomto případě dochází ke kliknutí na detektoru A ve 100 % případů.
- **Funkční bomba** – Pokud je bomba funkční, pak v 50 % případů dojde na bombě k detekci a následné explozi. Na detektorech A a B tak k detekci dále nedochází. I ve zbylých 50 % případů je ovšem spodní pulz zablokovan na bombě (neprojde dál) a nedochází tak k interferenci. Detekce na detektorech je v tomto případě náhodná v poměru 50:50. Z toho plyne, že ve 25 % případů dochází ke kliknutí na detektoru B.

Jinak řečeno, budou-li ověřovány pouze funkční bomby, bude docházet k níže popsaným výsledkům. Přestože je úspěšnost detekce funkční bomby pouze 25 %, je tento experiment důkazem funkčnosti měření bez interakce [65].

- **Bez detekce (50 %)** – Bomba je funkční a došlo k explozi
- **Detekce na A (25 %)** – Není průkazné a nedošlo k explozi
- **Detekce na B (25 %)** – Bomba je funkční a nedošlo k explozi

5.2 Kontrafaktuální kvantová kryptografie (CQC)

Princip CQC (Counterfactual quantum cryptography) spočívá v tom, že Alice náhodně generuje jednofotonové pulzy s horizontální a vertikální polarizací, kde $|\uparrow\rangle$ reprezentuje bit 0 a $|\rightarrow\rangle$ bit 1. Pulzy procházejí cirkulátorem a následně jsou rozděleny na dva stejné menší pulzy (uvažuje se dělič 50:50). Jeden setrvává uvnitř Alice (trasa a) zatímco druhý je odeslán k Bobovi (trasa b) [66].



Obr. 5.2: Možná implementace protokolu CQC [66].

Zde narazí na polarizační dělič svazků. Zatímco horizontálně polarizovaný pulz prochází přímo k optickému přepínači, pulz s vertikální polarizací prochází nejdříve optickou smyčkou. Bob si rovněž náhodně zvolí polarizaci, která reprezentuje bit. Pokud se shoduje s polarizací, kterou určila Alice (\parallel), je pulz přepnut přímo k detektoru C. Jsou-li polarizace vzájemně ortogonální (\perp), prochází přepínačem k Faradayově zrcadlu, kde dojde k otočení polarizace o 90° . Následně se vrací přímo přes přepínač k polarizačnímu dělič svazků. Nyní je situace opačná a přes smyčku je poslán nově vertikálně polarizovaný, dříve však horizontálně polarizovaný pulz. Tímto je zajištěno, že ať je polarizace jakákoliv, trvá cesta k Alici stejnou dobu. Podobně jako u pokusu s bombou dochází k následujícímu [66].

- **Alicin a Bobův bit se liší** – Tato situace odpovídá nefunkční bombě. Dochází k interferenci (zde se jedná o Michelsonův interferometr) a ke kliknutí na detektoru A ve 100 % případech.
- **Alicin a Bobův bit jsou shodné** – Odpovídá umístění funkční bomby (detektor C). V 50 % případech tak dochází ke kliknutí na Bobově detektoru C. Ve 25 % na detektoru A a stejně tak na detektoru B. Zde uvedené detektory umí kromě detekce fotonu rovněž rozlišit jejich stav (polarizaci).

Následně si Alice s Bobem předávají informace o tom, kdy který detektor klikl. V případě detektorů A a C si rovněž vymění detekovanou a původně zvolenou polarizaci. Tento postup slouží k případnému odhalení Evy. Pokud došlo k detekci na detektoru B a výsledek odpovídá původní polarizaci, nejsou žádné informace uveřejněny. V opačném případě Alice rovněž sdělí Bobovi výsledky měření. Ze správně detekovaných bitů na detektoru B je následně sestavován společný klíč. Efektivita protokolu je tak 25 %. Podobně jako u jiných protokolů mohou být k detekci odposlechu obětovány části klíče, rovněž následující procedury jsou podobné [66].

Výhodou je rozdělení protokolu na dva subsystémy (a , b). V případě subsystému a pulz nikdy neopustí Alici a Eva k němu tak nemá přístup. Praktickým důsledkem je tak např. přirozená odolnost vůči PNS útoku. V případě, že by se Eva pokusila o odposlech, mohou nastat tyto možnosti [66].

- **Alicin a Bobův bit jsou shodné** – Bez ohledu na Evinu volbu se v tomto případě pravděpodobnosti jednotlivých detekcí nezmění. Eva není detekována nezíská žádné informace.
- **Alicin a Bobův bit se liší**
 - **Alicin a Evin bit se liší** – Interference je zachována a dojde vždy k detekci na detektoru A. Tyto hodnoty jsou zahazovány a ačkoliv Eva opět není detekována nezíská žádné informace.
 - **Alicin a Evin bit jsou shodné** – Interference je přerušena, což generuje chyby na detektoru B, čímž je Eva odhalena.

6 Techniky prodloužení dosahu QKD

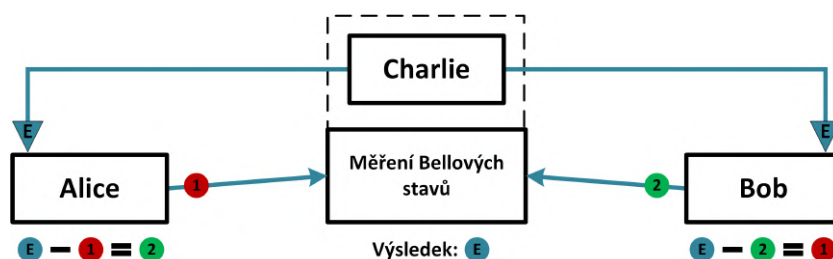
6.1 Důvěryhodný opakovač (Trusted repeater)

Pro zajištění delšího dosahu kvantového signálu není možné použít standardní zařízení uvedená na předchozí straně. V současnosti se nejčastěji používá tzv. **důvěryhodný opakovač**. Jedná se o zařízení mezi Alicí a Bobem, které ovšem neopakuje samotný kvantový signál. Princip spočívá v ustanovení kvantového klíče mezi Alicí a opakovačem Charliem (K_{AC}) a mezi opakovačem a Bobem (K_{CB}). Následně Alice vygeneruje finální klíč (K_{AB}), zašifruje jej pomocí K_{AC} . Po obdržení Charlie tento klíč přešifruje pomocí K_{CB} a odešle Bobovi. Tímto je bezpečně ustanoven kvantový klíč pomocí důvěryhodného opakovače. Charlie však již pracuje s klíčem v klasické podobě, proto se musí jednat o důvěryhodné zařízení [77]. Tento princip je detailněji popsán v kapitole 8.2.2.

6.2 QKD nezávislé na měřicím zařízení (MDI-QKD)

V současnosti MDI-QKD (Measurement-device independent) dosahuje významných úspěchů. Jedná se o protokoly založené na kvantovém provázání částic. Základem je použití prostředního uzlu k operaci zvané měření Bellových stavů (BSM – Bell state measurement), což je společný stav dvou provázaných částic. Tímto je možné zvýšit vzdálenost kvantového kanálu na dvojnásobek. Protokol funguje tak, že Alice a Bob odešlou foton k Charliemu. Zde se provede BSM a oba fotony se prováží. Charlie (případně Eva) neznají stav původních fotonů a dozví se až výsledek měření (jeden z Bellových stavů). Tento výsledek dále předá Alici a Bobovi. Ti jsou z něj a ze stavu, který sami odeslali schopni určit stav protistrany. Eva je tedy schopna určit pouze to, zda byly odeslány shodné nebo opačné fotony. Příklad, kdy oba odeslali stejné fotony, není považován za bezpečný a klíč z něj není odvozován [78].

Příkladem podobného protokolu může být např. protokol TF-QKD (Twin-field QKD), který již v experimentálních podmínkách dosahuje vzdálenosti až 830 km [80].



Obr. 6.1: Podstata MDI-QKD protokolů.

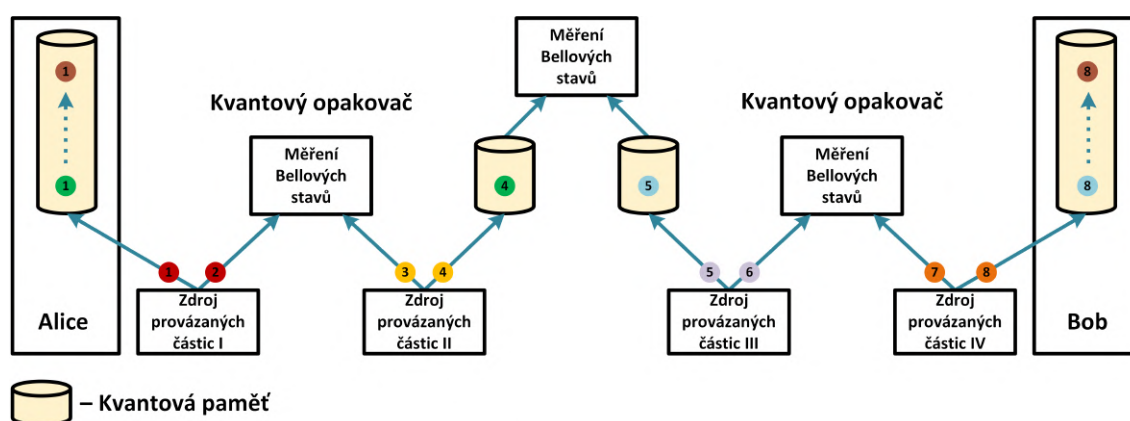
6.3 Kvantový opakovač

Pod pojmem kvantový opakovač se rozumí spíše komplexní návrh specifického QKD protokolu, než univerzální zařízení opakující libovolný kvantový signál. Princip částečně navazuje na předchozí možnost. Spíše je ale založen na jevu zvaném prohození kvantového provázání (Entanglement swap). Základním principem je existence dvou nezávislých dvojic provázaných fotonů. Bellovo měření nad jedním fotonem z první a z druhé dvojice vyústí ve zničení těchto fotonů, zatímco zbylé dva fotony se vzájemně prováží [79, 81].

Druhým předpokladem pro sestavení kvantového opakovače je funkční kvantová paměť. Tzn. místo, na kterém je možné uchovávat původní hodnotu kvantového stavu před další operací. Právě současná neexistence kvantových pamětí je důvodem, proč se kvantové opakovače dosud nevyskytují. I když i na tomto poli dochází postupně k pokrokům [82].

Zjednodušené schéma protokolu založeného na kvantových opakovačích se nachází na obrázku 6.2. Mezi Alicí a Bobem se nacházejí dva kvantové opakovače ve vzdálenostech, které umožňují bezproblémové doručení kvantového signálu. Každý opakovač obsahuje dva zdroje provázaných fotonových párů v některém z Bellových stavů. Jeden foton z každé dvojice je odeslán do kvantové paměti a druhý k měření Bellova stavu. Měření dojde k prohození provázání a fotony jsou zničeny. Nyní jsou provázány fotony v kvantových pamětech vždy mezi Alicí a prvním opakovačem a Bobem a opakovačem číslo dvě. V dalším kroku jsou zbylé fotony v opakovačích opět poslány k měření. Tímto dojde k provázání fotonů mezi Alicí a Bobem [79].

Před každým prohozením dochází k tzv. purifikaci (Entanglement purification), která zajistí, že jsou provázané fotony plně korelovány (tzn. odpovídají jednomu z Bellových stavů). Tato technika zde ovšem detailněji popisována nebude [81].



Obr. 6.2: Kvantová distribuce klíčů postavená na dvou kvantových opakovačích [79].

7 Nežádoucí jevy ve vlákně

V této kapitole jsou popsány nejčastěji se vyskytující nežádoucí jevy v optickém vlákně a vysvětlen jejich vliv na kvantový kanál. Současně jsou nastíněny možnosti, jak vliv daného jevu snížit.

7.1 Útlum

Podobně jako u všech přenosových médií, i v optickém vlákně dochází se zvyšující se vzdáleností k postupnému snižování výkonu signálu. Pro určitou vlnovou délku je definován jako poměr vstupního a výstupního světelného výkonu. Rozložení vhodných pásem pro umístění kanálu lze najít výše na obrázku 1.2. Mezi základní pojmy patří:

- **Útlum** – bezrozměrná veličina, která popisuje množství světla, určité vlnové délky, které bylo ztraceno (pohlčeno, odraženo...) při průchodu optickým vláknem. Vypočítá se jako poměr ztraceného a vstupního výkonu [83].

$$A = \frac{P_{\text{útlum|mW}}}{P_{\text{vstup|mW}}} [-] \quad (7.1)$$

- **Transmitance** – bezrozměrná veličina, která popisuje množství světla, určité vlnové délky, které prošlo optickým vláknem. Vypočítá se jako poměr výstupního a vstupního výkonu [84].

$$T = \frac{P_{\text{výstup|mW}}}{P_{\text{vstup|mW}}} [-] \quad (7.2)$$

- **Vztah útlumu a transmitance** – součet obou veličin musí dát 100 %. Tedy výstupní a ztracený výkon musejí být rovny vstupnímu výkonu.

$$A + T = 1 [-] \quad (7.3)$$

- **Výstupní výkon** – optický výkon v mW, který vystupuje z optického vlákna. Vypočte se jako součin vstupního výkonu a transmitance.

$$P_{\text{výstup|mW}} = P_{\text{vstup|mW}} \cdot T [mW] \quad (7.4)$$

7.1.1 Lineární útlum

Používá se u kratších tras, kdy je možné zanedbat nelineární vlastnosti vlákna. Útlum je tak považován za lineární funkci délky trasy a je možné jej převádět na logaritmické jednotky – decibely. Platí pro něj následující vzorce¹ [85]:

- **Transmitance** – lze ji vypočítat pomocí následujícího vzorce:

$$T = 1 - A = 1 - \alpha L [-] \quad (7.5)$$

- **Výstupní výkon** – po dosazení transmitance se vypočte takto:

$$P_{výstup|mW} = P_{vstup|mW} \cdot (1 - A) = P_{vstup|mW} \cdot (1 - \alpha L) [mW] \quad (7.6)$$

7.1.2 Nelineární útlum

V případě delších optovláknových tras již není možné použít aproximaci pomocí lineárního útlumu. Skutečný útlum je spíše exponenciální funkcí délky. Používají se následující vzorce¹ [85]:

- **Transmitance** – lze ji vypočítat pomocí následujícího vzorce:

$$T = e^{-A} = e^{-\alpha L} [-] \quad (7.7)$$

- **Výstupní výkon** – po dosazení transmitance se vypočte takto:

$$P_{výstup|mW} = P_{vstup|mW} \cdot e^{-A} = P_{vstup|mW} \cdot e^{-\alpha L} [mW] \quad (7.8)$$

¹ α – měrný útlum, L – délka trasy, e – Eulerovo číslo

7.1.3 Logaritmické jednotky

Útlum, případně zisk, optického výkonu se často vyjadřuje v logaritmických jednotkách zvaných decibel (dB). V případě lineárního útlumu je výhodou zejména jeho snadné přičítání. Kromě zmíněného útlumu (poměru dvou hodnot) je však nutné správně převést i výkony z mW na dBm. K tomu slouží vzorce v tabulce 7.1 níže. Útlum, respektive měrný útlum, v decibelech se dosazuje s kladným znaménkem.

Tab. 7.1: Převod na logaritmické jednotky.

| Převod na dB/dBm | | Převod z dB/dBm | |
|--|--------------|--|------------------------|
| Optický výkon | | | |
| $P_{dBm} = 10 \cdot \log(P_{mW})$ | <i>dBm</i> | $P_{mW} = 10^{P_{dBm}/10}$ | <i>mW</i> |
| Lineární útlum a transmitance | | | |
| $A_{dB} = -10 \cdot \log(T)$ | <i>dB</i> | $T = 10^{-A_{dB}/10}$ | – |
| Lineární měrný útlum | | | |
| $\alpha_{dB} = -10 \cdot \frac{\log(1-\alpha L)}{L}$ | <i>dB/km</i> | $\alpha = \frac{1-10^{-\frac{\alpha_{dB}L}{10}}}{L}$ | <i>km⁻¹</i> |
| Nelineární útlum a transmitance | | | |
| $A_{dB} = T \cdot \frac{10}{\ln 10}$ | <i>dB</i> | $T = A_{dB} \cdot \frac{\ln 10}{10}$ | – |
| Nelineární měrný útlum | | | |
| $\alpha_{dB} = \alpha \cdot \frac{10}{\ln 10}$ | <i>dB/km</i> | $\alpha = \alpha_{dB} \cdot \frac{\ln 10}{10}$ | <i>km⁻¹</i> |

V případě, kdy se počítá pouze s lineárním útlumem, je počítání v decibelech výhodné, neboť umožňuje převést vzorec 7.4 na²:

$$P_{výstup|dBm} = P_{vstup|dBm} - A_{dB} [dBm] \quad (7.9)$$

Za předpokladu, že se počítá s nelineárním útlumem, je nutné přepočítat logaritmické hodnoty zpět a útlum připočítat v základních jednotkách. Výsledný výkon je pak možné opětovně převést na dBm.

²Zatímco ve vzorci 7.4 se násobí transmitancí, ve vzorci 7.9 se již odčítá přímo útlum.

7.1.4 Útlum a ztráty

Celkový útlum trasy sestává z následujících složek [67].

$$A = \alpha \cdot L + \zeta \quad (7.10)$$

- $A = [dB]$ – Celkový útlum trasy
- $\alpha = [dB/km]$ – Měrný útlum (koeficient útlumu)
- $L = [m]$ – Délka optické trasy
- $\zeta = [dB]$ – Ztráty na optických prvcích a spojích

Měrný útlum jsou ztráty světelného výkonu v optickém vlákne za určitou vzdálenost. Skládá se z následujících několika složek [67].

$$\alpha = \alpha_{absorpce} + \alpha_{Rayleigh} + \alpha_{neregularity} + \alpha_{mikroohyby} + \alpha_{makroohyby} \quad (7.11)$$

- $\alpha_{absorpce} = [dB/km]$ – Útlum absorpcí
- $\alpha_{Rayleigh} = [dB/km]$ – Útlum vzniklý Rayleighovým rozptylem
- $\alpha_{neregularity} = [dB/km]$ – Útlum na neregularitách
- $\alpha_{mikroohyby} = [dB/km]$ – Útlum na mikroohybech
- $\alpha_{makroohyby} = [dB/km]$ – Útlum na makroohybech

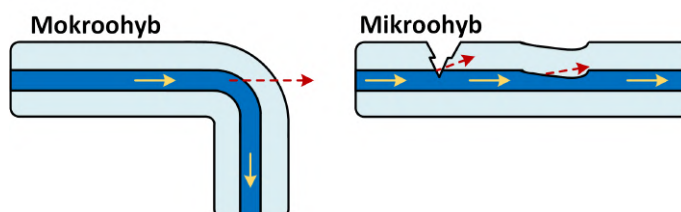
Obdobně lze na jednotlivé složky rozložit i výše zmíněné ztráty. Veškeré zde uváděné složky budou detailněji popsány dále.

$$\zeta = \zeta_{odraz} + \zeta_{navázání} + \zeta_{průřez} \quad (7.12)$$

- $\zeta_{odraz} = [dB]$ – Ztráty dané odrazem
- $\zeta_{navázání} = [dB]$ – Vazební ztráty na spojích
- $\zeta_{průřez} = [dB]$ – Ztráty dané rozdílným průřezem vláken

7.1.5 Složky celkového útlumu trasy

- **Útlum absorpcí** – Část optického výkonu je pohlcena materiálem jádra (vlastní absorpce) a vyskytujícími se nečistotami (nevlastní absorpce). Množství absorbovaného světla je závislé na jeho vlnové délce [67].
- **Útlum vzniklý Rayleighovým rozptylem** – Vzniká vlivem kolizí světelných fotonů s molekulami jádra. Důsledkem je roztržštění paprsků světla do různých směrů. Část je odražena zpět a pohlcena, část je odražena do pláště vlákna³ [67].
- **Útlum na neregularitách** – Jedná se především o makronečistoty, vzduchové bublinky, trhlinky. Dále různé poruchy tvaru a rozměrů vlákna, nepravidelné hranice mezi jádrem a pláštěm nebo excentricitu a eliptičnost jádra. Na některých nehomogenitách může docházet Mieově rozptylu³ [67].
- **Útlum na mikroohybech** – Mikroohyby jsou poruchy přímocárnosti osy vlákna a malé chyby v jeho geometrii. Vznikají při výrobě a deformačním působením okolí. Důsledkem je, že jsou některé vidy odraženy do pláště, tedy mimo jádro vlákna [67].
- **Útlum na makroohybech** – Makroohyby se běžně vyskytují při praktickém použití vlákna. Dojde-li k ohybu vlákna pod určitou mez, může docházet k vyzařování energie z vlákna ven. Toho se někdy využívá pro odposlech optického přenosu [67].

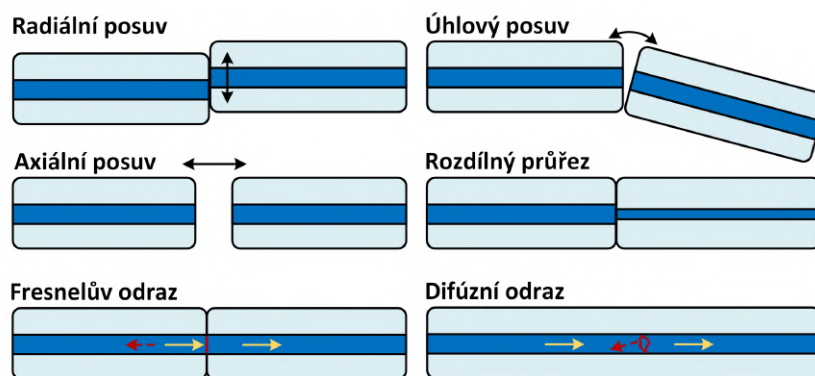


Obr. 7.1: Srovnání makroohybů a mikroohybů [67].

- **Ztráty odrazem**
 - **Fresnelův odraz** – Vzniká při navázání světla do vlákna. Část záření se odráží od čela vlákna a vrací se zpět. Podobně dochází k odrazu i na konci vlákna [67].
 - **Difúzní odraz** – Nastává na mikroskopických nerovnostech a vadách materiálu v oblasti odrazu nebo lomu optického záření. Množství difúzně odraženého optického záření je dáno koncentrací bodových poruch v místě dopadu optického záření [67].

³Bude popsáno dále v kapitole 7.4 Rozptyl

- **Vazební ztráty**
 - **Radiální posuv** – Ztráty vznikají radiálním posuvem vláken vůči jejich ose a tvoří největší podíl jejich celkové hodnoty [67].
 - **Axiální posuv** – Vzniká, pokud jsou čela vláken nebo ferulí od sebe příliš vzdálena a z tohoto důvodu část paprsků dopadá do oblasti pláště navazujícího vlákna [67].
 - **Úhlový posuv** – Vzhledem k přesnosti výroby ferulí a obecně nižší citlivosti ztrát se většinou nepodílí na ztrátách u konektorů [67].
- **Ztráty dané rozdílným průřezem vláken** – Jsou způsobeny spojováním vláken s rozdílným průřezem jader, kdy část paprsků dopadá na plášť následujícího vlákna [67].



Obr. 7.2: Příčiny vzniku ztrát [67].

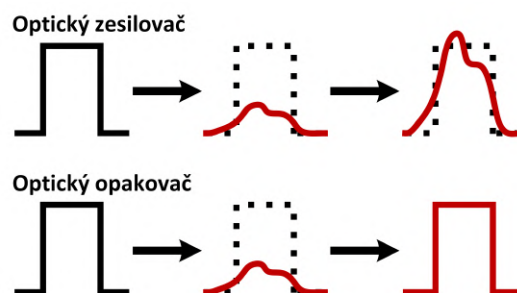
7.1.6 Útlumové články

Útlumový článek, někdy také označovaný jako optický atenuátor, je zařízení používané ke snížení optické intenzity světelného paprsku. Hodnota jeho útlumu se udává nejčastěji v decibelech. Atenuátor existuje v mnoha provedeních. Nejjednodušší variantou jsou fixní atenuátory (FOA – Fixed optical attenuator), na kterých není možné hodnotu měnit. Druhou možností jsou články proměnné (VOA – Variable optical attenuator). Jejich hodnotu je možné přizpůsobovat jak spojitě, tak diskrétně po krocích [68].

- **Mezerový atenuátor** – Využívá axiálního posuvu dvou optických vláken. Vzniklou mezerou je určité množství světelného výkonu vyzářeno mimo vlákno a dochází tak k jeho zeslabení [69].
- **Absorpční atenuátor** – Princip spočívá v pohlcení části světelného výkonu filtrem z absorpčního materiálu. Toto světlo následně přeměněno na teplo [70].
- **Reflexní atenuátor** – Existuje několik možných principů, které využívají Fresnelova nebo difúzního odrazu k odražení části výkonu vlákna pryč. Vyskytuje se i varianta s odrazem od zrcadla [70, 71].
- **Polarizační atenuátor** – Vhodné pro polarizované signály. Používá se půlvlnná destička v kombinaci s lineárním polarizátorem. Otáčením destičky lze přizpůsobit hodnotu útlumu [70].

7.1.7 Zesilovače a opakovače klasických signálů

Optický zesilovač je zařízení, které přijímá určitý světelný vstupní signál a generuje výstupní signál s vyšším optickým výkonem (včetně zkreslení). Podobným zařízením je opakovač, který však zkreslený vstupní signál převádí do elektrické podoby a na výstup odesílá signál zrekonstruovaný. Rozdíl je zřejmý z obrázku níže 7.3 [72].



Obr. 7.3: Rozdíl mezi optickým zesilovačem a opakovačem [72].

Kvantový signál je velmi slabý a je tak limitujícím prvkem každého QKD systému. Již z podstaty jej však není možné zesílit nebo zopakovat (klonovat). Řešením

tohoto problému může být tzv. kvantový opakovač, ten však není v tuto chvíli dostupný. Následující typy zesilovačů se však v optických sítích běžně používají (včetně kombinací) a mohou svými vedlejšími účinky kvantový kanál zarušit.

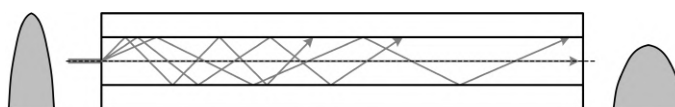
- **Erbium dopovaný zesilovač** (EDFA – Erbium doped fiber amplifier) – základem dopovaných zesilovačů je vzácnými prvky dopované optické vlákno. Nejčastěji se k tomuto účelu používá erbium pro zesílení signálů kolem vlnové délky 1550–1600 nm. Ionty erbia ve vlákně pohlcují fotony o vlnové délce 980 nm dodávané laserem (pumpa). Tím se dostanou na vyšší energetickou hladinu, která ovšem není stabilní. Z tohoto důvodu postupně klesají na hladinu základní, přičemž vyžáří foton o vlnové délce kolem 1550–1600 nm. Tento výkon se přičte k zesilovanému signálu. Pro jiné vlnové délky se používají jiné prvky např. ytterbium [73, 74, 75].
 - **Výhody:** vysoký zisk (30–50 dB) v pásmech C a L, nezávislost na polarizaci a teplotě
 - **Nevýhody:** neexistuje selektivita (zesiluje i šum)
- **Polovodičový zesilovač** (SOA – Semiconductor optical amplifier) – Na rozdíl od EDFA nepoužívá dopované optické vlákno. Současně není napájen laserovým čerpadlem, ale elektrickým proudem. Obvykle se používají na kratších spojích [73, 74, 75].
 - **Výhody:** nízká spotřeba, pracují na širokém spektru 850–1600 nm
 - **Nevýhody:** vysoký vstupní útlum, vlivem něhož je nižší zisk (15–20 dB), citlivost na polarizaci
- **Ramanovský zesilovač** (RFA – Raman fiber amplifier) – Využívá se stimulovaný Ramanův rozptyl v materiálu vlákna. Zdrojem energie je optický zdroj s kratší vlnovou délkou než zesilovaný signál. Pro zesílení signálu na vlnové délce 1550 nm se použije zdroj s vlnovou délkou 1450 nm. Ve vlákně následně dojde k Ramanově rozptylu, kdy je vlnová délka posunuta zhruba o 100 nm. Tím se zesílí původní signál [73, 74, 75].
 - **Výhody:** vysoký zisk (30 dB) na libovolné vlnové délce, nižší šum než u SOA a EDFA, Ramanův jev se vyskytuje v každém vlákně
 - **Nevýhody:** používají se výkonné pumpy, které mohou zapříčinit některé nelineární jevy, nižší účinnost než EDFA

Zesilovače mohou fungovat v různých režimech. Možnosti se liší podle konkrétního zařízení. Nejčastěji se ovšem vyskytuje **výkonový mód** (Power mode), který udržuje konstantní hodnotu optického výkonu a **ziskový mód** (Gain mode) udržující konstantní hodnotu zisku. [76].

7.2 Disperze

7.2.1 Vidová disperze

Vidová disperze se vyskytuje v mnohavidových vláknech (v jednovidových je možné zanedbat). Každý paprsek dorazí díky rozdílnosti délek drah na konec vlákna v rozdílných časových okamžicích. Impulz získaný z jednotlivých paprsků se liší tvarem i amplitudou od vstupního impulzu. Tento jev se projevuje u dlouhých vláken při přenosu dat na větší vzdálenosti a omezuje počet impulzů, které mohou být za určitý časový interval vyslány. Při přenosu na velké vzdálenosti (větší než 1 km) dochází k tomu, že různé paprsky (vidy) nejsou přeneseny od začátku vlákna na jeho konec za stejnou dobu. Dochází tak ke zkreslení [67, 86].



Obr. 7.4: Zkreslení pulzu dané vidovou disperzí v optickém vlákne [67].

7.2.2 Chromatická disperze

Chromatická disperze je vysvětlena pomocí níže uvedených vztahů. Rychlost propagace elektromagnetické vlny odpovídá její fázové rychlosti, tedy:

$$v_{fáze} = \frac{\lambda}{T} = \lambda \cdot \nu \quad (7.13)$$

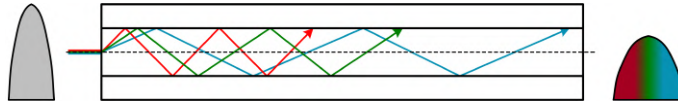
Je zřejmé, že fázová rychlost závisí na frekvenci vlny. Dále je definován index lomu jako:

$$n = \frac{c}{v_{fáze}} \quad (7.14)$$

Zde c odpovídá fázové rychlosti světla ve vakuu. Index lomu je tedy poměrem dvou fázových rychlostí. Protože je rychlost světla ve vakuu konstantní závisí index lomu na frekvenci daného záření. Jinými slovy, pro každou složku světla o jiné frekvenci má daný materiál odlišný index lomu. Níže je definován Snellův zákon:

$$n_1 \cdot \sin \alpha_1 = n_2 \cdot \sin \alpha_2 \quad (7.15)$$

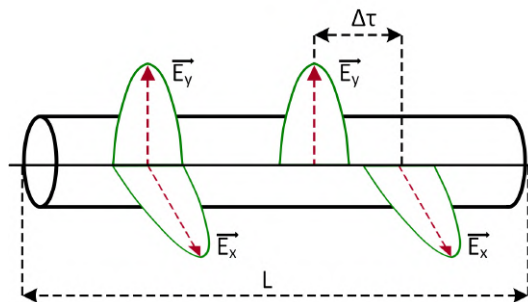
Z něj plyne, že odlišný index lomu vyvolá jiný úhel lomu. Tímto způsobem dochází k chromatické disperzi. Chromatická disperze narušuje koherenci signálu. V případě, že je chromatická disperze nulová dochází na multiplexorech k čtyřvlennému směšování (FWM). Tento jev bude popsán dále [67].



Obr. 7.5: Zkreslení pulzu dané chromatickou disperzí v optickém vlákne [67].

7.2.3 Polarizační vidová disperze (PMD)

PMD (Polarisation mode dispersion) je druh zkreslení optického impulzu ve vlákne, respektive závislosti polarizace na charakteristice šíření ve vlákne. Elektromagnetická vlna se skládá ze vzájemně kolmých vektorů intenzity elektrického pole \vec{E} a magnetické indukce \vec{B} . Kvůli jejich pevně dané vzájemné poloze je možné jeden z vektorů vynechat. Typicky se tak používá pouze vektor \vec{E} , který lze dále rozložit do dvou rovin \vec{E}_x a \vec{E}_y . V ideálním vlákne se obě složky šíří stejně rychle. Vlivem deformací vlákna (ohyby, stlačení...) ovšem dochází k tomu, že se jednotlivé složky šíří různou rychlostí. To způsobuje „roztahování“ pulzů a změny polarizace. Vyskytuje se zejména u jednovlenných vláken (SMF – Single mode fiber) [67, 87, 88].



Obr. 7.6: Změna polarizace zapříčiněná PMD v optickém vlákne [67].

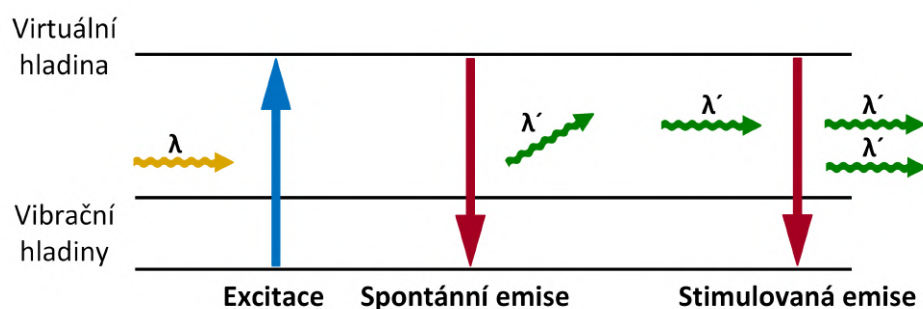
Současná vlákna mají typicky nízkou hodnotu $PMD = \Delta\tau/\sqrt{L} = 0,05 \text{ ps}/\sqrt{\text{km}}$. Význam hodnot je zřejmý z obrázku 7.6. Změny polarizace jsou problematické pro QKD protokoly využívající polarizační kódování jako BB84. Základní myšlenka protokolu COW je ovšem založena na udržení koherence. Z tohoto důvodu je vůči změnám polarizace odolný. Pro další uvažování je tak možné PMD zanedbat [67, 87, 88].

7.3 Šum a přeslech

7.3.1 Spontánní a stimulovaná emise

Při čerpání zesilovacího média je elektron excitován z nižší energetické hladiny na hladinu vyšší. Protože jsou vyšší hladiny obecně méně stabilní než hladiny nižší, dochází následně k uvolnění (deexcitaci) elektronu, který sestoupí na některou nižší energetickou hladinu vyzařováním energie (fotonu). Toto platí jak pro spontánní, tak stimulovanou emisi. Vlastnosti fotonů generovaných spontánní a stimulovanou emisí jsou však odlišné [89, 90].

- **Spontánní emise** – Probíhá bez interakce s jinými fotony a jejich směr, fáze a polarizace jsou tak náhodné. Energie fotonu a jeho vlnová délka odpovídají velikosti rozdílu energetických hladin poklesu elektronu. Výsledkem je Rayleighův a Ramanův rozptyl.
- **Stimulovaná emise** – Probíhá při interakci excitovaného elektronu s jiným fotonem. Při stimulované emisi jsou směr, fáze, vlnová délka (energie) a polarizace „okopírovány“ od jiného fotonu. Jedná se o nejdůležitější jev pro vytvoření vysoce směrového a vysoce koherentního zdroje světla (např. laserové diody, vláknového laseru a optického zesilovače).



Obr. 7.7: Spontánní a stimulovaná emise [90].

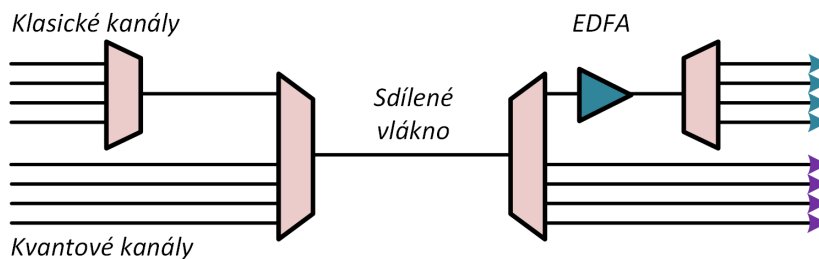
Ke stimulované emisi dochází pouze tehdy, je-li zesilovací médium čerpáno dostatečně silně a dojde k populační inverzi, zatímco spontánní emise probíhá bez ohledu na to, zda populační inverze existuje, či nikoli [89, 90].

7.3.2 Zesílená spontánní emise (ASE)

ASE (Amplified spontaneous emission) je světlo vzniklé pomocí spontánní emise, které je následně zesíleno pomocí stimulované emise. Jedná se o převážně nechtěný jev, vznikající zejména v optických zesilovačích (např. EDFA). Výsledkem ASE je „okopírování náhodných fotonů“ vzniklých spontánní emisí – tedy zesílení spontánní

emise. Tímto způsobem vzniká na optické lince šum. Výkon ASE je typicky mnohem nižší než výkon klasického kanálu, je ovšem mnohem širší (až desítky nanometrů). Většina optických linek dnes EDFA zesilovače používá. Z tohoto důvodu je nutné je v síti správně umístit tak, aby tento šum nepronikal do kvantového kanálu. Vliv ASE na kvantový kanál lze potlačit níže uvedenými způsoby [91, 92].

- **Polarizace** – ASE šum není polarizovaný, 50 % jeho výkonu lze tedy odstranit pomocí lineárního polarizátoru [93].
- **Umístění** – Zesilovače EDFA jsou na trase většinou umísťovány za WDM prvky, aby mohly zesílit více kanálů současně. To není velký problém u klasických kanálů, kvantový kanál by ovšem byl tímto šumem zarušen. Z tohoto důvodu je nutné kvantový kanál přidat až později. Filtry v druhém multiplexoru (OADM – Optical add-drop multiplexer) kvantový kanál odizolují. Případně je možné EDFA zesilovač přidat až po vydělení kvantového kanálu, kde by sloužil jako předzesilovač [94].



Obr. 7.8: Vhodné umístění zesilovače EDFA [94].

7.3.3 Kerrův jev

Jedná se o jev, při kterém dochází v závislosti na přiložení elektrického pole ke změně indexu lomu optického vlákna. Kerrův jev může být vyvolán buďto vnějším elektrickým polem, nebo elektrickým polem samotného světla (elektromagnetická vlna). Je zodpovědný za vznik několika nelineárních jevů. Nejčastější jsou uvedeny níže [95].

Vlastní a křížová fázová modulace (SPM a XPM)

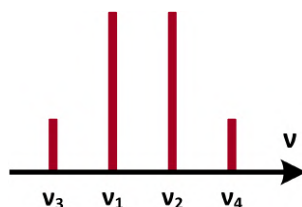
SPM (Self-phase modulation) je nelineární jev, vycházející z Kerrova jevu. Intenzivní světelný pulz změni index lomu vlákna. Tímto ovlivní vlastní fázi a tím i své frekvenční spektrum. XPM (Cross-phase modulation) je SPM velmi podobná. Rozdílem je, že pulz neovlivňuje sám sebe, nýbrž signál na jiné vlnové délce. Protože výkon kvantového kanálu je minimální není nutné SPM uvažovat. XPM lze omezit zvýšením chromatické disperze [96, 97].

Čtyřvlonné směšování (FWM)

FWM (Four-wave mixing) je společně s ASE a Ramanovým rozptylem jedním z hlavních zdrojů šumu. Jedná se o nelineární efekt ovlivněný Kerrovým jevem, vznikající zejména při multiplexování (mezikanálový přeslech). Za předpokladu, že se vláknem současně šíří dvě frekvenční složky ν_1 a ν_2 , dochází na rozdílové frekvenci ke změně indexu lomu. V takovém případě vznikají dvě nové frekvence, které jsou dány následujícími vzorci [98, 99].

$$\begin{aligned}\nu_3 &= \nu_1 - (\nu_2 - \nu_1) \\ \nu_4 &= \nu_2 + (\nu_2 - \nu_1)\end{aligned}\tag{7.16}$$

FWM vzniká u frekvencí, které jsou velmi blízko sebe a jejich efektivita je velmi závislá na fázovém přizpůsobení (phase-matching), fáze obou vysílaných signálů tedy musejí být ve stejné (velmi blízké) fázi. Chromatická disperze narušuje koherenci a tím pádem tlumí výkon FWM [98, 99].



Obr. 7.9: Rozložení původních a nových frekvencí vzniklých důsledkem FWM [98].

Při správném návrhu optické trasy je výkon čtyřvloného směšování na kvantovém kanálu v porovnání s Ramanovým šumem zanedbatelný. Je však potřeba zvážit následující.

- **Rozmístění kanálů** – Kvantový kanál je vhodné umístit tak, aby neležel v pásmu nově vzniklých frekvencí ν_3 a ν_4 [100].
- **Vysoká disperze** – Čím je chromatická disperze kanálů nižší, tím je vyšší FWM. Z tohoto důvodu je vhodné umístit klasické kanály do oblasti s nenulovou disperzí. Respektive zvolit vlákno s vhodně posunutou disperzní charakteristikou [101, 102].
- **Polarizační filtrování** – FWM je polarizováno stejně jako původní frekvence. Pokud je výkon FWM příliš vysoký, je možné použít pro všechny klasické kanály stejnou polarizaci (např. horizontální). Kvantovému kanálu je přidělena ortogonální polarizace (tedy vertikální). Následně se na kvantovém kanálu použijí polarizační filtry, které FWM pohltnou [101].

7.4 Rozptyl

Rozptyl je termín používaný ve fyzice k popisu široké škály fyzikálních procesů, kdy pohybující se částice nebo záření (např. světlo), jsou nuceny vychýlit se z přímé trajektorie přítomnými nerovnoměrnostmi v médium, kterým procházejí. Nejčastěji se uvádí následující dělení [103, 104].

- **Elastický (pružný) rozptyl** – Rozptyl, při kterém si odražený foton zanechává svoji energii (tedy i vlnovou délku) a mění se pouze jeho směr.
- **Neelastický (nepružný) rozptyl** – Rozptyl, při kterém se změní energie fotonu a tím i jeho vlnová délka (může klesat i růst).

V oblasti optických vláken se lze nejčastěji setkat s elastickým Rayleighovým a neelastickým Ramanovým rozptylem. Oba budou dále popsány.

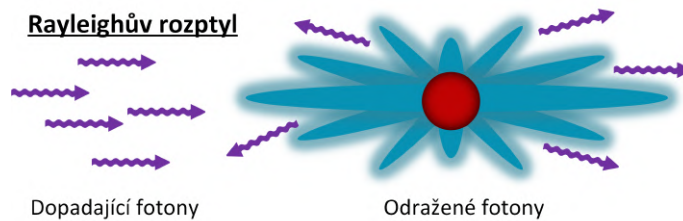
7.4.1 Elastický rozptyl

Jak již bylo řečeno, u elastického rozptylu nedochází ke změně vlnové délky. Dopadající foton se tedy od odraženého liší pouze směrem. V optice je možné se nejčastěji setkat s Rayleighovou teorií (pouze pro částice mnohem menší než vlnová délka), respektive s teorií Mieovou, která Rayleighovu teorii zobecňuje i pro větší částice. Čím je částice větší, tím větší je pravděpodobnost, že bude foton dále odražen v dopředném směru. Odražené fotony se nešíří „plynule“ do všech směrů, místo toho vznikají vinou interference laloky (interferenční obrazce) s vysokou pravděpodobností odrazu [104, 105].

Rayleighův rozptyl

Jedná se o rozptyl světla na molekulách prostředí, případně dalších částic, které jsou podstatně menší⁴ než vlnová délka záření. Vzniká v důsledku nepravidelnosti struktury materiálu optického vlákna, mikroskopických změn hustoty materiálu a změn indexu lomu. Fotony procházející daným optickým prostředím částečně excitují elektrony v elektronových obalech atomů daného materiálu. Foton je částicí pohlcen a následně je s určitou pravděpodobností vyemitován (odražen) v určitém směru (spontánní emise). Ačkoliv v případě Rayleighova rozptylu dochází k rozptylu do všech stran, nejvíce fotonů se odrazí v dopředném a zpětném směru. Tento typ rozptylu je v materiálech častější – nastává přibližně 10milionkrát častěji, než Ramanův rozptyl. Oba rozptyly budou později srovnány [106, 107, 108, 109].

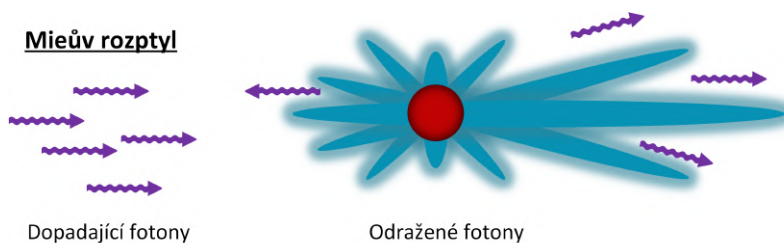
⁴To přibližně znamená: *částice* $< \lambda/10$



Obr. 7.10: Rayleighův rozptyl [106].

Mieův rozptyl

V případě větších⁵ částic se hovoří o tzv. Mieově rozptylu. Může se jednat např. o kapičky vody v atmosféře, nečistoty v optickém vlákně atd. V tomto případě je rozptyl značně dopředný [106, 107, 108].



Obr. 7.11: Mieův rozptyl [106].

Optický rozptyl

Mieův rozptyl na částici s rozměry většími než vlnová délka se někdy nazývá obecně optický rozptyl⁵. S rostoucími rozměry částice se dále zvyšuje počet dopředně odražených fotonů [106, 107, 108].



Obr. 7.12: Optický rozptyl [106].

⁵ V případě Mieova rozptylu se jedná o: $\lambda/10 < \text{částice} < \lambda$, pro optický rozptyl pak platí: $\lambda < \text{částice}$

7.4.2 Neelastický rozptyl

Podobně jako u elastického rozptylu i zde dochází k interakci elektromagnetického fotonu (světla) s částicí hmoty v prostředí (atom, molekula, respektive jejich elektron). Na rozdíl od pružného rozptylu zde dochází ke změně energie fotonu a tedy i jeho vlnové délky. Vztah mezi energií fotonu a vlnovou délkou: $E = h\nu = hc/\lambda$. Tedy čím vyšší má foton energii, tím vyšší je jeho frekvence a nižší vlnová délka [104].

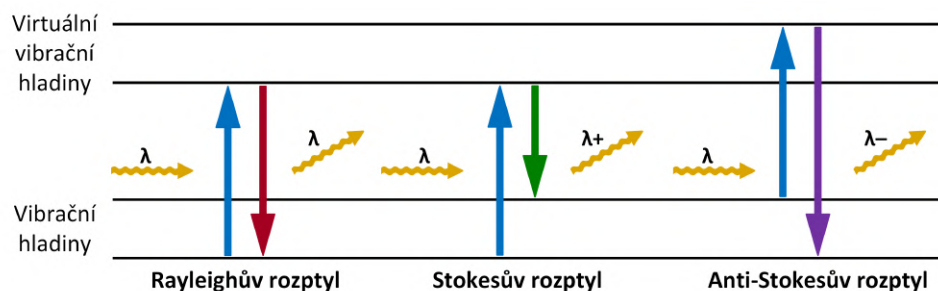
- **Absorpce fotonu** – Část energie fotonu je částicí látky pohlcena. Původní foton je absorbován a je vyzářen nový foton s nižší energií (větší λ).
- **Emise fotonu** – Foton, získá z částice energii. Původní foton je absorbován a je vyzářen nový foton s vyšší energií (menší λ).

Ramanův rozptyl

Molekuly mohou existovat v určitých stavech, kterým se říká vibrační a rotační energetické hladiny. Ramanův rozptyl je jev vznikající při interakci fotonů s těmito stavy (elektrony). Výsledkem je odražený foton o jiné vlnové délce než foton původní. Foton může energii, jak přijmout, tak ztratit. To je dále popsáno na obrázku 7.13, kde se nachází i srovnání s Rayleighovým rozptylem. V jeho případě dochází k excitaci molekuly ze základního vibračního stavu do tzv. virtuálního vibračního stavu. Jedná se o přechodný stav, který je dán energií záření. Molekula ovšem v excitovaném stavu dlouho nevydrží a následně se vrátí na původní hladinu. Z tohoto důvodu musí být vyzářeno stejné množství energie jako bylo absorbováno. V případě Ramanova rozptylu ovšem nedochází k návratu na původní hladinu. Naopak si molekula buď část energie fotonu ponechá nebo fotonu naopak energii dodá. Takto vznikají fotony odlišné vlnové délky. Kromě samotného rozptylu tak vzniká v médiu i šum. Ramanův rozptyl je tedy dvojího druhu [109, 110, 111].

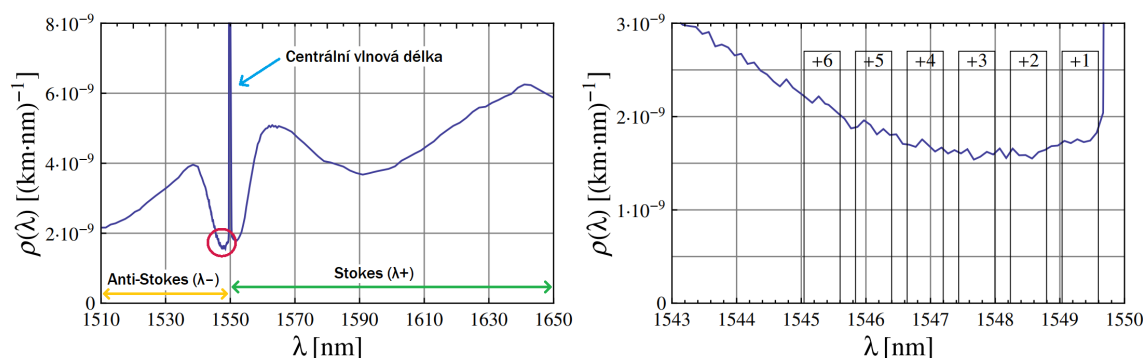
- **Stokesův posun (rozptyl)** – Foton ztrácí kvantum energie. Molekula je excitována na vyšší energetickou hladinu. Při deexcitaci ovšem vyzáří menší množství energie, a tak vzniká foton o větší vlnové délce [109].
- **Anti-Stokesův posun (rozptyl)** – Foton získá kvantum energie. Malá část molekul se už před interakcí s fotonem nachází v excitovaném stavu. Po interakci s fotonem je excitována na energeticky vyšší virtuální hladinu. Následně deexcituje až do základního vibračního stavu. Z tohoto důvodu musí být vyzářen energičtější foton s kratší vlnovou délkou [109].

V optickém vlákně dochází k tzv. spontánnímu Ramanově rozptylu (SRS nebo SpRS – Spontaneous Raman scattering). Hodnotu tohoto šumu lze určit z normalizovaného průřezu Ramanova rozptylu (cross-section). Níže uvedené grafy 7.14 popisují situaci pro optický vysílač (laser) na vlnové délce 1550 nm. Je jasně vidět, že kromě



Obr. 7.13: Srovnání Rayleighova a Ramanova rozptylu [109].

oblasti v blízkosti středu spektrální čáry (Rayleighův rozptyl) je výkon rozptýlen „do stran“. V oblastech s kratší vlnovou délkou se nachází Stokesův rozptyl. Na opačné straně pak rozptyl Anti-Stokesův. Ve většině případů je Stokesův rozptyl vyšší, jak rovněž plyne z levého grafu. Z tohoto důvodu je vhodné umístit kvantový kanál na vlnovou délku nižší, než mají klasické kanály. Druhý graf představuje přiblížení do oblasti s nejnižším Ramanovým Anti-Stokesovým rozptylem (vyznačeno červeně). Je vidět, že k nejmenšímu šumu dochází na kanálech vzdálených zhruba 2 až 3 nm od centrální vlnové délky laseru [100, 112].



Obr. 7.14: Stokesův a Anti-Stokesův rozptyl. Grafy převzaty z článku [100].

Výkon Ramanova šumu vyvolaného jedním klasickým kanálem v dopředném směru (\rightarrow) je možné spočítat jako [112]:

$$P_{\overrightarrow{SR\dot{S}}} = P_{výstup} \cdot \rho(\lambda) \cdot L \cdot \Delta\lambda \quad (7.17)$$

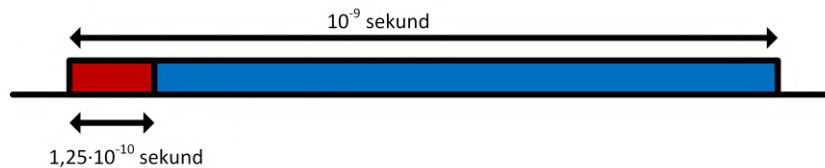
Výkon ve zpětném směru (\leftarrow) bývá obecně vyšší a vypočte se pomocí vzorce níže. Detailní postup pro výpočet výkonu škodlivého Ramanova šumu s příkladem je uveden v příloze B [112]:

$$P_{\overleftarrow{SR\dot{S}}} = P_{výstup} \cdot \rho(\lambda) \cdot \frac{\sinh(L\alpha)}{\alpha} \cdot \Delta\lambda \quad (7.18)$$

- $P = [mW]$ – Výstupní výkon laseru
- $L = [m]$ – Délka kanálu
- $\rho(\lambda) = [-]$ – Koeficient SRS (určen z grafu 7.14)
- $\Delta\lambda = [nm]$ – Šířka pásma
- $\alpha = [km^{-1}]$ – Měrný útlum

Minimalizace vlivu Ramanova rozptylu

1. **Snížení výkonu** – SRS se zvětšuje lineárně se vstupním výkonem klasických kanálů. Do jisté míry jej tak lze omezit snížením vysílacího výkonu těchto kanálů na minimum. Klasické kanály je možné následně zesílit pomocí EDFA zesilovače. Tyto zesilovače ovšem vytvářejí ASE šum, jak bylo popsáno v kapitole výše [113].
2. **Časová filtrace** – Jednofotonový detektor (APD) provádí časovou filtraci Ramanova rozptylu tak, že vždy přijme pouze takový foton, který dorazí v určitém časovém okamžiku (APD je aktivní pouze v určitém intervalu, v jiných okamžicích fotony nedetekuje – self-differencing mode) [114].



Obr. 7.15: Příklad časové filtrace.

Např. systém je taktován na rychlost generování klíče 1 GHz. Má tedy periodu 10^{-9} sekund. APD je aktivní vždy po dobu 125 ps, což odpovídá 12,5 % času. Tímto způsobem tak bude vyřazeno 87,5 % Ramanova šumu.

$$x = \frac{1,25 \cdot 10^{-10} \cdot 100}{10^{-9}} = 12,5\% \implies 100 - 12,5 = 87,5\%$$

3. **Rozmístění kanálů** – Anti-Stokesův rozptyl je většinou slabší než Stokesův. Vzniká tedy méně fotonů s kratší vlnovou délkou než s delší. Z tohoto důvodu by kvantový kanál měl být umístěn na kanále s vyšší vlnovou délkou než klasické kanály. Bude zde méně rušen. Stokesův rozptyl tak již nemusí být dále uvažován [87].
4. **Spektrální filtrace** – Filtrace spektra pomocí optických TFF (Thin film filter). Tyto filtry mohou být součástí multiplexorů, OADM (Optical add-drop multiplexer), ROADM (Reconfigurable OADM) a podobných zařízení [114].

7.4.3 Brillouinův rozptyl

Tento typ rozptylu opět vzniká interakcí světla s materiálem vlákna. V tomto případě je podstatná změna indexu lomu materiálu vlivem deformace optického vlákna (tah, tlak, krut, ...) akustickými vibracemi. Vlivem deformace se změní síly působící mezi jednotlivými atomy daného materiálu, což se projeví na změně energetických hladin. To způsobí rozptyl fotonů (změní se podmínky pro emisi a následnou absorpci světla). Výsledkem této interakce je změna frekvence části fotonů v určitém směru [100, 109, 115].

Šíří-li se intenzivní svazek světla (např. z laseru) optickým vláknem, mohou změny vnějšího elektrického pole, ve kterém se bude optické vlákno nacházet, indukovat v materiálu vlákna akustické vibrace. Ty se projeví jako tzv. elektrostrikce (tj. změna objemu vlivem vnějšího elektrického pole). Ve světelném svazku se tak může objevit Brillouinův rozptyl. Fotony rozptýleného světla mají přitom větší opačný směr pohybu ve srovnání se směrem pohybu původního světelného svazku [100, 109, 115].

Brillouinův rozptyl je zvláště významný pro signály s úzkou šířkou čáry, a proto je tento jev možné účinně potlačit snížením koherentní délky signálu neboli rozšířením jeho spektra. U rozptýleného světla zde dochází k posunu o cca 10 GHz (šířka WDM kanálu je 25, 50 nebo 100 GHz). V případě dostatečného odstupu od klasických kanálů by tak tento šum neměl do kvantového kanálu zasahovat [100, 109, 115].

8 Topologie a standardizace

Jelikož jsou praktické systémy QKD relativně novou záležitostí, zdaleka ne všechny aspekty jsou aktuálně standardizované. V posledních letech ovšem snahy o normalizaci stoupají. Mezi nejdůležitější organizace v oblasti patří:

- **ITU-T** (International Telecommunication Union Telecommunication Standardization Sector) – Jedná se o část ITU (mezinárodní agentura OSN) pro telekomunikační standardizaci. Agentura byla založena v roce 1865 v Paříži jako součást ITU. Aktuálně sídlí v Ženevě [116].
- **ETSI** (European Telecommunications Standards Institute) – Nezávislá nezisková organizace se sídlem ve Francii, odpovědná za standardizaci telekomunikačních a informačních technologií v Evropě. Reálně má ovšem organizace celosvětový dosah [117].
- **IEEE** (Institute of Electrical and Electronics Engineers) – Mezinárodní nezisková organizace se sídlem v New Jersey. Jejím cílem je podpora rozvoje v oblastech elektrotechniky, informatiky a telekomunikací [118].
- **ISO / IEC** (International Organization for Standardization / International Electrotechnical Commission) – Jedná se o dvě samostatné, avšak úzce spolupracující organizace. Obě sídlí ve švýcarské Ženevě a mají celosvětový dosah. V oblasti QKD vydávají doporučení společně [119] [120].

Z hlediska topologie QKD systémů patří mezi nejdůležitější standardizovaná rozhraní ETSI v tabulce 8.1 a standardy ITU-T uvedené v tabulce 8.2 níže. Z těchto norem vychází celá kapitola 8.1. Kompletní seznam aktuálně platných norem (respektive jejich návrhů) všech čtyř organizací je obsažen v příloze C.

Tab. 8.1: Nejdůležitější ETSI rozhraní pro prvky QKDN [117].

| | |
|---|--------|
| ETSI GS QKD 014 | 2/2019 |
| Rozhraní (REST API) pro doručování klíčů kryptografické aplikaci. | |
| ETSI GS QKD 015 | 4/2022 |
| Rozhraní pro řízení QKD pomocí SDN. | |
| ETSI GS QKD 018 | 4/2022 |
| Rozhraní pro orchestraci pomocí SDN. | |
| ETSI GS QKD 020 | návrh |
| Rozhraní (REST API) pro interoperabilitu na úrovni správy klíčů. | |

Tab. 8.2: Nejdůležitější ITU-T standardy definující architekturu QKDN [116].

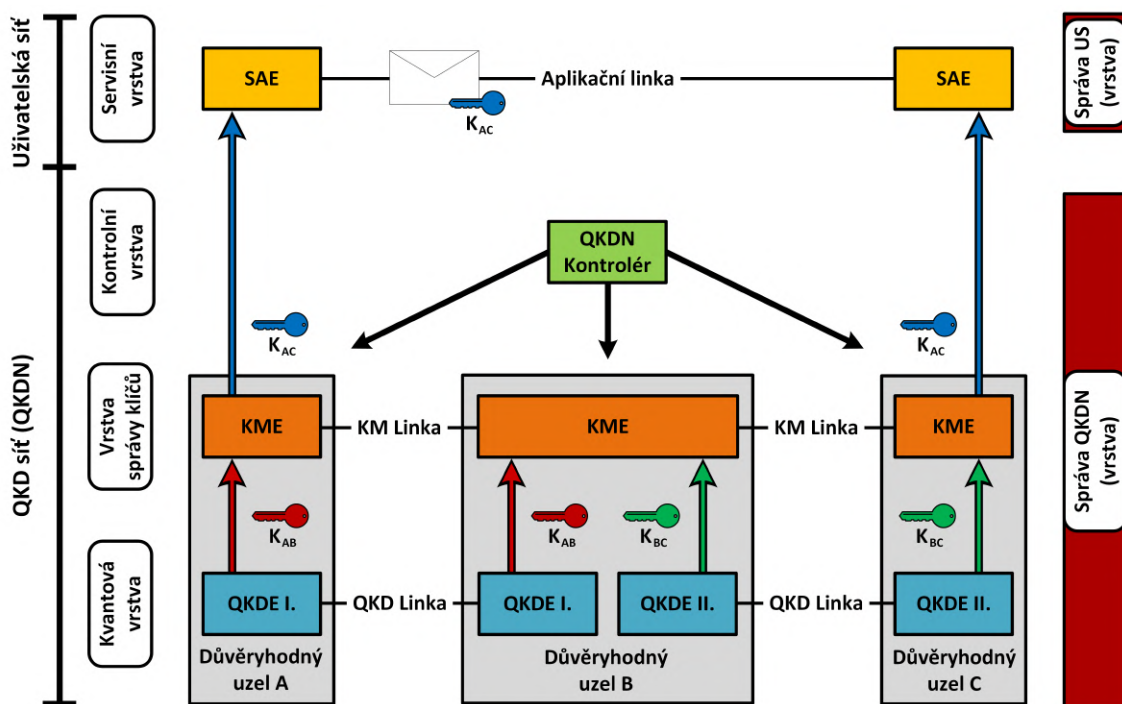
| | |
|---|---------|
| ITU-T Y.3800 | 10/2019 |
| Přehled problematiky a referenční model QKD sítí. | |
| ITU-T Y.3802 | 12/2020 |
| Funkční architektura jednotlivých prvků QKDN, zejména QKD modulu. | |
| ITU-T Y.3803 | 12/2020 |
| Systém pro správu klíčů. | |
| ITU-T Y.3804 | 9/2020 |
| Kontrola a správa. | |
| ITU-T Y.3805 | 12/2021 |
| Kontrola pomocí SDN. | |
| ITU-T Y.3810 | 9/2022 |
| Interoperabilita mezi QKD sítěmi. | |

8.1 Referenční model

Jak je patrné z nákresu 8.1 celá topologie je rozdělena do dvou samostatných sítí. Pod uživatelskou sítí je možné si představit libovolnou komunikační síť, která funguje jako konzument šifrovacích klíčů a z hlediska celkové topologie tvoří jedinou – servisní vrstvu. QKD síť (QKDN) zde naopak plní funkci dodavatelského subsystému a její struktura se skládá ze tří samostatných vrstev. Ty jsou podrobněji popsány níže. Nejdříve je ovšem nutné definovat následující pojmy, jejichž název se v jednotlivých standardech mírně odlišuje.

Základní pojmy

- **Důvěryhodný uzel** – Trusted Node (TN) – Samostatné zařízení, tvořící základ QKDN. Obsahuje QKDE, KME a případně i QKDN/SDN kontrolér. Jeho název je odvozen od faktu, že kromě „kvantových“ komponent obsahuje uzel i části „klasické“. Zde již není klíč uchovávan v kvantové podobě a je na něj již možné útočit. Samotnému uzlu je tak nutné důvěřovat a umístit jej do bezpečné oblasti. TN může ve složitější topologii zastávat různé funkce. Například může sloužit jako tzv. důvěryhodný opakovač nebo hraniční uzel. V praxi se lze rovněž setkat s pojmem QKD server.
- **Bezpečná oblast** – Oblast, do které nemá útočník přímý vstup, a ve které tak nemůže dojít ke zneužití QKD zařízení (chráněná budova, laboratoř atd.). Zde by se měla nacházet většina QKDN zařízení a konzumentských kryptografických aplikací. Výjimkou mohou být zařízení QKD linky.



Obr. 8.1: Základní referenční model tak, jak byl popsán ve standardu ITU-T Y.3800.

Entity QKD systému

- **Entita bezpečnostní aplikace** – Secure application entity (SAE) – Samostatné šifrovací zařízení obsahující kryptografickou aplikaci. Slouží jako konzument klíčů dodávaných QKDN.
- **QKDN/SDN kontrolér** – Entita obsahující funkce, pomocí kterých je celá QKDN řízena. Jedná se například o směrování mezi uzly, přeposílání klíčů, správa QKD a KM linek, zajištění kvality služeb (QoS – Quality of service) atd. V komplexnějších sítích lze používat dohromady s technologií SDN (Software-defined networking).
- **Entita pro správu klíčů** – Key management entity (KME) – „Nekvantová“ entita sloužící k ukládání a transformaci vygenerovaných klíčů a jejich následné dodávce SAE. Pod KME si lze rovněž představit logickou část uzlu, pomocí které je možné budovat složitější topologie QKDN jako například kruh či hvězda.
- **Entita pro kvantovou distribuci klíčů** – Quantum key distribution entity (QKDE) – Část zařízení zodpovědná za fyzické ustanovení společného klíče. Součástí je mimo jiné i kvantový generátor.
- **Správa QKDN a uživatelské sítě** – Entity zodpovědné za monitorování a komplexní správu (konfigurace, bezpečnost, výkon atd.) obou sítí.

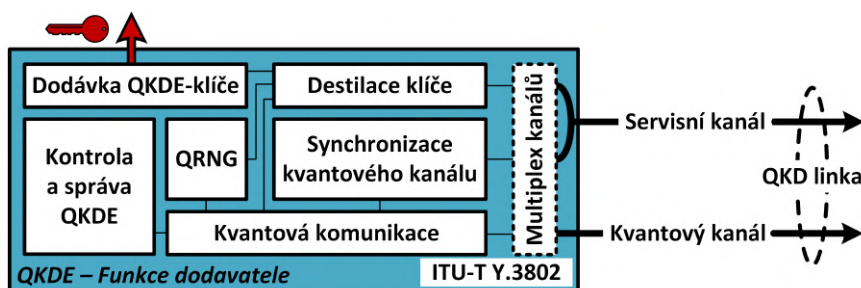
Funkce QKDN zařízení

- **Koncový uzel** – Základní prvek QKDN topologie. Zařízení je umístěno v blízkosti konzumenta, kterému pomocí standardizovaného rozhraní dodává vygenerované klíče. Linka mezi uzlem a kryptografickou aplikací má již nižší stupeň bezpečnosti a je tak nutné aby se obě zařízení nacházela v bezpečné oblasti.
- **Důvěryhodný opakovač** – Trusted repeater (TR) – Jedná se o zařízení, které se nachází mezi dvěma nebo více koncovými uzly a jeho úkolem je zejména prodloužení dosahu QKD systému. V současnosti nejsou dostupné kvantové paměti a kvantový signál tak nelze replikovat již na kvantové vrstvě při samotném přenosu klíče. Proto je distribuce klíčů na delší vzdálenosti zajišťována pomocí správy klíčů, avšak již v klasické podobě. Z tohoto důvodu se TR musejí nacházet v bezpečné oblasti stejně jako koncové body.
- **Hraniční uzel** – Různé segmenty QKDN mohou spadat pod různé operátory nebo mohou používat zařízení od různých výrobců. Tyto uzly se tak nacházejí na hranici segmentu a zprostředkovávají vzájemnou komunikaci (konverzi protokolů) na úrovni vrstvy správy klíčů a kontrolérů (případně i vrstvy správy QKDN). Jsou popsány dvě možnosti:
 - **Brána** – Gateway node (GWN) – Funkci brány zajišťují dva samostatné uzly, z nichž se každý nachází v jiném segmentu sítě. Zprostředkovávající funkce pracují na kontrolní vrstvě a vrstvě správy klíčů. Dále je mezi oběma branami funkční QKD linka.
 - **Propojovací uzel** – Interworking node (IWN) – Jedná se o jediný uzel, který sdružuje funkce obou bran. Jelikož se rozhraní obou segmentů nacházejí v jednom zařízení, QKD linka se zde nevyskytuje. Na rozdíl od GWN prochází propojovacím uzlem i linka pro správu QKDN.
- **Zařízení QKD linky** – Jedná se o zařízení, na úrovni kvantové vrstvy, která se nacházejí na QKD lince mezi dvěma důvěryhodnými uzly.
 - **Kvantové relé** – Zařízení, které pracuje na kvantové lince a nemusí být důvěryhodné (může být pod kontrolou útočníka). Používá se zejména jako středový uzel u protokolů jako E91, MDI-QKD nebo TF-QKD. Většinou slouží jako zdroj nebo detektor provázaných částic.
 - **Optický přepínač / switch** – Umožňuje přepínat nebo rozdělovat provoz kvantového nebo klasického kanálu mezi dvojicemi QKD modulů ve vícebodových sítích. Je tak možné různým uživatelům vystavit na vyžádání klíč.

8.1.1 QKD modul (QKDE)

Základní část celého zařízení zodpovědná za samotnou výměnu klíče. Implementuje konkrétní QKD protokoly a podle nich se také topologie může lišit. V případě PM protokolů se jedná o dvojici zdroj – detektor. V případě EB protokolů se využívá navíc i centrální prvek – kvantové relé. V závislosti na protokolu může obsahovat zdroj provázaných částic nebo sloužit jako měřicí zařízení. Koncové QKD moduly pak obsahují opačnou komponentu. Funkce QKDE modulu jsou následující:

- **Kvantová komunikace** – Přípravuje, přenáší a měří kvantové signály. Může se jednat jak o vysílače, tak o přijímače.
- **Synchronizace kvantového kanálu** – Zajišťuje synchronizaci hodin a časování pro kvantový kanál. Důležitá je vysoká přesnost pro správnou identifikaci přenášeného kvantového signálu při měření.
- **Destilace klíče** – Obsahuje funkce destilace (popsány v předchozích kapitolách). Tedy: prosévání, odhad chybovosti, opravu chyb a zesílení bezpečnosti.
- **Dodávka QKDE-klíče** – Přijímá požadavky na klíče QKD od agenta pro správu klíčů (část KME).
- **Kontrola a správa QKDE** – Funkce zodpovědná za celkovou správu a kontrolu QKDE modulu. Komunikuje s entitami v dalších vrstvách jako je KME, QKDN kontrolér a správa QKDN.
- **QRNG** – Generuje náhodná čísla a poskytuje je dalším funkcím. RNG by měl být nedeterministický např. QRNG.
- **Multiplexování kanálů** – Volitelná funkce umožňující multiplexování kvantových a klasických kanálů pomocí WDM.



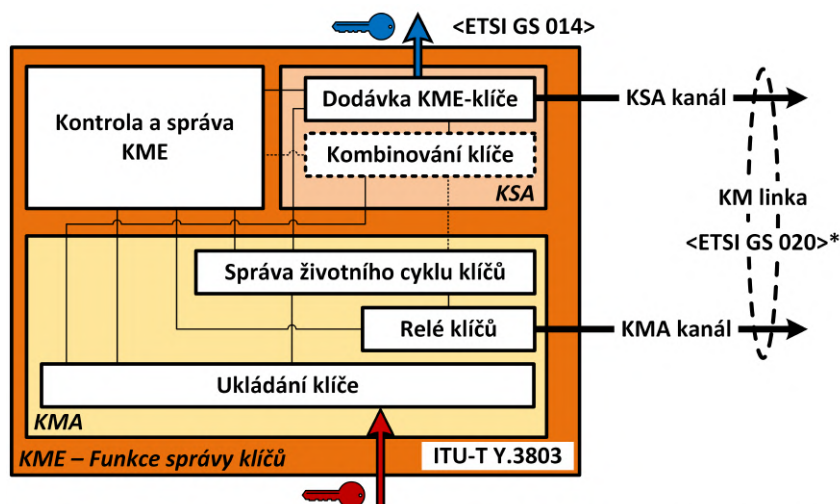
Obr. 8.2: Funkce QKD modulu tak, jak byly popsány ve standardu ITU-T Y.3802.

Na rozdíl od KMS nebo kontrolérů se zatím nevyskytují snahy o standardizaci jednotlivých QKD protokolů. Z tohoto důvodu je tak vždy nutné používat na obou stranách zařízení od stejného výrobce.

8.1.2 Systém pro správu klíčů (KME)

KME (případně též KM nebo KMS) je entita přijímající klíče od QKDE. Ty následně formátuje, přeposílá mezi uzly a dodává kryptografické aplikaci. KME se dělí na:

- **Agent pro správu klíčů** – Key management agent (KMA) – „Spodní část“ KME. Získává klíče od QKDE a propojuje uzly pomocí relé klíčů.
 - **Ukládání klíče** – Přijímá klíče od QKDE. Následně je synchronizuje, autentizuje a upravuje jejich velikost. Nakonec je uloží do paměti. Každému klíči dále přiřadí metadata, zejména pak identifikátor.
 - **Relé klíčů** – Pomocí Vernamovy šifry (OTP – One-time pad) bezpečně přeposílá klíče mezi jednotlivými důvěryhodnými uzly.
 - **Správa životního cyklu klíčů** – Stará se o životní cyklus klíčů od příjmu až po jejich dodávku spotřebitelské kryptografické aplikaci. Dále rozhoduje o vymazání nebo zachování klíčů v úložišti na základě politik.
- **Agent pro doručování klíčů** – Key supply agent (KSA) – „Horní část“ KME. Pracuje jako dodavatel klíčů pro SAE. V případě, že se nejedná o koncový uzel nemusí být přítomna.
 - **Kombinování klíče** – Volitelná funkce, která kombinuje klíče vytvořené pomocí QKD s jinými metodami výměny klíčů (např. PQC).
 - **Dodávka KME-klíče** – Synchronizuje a ověřuje klíče sdílené mezi koncovými uzly. Na vyžádání je dodává kryptografické aplikaci.
- **Kontrola a správa KME** – Funkce zodpovědná za celkovou správu a kontrolu KME modulu. Komunikuje s entitami v dalších vrstvách jako je QKDE, QKDN kontrolér a správa QKDN.



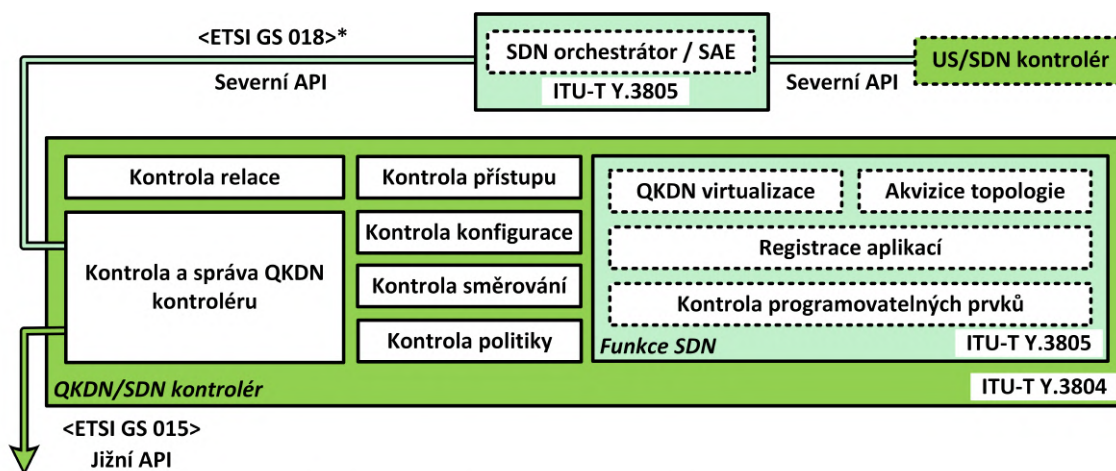
* rozhraní ETSI GS 020 se použije v případě, že jsou sousední KME od různých výrobců

Obr. 8.3: Funkce KMS tak, jak byly popsány ve standardu ITU-T Y.3803.

8.1.3 QKDN/SDN kontrolér

Na rozdíl od předchozích entit QKDN kontrolér nepracuje přímo s klíči. Jeho úkolem je zajistit stabilní, bezpečnou a efektivní funkci všech prvků systému. Kontrolér komunikuje s QKDE, KME a správou QKDN. Provádí následující funkce:

- **Kontrola relace** – Řídí postup přeposílání klíčů v rámci KMA a dodávku klíčů pro různé kryptografické aplikace pro KSA.
- **Kontrola přístupu** – Autentizuje funkční prvky pod kontrolou QKDN kontroléru a omezuje jejich přístup (autorizace) na základě přístupových práv.
- **Kontrola konfigurace** – Shromažďuje konfigurační informace a stav o QKDE, KME a jejich linkách. Upravuje konfigurace linek v případě poruchy apod.
- **Kontrola směrování** – Zajišťuje vhodnou trasu pro přeposílání klíčů mezi KME dvou koncových uzlů. Rovněž řídí přesměrovávání klíčů v závislosti na poruše, výkonu nebo stavu nižších vrstev.
- **Kontrola politiky** – Řídí prostředky QKDN na základě kvality služeb (QoS) a zpoplatnění kryptografických aplikací.
- **Kontrola a správa QKDN kontroléru** – Funkce zodpovědná za celkovou správu a kontrolu QKDN kontroléru. Komunikuje s entitami v dalších vrstvách jako je QKDE, KME a správa QKDN.



* rozhraní ETSI GS 018 se použije jako severní API pouze v případě použití orchestrátoru

Obr. 8.4: Funkce QKDN kontroléru, SDN modulu a SDN orchestrátoru tak, jak byly popsány ve standardech ITU-T Y.3804 a ITU-T Y.3805.

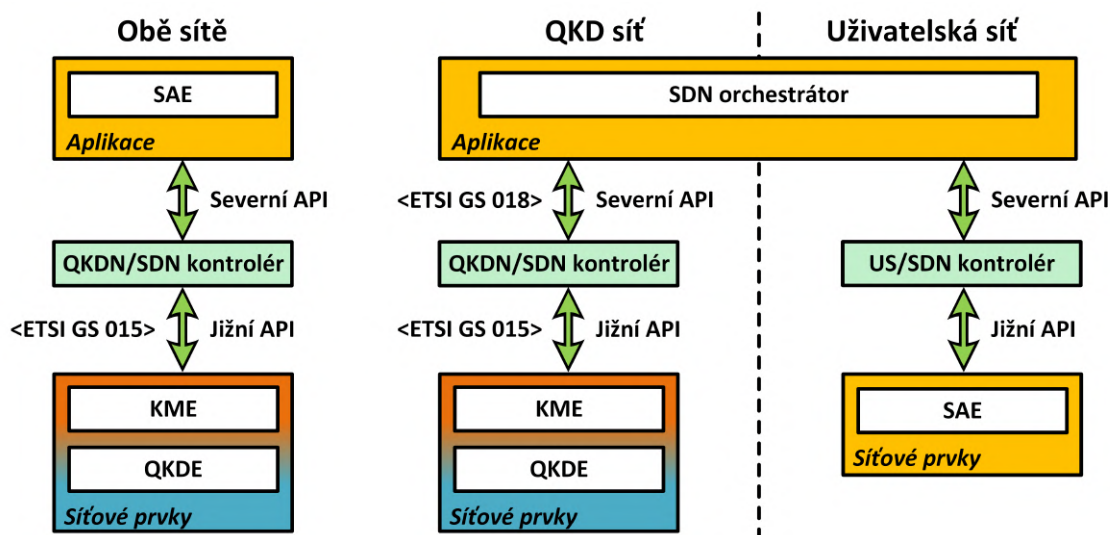
Způsobů implementace existuje několik. Kontrolér může být distribuovaný (nachází se v každém uzlu) nebo centralizovaný (je pouze jeden pro všechny uzly v segmentu). V některých případech se místo QKDN kontrolérů používá technologie SDN. Ta nabízí centralizovanou a jednodušší správu.

8.1.4 Softwarově definované sítě (SDN)

SDN je architektura počítačových sítí, jejímž základem je oddělení správy sítě od datového přenosu. Zatímco v tradičních sítích jsou řídicí funkce jako směrování a přepínání přímo uloženy do síťových prvků, v SDN jsou tyto funkce vyděleny do samostatné vrstvy. Celá topologie je pak řízena jedním centrálním kontrolérem [122].

Kromě kontroléru a síťových prvků se v SDN architektuře vyskytuje ještě třetí vrstva – aplikace. Jedná se o programy, které kontroléru přímo sdělují své požadavky na síť. Komunikace v SDN systému probíhá (zejména) vertikálně pomocí dvou typů rozhraní [122].

- **Severní rozhraní** – Northbound API – Slouží pro komunikaci mezi SDN kontrolérem a aplikacemi.
- **Jižní rozhraní** – Southbound API – Slouží ke komunikaci mezi SDN kontrolérem a síťovými prvky.



Obr. 8.5: Základní princip SDN systému [117] [122].

Již na první pohled je zřejmé, že se myšlenka SDN v mnohém podobá architektuře QKDN. Zejména v případě komplexnějších QKD sítí může být výhodné sloučit řízení celé sítě do jednoho SDN kontroléru. Ten kromě všech funkcí standardního QKDN kontroléru disponuje ještě dalšími pokročilejšími funkcemi navíc. Jejich popis je však nad rámec tohoto textu [122].

V případě použití SDN v kombinaci s QKD systémy se mezi nastavitelné síťové prvky počítají KME, QKDE a zařízení QKD linky. Mezi aplikace se naopak řadí kryptografické aplikace – SAE. Tato jednodušší varianta systému se nachází v levé části obrázku 8.5 [117].

Kromě QKDN však může SDN používat i uživatelská síť. V takovém případě disponuje vlastním kontrolérem a je nutné zajistit, aby spolu oba kontroléry spolupracovaly. K tomuto účelu slouží tzv. SDN orchestrátor, který je z pohledu obou sítí považován za aplikaci [117].

8.2 Reálné zapojení

Na základě výše popsaných prvků a jejich funkcí je v následující kapitole uveden příklad komplexnějšího QKD systému. Nejdříve je ovšem nutné vysvětlit pojem Postkvantová kryptografie (PQC) a vymezit její vztah ke QKD. Srovnání se nachází v tabulce 8.3.

8.2.1 Postkvantová kryptografie

Zatímco QKD je bezpodmínečně bezpečná technologie založená na principech kvantové mechaniky, pod pojmem PQC je možné si představit „standardní“ kryptografii, která je ovšem založena na matematických problémech, které kvantový počítač nedokáže vyřešit. Příkladem mohou být algoritmy založené na mřížkách, kde se vyskytují problémy jako je nalezení nejkratšího (NTRU) / nejbližšího (GGH) vektoru. Alternativou jsou rovněž tzv. Goppovy kódy (McEliece) a mnoho dalších přístupů [123].

Tab. 8.3: Srovnání PQC a QKD [123].

| Postkvantová kryptografie (PQC) | Kvantová kryptografie (QKD) |
|--------------------------------------|----------------------------------|
| Založeno na matematických problémech | Založeno na kvantové mechanice |
| Výpočetní bezpečnost | Bezpodmínečná bezpečnost |
| Krátkodobé řešení | Dlouhodobé řešení |
| Softwarová implementace | Hardwarová implementace |
| Levné a snadné implementovat | Nákladné a náročné implementovat |
| Přístupové sítě (last-mile) | Páteřní sítě (backbone) |

Ačkoliv se u PQC algoritmů očekává odolnost proti útokům kvantového počítače, na rozdíl od QKD to není možné 100% dokázat. Nespornou výhodou PQC oproti QKD je však snadná a levná implementace, jelikož algoritmy nevyžadují dedikovaný hardware [123].

V praxi se tak nabízí používat QKD pouze pro nejdůležitější páteřní linky, kterým zajistí dlouhodobou ochranu s vyšší úrovní bezpečnosti. V přístupových sítích je naopak vhodnou volbou PQC, z důvodů snazší implementace (například u bezdrátových zařízení) [123].

8.2.2 Příklad kvantově chráněné sítě

Obsah této kapitoly vychází ze zapojení 8.6 a jeho cílem je popsat příklad reálné sítě chráněné pomocí kvantových a postkvantových technologií. Ke každému vyskytujícímu se prvku a rozhraní je uveden příslušný standard.

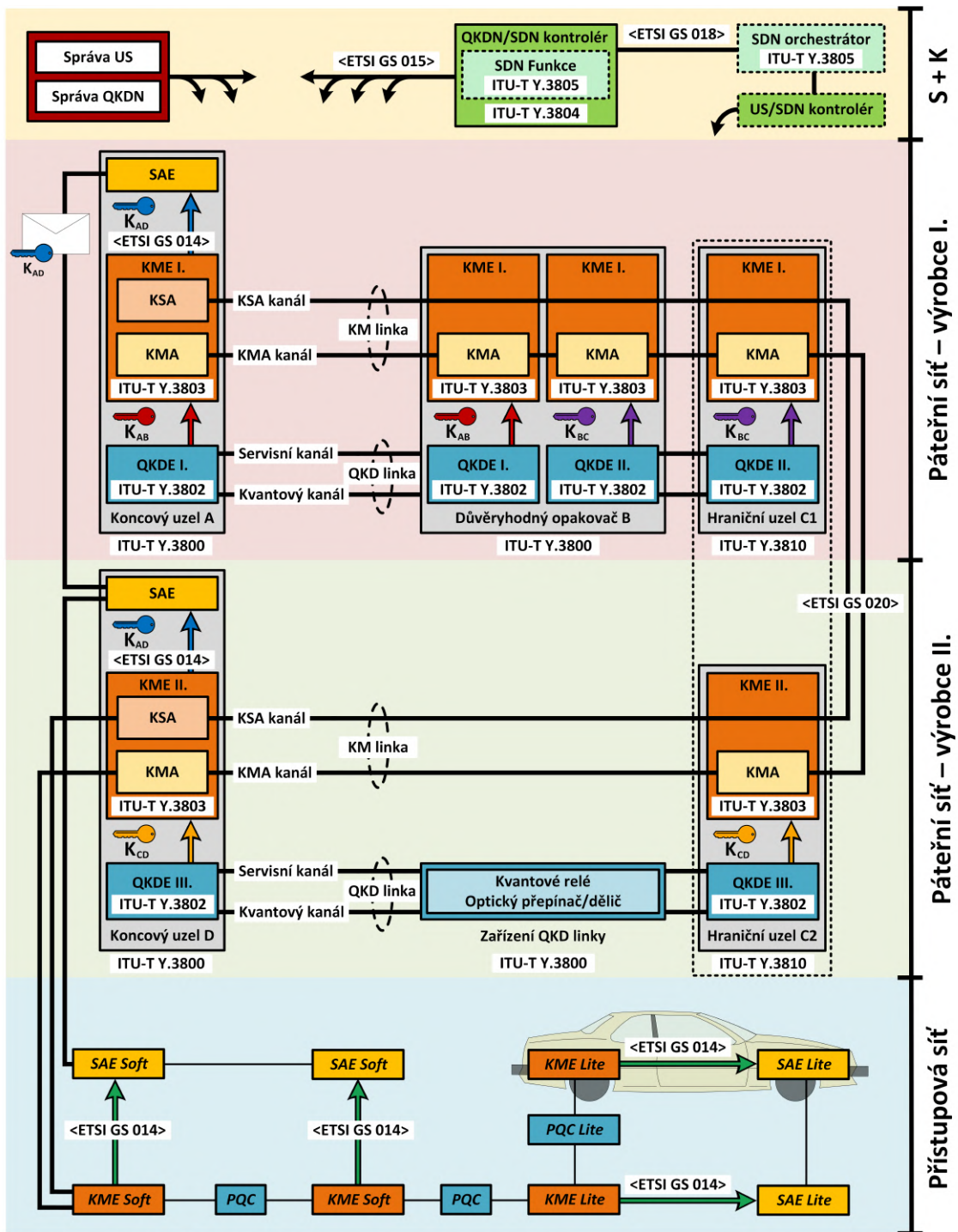
Popisovaná síť se skládá ze tří hlavních segmentů. Základem je páteřní síť, jejíž různé části ovšem patří dvěma různým operátorům (červená, zelená). Z nich každý používá zařízení od jiného výrobce QKD. Na páteřní síť je dále připojena síť přístupová (modrá), která je chráněna pomocí PQC. Vrstvy správy a kontroly jsou vyznačeny pouze zjednodušeně a pro přehlednost umístěny zvlášť (žlutá). Z pohledu uživatelské sítě se jedná o přímou páteřní linku propojující kryptografické aplikace dvou různých operátorů. Na ni dále navazuje síť přístupová. Z pohledu QKD subsystému je již situace složitější. QKDN se skládá z celkem pěti zařízení z nichž čtyři z nich jsou důvěryhodné uzly (A, B, C, D). V závislosti na výrobcu využívá dvou různých KMS a může implementovat až tři odlišné QKD protokoly.

Uzly A a D jsou klasické koncové uzly, které oproti ostatním obsahují i KSA. To je odpovědné za poskytování klíčů SAE pomocí rozhraní ETSI GS 014. K uzlu D je dále napojena přístupová síť. V případě uzlu B se jedná o důvěryhodný opakovač, který obsahuje dvě na sobě nezávislá QKD rozhraní (protokol se může lišit). Pomocí OTP přešlává klíče z uzlu A uzlu C a prodlužuje tak dosah linky. Na hranici obou systémů se nachází propojovací uzel (IWN). V tomto příkladu jsou jeho části (C1 a C2) nejen pod kontrolou odlišných operátorů, ale implementují i dva odlišné KM systémy. Oba KMS spolu komunikují skrze standardizované rozhraní ETSI GS 020, kterým si vzájemně předávají klíče. Kvantový spoj mezi uzly C a D obsahuje navíc zařízení QKD linky. To může sloužit buď jako centrální bod u některých QKD protokolů, nebo k přepínání QKD linky mezi uzly.

Samotná přístupová síť není žádným způsobem standardizována. Pouze vychází z návrhu IDQ a řešení Phio TX od firmy Quantum Xchange. Mezi komponentami KME Soft dochází k distribuci klíče pomocí postkvantové kryptografie. Podobně jako v případě QKDN je klíč následně předán přes rozhraní ETSI GS 014 kryptografické aplikaci – SAE Soft. Obě komponenty se mohou nacházet v jednom zařízení nebo tvořit dvě oddělené sítě podobně jako v případě QKD. Pro méně výkonné aplikace může existovat i odlehčená varianta (Lite).

Kontrolní vrstva a vrstva správy jsou vyznačeny pouze zjednodušeně a jejich linky směrem ke QKDN a uživatelské síti jsou ve schématu pouze naznačeny. Rovněž je pravděpodobné, že by každý segment sítě (operátor) měl vlastní kontrolér. Linky správy směřují ke všem prvkům (SAE, kontrolér, KME a QKDE) v nákresu. Rozhraní ETSI GS 015 se používá jako jižní rozhraní pouze v případě použití SDN kontroléru a vede ke všem prvkům v QKDN. Uživatelská síť (SAE) má svůj vlastní

kontrolér. Oba SDN kontroléry spolu komunikují prostřednictvím orchestrátoru. Spoj mezi QKDN/SDN kontrolérem a orchestrátorem implementuje severní rozhraní ETSI GS 018.



* Správa a kontrola – zjednodušeno

Obr. 8.6: Příklad QKD sítě. Kontrolní a správní vrstva jsou zjednodušeny.

9 Zařízení Clavis³

Clavis³ je systém pro kvantovou distribuci klíčů od švýcarské společnosti ID Quantique (IDQ). Jedná se o základní výzkumnou platformu s krátkým dosahem disponující třístavovou i čtyřstavovou verzí protokolu COW. Výhodou je zejména možnost sledovat a upravovat základní parametry QKD systému pomocí nástrojů příkazové řádky.

9.1 Popis systému

Základem topologie jsou dva QKD servery. Obě zařízení se však liší a mají rozdílný účel. Zatímco Alice slouží zejména jako vysílač kvantového signálu, Bob pulzy přijímá. Na obrázku 9.1 níže jsou vyznačeny nejdůležitější části obou zařízení. Rozhraní kvantového kanálu je osazeno optickým konektorem FC/APC (zelený). Pro správnou funkci zařízení je nutné, aby byl na kvantovém kanálu útlum minimálně 10 dB. Z tohoto důvodu může být nutné přidat hned za konektor útlumový článek. Podle výrobce maximální možný útlum na trase činí 14 dB. Měřením však bylo zjištěno, že jak vyšší tak výrazně nižší útlum na trase zpravidla ústí v nižší rychlost doručování klíčů. Systém však zůstává nadále funkční.



Obr. 9.1: Rozdíl mezi QKD servery Alicí a Bobem.

Pro připojení servisních kanálů poskytuje systém sloty pro SFP moduly. V tomto případě je pro duplexní komunikaci použita dvojice konektorů LC-UPC (modré). Tento kanál ovšem může teoreticky probíhat na libovolném médiu. Nemusí tak být pouze optický. Čím se Bob od Alice na první pohled liší je přítomnost portů pro zapojení vlastních datových a monitorovacích detektorů.

Zadní panel je u obou zařízení shodný a obsahuje ethernetový port pro KM linku a odesílání klíčů klientům (šifrátoru). Rovněž je přítomen port USB, jehož hlavní funkcí je přístup pro nahrávání bezpečnostních TLS certifikátů, pomocí nichž jsou tyto linky zabezpečeny.

9.2 Parametry systému

Vybrané parametry systému jsou uvedeny v tabulce 9.1 níže. Ačkoliv se nejedná o doporučené řešení, výzkumná verze navíc umožňuje některé parametry systému měnit. V této práci ovšem budou uvažovány pouze výchozí hodnoty parametrů. Mezi nejdůležitější patří zejména fotonové číslo.

Tab. 9.1: Známé parametry systému Clavis³.

| Známé parametry systému | | | |
|---------------------------|-----------|------------------------|---------|
| Výrobce | — | ID Quantique (IDQ) | |
| QKD protokol | — | Coherent one-way (COW) | |
| Rychlost generování pulzů | v_p | 1,25 GHz | |
| Rychlost doručování klíče | — | 1,4 kb/s | |
| Dynamický rozsah | — | 10–14 dB | |
| Fotonové číslo | μ | 0,03 | |
| Kvantový kanál | λ | 1551,72 nm | DWDM 32 |
| Servisní kanál I | — | 1553,33 nm | DWDM 30 |
| Servisní kanál II | — | 1554,13 nm | DWDM 29 |

Cílem této práce je navrhnout řešení, pomocí kterého by bylo možné sloučit kvantový kanál do jednoho vlákna s ostatními klasickými linkami. Z tohoto důvodu musí být znám výkon kvantového kanálu. Nejdříve je spočítána energie jednoho fotonu:

$$E_f = \frac{hc}{\lambda} = 1,28 \cdot 10^{-19} \text{ J} = 0,8 \text{ eV} \quad (9.1)$$

Následně je ještě pomocí rychlosti generování pulzů na straně Alice a fotonového čísla možné dopočítat celkový výkon na kvantovém kanále:

$$P_k = E_f v_p \mu = 4,8 \cdot 10^{-12} \text{ W} = -83,2 \text{ dBm} \quad (9.2)$$

Z výsledku je zřejmé, že se jedná o velmi nízký výkon, který vyžaduje speciální zacházení. V opačném případě by mohlo dojít k pohlcení kanálu šumem ostatních linek. Další problematickou možností je rušení kanálu nelineárními jevy. Zejména pak Ramanovým šumem. Z tohoto důvodu je nutné zvážit vhodné umístění kanálu a zajistit jeho dostatečnou filtraci.

Tab. 9.2: Vypočtené parametry systému Clavis³.

| Vypočtené parametry systému | | |
|-----------------------------|-------|-----------|
| Energie fotonu | E_f | 0,8 eV |
| Výkon kvantového kanálu | P_k | -83,2 dBm |

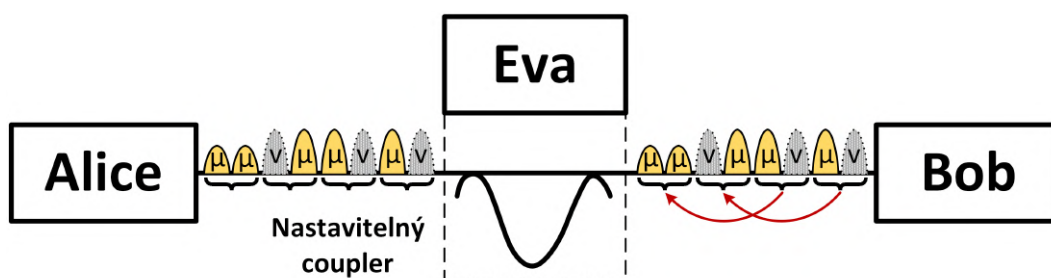
9.3 Eva

Kromě výše zmíněných QKD serverů je rovněž možné zapojit do kvantového kanálu simulátor útoku. Zařízení, respektive Eva neimplementuje žádný konkrétní útok. Jedná se spíše o simulátor útoku, jehož působení vyvolává v systému podobné účinky jako skutečný útok.



Obr. 9.2: Zařízení Eva sloužící k odposlechu na kvantovém kanále.

Princip spočívá v nastavitelném coupleru, který oddělí malou část pulzů a zpozdí je o fixní počet bitů. Na jedné straně je Eva vybavena otočným potenciometrem, který slouží k nastavení množství zpožděných pulzů. Se zvětšujícím se množstvím pulzů roste i QBER. Systém reaguje zvýšením komprese, což snižuje rychlost doručování klíčů. Kvantový kanál se k Evě připojuje pomocí FC/APC konektorů.



Obr. 9.3: Princip zařízení Eva.

9.4 Současná topologie systému

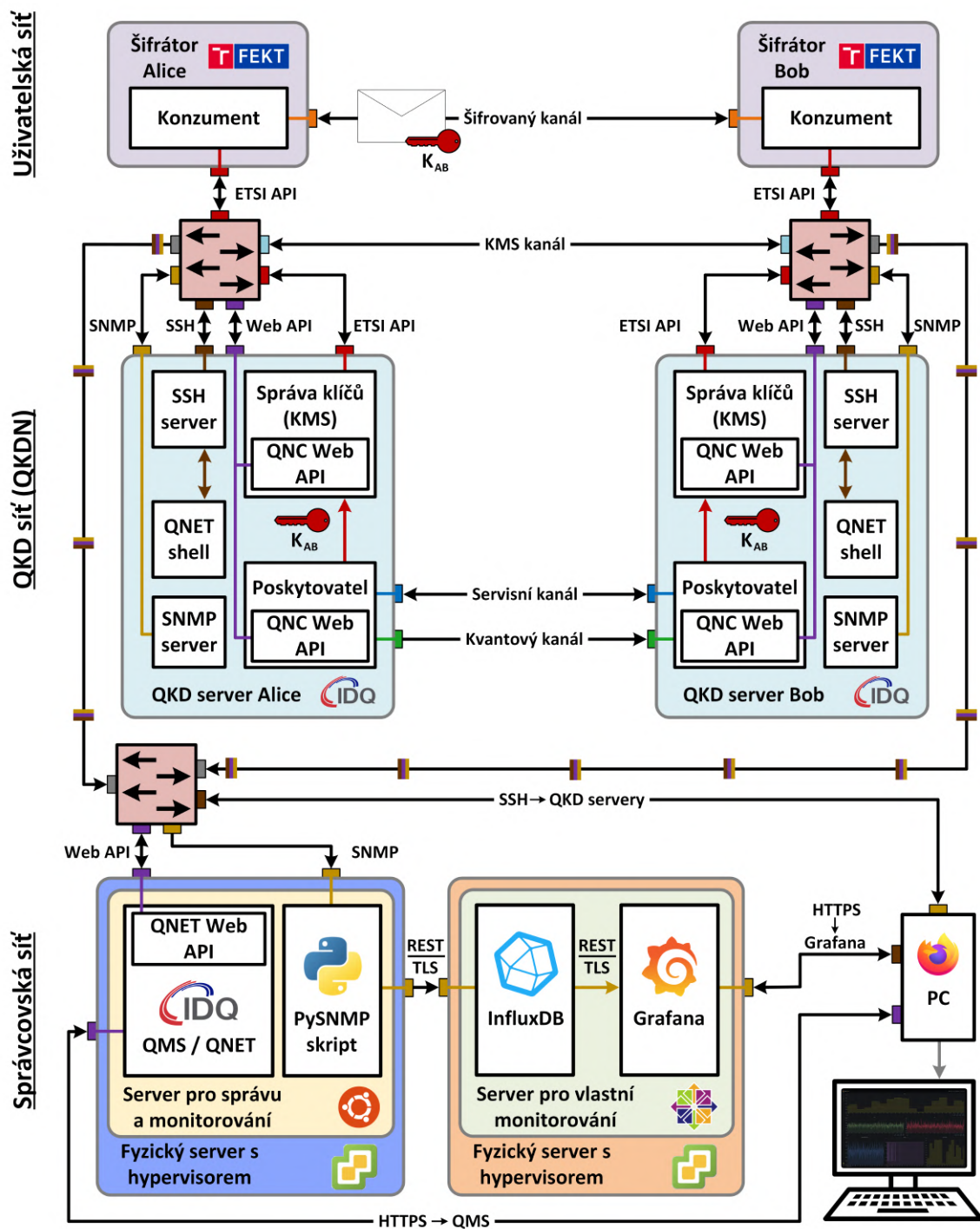
V současnosti se polygon pro kvantovou distribuci klíčů na VUT FEKT nachází ve stavu zachyceném na obrázku 9.4. Celý systém lze rozdělit do tří základních sítí, kde každá z nich plní odlišné úkony.

- **Uživatelská síť** – Jedná se o libovolnou síť, která od QKD systému odebírá na obou (všech) stranách vygenerované klíče. Ty následně použije k šifrování uživatelských dat.
- **QKD síť** – Mnohdy známá jako QKDN je samostatná síť obsahující kvantový, servisní a KMS kanál. Jejím hlavním úkolem je dodávat klíče uživatelské síti.
- **Správčovská síť** – Síť sloužící ke správě systému a monitorování parametrů QKD přenosu. Může využívat jak nástroje dodané výrobcem, tak vlastní řešení.

9.4.1 Prvky systému

Základem topologie jsou QKD servery Clavis³ pracující v rámci QKDN. Jejich účelem je generovat sdílené šifrovací klíče a dodávat je libovolnému konzumentovi. Topologie IDQ rozděluje QKDN na tři části:

- **Poskytovatel** – Část QKD serveru, která má na starost samotnou kvantovou výměnu klíčů. Implementuje konkrétní QKD protokol, který využívá servisního a kvantového kanálu. Odpovídá standardizované komponentě QKDE.
- **Systém správy klíčů / KMS** – Část QKD serveru, která je zodpovědná za udržování síťové topologie a distribuci klíčů ke konzumentovi, případně dalším uzlům. Pro komunikaci používá vlastní kanál na IP vrstvě. Odpovídá standardizované komponentě KME.
- **Konzument** – Libovolné šifrovací zařízení, které dostává od QKD serveru klíče. Ty potom použije pro šifrování v libovolné uživatelské síti. Odpovídá standardizované komponentě SAE.



Obr. 9.4: Současný stav logické topologie QKD polygonu.

9.4.2 Správa a monitorování

V případě zařízení Clavis³ nabízí výrobce tři nástroje pro monitorování a správu. Rozsah možností konfigurace a postup se u každého nástroje liší. Pro centralizovanou správu slouží QMS (Quantum management system), případně je možné jednotky částečně nastavit samostatně při připojení přes SSH pomocí QNET shell.

- **QMS** – Jedná se o nástroj pro centrální monitorování a správu QKDN. Je dodáván jako Docker kontejner, který běží na operačním systému Ubuntu LTS. Disponuje jak grafickým rozhraním, tak příkazovou řádkou. Vše se zasílá přes společné Web API (Application programming interface) přímo QKD serveru. Zmíněné API má dvě části. QNET Web API, které se nachází na QMS serveru a QNC Web API v každé KMS a QKD jednotce QKD serveru (QNC – Quantum node controller).
 - **WebUI QMS** – Grafické rozhraní, ve kterém je možné provádět konfiguraci celého QKD systému. Rovněž jej lze použít k základnímu monitorování parametrů.
 - **QNET tool** – Nástroj příkazové řádky, běžící na stroji se spuštěným QMS kontejnerem. Slouží k centralizované konfiguraci QKDN.
- **QNET shell** – Jedná se o textový shell, který není součástí QMS a běží přímo na QNC. Po připojení k danému QKD serveru pomocí SSH lze použít k některým nastavením. Nástroje QNET tool a QNET shell nepoužívají stejné příkazy.

9.4.3 Vlastní monitorování

Systém Clavis³ disponuje SYSLOG a SNMP servery. Momentálně je v provozu pouze SNMP server, který využívá třetí verzi daného protokolu. Vlastní skript v jazyce Python založený na PySNMP a spuštěný na serveru Ubuntu odesílá každou sekundu požadavek na Alici (lze přidat i Boba) na zaslání vybraných parametrů. O spuštění skriptu po spuštění počítače se stará služba SystemD. Data jsou pak odesílána do databáze InfluxDB pomocí rozhraní REST API a zabezpečení TLS. Webová aplikace Grafana slouží k zobrazení daných dat v grafu a k samotnému monitorování. InfluxDB i Grafana běží na jednom virtuálním počítači s operačním systémem CentOS Stream. Do webové aplikace (klienta), kterou poskytuje server Grafana, se lze přihlásit z libovolného webového prohlížeče. To je výhodné zejména z toho důvodu, že není nutné používat konkrétní operační systém. Rovněž je možné ke statistikám přistupovat z několika klientů současně.

9.5 Analýza bezpečnosti

Clavis³ je proprietární systém a není tak možné jednoduše získat informace o způsobu jakým fungují jeho nekvantové komponenty. Například jakým způsobem jsou klíče v KMS ukládány a následně zase bezpečně smazány. Tato kapitola se tak věnuje pouze přístupným a známým klasickým komponentám tohoto systému.

9.5.1 Klasické algoritmy v QKD systému

Ačkoliv kvantová kryptografie teoreticky nabízí bezpodmínečnou bezpečnost je nutné si uvědomit, že kromě samotného QKD protokolu disponuje praktický systém řadou klasických algoritmů, které mezi sebou komunikují po nechráněné síti. Jedná se zejména o destilační funkce jako autentizace (založeno na ISK a haš), proces opravy chyb (založeno na LDPC) a následné komprese (založeno na haš). Tyto funkce již disponují pouze výpočetní bezpečností.

Dále dochází k přeposílání klíčů na úrovni KMS. K tomuto účelu se nejčastěji používá OTP, které je v kombinaci s QKD již z podstaty neprolomitelné. To je nutné zejména z důvodu, že se klíč přeposílá i mimo bezpečnou zónu. Komunikace v rámci bezpečné zóny je však chráněna pouze na základě standardních TLS certifikátů. Jedná se zejména o dodávku klíčů z KM systému kryptografické aplikaci, nebo konfiguraci pomocí QNET tool. Rovněž přímá konfigurace zařízení probíhá pomocí protokolu SSH, většina jehož implementací aktuálně disponuje pouze současnými asymetrickými schémata.

9.5.2 Správa systému

Celý systém uzlu Clavis³ je založen na Linuxu. S operačním systémem však síťový administrátor přímo nekomunikuje. K dispozici má pouze QNET shell, ke kterému se lze připojit pomocí protokolu SSH, a který nabízí pouze velmi omezené množství příkazů. Pro podrobnější správu systému, včetně úpravy většiny parametrů přenosu, je nutné použít privilegovaný účet (idq). Tím však disponuje pouze výrobce, nikoli koncový uživatel (majitel) systému.

Celou síť je možné spravovat i centralizovaně pomocí QNET tool. Jedná se o nástroj, který s uzly komunikuje pomocí API založeného na architektuře REST. Možnou nevýhodou tohoto řešení je, že přihlašovací údaje uživatelů (jejich jména a otisky hesel) jsou uloženy v souboru `~/.qnet/default` a jsou tak v rámci prostředí uživatele volně přístupné. Struktura souboru se nachází na obrázku 9.5. Nástroj funguje tak, že při prvním spuštění je nakonfigurován odpovídající QNET tool uživatel, jehož přihlašovací údaje jsou uloženy právě do zmíněného souboru. Tento uživatel je následně vždy automaticky použit při komunikaci s QKD servery. Je tedy nutné

počítat s tím, že přístup k centrální konfiguraci celé QKDN stojí na zabezpečení daného linuxového uživatele.

```
idq@idq-virtual-machine:~/qnet$ cat default
{
  "ConfigWebApi": {
    "Url": "https://localhost:443",
    "AuthenticationScheme": "basic",
    "OAuthTokenServiceUrl": null,
    "Username": "Admin",
    "Password": "+os2TWkkgBrc4mHNxU4uKnRnCc9BYPH7ed6H43zxXHI="
  },
  "AdminWebApi": {
    "Port": 8443,
    "AuthenticationScheme": "basic",
    "Username": "kms",
    "Password": "tkiQuiMaWwcojdcQXSh0827sYTVHhMe+7MDP8BG7Ab8="
  },
  "IdentityServer": {
    "Url": null,
    "AuthenticationScheme": "basic",
    "OAuthTokenServiceUrl": null,
    "Username": null,
    "Password": null
  },
  "Staging": false,
  "OutputFormat": null,
  "Language": 0,
  "QncWebApis": [
    {
      "name": "QNCA",
      "uid": "4a739570de2848d89cd75432dd730a6c",
      "url": "https://192.168.10.102:8443/",
      "scheme": "basic",
      "username": "kms",
      "password": "vQxh6hY1kvnkFNV5cr2cudsjjm9jg3VW0IB0+tiG0c=",
      "lastSignIn": "2023-05-13T01:10:20.0436855Z"
    },
    {
      "name": "QNCB",
      "uid": "11ef6b184cd04648bc63c900993faf7c",
      "url": "https://192.168.10.107:8443/",
      "scheme": "basic",
      "username": "kms",
      "password": "gmCX0TLbDET670RQcBax9pka739jB4y4VRS0ereuFDg=",
      "lastSignIn": "2023-05-13T01:16:25.8412444Z"
    }
  ]
}
```

**Ručně
nakonfigurovaný
uživatel Admin**

**Předvytvořený
uživatel kms
(superadmin)**

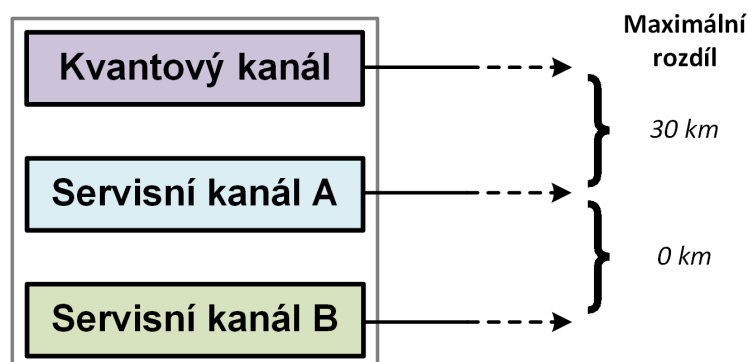
**Informace o QKD
serverech**

Obr. 9.5: Výpis souboru obsahující informace o uživateli a QKD serverech.

Obě zmíněné možnosti slouží výhradně ke konfiguraci zařízení a nenabízí přístup k uloženým klíčům v KM systému. Dokud tak nebude v těchto nástrojích nalezena softwarová zranitelnost, je možné tuto část systému považovat za bezpečnou.

9.5.3 Klasický kanál

Ačkoliv je teoreticky možné použít pro klasický kanál libovolné přenosové médium, aktuální stav systému dovoluje používat pouze optický přenos. Současně je nutné počítat s tím, že délka kvantového a servisního kanálu se může lišit maximálně o 30 km. Povolený rozdíl mezi oběma servisními kanály není výrobcem přesně specifikován, lišit by se však měl pouze minimálně. V ostatních případech může docházet k neočekávaným výpadkům komunikace. Klasický kanál rovněž nekomunikuje pomocí standardní sady protokolů a není jej tak možné snadno vést přes běžné IP síť.



Obr. 9.6: Maximální povolený rozdíl mezi jednotlivými kanály QKD systému.

Prakticky je servisní kanál řešen pomocí sady dvou SFP modulů, jejichž vybrané parametry jsou vypsány v tabulce 9.3. V rámci praktické části této práce byly používány dvě sady modulů od různých výrobců. SFP od Skylane jsou určeny pro komunikaci rychlostí 10 Gb/s. Zde byla ovšem použita rychlost nižší.

Tab. 9.3: Parametry SFP modulů Finisar a Skylane [121, 124].

| Vybrané parametry SFP | | |
|-------------------------|---------------|---------------|
| Výrobce | Finisar | Skylane |
| Model | FWLF1632xx | SPDTU080100D |
| Zdroj | | |
| Rychlost | 2,7 Gb/s | 2,7 Gb/s |
| Vlnová délka (CH29) | 1554,13 nm | 1554,13 nm |
| Vlnová délka (CH30) | 1553,33 nm | 1553,33 nm |
| Výstupní výkon (měřeno) | -1 až 1 dBm | -3 dBm |
| Detektor | | |
| Vstupní výkon | -28 až -9 dBm | -24 až -7 dBm |

Rozdílů v délce a vlastností použitých SFP je možné zneužít jak k dočasným, tak trvalým DoS útokům. Útočník může cílit jak na kvantový, tak servisní kanál. Na příklad:

- **Zarušení kanálu** – Útočník vysílá na kanál signál o vysokém výkonu, který zašumí užitečný signál, případně zasaturuje fotodetektor.
- **Poškození detektoru** – V případě, že vysílaný výkon přesáhne maximální možnou hranici, hrozí trvalé poškození detektoru.
- **Zatlumení kanálu** – S klesajícím výkonem se může zvyšovat chybovost servisního kanálu a ten se tak nezvládne synchronizovat. Podobným způsobem lze vyřadit i kanál kvantový.
- **Rozdíl v délce kanálů** – Útočník může jeden z kanálů přesměrovat na trasu o jiné délce a tím narušit komunikaci.

10 Měření na mezifakultní optické trase

První sada měření je věnována ověření odolnosti systému Clavis³ vůči změnám polarizace. Současně bude z hlediska výkonu srovnána třístavová a čtyřstavová verze COW protokolu. Veškerá měření budou prováděna na níže popsané mezifakultní optické trase.

10.1 Trasa FEKT–FIT v Brně

V době měření byla mezi VUT FEKT (Alice) a VUT FIT (Bob) zprovozněna optická trasa o celkové délce zhruba 7 km. Ve výchozím stavu je kvantový kanál veden zvláště tmavým vláknem. Trasa je postavena na UPC konektorech s odrazivostí kolem -55 dB. Čistý útlum na trase je 2,1 dB. Tyto hodnoty byly získány na základě OTDR náměru. Mapa zmíněné trasy se nachází na obrázku 10.1 níže. K dalšímu útlumu dochází na krátkých úsecích trasy v rámci budov obou fakult. Navíc je na trase umístěn 5dB útlumový článek. Celkový útlum kvantového kanálu se tak pohybuje kolem 10 dB.



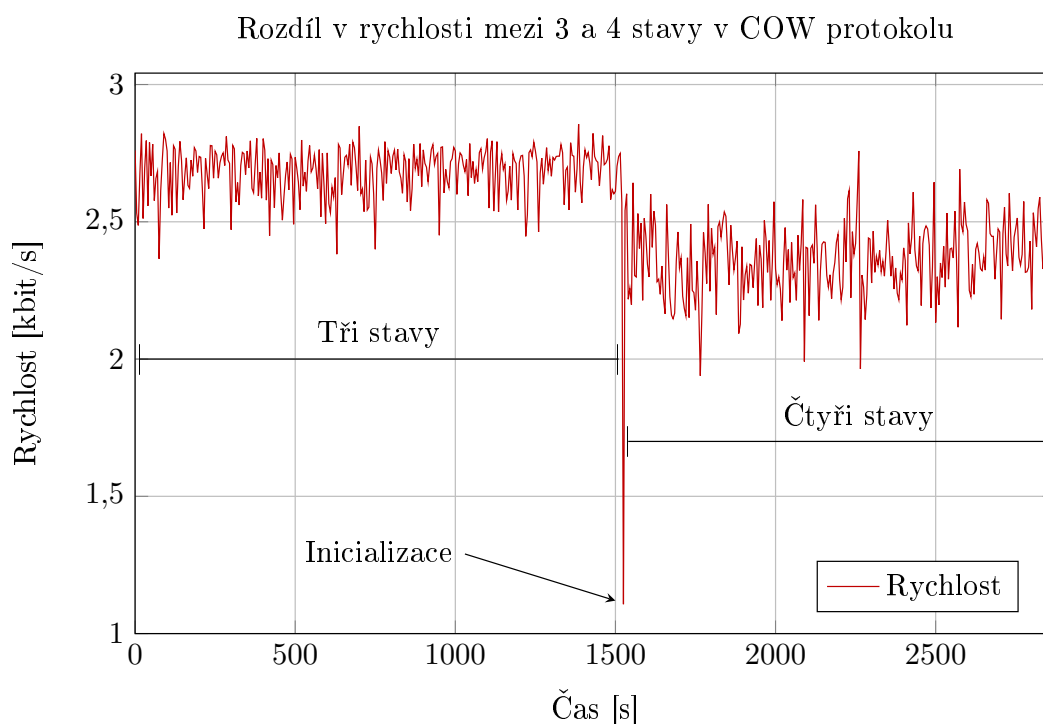
Obr. 10.1: Optická trasa mezi VUT FEKT a VUT FIT v Brně.

10.2 Třístavový a čtyřstavový COW protokol

Protokol COW existuje v mnoha modifikacích. Aktuálně používaná verze firmware systému Clavis³ obsahuje kromě základní třístavové verze i čtyřstavovou verzi protokolu. Ta je navíc nastavena jako výchozí. Důvodem jejího nasazení je odolnost proti útoku s nulovou chybou popsaném v článku [49]. Základem je přidání druhého návnadového stavu, který se skládá ze dvou vakuových pulzů. Tento protokol je detailněji popsán v následujícím článku [50]. Toto opatření výrazně snižuje pravděpodobnost, že v průběhu útoku pomocí USD bude výsledek průkazný. Bezpečnost je však zvýšena na úkor rychlosti doručování klíče.

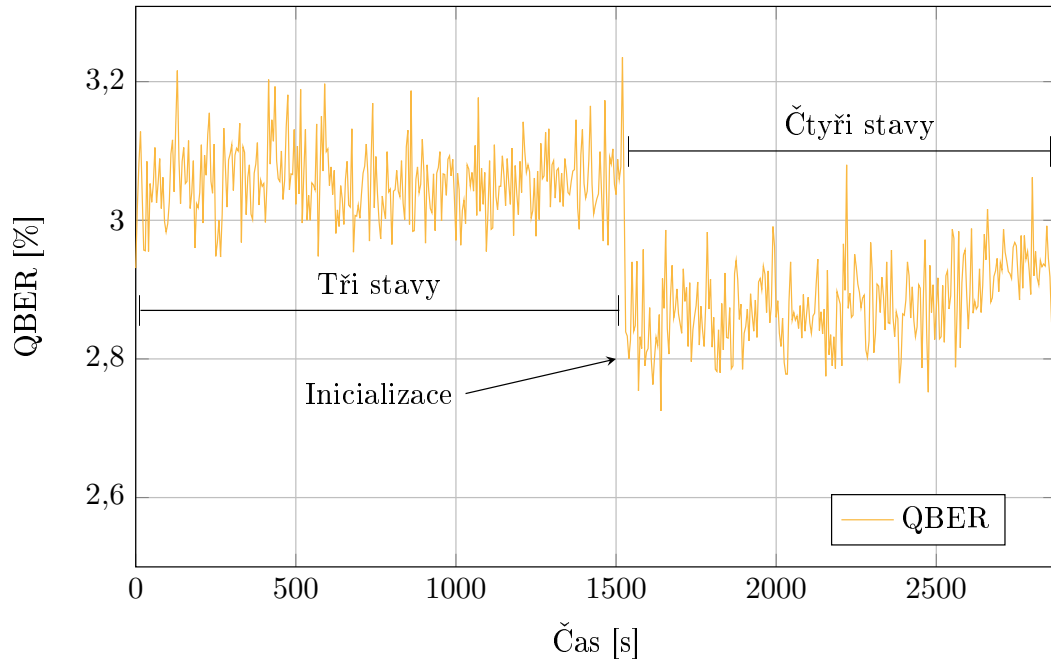
10.2.1 Srovnání

Cílem následujícího měření bylo srovnat výkon systému při použití čtyřstavového a třístavového COW protokolu. Měřeny byly tři základní parametry, tedy rychlost doručování klíčů (dále jen „rychlost“), QBER a viditelnost. Všechny parametry jsou vyneseny do grafů níže.



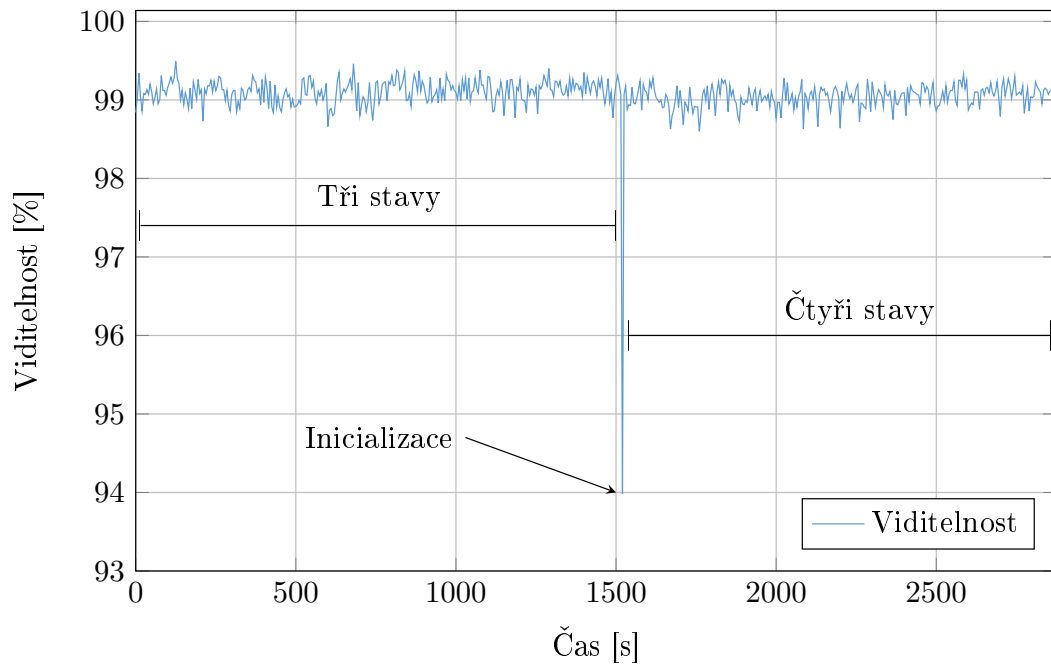
Obr. 10.2: Rozdíl v rychlosti mezi třístavovým a čtyřstavovým COW.

Rozdíl v QBER mezi 3 a 4 stavy v COW protokolu



Obr. 10.3: Rozdíl v chybovosti (QBER) mezi třístavovým a čtyřstavovým COW.

Rozdíl ve viditelnosti mezi 3 a 4 stavy v COW protokolu



Obr. 10.4: Rozdíl ve viditelnosti mezi třístavovým a čtyřstavovým COW.

10.2.2 Výsledky měření

Na začátku měření byl systém nastaven na používání třístavového protokolu. Po nasbírání dostatečného množství vzorků byl systém přepnut na čtyřstavovou verzi protokolu. Před opětovným generováním klíče dochází vždy k inicializaci, která systém vhodně nastaví. V průběhu měření nebyla žádným způsobem pozměněna fyzická trasa. Do sledovaných parametrů se tak neodrazil vliv daný opětovným přepojováním. Příkladem může být změna útlumu při přílišném dotažení konektoru apod. Samotné měření probíhalo opakovaně a vždy vyústilo ve shodné výsledky. Průměrné hodnoty sledovaných parametrů pro obě verze jsou vypočteny v tabulkách níže.

Tab. 10.1: Průměrná rychlost u třístavového a čtyřstavového COW.

| Protokol COW | Průměrná rychlost |
|--------------|-------------------|
| Třístavový | 2,684 kb/s |
| Čtyřstavový | 2,365 kb/s |
| Rozdíl | 0,319 kb/s |

Tab. 10.2: Průměrná chybovost (QBER) u třístavového a čtyřstavového COW.

| Protokol COW | Průměrná QBER |
|--------------|---------------|
| Třístavový | 3,056 % |
| Čtyřstavový | 2,881 % |
| Rozdíl | 0,175 % |

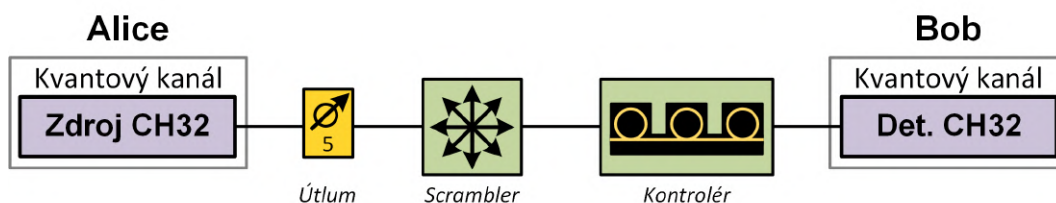
Tab. 10.3: Průměrná viditelnost u třístavového a čtyřstavového COW.

| Protokol COW | Průměrná viditelnost |
|--------------|----------------------|
| Třístavový | 99,091 % |
| Čtyřstavový | 99,040 % |
| Rozdíl | 0,051 % |

Z výsledků je zřejmé, že změna chybovosti i viditelnosti je v obou případech zanedbatelná. Jelikož ale využívá čtyřstavový protokol druhého návadového stavu na úkor datových stavů, je rychlost doručování klíče v souladu s očekáváním nižší. Při daném nastavení systému činil rozdíl více jak 0,3 kb/s.

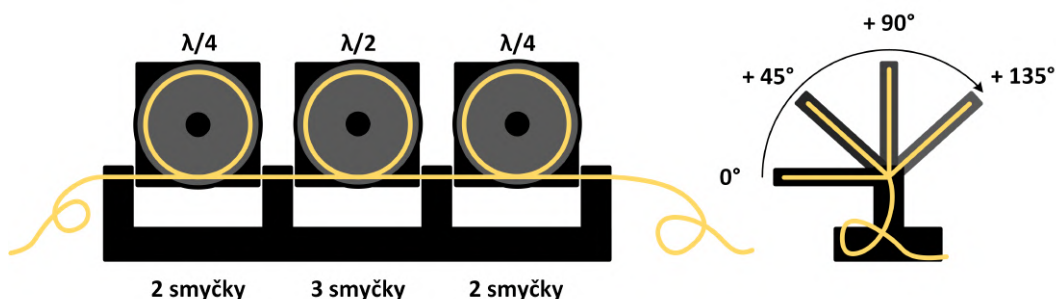
10.3 Vliv změn polarizace

Cílem tohoto měření bylo ověřit tvrzení výrobce systému, vztahující se k nezávislosti systému a protokolu na změnách polarizace. COW protokol je postaven na slabých koherentních pulzech, jejichž zdrojem je koherentní laser. Z tohoto důvodu lze předpokládat, že kvantový kanál je polarizován. Směr polarizace však znám není a dle výrobce se systém změnami polarizace nezabývá.



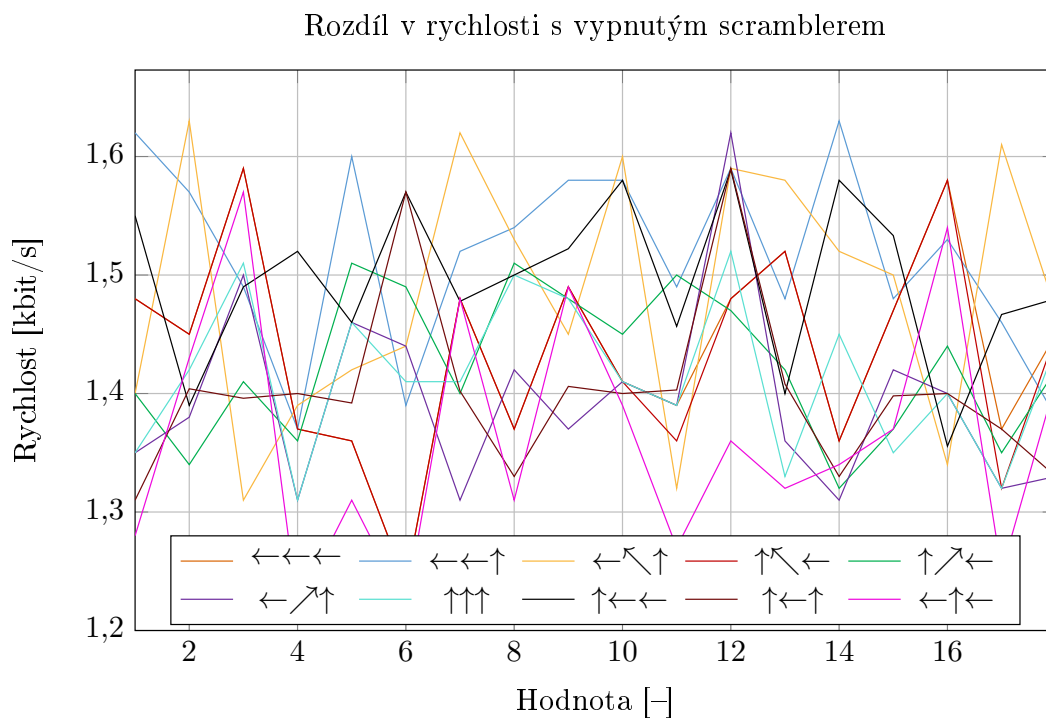
Obr. 10.5: Zapojení pro testování vlivu polarizace.

K samotnému měření byla sestavena testovací trasa zobrazená na schématu 10.5. Ta sestává ze tří za sebou zapojených prvků a její celkový útlum se pohybuje kolem 10 dB. Zatímco polarizační kontrolér slouží spíše k jednorázovému manuálnímu nastavení polarizace, zapojený scrambler mění polarizaci náhodně 10 krát za sekundu. To, zda je scrambler zapnutý či ne, nemá vliv na jeho vložený útlum.

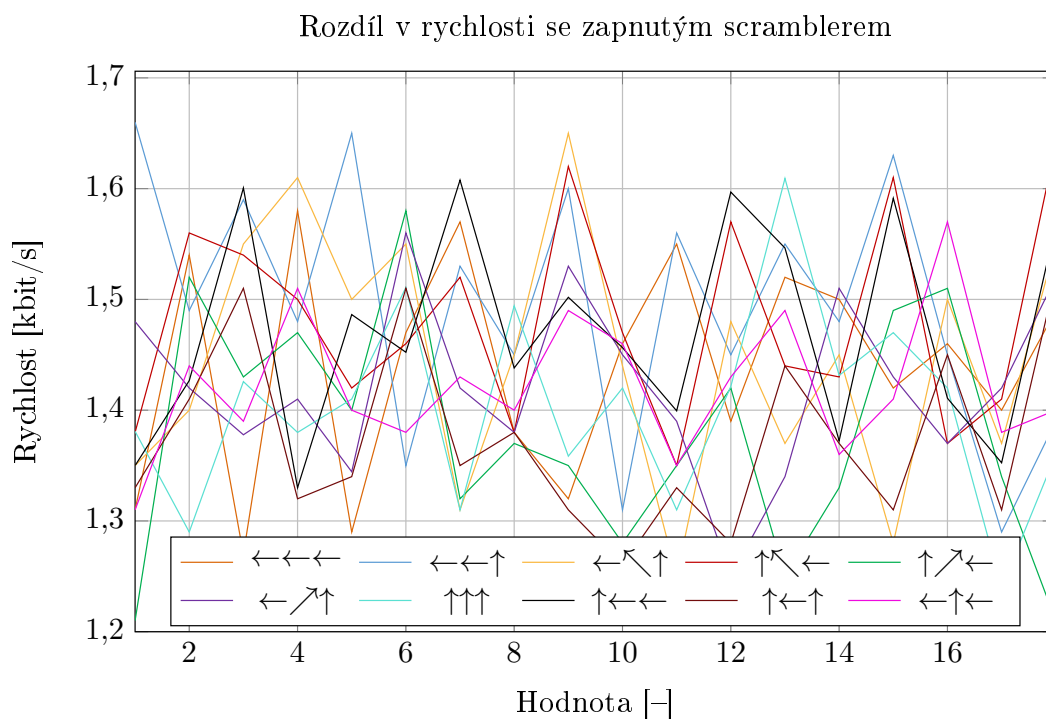


Obr. 10.6: Polarizační kontrolér.

Manuální polarizační kontrolér od firmy Thorlabs, který je znázorněn na obrázku 10.6 napodobuje funkci tří retardačních destiček ($\lambda/4$, $\lambda/2$, $\lambda/4$), které je vůči sobě možné natočit o libovolný úhel. Rovněž jeho vložený útlum zůstává s natáčením destiček neměnný. V rámci tohoto měření mohla být libovolná destička nastavena v jedné ze čtyř pozic tak, jak je zobrazeno v pravé části výše zmíněného obrázku. Pro jednodušší orientaci jsou v následujícím textu používány místo úhlů šipky, odpovídající jedné ze čtyř pozic.













Obr. 10.7: Rychlost při vypnutém scrambleru a různých nastaveních kontroléru.



Obr. 10.8: Rychlost při zapnutém scrambleru a různých nastaveních kontroléru.

Tab. 10.4: Průměrná rychlost doručování klíčů, pro různá nastavení úhlu destiček.

| Nastavení | | | | Pouze kontrolér | Se scramblerem |
|---------------|---|---|---|------------------|------------------|
| ← | ← | ← |  | 1,44 kb/s | 1,43 kb/s |
| ← | ← | ↑ |  | 1,52 kb/s | 1,50 kb/s |
| ← | ↖ | ↑ |  | 1,48 kb/s | 1,45 kb/s |
| ↑ | ↖ | ← |  | 1,43 kb/s | 1,48 kb/s |
| ↑ | ↗ | ← |  | 1,42 kb/s | 1,38 kb/s |
| ← | ↗ | ↑ |  | 1,39 kb/s | 1,42 kb/s |
| ↑ | ↑ | ↑ |  | 1,41 kb/s | 1,40 kb/s |
| ↑ | ← | ← |  | 1,50 kb/s | 1,47 kb/s |
| ↑ | ← | ↑ |  | 1,40 kb/s | 1,37 kb/s |
| ← | ↑ | ← |  | 1,36 kb/s | 1,42 kb/s |
| Průměr | | | | 1,44 kb/s | 1,43 kb/s |

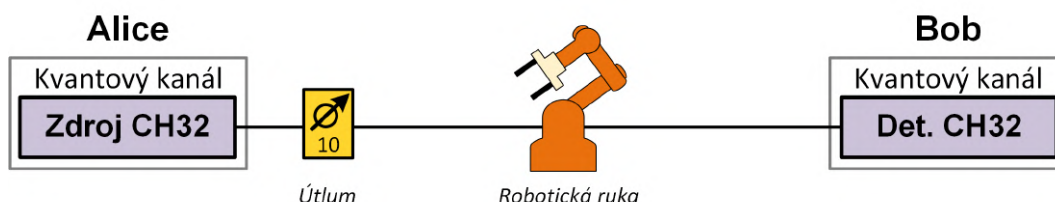
Oba přípravky byly zapojeny do výše popsané trasy a následně byly provedeny dvě série měření – s vypnutým a zapnutým scramblerem. V obou sériích byly na kontroléru nastavovány pozice destiček podle tabulky 10.4 (vstup do kontroléru je dán levou šipkou). Celkem tak bylo opakovaně provedeno 20 měření. Podobně jako u předchozího měření nedocházelo k rozpojování optické trasy. Měření bylo provedeno v noci, kdy systém nemohl být ovlivněn slunečním zářením a pohybem osob.

10.3.1 Výsledky měření

Z výsledků uvedených v tabulce 10.4 a grafu 10.7 plyne, že změna polarizace kvantového kanálu má na přenosovou rychlost systému minimální vliv. Změny QBER (cca 2,5 %) a viditelnosti (cca 98 %) jsou rovněž zanedbatelné a grafy těchto parametrů zde tak nejsou uvedeny. Pro různé konfigurace trasy byl rovněž změřen útlum pomocí přímé metody a proveden OTDR náměr. Změny útlumu a odrazivosti u jednotlivých nastavení polarizačních prvků je rovněž možné zanedbat.

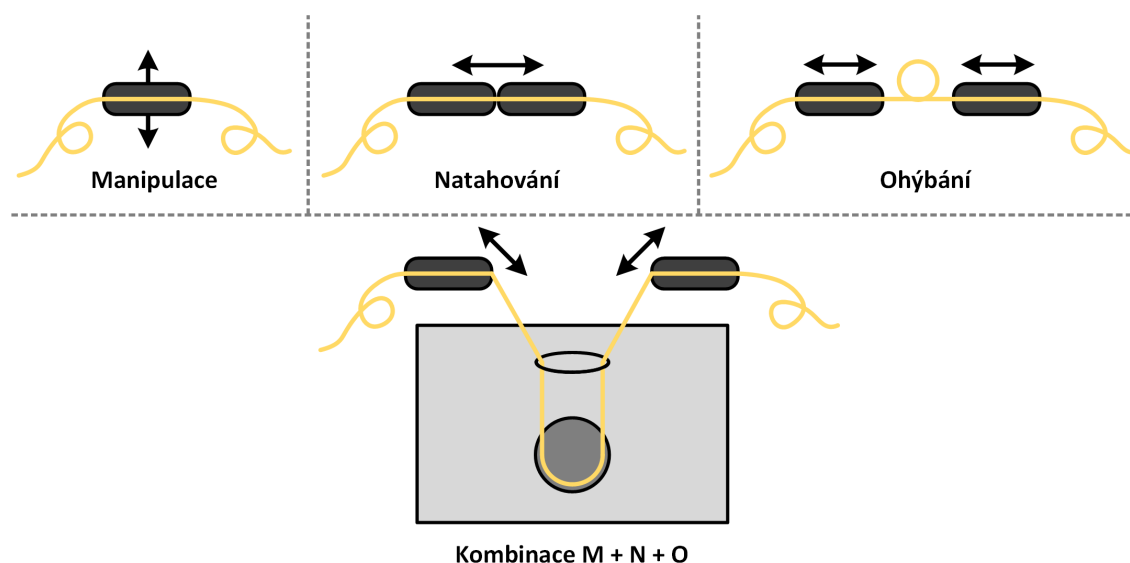
10.4 Vliv manipulace s vláknem

Cílem měření bylo otestovat vliv pohybu vlákna na kvantový kanál. Pomocí robotické ruky byly periodicky vyvolávány pohyby optického kabelu, kterými byla simulována manipulace vlákna člověkem. Zapojení celé trasy se nachází na obrázku 10.9. Celkový útlum trasy se pohyboval kolem 10 až 11 dB.



Obr. 10.9: Zapojení trasy s robotickou rukou.

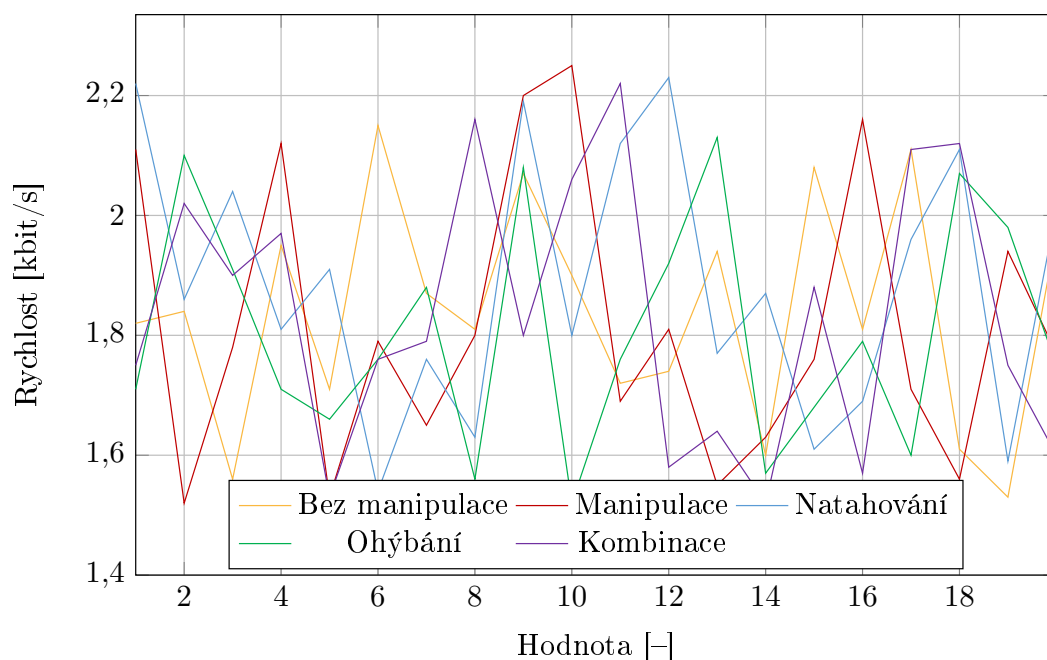
Samotná robotická ruka disponuje dvěma rozevratelnými prsty a její rameno se pohybuje ve vertikálním směru nahoru a dolů. Ruka se tedy postupně zvedá a rozevívá prsty. Následně opět klesá a prsty svírá. Celý pohyb trvá zhruba 9 sekund a periodicky se opakuje.



Obr. 10.10: Pohyby robotické ruky s vláknem.

Celkem bylo provedeno pět měření. Nejdříve byla naměřena referenční hodnota, tedy výkon systému v případě, že k žádné manipulaci s vláknem nedochází. Následně bylo vlákno zvedáno, natahováno a ohýbáno (průměr cca 2 cm). Princip těchto technik je zaznamenán v horní části obrázku 10.10.

Vliv manipulace s kabelem na rychlost



Obr. 10.11: Rychlost při různé manipulaci s optickým kabelem.

Poslední měření je kombinací všech předchozích technik. Vlákno je zvedáno do výšky a prsty se rozevírají. Ve spodní části je vlákno obtočeno kolem ohybu s průměrem 2 cm. Nad ohybem je vlákno sepnuto tak, aby se obě jeho strany nacházely ve vzájemné vzdálenosti odpovídající průměru ohybu. Tímto způsobem dochází k poloovičnímu ohybu. Pohybem nahoru se vlákno rovněž mírně natahuje.

Tab. 10.5: Průměrná rychlost, chybovost a viditelnost při manipulaci s vláknem.

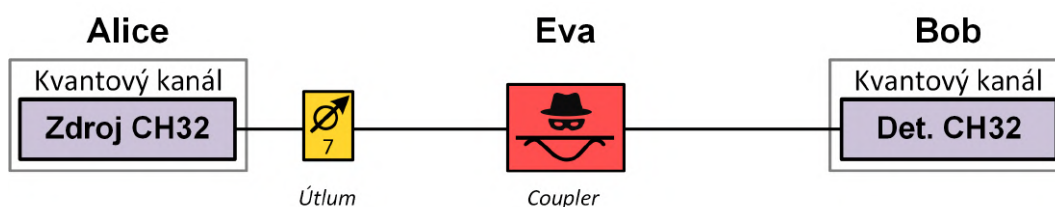
| Nastavení | | Rychlost | QBER | Viditelnost |
|----------------|--|-----------|--------|-------------|
| Bez manipulace | | 1,84 kb/s | 2,87 % | 98,30 % |
| Manipulace | | 1,82 kb/s | 2,93 % | 98,30 % |
| Natahování | | 1,89 kb/s | 2,83 % | 98,30 % |
| Ohýbání | | 1,81 kb/s | 2,85 % | 98,20 % |
| Kombinace | | 1,84 kb/s | 2,91 % | 98,20 % |

10.4.1 Výsledky měření

Z výsledků provedených měření uvedených v tabulce 10.5 je zřejmé, že se hodnoty všech tří sledovaných parametrů mění jen minimálně. Je tak možné prohlásit, že běžná manipulace s kabelem nemá na výkon systému vliv.

10.5 Vliv zpoždění části pulzů

V rámci simulace byl využit modul Eva od IDQ, který byl popsán v kapitole 9.3. Ten obsahuje nastavitelný coupler, který část pulzů zpozdí. Tím, že pulzy dorazí v nesprávný čas, dochází ke zvýšení chybovosti a snížení přenosové rychlosti. Změny v interferometrické viditelnosti se naproti tomu projevují minimálně.



Obr. 10.12: Zapojení pro simulaci útoku pomocí modulu Eva.

Princip simulace spočívá v otáčení potenciometru vždy o 5° , čímž se postupně zvyšuje množství zpožděného světla. Celkový útlum trasy se pohybuje okolo 11 dB. Samotný modul má vložený útlum kolem 3,5 dB a útlumový článek 7 dB. Dle návodu výrobce, by mělo docházet ke zdatelnému zvýšení chybovosti a snížení rychlosti při otočení na cca 20° . Systém by dále měl přestat generovat klíče, pokud QBER dosáhne hranice cca 6 %. To nastává při nastavení potenciometru na 35° . Potenciometr je možné nastavit maximálně na 60° jinak hrozí poškození modulu. Za minimální možnou hranici viditelnosti je považováno 95 %. Výsledky měření pro jednotlivé úhly je možné najít v tabulce 10.6.

Tab. 10.6: Vliv útoku na QKD systém Clavis³.

| Úhel | Rychlost | QBER | Viditelnost |
|------------|-----------|---------|-------------|
| 0° | 1,78 kb/s | 2,28 % | 98,50 % |
| 5° | 1,67 kb/s | 2,29 % | 98,40 % |
| 10° | 1,60 kb/s | 2,41 % | 98,50 % |
| 15° | 1,62 kb/s | 2,40 % | 98,30 % |
| 20° | 1,61 kb/s | 2,68 % | 98,50 % |
| 25° | 1,51 kb/s | 3,12 % | 98,20 % |
| 30° | 0,30 kb/s | 4,91 % | 97,00 % |
| 35° | 0 kb/s | 5,96 % | 97,40 % |
| 60° | 0 kb/s | 29,20 % | 87,50 % |

10.5.1 Výsledky měření

Doručený modul odpovídá svými vlastnostmi parametrům, které byly popsány výrobcem. Simulace rovněž potvrzuje předpokládanou 6% hranici pro bezpečný přenos. Z měření je rovněž patrné, že útok má na viditelnost mnohem nižší dopad než na chybovost. To může být dáno tím, že vzájemná koherence dvou porovnávaných pulzů je narušena v menším množství případů. Jak ovšem dokazuje poslední řádek tabulky 10.6, při větším množství zpožděného světla se útok projevuje i snížením viditelnosti. Kromě tohoto posledního (extrémního) měření však viditelnost nikdy neklesla pod hranici 95 %.

11 Sloučení kvantového a servisních kanálů

Hlavním cílem této práce je ověření možnosti sloučení kvantového kanálu do jednoho optického vlákna s dalšími klasickými kanály (zejména servisními). Jelikož je kvantový kanál velmi slabý, je jeho zkombinování do jednoho vlákna s mnohem silnějšími klasickými kanály obtížné. Důležitá je tak zejména dostatečně kvalitní filtrace, která zabráni možnému přeslechu. Druhým a hůře řešitelným problémem je rušení způsobené Ramanovým šumem, který roste s délkou vlákna a je rovněž závislý na vstupním výkonu klasického kanálu. Rovněž je potřeba dávat pozor, aby kvantový kanál nebyl umístěn do oblasti postižené čtyřvlenným směřováním. Je tak nutné vhodně vybrat vzájemné umístění všech kanálů. Vliv ostatních nelineárních jevů byl zanedbán.

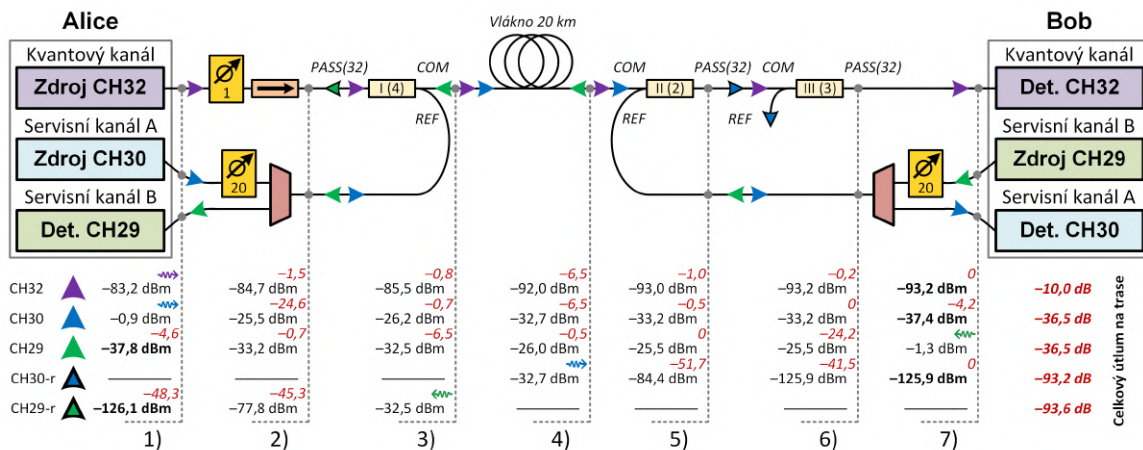
V současnosti je možné získat QKD systémy podporující WDM přímo od výrobce. Ty jsou ovšem založeny na co největším odstupu kvantového a klasických signálů. Typicky je kvantový kanál poslán v O-pásmu, zatímco oba servisní kanály v C-pásmu. Níže provedená měření demonstrují schopnost systému efektivně doručovat klíče přes krátkou optickou trasu sdílenou mezi kvantový kanál (CH32) a dva, v těsné blízkosti, umístěné servisní kanály (CH30 a CH29). Podobný problém je rovněž řešen v článku [125]. Zatímco v článku je řešení postaveno na užším filtrování, zde stojí na ztlumení a následném zesílení servisních kanálů. Celé měření probíhalo ve třech postupných krocích:

- **Návrh a ověření bezpečnosti prvotní trasy** – V rámci této fáze byl navržen potenciálně funkční QKD polygon s délkou trasy 20 km. Délka vlákna je dostatečná na to, aby se v něm projevíly nelineární jevy a současně nebyl překročen maximální možný útlum kvantového kanálu. Ke sloučení kvantového a klasických kanálů byly použity DWDM filtry, jejichž vlastnosti byly otestovány pomocí optického spektrálního analyzátoru (OSA – Optical spectrum analyzer). Na základě výsledků pak byly tyto filtry začleněny na vhodné místo v zapojení. Rovněž byl naměřen výkon původně používaných SFP modulů a útlum na všech použitých optických prvcích. Na základě výpočtů bylo ověřeno, že nemůže dojít k poškození žádných detekčních zařízení v topologii, zejména pak detektorů kvantového signálu.
- **Tlumení servisních kanálů** – Druhá fáze spočívala v hledání minimálního ztlumení servisních kanálů tak, aby byl kvantový kanál stále funkční. Testování bylo provedeno pomocí dvou dvojic SFP. Zatímco první dvojice byla použita pouze k testování, tj. nebyl odeslán užitečný signál, druhá dvojice zajistila přímý spoj servisního kanálu. Jedině takto bylo možné zajistit správnou funkci celého systému.

- **Sestavení a ladění finální trasy** – Posledním krokem bylo sestavení a otestování plně funkčního QKD polygonu. Na rozdíl od předchozí fáze již byla věnována pozornost i servisním kanálům, které jsou při dostatečném ztlumení rovněž limitujícím prvkem. Z tohoto důvodu bylo na trase provedeno několik úprav. Zejména se jedná o nahrazení ztrátových multiplexorů šetrnějšími cirkulátory nebo přidání EDFA zesilovače na konec obou servisních kanálů. Funkčnost této trasy byla testována pro vzdálenosti 0, 5, 10, 15 a 20 km.

11.1 Fáze I: Návrh a ověření bezpečnosti prvotní trasy

V rámci první fáze byla navržena jednoduchá trasa multiplexovaného QKD polygonu zobrazená na schématu 11.1. V případě zanedbání spojů mezi jednotlivými optickými prvky, činí její celková délka 20 km. Tato vzdálenost byla zvolena kvalifikovaným odhadem, jelikož je dostatečně dlouhá na to, aby se na ní projevil nelineární jevy. Z hlediska útlumu však, při dodatečném ztlumení, respektuje výrobcem specifikovaný rozsah kvantového kanálu, tedy 10–14 dB.



Obr. 11.1: Prvotní navržené zapojení QKD polygonu.

Představené zapojení kombinuje kvantový kanál (CH32) do jednoho vlákna s kanály servisními (CH29 a CH30). Zatímco kanál CH30 pracuje ve stejném směru jako kanál kvantový, tedy je vyslán z Alice směrem k Bobovi, směr druhého servisního kanálu je opačný. Pro kvalitní odfiltrování šumu z kvantového kanálu je nejen nutné správně odfiltrovat cizí vlnové délky, ale rovněž zařídit, aby se na sdílené vlákno nedostal šum v oblasti kanálu 32. Ten by následně již nebylo možné od kvantového kanálu odlišit.

Servisní kanály jsou implementovány pomocí SFP modulů Finisar popsaných v tabulce 9.3. Samy jsou nejdříve sloučeny do jediného vlákna pomocí klasického multiplexoru. Kromě své hlavní úlohy však MUX slouží jako filtr, který odstraní většinu šumu na kanále 32. Aby byl kvantový kanál rušen nelineárními jevy co nejméně, je u zdroje zeslaben o 20 dB.

Základem topologie jsou však tři DWDM filtry propouštějící CH32 a zapojené na pozicích I, II a III. Na základě měření jejich reálných parametrů v příloze A, byl pro každou z poloh vybrán jeden z reálných filtrů (označeny 1–5). Každá z poloh plní odlišné funkce:

- **I. Poloha** – Hlavní funkcí filtru je navázat servisní kanál A (CH30) na společné vlákno s kvantovým kanálem a současně z vlákna vydělit servisní kanál B (CH29). Jeho sekundární funkce je podobná jako v případě výše popsaných multiplexorů. Tedy odfiltrovat šum, který produkuje servisní kanál A v oblasti CH32. Většina šumu, která prošla MUXem je propuštěna na port PASS, kde je následně spolu se zbytky kanálu 29 pohlcena izolátorem. Z tohoto důvodu byl vybrán filtr číslo 4.
- **II. Poloha** – Podobně jako v předchozím případě je hlavní funkcí filtru navázat a vyvázat servisní kanály na společné vlákno. V tomto případě již však není vhodné, aby filtr propouštěl šum servisního kanálu B. Na rozdíl od filtru I musí být většina šumu v oblasti CH32 odražena směrem k Alici, kde opět projde k izolátoru a je pohlcena. Na základě charakteristik byl vybrán filtr číslo 2.
- **III. Poloha** – Filtr slouží zejména ke zvýšení OSNR (Optical signal to noise ratio) kvantového kanálu. Důležitá je tedy jeho izolace ve směru COM-PASS. Zbytky servisních kanálů, které nebyly potlačeny předchozím filtrem, jsou z vlákna odvedeny portem REF. Vybrán byl filtr číslo 3.

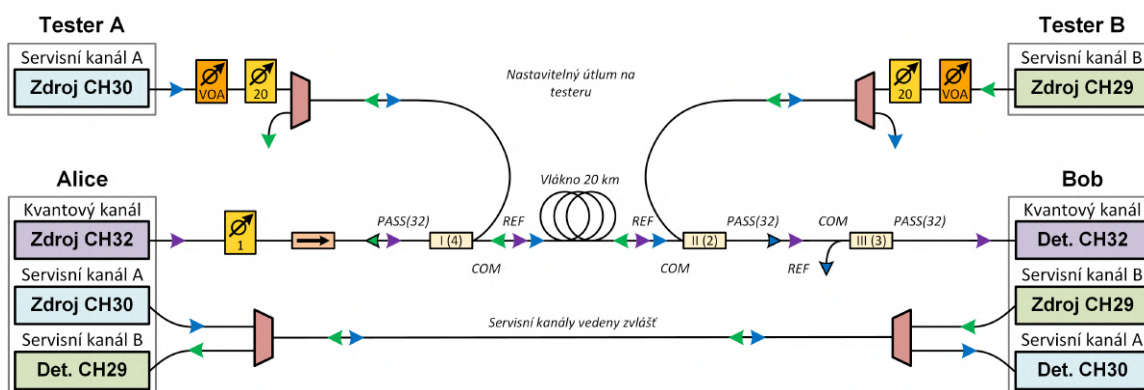
Na kvantovém kanále (CH32) se ještě nachází dva optické prvky. Jedná se o izolátor, který brání průchodu jakéhokoliv filtrem propuštěného světla ke zdroji a útlumový článek, který zvyšuje útlum na kvantovém kanálu na celkových 10 dB.

Pro ověření bezpečnosti zapojení byly v sedmi významných bodech navržené trasy změřeny, případně vypočteny hodnoty výkonu kvantového a obou servisních kanálů (včetně propuštěného zbytkového výkonu za filtry). Z výsledků vyplývá, že zapojení se nikde neblíží hodnotám, které by mohly poškodit některý z fotodetektorů. Ta se většinou pohybuje v hodnotách nad 0 dBm.

Pro popsané zapojení byl v příloze B vypočten Ramanův šum, který má vliv na kvantový kanál. Hodnota jeho škodlivého výkonu je zhruba $-104,07$ dBm. Stejný postup je použit i pro výpočet Ramanova šumu v následujících kapitolách.

11.2 Fáze 2: Tlumení servisních kanálů

Následující měření přímo navazuje na předchozí fázi a je zaměřeno na hledání minimálního možného útlumu servisních kanálů tak, aby po sloučení nezarušily kvantový kanál a systém tak zůstal funkční. Na rozdíl od první fáze však toto měření vyžaduje funkční QKD systém. Aby bylo možné něco takového testovat je nutné propojit servisní kanály na přímo tak, aby nerušily kanál kvantový a současně nedošlo k narušení jejich synchronizace při jejich tlumení. K tomuto účelu je nutné použít druhý pár SFP modulů. Tentokrát se jedná o moduly Skylane, které jsou rovněž popsány v tabulce 9.3.



Obr. 11.2: Testování tolerance kvantového kanálu.

Originální SFP jsou oproti tomu zapojeny do SFP switche (lze použít libovolné zařízení) a slouží výhradně k testování rušení. Nepřenáší tak žádný užitečný signál a je možné je libovolně tlumit pomocí nastavitelného útlumového článku (VOA). Ten přidává dodatečný útlum k již původně navrženým 20 dB. Jelikož není kvantový kanál při útlumu 20 dB funkční, nemá význam útlum snižovat.

Podobně jako v předchozí fázi i zde je monitorován procházející výkon. Z hlediska funkčnosti je nutné sledovat zejména výkon u zdroje, výkon vstupující do 20km optické trasy a konečný výkon dopadající na detektory. Hodnoty výkonu jsou ovlivňovány útlumem instalovaných optických prvků. Samotný princip měření spočívá v postupném přidávání útlumu na VOA a sledování změn u parametrů QKD systému. Hodnoty výkonu na trase pro různé konfigurace (nastavený útlum) se nacházejí v tabulce 11.1 na další straně.

Tab. 11.1: Výkon kvantového kanálu při sloučení s oběma servisními kanály.

| VZ [dBm] | DÚ [dB] | ÚÚ [dB] | VV [dBm] | CÚ [dB] | VD [dBm] |
|----------|---------|---------|----------|---------|----------|
| -1 | +20 dB | 44,5 | -45,5 | 56,5 | -57,5 |
| -1 | +10 dB | 34,5 | -35,5 | 46,5 | -47,5 |
| -1 | +7 dB | 31,5 | -32,5 | 43,5 | -44,5 |
| -1 | +5 dB | 29,5 | -30,5 | 41,5 | -42,5 |
| -1 | +4 dB | 28,5 | -29,5 | 40,5 | -41,5 |
| -1 | +3 dB | 27,5 | -28,5 | 39,5 | -40,5 |
| -1 | +2 dB | 26,5 | -27,5 | 38,5 | -39,5 |
| -1 | +1 dB | 25,5 | -26,5 | 37,5 | -38,5 |
| -1 | +0 dB | 24,5 | -25,5 | 36,5 | -37,5 |

- **Výkon zdroje (VZ)** – Hodnota špičkového výkonu přímo u zdroje (SFP) servisního kanálu. V textu je uvedena stejná hodnota pro všechna měření. V praxi ovšem výkon modulů běžně osciluje mezi -1 a +1 dBm (někdy i více).
- **Dodatečný útlum (DÚ)** – Útlum, který je postupně přidáván k navržené trase pomocí VOA za účelem zatlumení servisních kanálů.
- **Účinný útlum (ÚÚ)** – Útlum sestávající z útlumu na všech optických prvcích (MUX, útlumové články, filtry) před vstupem do 20km optické trasy.
- **Vstupní výkon (VV)** – Výkon, který vstupuje do 20km optické trasy a vyvolává nelineární jevy včetně Ramanova šumu. Je závislý na účinném útlumu.
- **Celkový útlum (CÚ)** – Celkový útlum servisního kanálu, který vzniká v rámci celého zapojení.
- **Výkon na detektoru (VD)** – Výsledný výkon, který dopadá na detektory servisních kanálů. Je závislý na celkovém útlumu.

Testování bylo celkem provedeno třikrát po devíti respektive deseti krocích. Tedy pouze pro kanál 30, pouze pro kanál 29 a pro oba kanály současně. Následně bylo pomocí monitorovacího nástroje Grafana získáno 10 hodnot rychlosti, viditelnosti a QBER. Jejich průměry pro jednotlivé hodnoty útlumu se nacházejí v tabulkách 11.2, 11.3 a 11.4.

Z výsledků uvedených v prvních dvou tabulkách vyplývá, že pro stabilní spojení je nutné oba servisní kanály ztlumit nejméně o další 3 dB. Za předpokladu, že je pokles rychlosti způsoben Ramanovým šumem, lze předpokládat, že je jeho hodnota v obou směrech velice podobná (rozdíl ve vzdálenosti mezi CH29 a CH30 od CH32 je zanedbán).

Tab. 11.2: Výkon kvantového kanálu při sloučení s kanálem CH30.

| SFP 30 | Rychlost [kb/s] | QBER [%] | Viditelnost [%] |
|---------------|------------------------|-----------------|------------------------|
| Vypnuté | 2,07 | 3,04 | 98,60 |
| +20 dB | 1,90 | 3,53 | 97,70 |
| +10 dB | 1,89 | 3,47 | 98,00 |
| +5 dB | 1,73 | 3,91 | 97,70 |
| +4 dB | 1,02 | 4,20 | 97,70 |
| +3 dB | 0,71 | 4,37 | 97,10 |
| +2 dB | nefunkční | 4,73 | 98,00 |
| +1 dB | nefunkční | 5,18 | 98,10 |
| +0 dB | nefunkční | 5,37 | 96,60 |

Tab. 11.3: Výkon kvantového kanálu při sloučení s kanálem CH29.

| SFP 29 | Rychlost [kb/s] | QBER [%] | Viditelnost [%] |
|---------------|------------------------|-----------------|------------------------|
| Vypnuté | 2,07 | 3,04 | 98,60 |
| +20 dB | 1,91 | 3,31 | 98,30 |
| +10 dB | 1,91 | 3,36 | 98,10 |
| +5 dB | 1,88 | 3,42 | 98,10 |
| +4 dB | 1,87 | 3,89 | 97,70 |
| +3 dB | 0,80 | 4,27 | 96,90 |
| +2 dB | nefunkční | 4,47 | 97,30 |
| +1 dB | nefunkční | 5,27 | 97,80 |
| +0 dB | nefunkční | 5,35 | 96,20 |

Tab. 11.4: Výkon kvantového kanálu při sloučení s oběma servisními kanály.

| SFP 29 a 30 | Rychlost [kb/s] | QBER [%] | Viditelnost [%] |
|-------------|-----------------|----------|-----------------|
| Vypnuté | 2,07 | 3,04 | 98,60 |
| +20 dB | 2,04 | 3,22 | 98,40 |
| +10 dB | 1,59 | 3,41 | 97,70 |
| +7 dB | 1,26 | 4,10 | 97,20 |
| +5 dB | 0,65 | 4,45 | 97,40 |
| +4 dB | nefunkční | 5,05 | 97,10 |
| +3 dB | nefunkční | 5,27 | 96,70 |
| +2 dB | nefunkční | 5,32 | 96,50 |
| +1 dB | nefunkční | 6,56 | 96,00 |
| +0 dB | nefunkční | 8,96 | 94,80 |

Poslední tabulka obsahuje hodnoty pro oba zapojené směry současně. Výsledky potvrzují očekávání, že se zvyšujícím se počtem klasických kanálů narůstá chybovost a klesá viditelnost s přenosovou rychlostí. Minimální konfigurace trasy by tak měla obsahovat minimálně 5 dB přidaného útlumu.

11.2.1 Přeslech nebo šum?

Aby bylo možné určit, co je důvodem snižující se rychlosti, bylo v rámci etapy provedeno rychlé měření. Z výše popsaných konfigurací byla vybrána ta s oběma zapojenými servisními kanály a přidaným útlumem +7 dB. Jedná se o zapojení, při kterém je systém ve stabilním stavu a současně lze pozorovat zvýšení a snížení rychlosti viditelnosti a chybovosti. Tyto hodnoty jsou zaznamenány v tabulce 11.5. Následně bylo 20km vlákno odstraněno a filtry I a II byly propojeny na přímo. Ohybem zanedbatelně dlouhého propojovacího kabelu mezi filtry byl přidán stejný útlum jaký měla původně zapojená trasa (asi 6 dB).

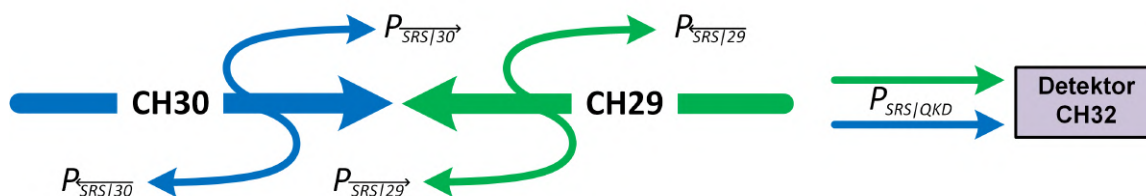
Tab. 11.5: Výkon kvantového kanálu při sloučení s oběma servisními kanály.

| Zapojení | Útlum | Rychlost [kb/s] | QBER [%] | Viditelnost [%] |
|----------|--------------|-----------------|----------|-----------------|
| Přímo | +7 (44,5) dB | 2,11 | 3,33 | 98,70 |
| 20 km | +7 (44,5) dB | 1,21 | 4,05 | 97,40 |

Pokud by bylo rušení kvantového kanálu způsobeno přeslechem, jeho hodnota by se s délkou kanálu již nezvyšovala a parametry systému by zůstaly v obou případech stejné. Naopak Ramanův šum s délkou kanálu rychle roste. Z výsledků uvedených v tabulce tak vyplývá, že hlavní příčinou rušení kvantového kanálu je Ramanův šum. Možné příspěvky ostatních nelineárních jevů jsou zanedbány.

11.2.2 Ramanův šum

Ramanův šum je hlavním limitujícím prvkem celého zapojení, z tohoto důvodu je vhodné vypočítat jeho přibližný výkon. Na základě informací v kapitole 7.4.2 byly vypočteny jeho hodnoty pro nejmenší a největší použité zatlumení servisních kanálů. Detailní postup s příkladem se nachází v příloze B. Pro výpočet je nutné znát hodnotu výkonu vystupujícího z 20 km optické trasy. Za předpokladu, že bude uvažován výkon 0,3 dB/km činí útlum této trasy 6 dB. Výstupní výkon se pak vypočte odečtením této hodnoty výkonu od výkonu vstupního, který se nachází v tabulce 11.1.



Obr. 11.3: Výpočet Ramanova šumu.

Oba kanály mají podíl na tvorbě Ramanova šumu, který vzniká jak v dopředném tak ve zpětném směru. Jelikož vysílají oba kanály v jiném směru, dopadá na QKD detektor pouze dopředný Ramanův šum CH30 a zpětný šum CH29. Celkový výkon škodlivého Ramanova šumu se pak určí jako součet těchto dvou výkonů.

- **Pro nejmenší zatlumení** (+0 dB, tedy výstupní výkon $-31,5$ dBm)

- $P_{SRS|30} = -106,79$ dBm
- $P_{SRS|29} = -105,48$ dBm
- $P_{SRS|QKD} = -103,08$ dBm

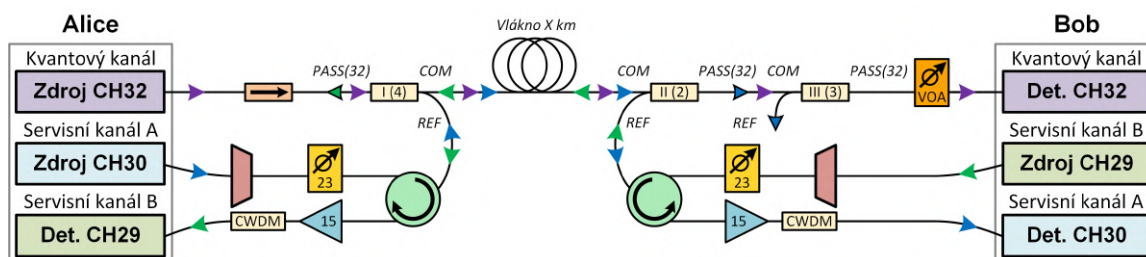
- **Pro největší zatlumení** (+20 dB, tedy výstupní výkon $-51,5$ dBm)

- $P_{SRS|30} = -126,79$ dBm
- $P_{SRS|29} = -125,48$ dBm
- $P_{SRS|QKD} = -123,08$ dBm

V souladu s očekáváním je v obou případech zpětný Ramanův rozptyl mírně vyšší, než rozptyl v dopředném směru. Celkově je však rozdíl minimální a s přibývajícím útlumem se příliš nemění. Z tohoto důvodu je tak možné rozdíl zanedbat a prohlásit výkon škodlivého Ramanova šumu v obou směrech za shodný. Jejich součtem je tedy získán dvojnásobný, škodlivý výkon (+3 dB).

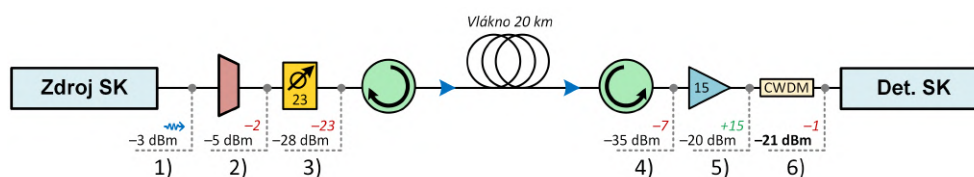
11.3 Fáze 3: Sestavení a ladění finální trasy

Posledním krokem této práce je sestavení finálního a funkčního zapojení plně využívající sdílené vlákno pro přenos kvantového a obou servisních kanálů. Na rozdíl od předchozího kroku je nyní nutné brát v potaz i funkčnost servisních kanálů, jejichž detektory mají rovněž pouze omezenou citlivost. Z tohoto důvodu bylo oproti předchozímu zapojení provedeno několik změn, jak je vidět na schématu 11.4. Zatímco většina z nich se týká servisních kanálů, ke kvantovému kanálu se vztahuje pouze jediná. Tou je přemístění útlumového článku blíže k detektoru. Zeslaben už tak není pouze CH32, ale i vzniklý šum. Toto řešení zajišťuje vyšší OSNR.



Obr. 11.4: Výsledná funkční trasa s provedenými změnami.

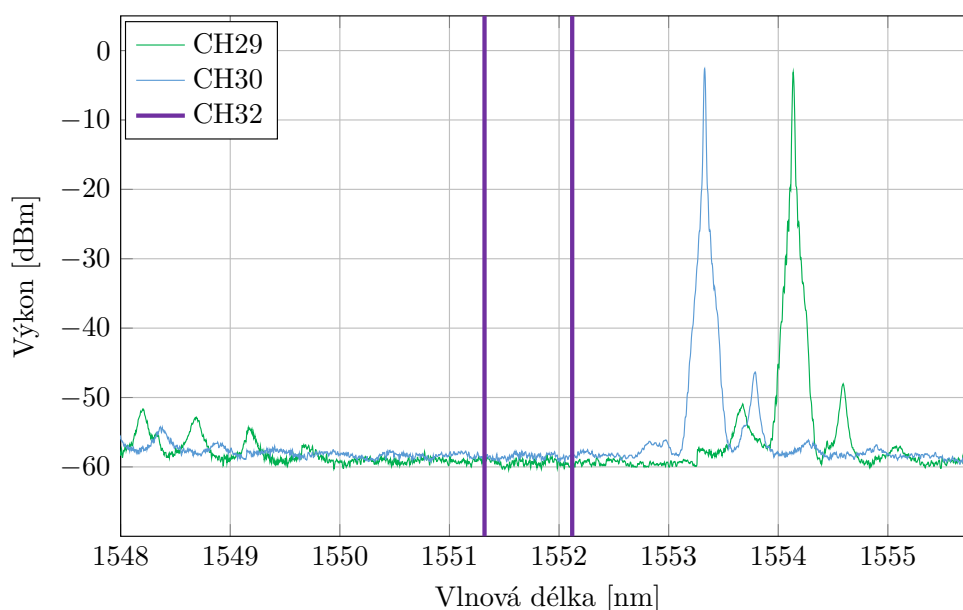
Jak již bylo naznačeno, limitujícím prvkem už není pouze kvantový kanál. Pro jeho správnou funkci je totiž nutné servisní kanály ztlumit takovým způsobem, že je jejich výsledný výkon hluboko pod požadovanou citlivostí. Z tohoto důvodu je tak nutné použít EDFA předzesilovače a prvky s nižším útlumem. Nové zapojení s analýzou výkonu jednoho servisního kanálu je uvedeno na obrázku 11.5. Útlum na DWDM filtrech je zanedbáván.



Obr. 11.5: Postupná změna výkonu servisních kanálů při průchodu trasou.

První změnou je nahrazení originálních SFP modulů. Při použití modulů Finisar byly zaznamenány problémy se synchronizací servisních kanálů. Navíc vykazovaly moduly výkonovou nestálost, kdy jejich výkon kolísal mezi +1 a -1 dBm. Z tohoto důvodu muselo být v předchozí fázi použito silnější tlumení. Nově používaná SFP od Skylane vysílají stejnou rychlostí a mají stálý výkon -3 dBm. To umožňuje odebrat 2 dB přidaného útlumu. Oba kanály byly změřeny a jejich spektra se nacházejí v grafu 11.6. Pro srovnání je rovněž fialově vyznačena oblast kvantového kanálu.

Spektrum servisních kanálů u zdroje

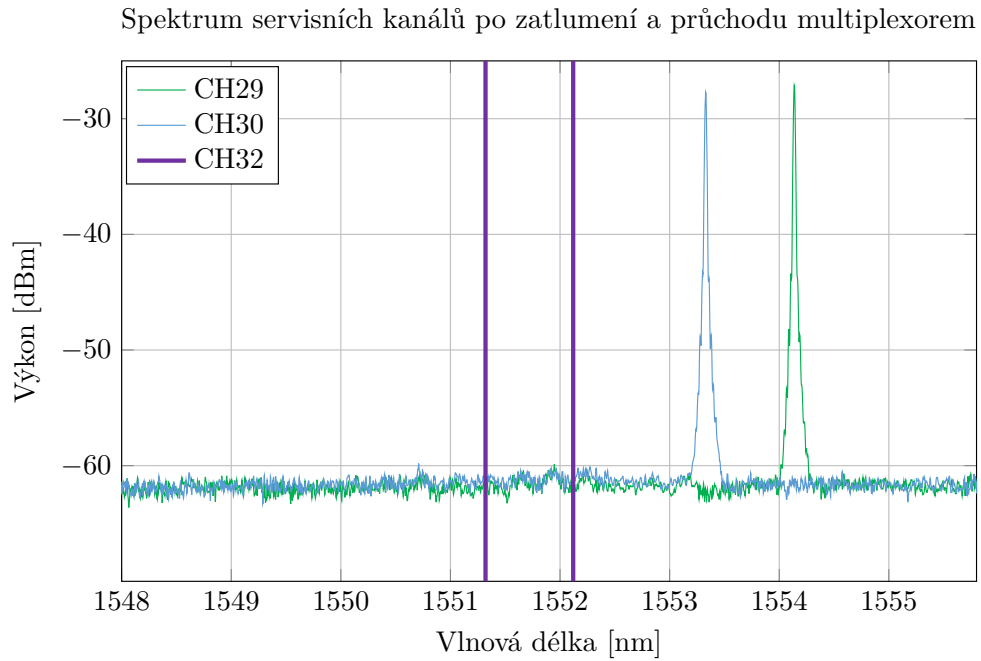


Obr. 11.6: Graf výkonu servisních kanálů u zdroje.

V původní topologii byly servisní kanály nejdříve sloučeny do jednoho vlákna pomocí multiplexorů s útlumem kolem 4,5 dB. Stejným způsobem docházelo i k jejich vydělení na opačné straně. Takové zapojení ovšem přidává do trasy vysoký útlum, což není problematické v úseku před napojením na sdílenou trasu, kde jsou servisní kanály schválně tlumeny. Po překonání sdíleného úseku je ale nutné, aby výkon servisních kanálů odpovídal alespoň citlivosti detektorů. Z tohoto důvodu není další útlum žádoucí. Oba kanály vysílají proti sobě, což umožňuje nahradit multiplexory za cirkulátory s mnohem nižším útlumem (asi 0,5 dB).

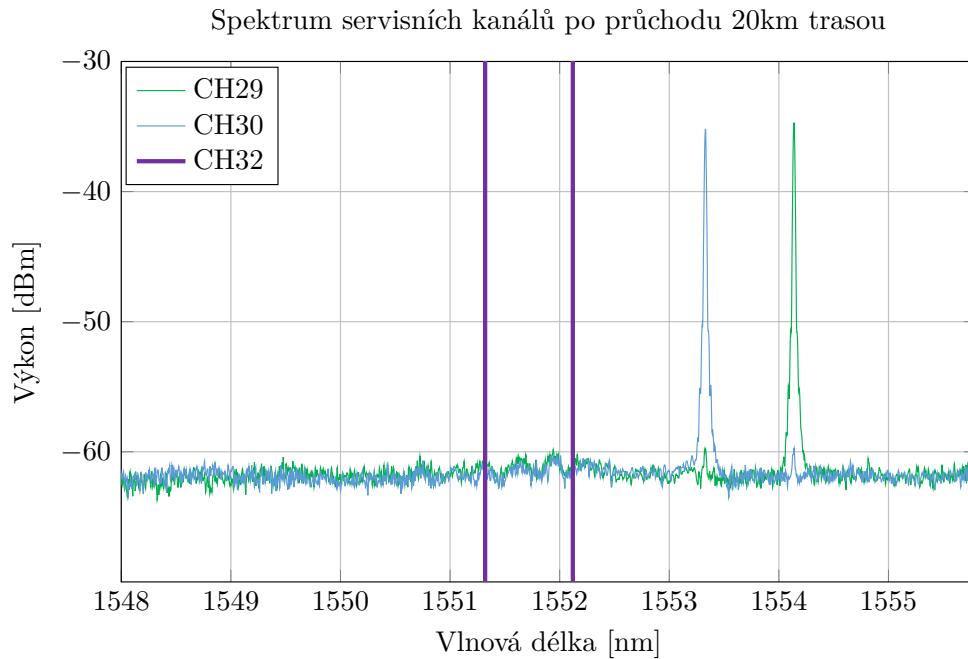
Odstranění multiplexorů ovšem vede k zašumění kvantového kanálu. Servisní kanály sice vysílají na sousedních kanálech, ale kromě užitečného signálu produkují i šum v oblasti CH32. Ten je nutné odfiltrovat ještě před sloučením všech kanálů. Z tohoto důvodu byl na začátek trasy zapojen multiplexor s útlumem cca 2 dB, který ale slouží pouze jako filtr. Útlum MUXu byl odečten od dodatečného útlumu (25 dB → 23 dB). Použitím stabilnějších SFP modulů a prvků s nižším útlumem byl získán stejný vstupní výkon jako v předchozí fázi. To je vyjádřeno výpočty níže a zobrazeno v grafu 11.7.

| |
|--|
| Původní zapojení: |
| $P_{zdroj} - A_{MUX} - A_{útlum} = 1 - 4,5 - 25 = -28,5 \text{ dBm}$ |
| Nové zapojení: |
| $P_{zdroj} - A_{MUX} - A_{útlum} - A_{cirkulátor} = -3 - 2 - 23 - 0,5 = -28,5 \text{ dBm}$ |



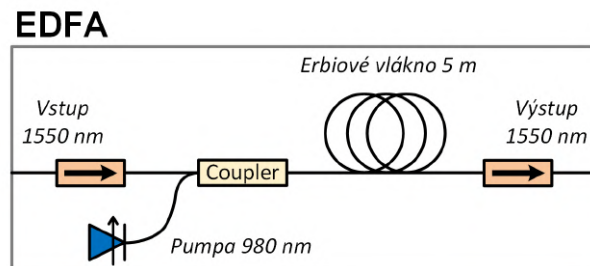
Obr. 11.7: Graf výkonu servisních kanálů po průchodu multiplexorem a zatlumení.

Jak je patrné z grafu 11.8 po průchodu sdílenou trasou a cirkulátory (dohromady útlum cca 7 dB) je výkon obou servisních kanálů mnohem nižší (-35 dBm) než je citlivost použitých SFP modulů (-24 dBm). Z tohoto důvodu byl tak na každé straně přidán EDFA zesilovač, jehož schéma se nachází na obrázku 11.9.



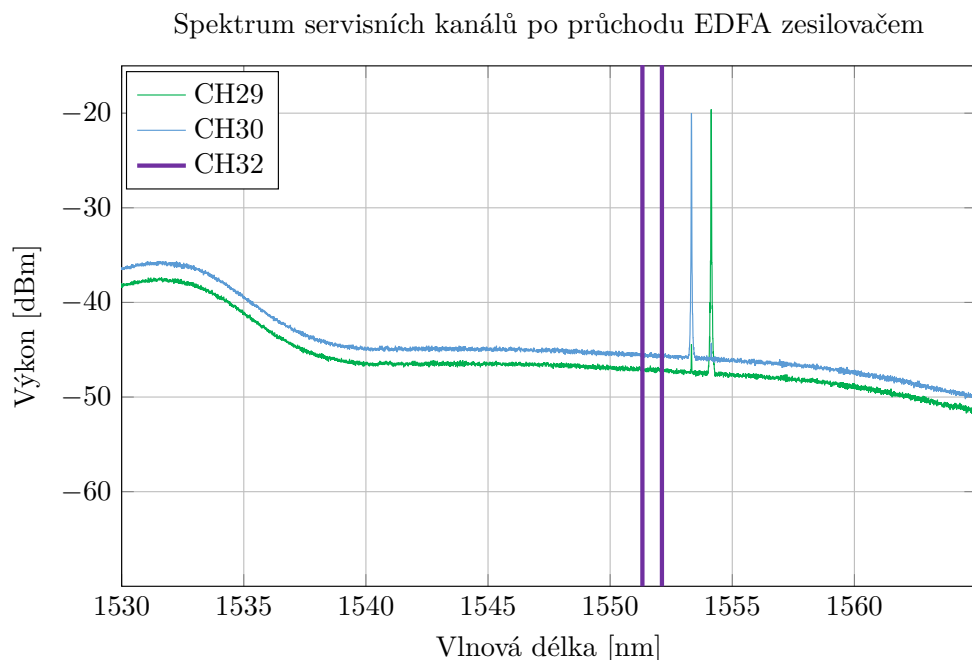
Obr. 11.8: Graf výkonu servisních kanálů po průchodu cirkulátory a sdílenou trasou.

Základem zesilovače je 5m erbiové vlákno s pumpujícím laserem ($\lambda = 980 \text{ nm}$), které zajišťují zesílení v oblasti 1550 nm. Na obou stranách jsou rovněž zapojeny izolátory. Zatímco izolátor na vstupu blokuje šum zesilovače tak, aby nerušil kvantový kanál, výstupní izolátor brání odrazům vstoupit do zesilovače z druhé strany. Celkově dochází k zisku v C-pásmu kolem 15 dB.



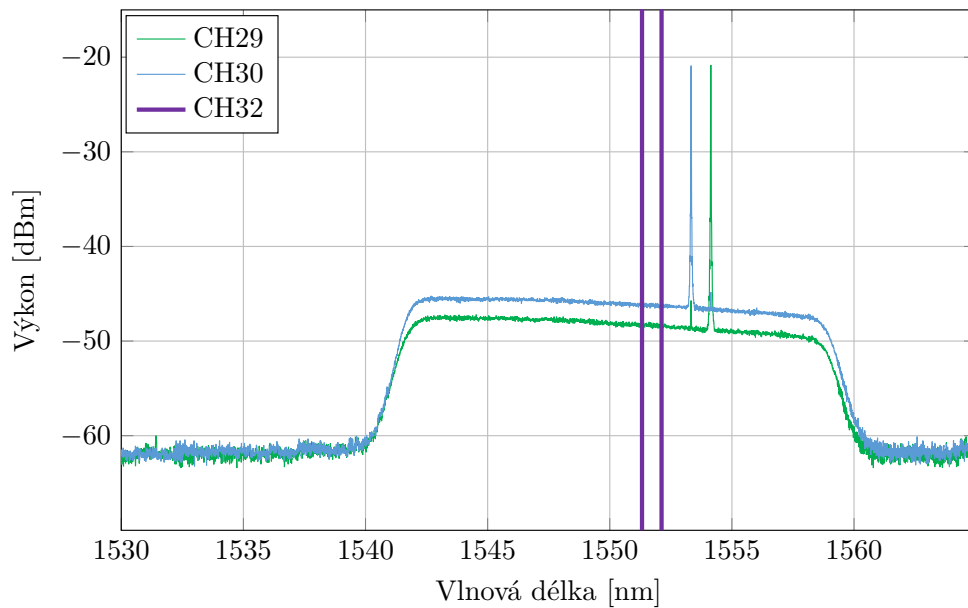
Obr. 11.9: Schéma použitých zesilovačů.

Stav obou kanálů po průchodu zesilovačem, se nachází na grafu 11.10. Z něj vyplývá, že EDFA zesiluje nejvíce v oblasti kolem 1530 nm. Jelikož detektor přímá vlnové délky v rozsahu cca 1528–1569 nm, docházelo by k příliš vysoké chybovosti dané malým odstupem signálu od šumu [124]. Z tohoto důvodu byl mezi zesilovač a samotný detektor umístěn ještě CWDM filtr operující na $\lambda = 1550 \text{ nm}$. Výsledný signál tedy vypadá tak jako v grafu 11.11.



Obr. 11.10: Graf výkonu servisních kanálů po zesílení EDFA zesilovačem o 15 dB.

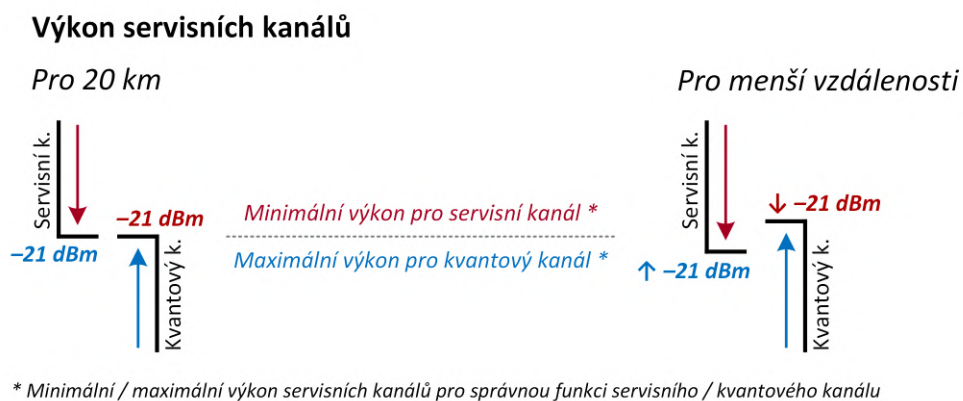
Spektrum servisních kanálů po průchodu CWDM filtrem



Obr. 11.11: Graf výkonu servisních kanálů po oříznutí signálu pomocí CWDM filtru.

11.3.1 Snižování délky trasy

Ačkoliv se citlivost použitých SFP detektorů pohybuje kolem -24 dBm, přenášený signál je silným ztlumováním a následným zesilováním natolik poškozen, že pro správný chod systému je potřeba doručit výkon alespoň -21 dBm. Na základě výše uvedeného a obrázku 11.5 vyplývá, že se shodou okolností jedná o stejný výkon, jaký je získán při minimálním ztlumení nutným pro fungování kvantového kanálu. Problematika je vysvětlena na obrázku 11.12 níže.



Obr. 11.12: Problematika tlumení servisních kanálů.

Je však nutné dodat, že se jedná o limitní stav, při kterém sice dochází k přenosu klíčů, avšak jen velmi nízkou rychlostí a pouze po omezenou dobu. Systém je totiž

nestabilní a po určité době dochází k restartování celého procesu přenosu klíčů. Se snižující se vzdáleností (útlum na trase je ale stále dorovnáván) a při použití stejných optických prvků je ovšem kvantový kanál méně rušen Ramanovým šumem a je tak schopen pracovat i při vyšším výkonu servisních kanálů. Pokud je ale výkon servisních kanálů zachován, vede to k vyšší stabilitě systému a v konečném důsledku i vyšším přenosovým rychlostem.

Trasa tedy byla s krokem 5 km čtyřikrát zkrácena a to až do stavu, kdy byly oba DWDM filtry propojeny na přímo. Útlum na trase byl ohybem vždy dorovnán na původní hodnotu (tedy cca 6 dB) podobně jako u měření 11.2.1. Tlumení servisních kanálů a rovněž jejich konečný výkon tak zůstal zachován. Rozdíly v rychlosti, chybovosti a viditelnosti je tak možné přičítat pouze Ramanovu šumu. Při jeho výpočtu bylo postupováno stejně jako v předchozích kapitolách. Hodnota vstupního výkonu do sdílené trasy byla určena jako $-28,5$ dBm, což odpovídá obrázku 11.5 (další 0,5 dB je přidán cirkulátorem). Hodnota výstupního výkonu je tak rovna $-34,5$ dBm. Výsledky měření pro různé vzdálenosti se nacházejí v tabulce 11.6

Tab. 11.6: Konečné výsledky měření.

| Trasa | Raman [dBm] | Rychlost [kbit/s] | QBER [%] | Viditelnost [%] |
|-------|-------------|-------------------|----------|-----------------|
| Přímo | ———— | 2,52 | 2,78 | 99,30 |
| 5 km | -112,75 | 2,19 | 3,57 | 98,00 |
| 10 km | -109,61 | 2,04 | 3,67 | 97,50 |
| 15 km | -107,63 | 1,69 | 3,92 | 97,50 |
| 20 km | -106,08 | 0,45 | 4,61 | 97,30 |

Zapojení bylo testováno i bez zapojeného filtračního multiplexotu. Respektive s DWDM filtry pro CH32 zapojené ve směru REF \rightarrow COM. V těchto případech byla ovšem přenosová rychlost výrazně nižší, což lze přičítat vysokému přeslechu. Použití MUXu tento problém efektivně potlačuje.

11.4 Výsledky měření

Provedené měření se skládalo ze tří na sebe navazujících fází. Nejdříve byl navržen prototyp QKD polygonu a otestována bezpečnost všech optických prvků. V následující fázi byla pomocí postupného zatlumování určena limitní hodnota výkonu, který vstupuje do sdílené trasy. Na základě tohoto měření byly do polygonu přidány další optické prvky. Mezi nejdůležitější patří zejména EDFA zesilovače servisních kanálů.

Ačkoliv se 20km délka sdíleného vlákna podepsala na rychlosti a stabilitě systému, lze konstatovat, že přenos kvantových klíčů sdíleným vláknem na tuto vzdálenost je možný. Stejně měření bylo provedeno i pro kratší vzdálenosti, na kterých byl ale zachován původní útlum. Z výsledků v tabulce 11.6 vyplývá, že se snižující se vzdáleností roste přenosová rychlost systému. Přenos je tak méně rušen Ramanovým šumem, což dokládá snižující se chybovost a zvyšující se viditelnost. Poslední fázi lze tak rovněž považovat za důkaz toho, že nelineární jevy, a zejména Ramanův šum, mají na kvantový kanál zásadní vliv.

Je pravděpodobné že, při použití dokonalejších optických prvků by mohlo jít uvažovanou trasu dále prodloužit. Předpokladem jsou např. citlivější SFP detektory a silnější EDFA zesilovače, které dovolí více zatlumit servisní kanál. Druhou navrhovanou možností je použít užší filtry (např. 50 GHz a méně), které těsněji oříznou kvantový kanál a odfiltrují tak více Ramanova šumu. Uvedený experiment využíval umístění servisních kanálů v nejnižším bodě Stokesovy oblasti šumu. Umístěním servisních kanálů do Anti-Stokesovy oblasti by ovšem mělo ještě více snížit celkový výkon škodlivého Ramanova šumu.

Závěr

V průběhu diplomové práce byly vymezeny základní pojmy nutné k pochopení základů kvantové distribuce klíčů. Zvláštní pozornost byla věnována zejména základům interferometrie. Dále byly popsány pokročilé techniky QKD založené na fázovém kódování, zejména pak protokol COW, jenž se využívá v systému Clavis³. Rozebrána byla i témata destilace klíče, kvantového hackingu a nastíněny byly i principy experimentálních schémat, jako jsou CQC nebo kvantové opakováče. Teoretická část práce se dále detailně věnovala tématu nežádoucích jevů, které mohou mít vliv na kvantový kanál. Mezi nejškodlivější z nich patří zejména Ramanův šum. Posledním tématem byla standardizace QKD sítí a její současný stav. V rámci dané kapitoly a přílohy C byly popsány organizace zabývající se standardizací technologií kvantové a postkvantové kryptografie a sestaven seznam jak aktuálně platných, tak navrhovaných standardů. Standardy popisující topologii QKD systémů byly v rámci dané kapitoly podrobně rozebrány a představen byl i příklad možné komplexní sítě zabezpečené pomocí QKD.

V rámci praktické části byl popsán samotný systém Clavis³ a dopočteny některé jeho parametry. Dále byl nastíněn aktuální stav kvantového polygonu, tedy jeho reálné zapojení v síti, a systémy pro jeho správu a monitorování. Rovněž byla provedena stručná analýza bezpečnosti jeho „klasických“ částí. Na zmíněném systému bylo provedeno několik měření. Nejdříve byl srovnán výkon systému při použití třístavového a čtyřstavového COW protokolu. Následně bylo provedeno několik testů na odolnost systému. Sledována byla rezistence proti chování, které by bylo možné zneužít k útoku odepřením služby (DoS). Jedná se o změnu polarizace a manipulaci s vláknem. Rovněž byl otestován výrobcem dodaný modul „Eva“, který simuluje pokusy o odposlech. Nejrozsáhlejší je část, která se věnuje sloučení kvantového kanálu do jednoho vlákna spolu se servisními kanály. Tato část probíhala ve třech fázích, ve kterých byl postupně připraven funkční QKD polygon a nakonec uskutečněn funkční společný přenos. Výsledky měření rovněž potvrzují, významný nežádoucí vliv Ramanova šumu na kvantový signál.

Literatura

- [1] KLÍČNÍK, Ondřej. *Kvantová distribuce klíčů přes optickou vláknovou infrastrukturu* [online]. Brno, 2021 [cit. 2022-12-02]. Dostupné z: https://www.vut.cz/studenti/zav-prace?zp_id=133531#_ga=2.58518446.5601866.1669927676-1124779664.1664226306. Bakalářská práce. Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav telekomunikací. Vedoucí práce Petr Münster.
- [2] PASCHOTTA, Rüdiger. Photons. *RP Photonics Encyclopedia* [online]. [cit. 2022-10-05]. Dostupné z: <https://www.rp-photonics.com/photons.html>
- [3] What is a photon? *EWT* [online]. [cit. 2022-10-05]. Dostupné z: <https://energywavetheory.com/photons/>
- [4] Foton. In: *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2001 [cit. 2022-10-05]. Dostupné z: <https://cs.wikipedia.org/wiki/Foton>
- [5] What is the difference between a photon and a quantum? *Quantum Physics Lady* [online]. 2019-04-13 [cit. 2022-10-05]. Dostupné z: <http://www.quantumphysicslady.org/what-is-the-difference-between-a-photon-and-a-quantum/>
- [6] The Electromagnetic Spectrum. *Government of Canada* [online]. 2015-11-20 [cit. 2022-10-05]. Dostupné z: <https://www.nrcan.gc.ca/maps-tools-publications/satellite-imagery-air-photos/remote-sensing-tutorials/introduction/electromagnetic-spectrum/14623>
- [7] FILKA, Miloslav. *Optické sítě — přednášky* [online]. Brno, 30. 11. 2007 [cit. 2022-10-06]. Dostupné z: https://optolab.utko.fekt.vut.cz/wp-content/uploads/Opticke_site_prednasky_P.pdf. Skripta. Vysoké učení technické.
- [8] PASCHOTTA, Rüdiger. Polarization of Light. *RP Photonics Encyclopedia* [online]. [cit. 2022-10-06]. Dostupné z: https://www.rp-photonics.com/polarization_of_light.html
- [9] Polarizace světla. *Fyzika 007* [online]. [cit. 2022-10-06]. Dostupné z: <https://sites.google.com/site/fyzika007/optika/polarizace-svetla>

- [10] REICHL, Jaroslav a Martin VŠETIČKA. Vlnové destičky. *Encyklopedie fyziky* [online]. 2006, 2018-04-01 [cit. 2022-10-06]. Dostupné z: <http://fyzika.jreichl.com/main.article/view/1673-vlnove-desticky>
- [11] Polarizátor. *Encyclopedia* [online]. [cit. 2022-10-06]. Dostupné z: <https://wikijii.com/wiki/Polarizer>
- [12] Circular Polarization. *Harvard Natural Sciences Lecture Demonstrations* [online]. Harvard University [cit. 2022-10-06]. Dostupné z: <https://sciencedemonstrations.fas.harvard.edu/presentations/circular-polarization>
- [13] Polarization: Linear & Circular Polarizers. *Japanistry* [online]. Japanistry [cit. 2022-10-06]. Dostupné z: <https://www.japanistry.com/polarization/>
- [14] Wave interference. In: *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2020 [cit. 2022-10-6]. Dostupné z: https://en.wikipedia.org/wiki/Wave_interference
- [15] PASCHOTTA, Rüdiger. Interference. *RP Photonics Encyclopedia* [online]. [cit. 2022-10-06]. Dostupné z: <https://www.rp-photonics.com/interference.html>
- [16] ZETIE, K. P., S. F. ADAMS a R. M. TOCKNELL. *How does a Mach—Zehnder interferometer work?* [online]. Westminster school [cit. 2022-10-06]. Dostupné z: https://www.cs.princeton.edu/courses/archive/fall06/cos576/papers/zetie_et_al_mach_zehnder00.pdf
- [17] Mach-Zehnder Interferometer. In: *YouTube* [online]. 18. 12. 2018 [cit. 2022-10-06]. Dostupné z: <https://www.youtube.com/watch?v=0HDDn1YsCYU>
- [18] CAVALCANTI, C J H, F OSTERMANN, J S NETTO a N W LIMA. Teaching wave-particle complementarity using the Virtual Mach-Zehnder Interferometer. *Revista Brasileira de Ensino de Física* [online]. 2020, **42** [cit. 2022-10-08]. ISSN 1806-9126. Dostupné z: [doi:10.1590/1806-9126-rbef-2019-0283](https://doi.org/10.1590/1806-9126-rbef-2019-0283)
- [19] Improved coherent one-way quantum key distribution for high-loss channels. *YouTube* [online]. Centre for Quantum Technologies, 2022 [cit. 2022-10-08]. Dostupné z: https://www.youtube.com/watch?v=CI55StWjp_E
- [20] SYSOJEV, Sergej Sergejevič. PETROHRADSKÁ STÁTNÍ UNIVERZITA. *Quantum Computing. Less Formulas - More Understanding* [online]. Coursera.org [cit. 2022-10-10]. Dostupné z: <https://www.coursera.org/learn/quantum-computing-lfmu>

- [21] IVANOVIC, I.D. How to differentiate between non-orthogonal states. *Physics Letters A* [online]. 1987, **123**(6), 257-259 [cit. 2022-12-06]. ISSN 03759601. Dostupné z: doi:10.1016/0375-9601(87)90222-2
- [22] GOEL, Suraj, Max TYLER, Feng ZHU, Saroch LEEDUMRONGWATTHANAKUN, Mehul MALIK a Jonathan LEACH. Simultaneously Sorting Overlapping Quantum States of Light. *Physical Review Letters* [online]. 2023, **130**(14) [cit. 2023-04-26]. ISSN 0031-9007. Dostupné z: doi:10.1103/PhysRevLett.130.143602
- [23] PIRANDOLA, Stefano, Ulrik ANDERSEN, Leonardo BANCHI, et al. Advances in Quantum Cryptography. *Advances in Optics and Photonics* [online]. [cit. 2022-10-10]. ISSN 1943-8206. Dostupné z: doi:10.1364/AOP.361502
- [24] PROTOCOLE BB84. *ALICE TO BOB: Cryptographie Quantique* [online]. Université de Nice, 2015 [cit. 2022-10-10]. Dostupné z: <http://physique.unice.fr/sem6/2014-2015/PagesWeb/PT/Tomographie/?page=bb84>
- [25] LUCAMARINI, M., K. A. PATEL, J. F. DYNES, et al. Efficient decoy-state quantum key distribution with quantified security. *Optics Express* [online]. 2013, **21**(21) [cit. 2022-10-10]. ISSN 1094-4087. Dostupné z: doi:10.1364/OE.21.024550
- [26] ENGLE, Ryan D, Logan O MAILLOUX, Michael R GRIMAILA, Douglas D HODSON, Colin V MCLAUGHLIN a Gerald BAUMGARTNER. Implementing the decoy state protocol in a practically oriented Quantum Key Distribution system-level model. *The Journal of Defense Modeling and Simulation: Applications, Methodology, Technology* [online]. 2017, **16**(1), 27-44 [cit. 2022-10-10]. ISSN 1548-5129. Dostupné z: doi:10.1177/1548512917698053
- [27] FERENCZI, Agnes, Varun NARASIMHACHAR a Norbert LÜTKENHAUS. Security proof of the unbalanced phase-encoded Bennett-Brassard 1984 protocol. *Physical Review A* [online]. 2012, **86**(4) [cit. 2022-10-10]. ISSN 1050-2947. Dostupné z: doi:10.1103/PhysRevA.86.042327
- [28] INOUE, K. Quantum key distribution technologies. *IEEE Journal of Selected Topics in Quantum Electronics* [online]. 2006, **12**(4), 888-896 [cit. 2022-10-10]. ISSN 1077-260X. Dostupné z: doi:10.1109/JSTQE.2006.876606
- [29] STUCKI, Damien, Nicolas BRUNNER, Nicolas GISIN, Valerio SCARANI a Hugo ZBINDEN. Fast and simple one-way quantum key distribution. *Applied Physics Letters* [online]. 2005, **87**(19) [cit. 2022-10-10]. ISSN 0003-6951. Dostupné z: doi:10.1063/1.2126792

- [30] GISIN, Nicolas, Gregoire RIBORDY, Hugo ZBINDEN, Damien STUCKI, Nicolas BRUNNER a Valerio SCARANI. Towards practical and fast Quantum Cryptography. *Arxiv* [online]. [cit. 2022-11-20]. Dostupné z: <https://arxiv.org/abs/quant-ph/0411022>
- [31] STUCKI, Damien, Nicolas BRUNNER, Nicolas GISIN, Valerio SCARANI a Hugo ZBINDEN. Fast and simple one-way quantum key distribution. *Applied Physics Letters* [online]. 2005, **87**(19) [cit. 2022-11-20]. ISSN 0003-6951. Dostupné z: doi:10.1063/1.2126792
- [32] GAO, Rui-Qi, Yuan-Mei XIE, Jie GU, Wen-Bo LIU, Chen-Xun WENG, Bing-Hong LI, Hua-Lei YIN a Zeng-Bing CHEN. Simple security proof of coherent one-way quantum key distribution. *Optics Express* [online]. 2022, **30**(13) [cit. 2022-11-20]. ISSN 1094-4087. Dostupné z: doi:10.1364/OE.461669
- [33] LAVIE, Lavie a Charles LIM. Improved coherent one-way quantum key distribution for high-loss channels. *Arxiv* [online]. 2022-06-20 [cit. 2022-11-20]. Dostupné z: <https://arxiv.org/pdf/2206.08490.pdf>
- [34] BRANCIARD, Cyril, Nicolas GISIN a Valerio SCARANI. Upper bounds for the security of two distributed-phase reference protocols of quantum cryptography. *New Journal of Physics* [online]. 2008, **10**(1) [cit. 2022-11-20]. ISSN 1367-2630. Dostupné z: doi:10.1088/1367-2630/10/1/013031
- [35] Quantum Repeaters: Key Distillation. *QuRep* [online]. [cit. 2022-11-20]. Dostupné z: <http://www.quantumrepeaters.eu/quantumrepeaters.eu/index.php/component/content/article/75-distillation/>
- [36] CONSTANTIN, Jeremy, Raphael HOULMANN, Nicholas PREYSS, Nino WALENTA, Hugo ZBINDEN, Pascal JUNOD a Andreas BURG. An FPGA-Based 4 Mbps Secret Key Distillation Engine for Quantum Key Distribution Systems. *Journal of Signal Processing Systems* [online]. 2017, **86**(1), 1-15 [cit. 2022-11-20]. ISSN 1939-8018. Dostupné z: doi:10.1007/s11265-015-1086-1
- [37] WALENTA, N, A BURG, D CASELUNGHE, et al. A fast and versatile quantum key distribution system with hardware key distillation and wavelength multiplexing. *New Journal of Physics* [online]. 2014, **16**(1) [cit. 2022-12-04]. ISSN 1367-2630. Dostupné z: doi:10.1088/1367-2630/16/1/013047
- [38] LI, Qiong, Bing-Ze YAN, Hao-Kun MAO, Xiao-Feng XUE, Qi HAN a Hong GUO. High-Speed and Adaptive FPGA-Based Privacy Amplification in Quantum Key Distribution. *IEEE Access* [online]. 2019, **7**, 21482-21490 [cit. 2022-12-04]. ISSN 2169-3536. Dostupné z: doi:10.1109/ACCESS.2019.2896259

- [39] Low Density Parity Check Codes: definition, properties and introduction to protograph construction. *YouTube* [online]. NPTEL-NOC IITM [cit. 2022-11-20]. Dostupné z: <https://www.youtube.com/watch?v=bAZnP4kdb44>
- [40] SHOKROLLAHI, Amin. LDPC Codes: An Introduction. *Carnegie Mellon University* [online]. 2003-04-02 [cit. 2022-11-20]. Dostupné z: <https://www.cs.cmu.edu/afs/cs/project/pscico-guyb/realworld/www/slidesS14/ldpc-amin.pdf>
- [41] NAKASSIS, Anastase a Alan MINK. LDPC error correction in the context of Quantum Key Distribution*. *NIST* [online]. [cit. 2022-11-20]. Dostupné z: https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=910418
- [42] WANG, Liu-Jun, Kai-Yi ZHANG, Jia-Yong WANG, et al. Experimental authentication of quantum key distribution with post-quantum cryptography. *Npj Quantum Information* [online]. 2021, **7**(1) [cit. 2022-11-20]. ISSN 2056-6387. Dostupné z: doi:10.1038/s41534-021-00400-7
- [43] BIHAM, Eli, Michel BOYER, P. Oscar BOYKIN, Tal MOR a Vwani ROYCHOWDHURY. A Proof of the Security of Quantum Key Distribution. *Journal of Cryptology* [online]. 2006, **19**(4), 381-439 [cit. 2022-11-20]. ISSN 0933-2790. Dostupné z: doi:10.1007/s00145-005-0011-3
- [44] QCrypt 2020: Experimental Measurement-Device-Independent QKD with Uncharacterized Sources. In: *YouTube* [online]. QCrypt conference, 3. 8. 2020 [cit. 2022-11-20]. Dostupné z: https://www.youtube.com/watch?v=Gif4eh5lenA&ab_channel=QCrypt-conference
- [45] Quantum Hacking - Evan Meyer-Scott - QCSYS 2011. In: *YouTube* [online]. Institute for Quantum Computing, 11. 11. 2011 [cit. 2022-11-20]. Dostupné z: https://www.youtube.com/watch?v=C1wOIXMV14k&abq_channel=InstituteforQuantumComputing
- [46] LO, Hoi-Kwong, Xiongfeng MA a Kai CHEN. Decoy State Quantum Key Distribution. *Physical Review Letters* [online]. 2005, **94**(23) [cit. 2022-11-20]. ISSN 0031-9007. Dostupné z: doi:10.1103/PhysRevLett.94.230504
- [47] Optics. Beam splitter attack and decoy protocol. *YouTube* [online]. Physics with Andrés Aragonés [cit. 2022-11-20]. Dostupné z: <https://www.youtube.com/watch?v=uzj6AxERzz8>

- [48] Beam Splitting and Photon Number Splitting Attack on Micius Satellite. *YouTube* [online]. Sparrow Tian [cit. 2022-11-20]. Dostupné z: <https://www.youtube.com/watch?v=QmcpSVow2x8>
- [49] TRÉNYI, Róbert a Marcos CURTY. Zero-error attack against coherent-one-way quantum key distribution. *New Journal of Physics* [online]. 2021, **23**(9) [cit. 2022-11-20]. ISSN 1367-2630. Dostupné z: doi:10.1088/1367-2630/ac1e41
- [50] CURTY, Marcos. Foiling zero-error attacks against coherent-one-way quantum key distribution. *Physical Review A* [online]. 2021, **104**(6) [cit. 2022-12-06]. ISSN 2469-9926. Dostupné z: doi:10.1103/PhysRevA.104.062417
- [51] GONZÁLEZ-PAYO, Javier, Róbert TRÉNYI, Weilong WANG a Marcos CURTY. Upper Security Bounds for Coherent-One-Way Quantum Key Distribution. *Physical Review Letters* [online]. 2020, **125**(26) [cit. 2022-11-20]. ISSN 0031-9007. Dostupné z: doi:10.1103/PhysRevLett.125.260510
- [52] Improved coherent one-way quantum key distribution for high-loss channels. *YouTube* [online]. Centre for Quantum Technologies [cit. 2022-11-20]. Dostupné z: https://www.youtube.com/watch?v=CI55StWjp_E
- [53] PACHER, C, A ABIDIN, T LORÜNSER, M PEEV, R URSIN, A ZEILINGER a J LARSSON. Attacks on quantum key distribution protocols that employ non-ITS authentication. *Arxiv* [online]. [cit. 2022-11-20]. Dostupné z: <https://arxiv.org/pdf/1209.0365.pdf>
- [54] LUCAMARINI, M., I. CHOI, M.-B. WARD, J.-F. DYNES, Z.-L. YUAN a A.-J. SHIELDS. Practical Security Bounds Against the Trojan-Horse Attack in Quantum Key Distribution. *Physical Review X* [online]. 2015, **5**(3) [cit. 2022-11-20]. ISSN 2160-3308. Dostupné z: doi:10.1103/PhysRevX.5.031030
- [55] GISIN, N., S. FASEL, B. KRAUS, H. ZBINDEN a G. RIBORDY. Trojan-horse attacks on quantum-key-distribution systems. *Physical Review A* [online]. 2006, **73**(2) [cit. 2022-11-20]. ISSN 1050-2947. Dostupné z: doi:10.1103/PhysRevA.73.022320
- [56] WEIER, Henning, Harald KRAUSS, Markus RAU, Martin FÜRST, Sebastian NAUERTH a Harald WEINFURTER. Quantum eavesdropping without interception: an attack exploiting the dead time of single-photon detectors. *New Journal of Physics* [online]. 2011, **13**(7) [cit. 2022-11-20]. ISSN 1367-2630. Dostupné z: doi:10.1088/1367-2630/13/7/073024

- [57] LYDERSEN, Lars, Carlos WIECHERS, Christoffer WITTMANN, Dominique ELSER, Johannes SKAAR a Vadim MAKAROV. Hacking commercial quantum cryptography systems by tailored bright illumination. *Nature Photonics* [online]. 2010, **4**(10), 686-689 [cit. 2022-11-20]. ISSN 1749-4885. Dostupné z: doi:10.1038/nphoton.2010.214
- [58] DENNY, Travis. Faked states attack and quantum cryptography protocols. *Arxiv* [online]. Oklahoma State University, 2011-12-13 [cit. 2022-11-20]. Dostupné z: <https://arxiv.org/pdf/1112.2230.pdf>
- [59] QI, B., C.-H. F. FUNG, H.-K. LO a F.-X. MA. Time-shift attack in practical quantum cryptosystems. *Quantum Information and Computation* [online]. 2007, **7**(1&2), 73-82 [cit. 2022-11-20]. ISSN 15337146. Dostupné z: doi:10.26421/QIC7.1-2-3
- [60] ZHAO, Yi, Chi-Hang Fred FUNG, Bing QI, Christine CHEN a Hoi-Kwong LO. Quantum hacking: Experimental demonstration of time-shift attack against practical quantum-key-distribution systems. *Physical Review A* [online]. 2008, **78**(4) [cit. 2022-11-20]. ISSN 1050-2947. Dostupné z: doi:10.1103/PhysRevA.78.042333
- [61] XU, Feihu, Bing QI a Hoi-Kwong LO. Experimental demonstration of phase-remapping attack in a practical quantum key distribution system. *New Journal of Physics* [online]. 2010, **12**(11) [cit. 2022-11-20]. ISSN 1367-2630. Dostupné z: doi:10.1088/1367-2630/12/11/113026
- [62] FUNG, Chi-Hang Fred, Bing QI, Kiyoshi TAMAKI a Hoi-Kwong LO. Phase-remapping attack in practical quantum-key-distribution systems. *Physical Review A* [online]. 2007, **75**(3) [cit. 2022-11-20]. ISSN 1050-2947. Dostupné z: doi:10.1103/PhysRevA.75.032314
- [63] WIECHERS, C, L LYDERSEN, C WITTMANN, D ELSER, J SKAAR, Ch MARQUARDT, V MAKAROV a G LEUCHS. After-gate attack on a quantum cryptosystem. *New Journal of Physics* [online]. 2011, **13**(1) [cit. 2022-11-20]. ISSN 1367-2630. Dostupné z: doi:10.1088/1367-2630/13/1/013043
- [64] Interaction-free measurement. In: *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2022 [cit. 2022-11-20]. Dostupné z: https://en.wikipedia.org/wiki/Interaction-free_measurement
- [65] The Quantum Bomb-Tester!. *YouTube* [online]. Up and Atom [cit. 2022-11-20]. Dostupné z: <https://www.youtube.com/watch?v=wiW7jhdKDVA>

- [66] NOH, Tae-Gon. Counterfactual Quantum Cryptography. *Physical Review Letters* [online]. 2009, **103**(23) [cit. 2022-11-20]. ISSN 0031-9007. Dostupné z: doi:10.1103/PhysRevLett.103.230501
- [67] BUBNÍK, Lukáš, Petr MAZUCH a Jiří KLAJBL. Parametry optických vláken. *Optoelektrotechnika* [online]. Code Creator, s.r.o [cit. 2022-10-14]. Dostupné z: <https://publi.cz/books/185/06.html>
- [68] The Basics: Optical attenuators. *Edge Optical Solutions* [online]. [cit. 2022-10-15]. Dostupné z: https://edgeoptic.com/kb_article/the-basics-optical-attenuators/
- [69] IRVING. The Ultimate Guide to Fiber Optic Attenuators. *FS/community* [online]. 2021-10-29 [cit. 2022-10-15]. Dostupné z: <https://community.fs.com/blog/basics-of-fiber-optic-attenuator.html>
- [70] PASCHOTTA, Rüdiger. Optical Attenuators. *RP Photonics Encyclopedia* [online]. [cit. 2022-10-15]. Dostupné z: https://www.rp-photonics.com/optical_attenuators.html
- [71] MEMS Variable Optical Attenuators. *DiCon fiberoptics* [online]. [cit. 2022-10-15]. Dostupné z: https://www.diconfiberoptics.com/products/mems_variable_optical_attenuators.php
- [72] Difference between Optical Repeater vs Optical Amplifier. *RF Wireless World* [online]. [cit. 2022-10-16]. Dostupné z: <https://www.rfwireless-world.com/Terminology/Optical-Repeater-vs-Optical-Amplifier.html>
- [73] LUCKI, Michal. Optické zesilovače — EDFA, Raman a polovodičové zesilovače. *Nové trendy v elektronických komunikacích: Optické systémy a sítě* [online]. [cit. 2022-10-16]. Dostupné z: <https://publi.cz/books/241/04.html>
- [74] Pasivní optické zesilovače: EDFA, SOA a RFA. *FOCC Fiber Optic CO* [online]. 2019-03-14 [cit. 2022-10-16]. Dostupné z: <http://m.cz.opticalpatchcable.com/news/passive-optical-amplifiers-edfa-soa-and-rfa-24306741.html>
- [75] PASCHOTTA, Rüdiger. Fiber Amplifiers. *RP Photonics Encyclopedia* [online]. [cit. 2022-10-16]. Dostupné z: https://www.rp-photonics.com/fiber_amplifiers.html

- [76] Basic Knowledge About EDFA. *Fiber Optic Network Products* [online]. 2016-06-08 [cit. 2022-10-16]. Dostupné z: <https://www.fiberopticsshare.com/basic-knowledge-edfa.html>
- [77] ITU-T Y.3800 (10/2019). *Overview on networks supporting quantum key distribution*. 2019-11-20. Ženeva: ITU-T, 2019 [cit. 2022-10-16]. Dostupné také z: <https://www.itu.int/rec/T-REC-Y.3800-201910-I>
- [78] SIMON, Garrett, Blake HUFF, William MEIER, Logan MAILLOUX a Lee HARRELL. Quantification of the Impact of Photon Distinguishability on Measurement-Device- Independent Quantum Key Distribution. *Electronics* [online]. 2018, **7**(4) [cit. 2022-10-18]. ISSN 2079-9292. Dostupné z: [doi:10.3390/electronics7040049](https://doi.org/10.3390/electronics7040049)
- [79] Quantum Repeaters. *QuReP* [online]. 2010 [cit. 2022-10-18]. Dostupné z: <http://www.quantumrepeaters.eu/quantumrepeaters.eu/index.php/qcomm/quantum-repeaters/#Q3rep>
- [80] WANG, Shuang, Zhen-Qiang YIN, De-Yong HE, et al. Twin-field quantum key distribution over 830-km fibre. *Nature Photonics* [online]. 2022, **16**(2), 154-161 [cit. 2022-10-18]. ISSN 1749-4885. Dostupné z: [doi:10.1038/s41566-021-00928-2](https://doi.org/10.1038/s41566-021-00928-2)
- [81] WEBER, Markus. *Experimental Quantum Memory Applications and Demonstration of an Elementary Quantum Repeater Link with Entangled Light-Matter Interfaces* [online]. Ludwig-Maximilians-Universität München, 2012, 102 [cit. 2022-10-18]. Dostupné z: https://www.researchgate.net/profile/Markus-Weber-3/publication/283122108_Experimental_Quantum_Memory_Applications_and_Demonstration_of_an_Elementary_Quantum_Repeater_Link_with_Entangled_Light-Matter_Interfaces/links/562bb50b08ae04c2aeb3565a/Experimental-Quantum-Memory-Applications-and-Demonstration-of-an-Elementary-Quantum-Repeater-Link-with-Entangled-Light-Matter-Interfaces.pdf
- [82] New quantum repeaters could enable a scalable quantum internet. *Physics world* [online]. 2021-06-11 [cit. 2022-10-18]. Dostupné z: <https://physicsworld.com/a/new-quantum-repeaters-could-enable-a-scalable-quantum-internet/>
- [83] PASCHOTTA, Rüdiger. Absorptance. *RP Photonics Encyclopedia* [online]. [cit. 2023-05-05]. Dostupné z: <https://www.rp-photonics.com/absorptance.html>

- [84] PASCHOTTA, Rüdiger. Transmittance. *RP Photonics Encyclopedia* [online]. [cit. 2023-05-05]. Dostupné z: <https://www.rp-photonics.com/transmittance.html>
- [85] PASCHOTTA, Rüdiger. Absorption Coefficient. *RP Photonics Encyclopedia* [online]. [cit. 2023-05-05]. Dostupné z: https://www.rp-photonics.com/absorption_coefficient.html
- [86] Mnohovidová vlákna. *ELUC* [online]. [cit. 2022-10-14]. Dostupné z: <https://eluc.ikap.cz/verejne/lekce/824>
- [87] MLEJNEK, Michal, Nikolay KALITEEVSKIY a Dan NOLAN. Reducing spontaneous Raman scattering noise in high quantum bit rate QKD systems over optical fiber. *Arxiv.org* [online]. 2017 [cit. 2022-10-14]. Dostupné z: <https://arxiv.org/abs/1712.05891>
- [88] PASCHOTTA, Rüdiger. Polarization Mode Dispersion. *RP Photonics Encyclopedia* [online]. [cit. 2022-10-14]. Dostupné z: https://www.rp-photonics.com/polarization_mode_dispersion.html
- [89] Population inversion. *FiberLabs Inc.* [online]. 2021-07-05 [cit. 2022-10-18]. Dostupné z: <https://www.fiberlabs.com/glossary/population-inversion/>
- [90] Laser: Princip. *Czechlasers.cz: Vzdělávací web o laseru* [online]. [cit. 2022-10-18]. Dostupné z: <https://czechlasers.cz/studovna/laser-2/>
- [91] PASCHOTTA, Rüdiger. Amplified Spontaneous Emission. *RP Photonics Encyclopedia* [online]. [cit. 2022-10-18]. Dostupné z: https://www.rp-photonics.com/amplified_spontaneous_emission.html
- [92] POLSON, R.C. a Z.V. VARDENY. Laser Action in Organic Semiconductors. In: *Comprehensive Nanoscience and Technology* [online]. Elsevier, 2011, 2011, s. 41-71 [cit. 2022-10-18]. ISBN 9780123743961. Dostupné z: doi:10.1016/B978-0-12-374396-1.00017-9
- [93] HUI, Rongqing a Maurice O'SULLIVAN. Characterization of Optical Devices. In: *Fiber Optic Measurement Techniques* [online]. Elsevier, 2009, 2009, s. 259-363 [cit. 2022-10-18]. ISBN 9780123738653. Dostupné z: doi:10.1016/B978-0-12-373865-3.00003-3
- [94] QI, Bing, Wen ZHU, Li QIAN a Hoi-Kwong LO. Feasibility of quantum key distribution through a dense wavelength division multiplexing network. *New Journal of Physics* [online]. 2010, **12**(10) [cit. 2022-10-18]. ISSN 1367-2630. Dostupné z: doi:10.1088/1367-2630/12/10/103042

- [95] PASCHOTTA, Rüdiger. Kerr Effect. *RP Photonics Encyclopedia* [online]. [cit. 2022-10-18]. Dostupné z: https://www.rp-photonics.com/kerr_effect.html
- [96] PASCHOTTA, Rüdiger. Self-phase Modulation. *RP Photonics Encyclopedia* [online]. [cit. 2022-10-18]. Dostupné z: https://www.rp-photonics.com/self_phase_modulation.html
- [97] PASCHOTTA, Rüdiger. Cross-phase Modulation. *RP Photonics Encyclopedia* [online]. [cit. 2022-10-18]. Dostupné z: https://www.rp-photonics.com/cross_phase_modulation.html
- [98] PASCHOTTA, Rüdiger. Four-wave Mixing. *RP Photonics Encyclopedia* [online]. [cit. 2022-10-18]. Dostupné z: https://www.rp-photonics.com/four_wave_mixing.html
- [99] SCHNEIDER, Thomas. Four-Wave-Mixing (FWM). In: SCHNEIDER, Thomas. *Nonlinear Optics in Telecommunications* [online]. Berlin, Heidelberg: Springer Berlin Heidelberg, 2004, 2004, s. 167-200 [cit. 2022-10-18]. Advanced Texts in Physics. ISBN 978-3-642-05772-4. Dostupné z: doi:10.1007/978-3-662-08996-5_7
- [100] ERAERDS, P, N WALENTA, M LEGRÉ, N GISIN a H ZBINDEN. Quantum key distribution and 1-Gbps data encryption over a single fibre. *New Journal of Physics* [online]. 2010, **12**(6) [cit. 2022-10-18]. ISSN 1367-2630. Dostupné z: doi:10.1088/1367-2630/12/6/063027
- [101] PETERS, N A, P TOLIVER, T E CHAPURAN, et al. Dense wavelength multiplexing of 1550-nm QKD with strong classical channels in reconfigurable networking environments. *New Journal of Physics* [online]. 2009, **11**(4) [cit. 2022-10-18]. ISSN 1367-2630. Dostupné z: doi:10.1088/1367-2630/11/4/045012
- [102] MLEJNEK, M, N KALITEEVSKIY a D NOLAN. *Reducing spontaneous Raman scattering noise in high quantum bit rate QKD systems over optical fiber* [online]. Arxiv [cit. 2022-10-18]. Dostupné z: <https://arxiv.org/abs/1712.05891>
- [103] Scattering. In: *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2001-2022 [cit. 2022-10-18]. Dostupné z: <https://en.wikipedia.org/wiki/Scattering>
- [104] Pružný a nepružný rozptyl. *WikiSkripta* [online]. [cit. 2022-10-18]. Dostupné z: https://www.wikiskripta.eu/w/Pru%C5%BEn%C3%BD_a_nepru%C5%BEn%C3%BD_rozptyl

- [105] Elastic scattering. In: *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2022 [cit. 2022-10-18]. Dostupné z: https://en.wikipedia.org/wiki/Elastic_scattering
- [106] VAN BIEZEN, Michel. MODERN PHYSICS 2: ATOMIC AND NUCLEAR PHYSICS, PARTICLE PHYSICS. *YouTube* [online]. [cit. 2022-10-18]. Dostupné z: https://www.youtube.com/playlist?list=PLX2gX-ftPVXVqAS_q3OfJDmPn8-EQld_r
- [107] MAŇÁK, Roman. Rayleighův a Mieův rozptyl. *Optické úkazy v atmosféře* [online]. 2012-04-24 [cit. 2022-10-18]. Dostupné z: <http://ukazy.astro.cz/Rayleighuv-a-Mieuv-rozptyl.php>
- [108] LOCKWOOD, David J. Rayleigh and Mie Scattering. In: LUO, Ming Ronnier, ed. *Encyclopedia of Color Science and Technology* [online]. New York, NY: Springer New York, 2016, 2016-7-5, s. 1097-1107 [cit. 2022-10-18]. ISBN 978-1-4419-8070-0. Dostupné z: doi:10.1007/978-1-4419-8071-7_218
- [109] REICHL, Jaroslav. [Http://fyzika.jreichl.com/main.article/view/1671-rozptyl-svetla-v-optickem-vlaknu](http://fyzika.jreichl.com/main.article/view/1671-rozptyl-svetla-v-optickem-vlaknu). *Encyklopedie fyziky* [online]. [cit. 2022-10-18]. Dostupné z: <http://fyzika.jreichl.com/main.article/view/1671-rozptyl-svetla-v-optickem-vlaknu>
- [110] NUTT, David. Topic 7: Raman scattering. *YouTube* [online]. University of Reading [cit. 2022-10-18]. Dostupné z: https://www.youtube.com/watch?v=1_IqMY6t6w0
- [111] Raman Basics. *YouTube* [online]. ThermoScientific [cit. 2022-10-18]. Dostupné z: <https://www.youtube.com/watch?v=Gok7jRuer1k>
- [112] ERIKSSON, Tobias A., Takuya HIRANO, Benjamin J. PUTTNAM, et al. Wavelength division multiplexing of continuous variable quantum key distribution and 18.3 Tbit/s data channels. *Communications Physics* [online]. 2019, **2**(1) [cit. 2022-10-18]. ISSN 2399-3650. Dostupné z: doi:10.1038/s42005-018-0105-5
- [113] LIN, Rui a Jiajia CHEN. Minimizing Spontaneous Raman Scattering Noise for Quantum Key Distribution in WDM Networks. In: *Optical Fiber Communication Conference (OFC) 2021* [online]. Washington, D.C: Optica Publishing Group, 2021, 2021, F4E.6- [cit. 2022-10-18]. ISBN 978-1-943580-86-6. Dostupné z: doi:10.1364/OFC.2021.F4E.6
- [114] DYNES, James F., Winci W-S. TAM, Alan PLEWS, et al. Ultra-high bandwidth quantum secured data transmission. *Scientific Reports* [online]. 2016, **6**(1) [cit. 2022-10-18]. ISSN 2045-2322. Dostupné z: doi:10.1038/srep35149

- [115] Tlumení optického vlákna. *Delta.eu* [online]. [cit. 2022-10-18]. Dostupné z: https://shopdelta.eu/tlumeni-optickeho-vlakna_18_aid811.html
- [116] *ITU-T: ITU Telecommunication Standardization Sector* [online]. Ženeva: ITU, 2023 [cit. 2023-05-06]. Dostupné z: <https://www.itu.int>
- [117] *ETSI: European Telecommunications Standards Institute* [online]. Sophia Antipolis: ETSI, 2023 [cit. 2023-05-06]. Dostupné z: <https://www.etsi.org>
- [118] *IEEE: Institute of Electrical and Electronics Engineers* [online]. New York: IEEE, 2023 [cit. 2023-05-06]. Dostupné z: <https://www.ieee.org>
- [119] *ISO: International Organization for Standardization* [online]. Ženeva: IEC, 2023 [cit. 2023-05-06]. Dostupné z: <https://www.iso.org/home.html>
- [120] *IEC: International Electrotechnical Commission* [online]. Ženeva: IEC, 2023 [cit. 2023-05-06]. Dostupné z: <https://iec.ch/homepage>
- [121] *DWDM 2.7G SFP Transceiver: Datasheet* [online]. 2015 [cit. 2023-05-05]. Dostupné z: https://www.mouser.com/datasheet/2/610/finisar_fwlf1632xx_dwdm_2.7gsfp_sfp_optical_transc-934543.pdf
- [122] FROLO, Peter. Základní principy fungování softwarově definovaných sítí (SDN). *ROOT.CZ* [online]. 2019-08-29 [cit. 2023-05-06]. Dostupné z: <https://www.root.cz/clanky/zakladni-principy-fungovani-softwarove-definovanych-siti-sdn/>
- [123] A Brief Guide to Quantum Encryption vs. Post-Quantum Cryptography. *QuantumXchange* [online]. [cit. 2023-05-06]. Dostupné z: <https://quantumxc.com/blog/quantum-encryption-vs-post-quantum-cryptography-infographic/>
- [124] *SPDTU080100D — SFP+ Dual Fiber DWDM Tunable: Datasheet* [online]. [cit. 2023-05-05]. Dostupné z: <https://portal.skylaneoptics.com/datasheet/SPDTU080100D.pdf>
- [125] ZAVITSANOS, Dimitris, Argiris NTANOS, Panagiotis TOUMASIS, et al. Co-existence Studies for DV-QKD Integration in Deployed RAN Infrastructure. In: *2022 International Workshop on Fiber Optics in Access Networks (FOAN)* [online]. IEEE, 2022, 2022-10-11, s. 6-9 [cit. 2023-05-01]. ISBN 978-1-6654-6503-8. Dostupné z: doi:10.1109/FOAN56774.2022.9939691

Seznam symbolů a zkratek

| | |
|----------------|---|
| APC/UPC | Angled / Ultra Physical Contact (konektor) |
| APD | Avalanche photodiode |
| API | Application Programming Interface |
| ASE | Amplified Spontaneous Emission |
| B92 | Bennett roku 1992 (protokol) |
| BB84 | Bennett a Brassard roku 1984 (protokol) |
| BBM92 | Bennett, Brassard a Mermin roku 1992 (protokol) |
| BS | Beam-splitting (útok) |
| BSM | Bell State Measurement |
| C band | Conventional band |
| COW | Coherent One-way (protokol) |
| CQC | Counterfactual Quantum Cryptography |
| dB | Decibel |
| dBm | Decibel-miliwatt |
| DoS | Denial of Service (útok) |
| DPR | Distributed Phase-Reference (protokoly) |
| DWDM | Dense Wavelength-Division Multiplexing |
| E91 | Ekert roku 1991 (protokol) |
| E band | Extended band |
| EDFA | Erbium Doped Fiber Amplifier |
| ETSI | European Telecommunications Standards Institute |
| FC | Ferrule Connector |
| FEKT | Fakulta elektrotechniky a komunikačních technologií |
| FOA | Fixed Optical Attenuator |

| | |
|---------------|--|
| FWM | Four-wave Mixing |
| GGH | Goldreich, Goldwasser, Halevi (šifra) |
| GHz | Gigahertz |
| GWN | Gateway Node |
| Hz | Hertz |
| IDQ | ID Quantique |
| IEC | International Electrotechnical Commission |
| IEEE | Institute of Electrical and Electronics Engineers |
| ISK | Initialization Shared Key |
| ISO | International Organization for Standardization |
| ITU-T | International Telecommunication Union Telecommunication Standardization Sector |
| IWN | Interworking Node |
| J | Joule |
| kb | Kilobit |
| km | Kilometr |
| KM | Key Management |
| KMA | Key Management Agent |
| KME | Key Management Entity |
| KMS | Key Management System |
| KSA | Key Supply Agent |
| L band | Long band |
| LC | Lucent Connector |
| LDPC | Low-density Parity Check |
| LM05 | Lucamarini a Mancini roku 2005 (protokol) |

| | |
|----------------|--|
| m | Metr |
| MDI-QKD | Measurement-device Independent QKD |
| MED | Minimum Error Discrimination |
| MITM | Man In The Middle (útok) |
| mm | Milimetr |
| mW | Miliwatt |
| MUX | Multiplexor |
| MZI | Machův-Zehnderův interferometr |
| nm | Nanometr |
| NTRU | Number Theory Research Unit (šifra) |
| O band | Original band |
| OADM | Optical Add-drop Multiplexer |
| OFDR | Optical Frequency Domain Reflectometry |
| OSA | Optical Spectrum Analyzer |
| OSNR | Optical Signal To Noise Ratio |
| OTDR | Optical Time Domain Reflectometry |
| OTP | One-time Pad (šifra) |
| PMD | Polarization Mode Dispersion |
| PNS | Photon-number Splitting (útok) |
| PQC | Post-quantum Cryptography |
| ps | Pikosekunda |
| QBER | Quantum-bit Error Rate |
| QKD | Quantum Key Distribution |
| QKDE | Quantum Dey Distribution Entity |
| QKDN | Quantum Dey Distribution Network |

| | |
|---------------|---|
| QMS | Quantum Management System |
| QNC | Quantum Node Controller |
| QoS | Quality of Service |
| QRNG | Quantum Random Number Generator |
| REST | Representational State Transfer |
| RFA | Raman Fiber Amplifier |
| ROADM | Reconfigurable Optical Add-drop Multiplexer |
| s | Sekunda |
| S band | Short band |
| SAE | Secure Application Entity |
| SARG04 | Scarani, Acin, Ribordy a Gisin roku 2004 (protokol) |
| SDN | Software-defined Networking |
| SFP | Small Form-factor Pluggable (transceiver) |
| SMF | Single Mode Fiber |
| SNMP | Simple Network Management Protocol |
| SOA | Semiconductor Optical Amplifier |
| SPC | Single Parity Check |
| SPM | Self-phase Modulation |
| SRS | Spontaneous Raman Scattering |
| SSH | Secure Shell |
| T12 | Toshiba roku 2012 (protokol) |
| TFF | Thin Film Filter |
| TF-QKD | Twin-field QKD |
| THz | Terahertz |
| TLS | Transport Layer Security |

| | |
|---------------|----------------------------------|
| TN | Trusted Node |
| U band | Ultra-long band |
| USB | Universal Serial Bus |
| USD | Unambiguous State Discrimination |
| VOA | Variable Optical Attenuator |
| VUT | Vysoké učení technické v Brně |
| WCP | Weak Coherent Pulse |
| WDM | Wavelength-division Multiplexing |
| XPM | Cross-phase Modulation |

Matematické veličiny

| | |
|-----------------|--|
| α | Koeficient α nebo měrný útlum |
| β | Koeficient β |
| γ | Úhly dopadajícího a lomeného svazku |
| $\Delta\tau$ | Rozdíl mezi propagací pulzu v rovině X a Y (PMD) |
| ζ | Ztráty na optických prvcích a spojích |
| θ | Úhel θ definující Blochovu kouli |
| λ | Vlnová délka |
| μ | Fotonové číslo |
| ν | Frekvence |
| $\rho(\lambda)$ | Koeficient SRS |
| φ | Úhel φ definující Blochovu kouli |
| a | Útlum |
| B | Matice obsahující opravené bity (Toeplitz) |
| \vec{B} | Vektor magnetického pole |
| c | Rychlost světla |
| d | Délka klíče (Kompresní poměr) |
| C/D | Kontrolní bity (LDPC) |
| E | Energie |
| \vec{E} | Vektor elektrického pole |
| e | Eulerovo číslo |
| G | Gallagerova matice |
| $H(Z)$ | Hašovací funkce |
| h | Planckova konstanta |
| K | Matice obsahující zesílený klíč (Toeplitz) nebo klíč |

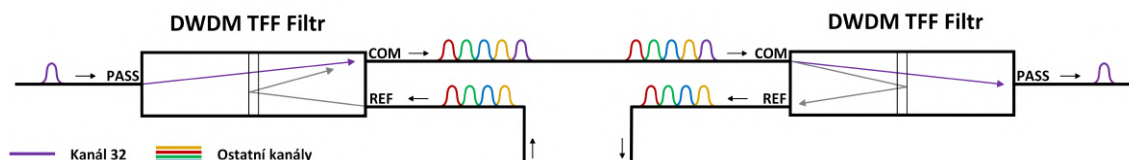
| | |
|----------------|--|
| l, t | Délky tras v interferometru |
| L | Délka optické trasy |
| M/N | Počet kontrolních bitů (LDPC) |
| n | Index lomu |
| P | Detekované pulzy, pravděpodobnost nebo výkon |
| T | Toeplitzova matice, transmisivita nebo perioda |
| V | Viditelnost |
| v | Rychlost |
| X/Y | Proseté bity (LDPC) |
| $ \Psi\rangle$ | Kvantový stav zapsaný pomocí KET vektoru |

Seznam příloh

| | | |
|----------|---|------------|
| A | Srovnání kvality 100GHz filtrů | 161 |
| A.1 | Výkon laseru | 162 |
| A.2 | Směr PASS → COM | 163 |
| A.3 | Směr PASS → REF | 166 |
| A.4 | Směr REF → COM | 169 |
| A.5 | Kvalita provedení filtrů | 172 |
| A.6 | Vložný útlum a izolace filtrů | 174 |
| A.6.1 | Vložný útlum | 174 |
| A.6.2 | Izolace sousedních kanálů | 175 |
| B | Výpočet Ramanova rozptylu | 177 |
| C | Standards pro QKD | 179 |
| C.1 | ETSI | 179 |
| C.2 | ITU-T | 182 |
| C.3 | IEEE | 185 |
| C.4 | ISO/IEC | 185 |

A Srovnání kvality 100GHz filtrů

Pro testování tras popsaných v práci bylo používáno pět optických 100GHz DWDM filtrů propouštějících kanál 32 (1551,72 nm). Směry měření vybrané trasy (např. REF-COM × COM-REF) jsou považovány za ekvivalentní.



Obr. A.1: Princip funkce DWDM filtrů.

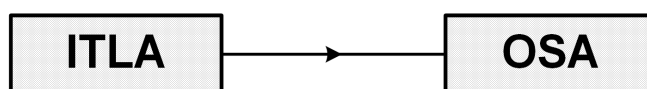
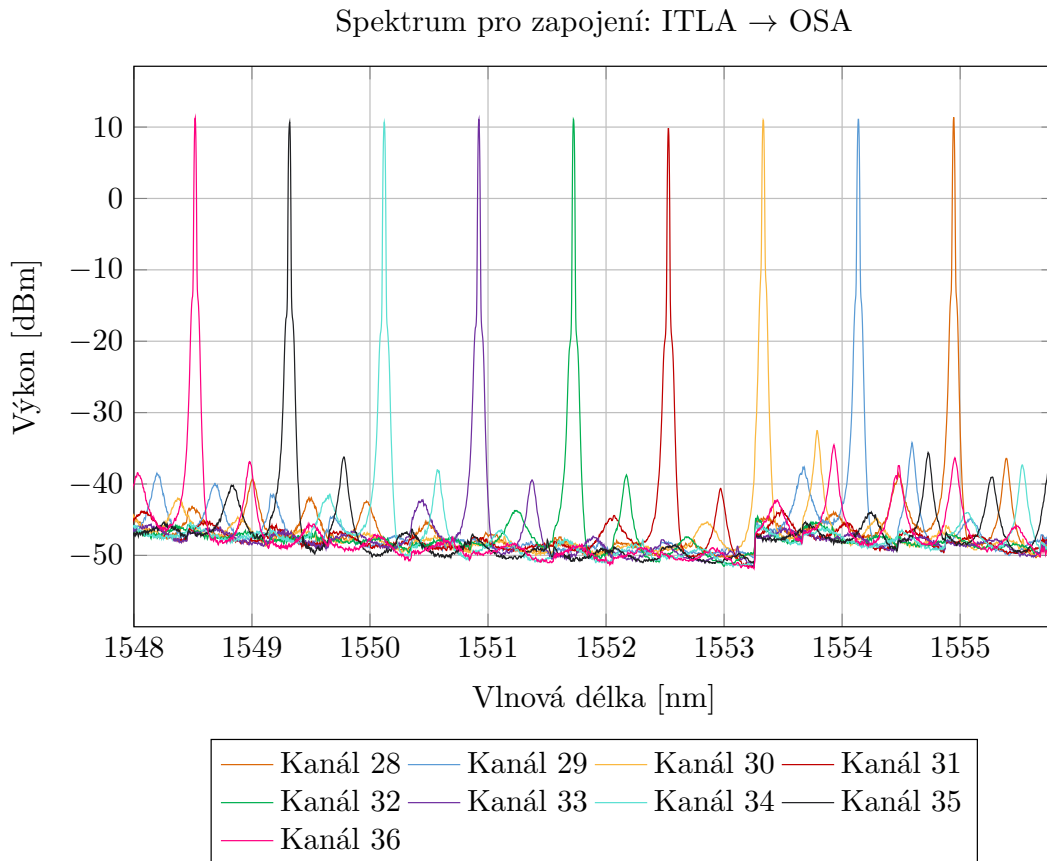
Filtry disponují třemi porty, mezi kterými dochází k vydělení / sloučení kanálů různých vlnových délek. V příloze jsou srovnávány tři níže uvedená zapojení. V ideálním případě je jejich funkce následující:

- **Filtry ve směru PASS → COM** – Z portu PASS prochází na port COM pouze kanál 32. Ostatní kanály jsou odraženy na port REF.
- **Filtry ve směru PASS → REF** – Mezi porty nedochází k průchodu světla žádné vlnové délky.
- **Filtry ve směru REF → COM** – Z portu REF jsou na port COM odraženy všechny kanály kromě CH32. Ten prochází přes port PASS.

K měření byl použit spektrální analyzátor (OSA – Optical spectrum analyzer) a laditelný laser (ITLA – Integrable tunable laser assembly). Pomocí něj bylo měřeno chování filtru na celkem devíti kanálech (CH32 a čtyři další kanály z každé strany). Spektrum laseru pro jednotlivé DWDM kanály se nachází na další straně.

A.1 Výkon laseru

První graf A.2 zobrazuje spektrum výše popsanych devíti kanálů přímo u výstupu z laditelného laseru. Pro přesnost byly výsledky otestovány i přímou metodou. Zde byla naměřena hodnota 11,1 dBm, což odpovídá tvaru spektra.



Obr. A.2: Zapojení trasy.

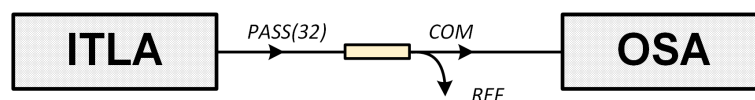
Tab. A.1: Srovnání sousedních kanálů.

| Kanál | | CH32 | CH33 | Rozdíl |
|-------|-------|-----------|-----------|---------|
| Výkon | P_R | 11,08 dBm | 11,08 dBm | 0,00 dB |

Hodnoty uvedené v tabulce A.1 slouží v následujících tabulkách jako referenční a je z nich dále odvozován úbytek na trase jako: $a = P_R - P$

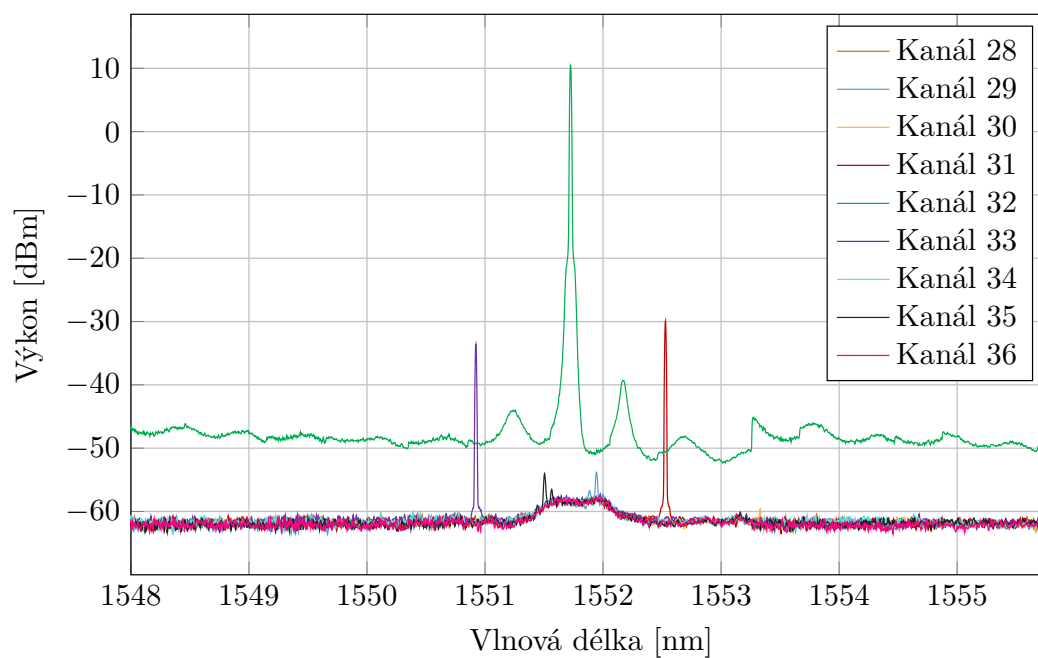
A.2 Směr PASS → COM

Trasa je nastavena tak, aby CH32 byl jediným procházejícím kanálem. Čím blíže CH32 se ostatní kanály nacházejí, tím nižší je jejich izolace. Z tohoto důvodu jsou tak v grafech jasně patrné kanály 31 a 33. Filtrem současně vždy prochází část šumu, který je vyvolaný ostatními kanály.



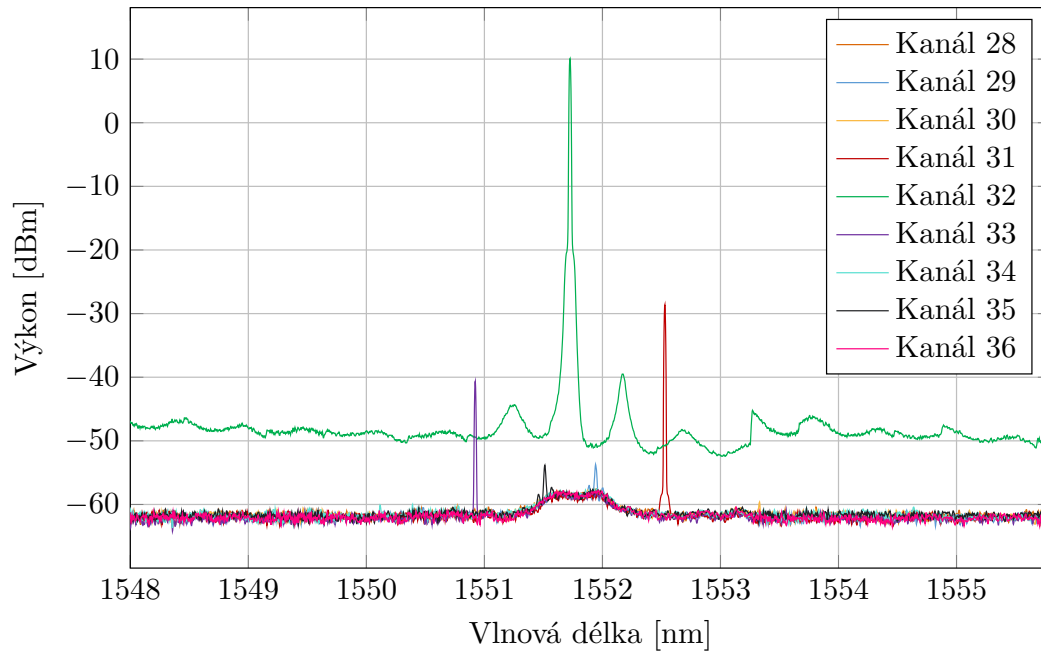
Obr. A.3: Zapojení trasy.

Spektrum pro zapojení: Filtr 1, PASS → COM



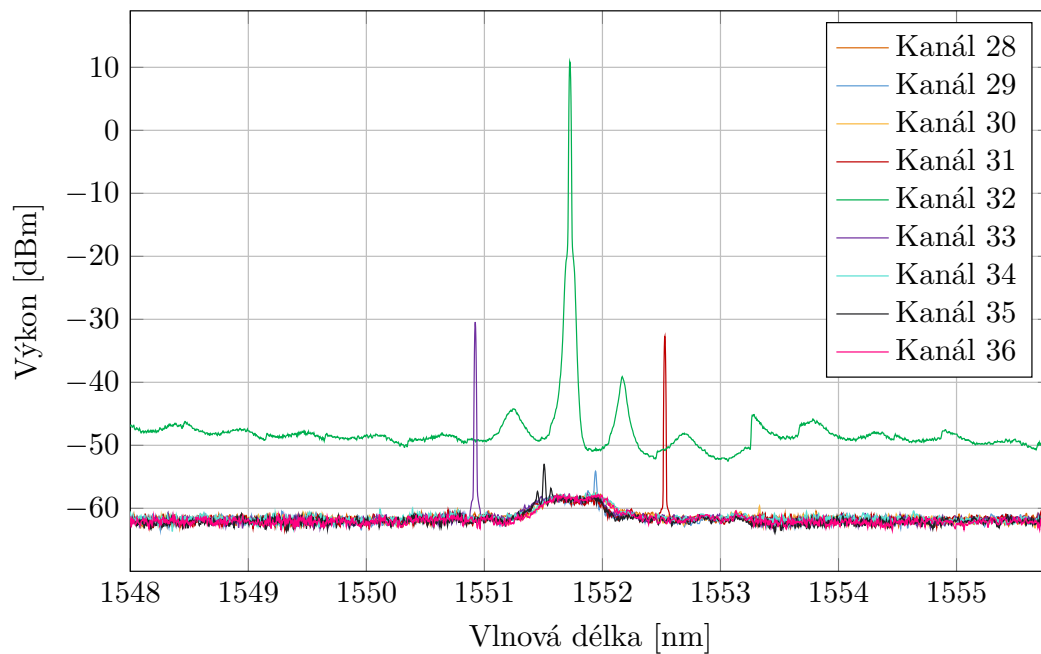
Obr. A.4: Charakteristika filtru 1 pro zapojení PASS → COM.

Spektrum pro zapojení: Filtr 2, PASS → COM



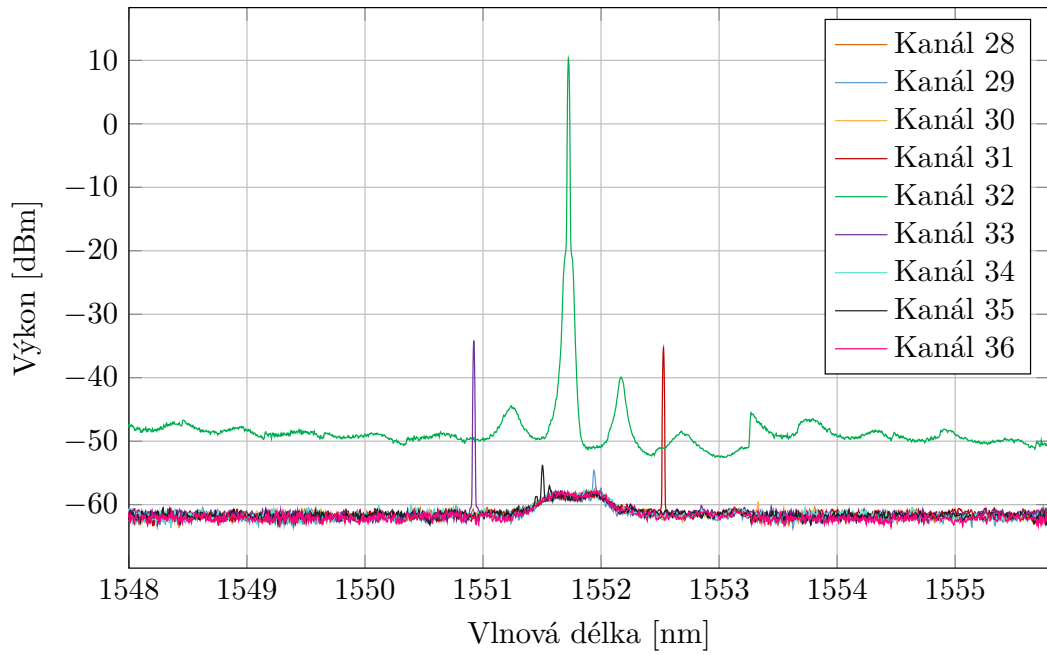
Obr. A.5: Charakteristika filtru 2 pro zapojení PASS → COM.

Spektrum pro zapojení: Filtr 3, PASS → COM



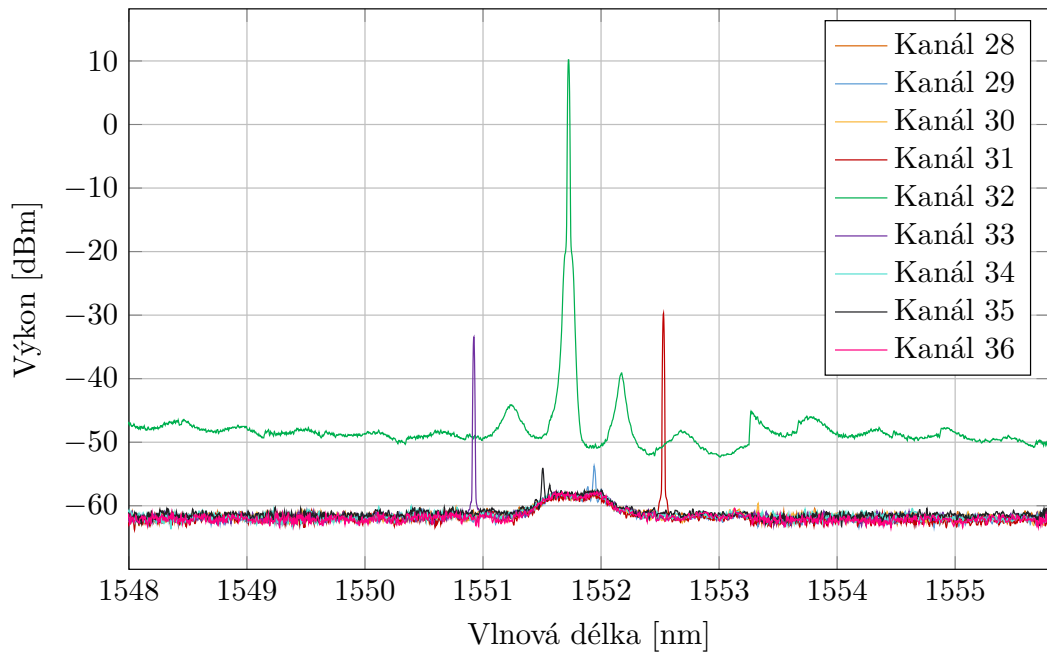
Obr. A.6: Charakteristika filtru 3 pro zapojení PASS → COM.

Spektrum pro zapojení: Filtr 4, PASS → COM



Obr. A.7: Charakteristika filtru 4 pro zapojení PASS → COM.

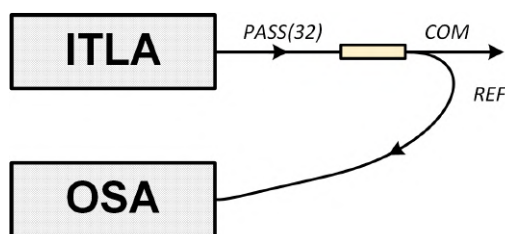
Spektrum pro zapojení: Filtr 5, PASS → COM



Obr. A.8: Charakteristika filtru 5 pro zapojení PASS → COM.

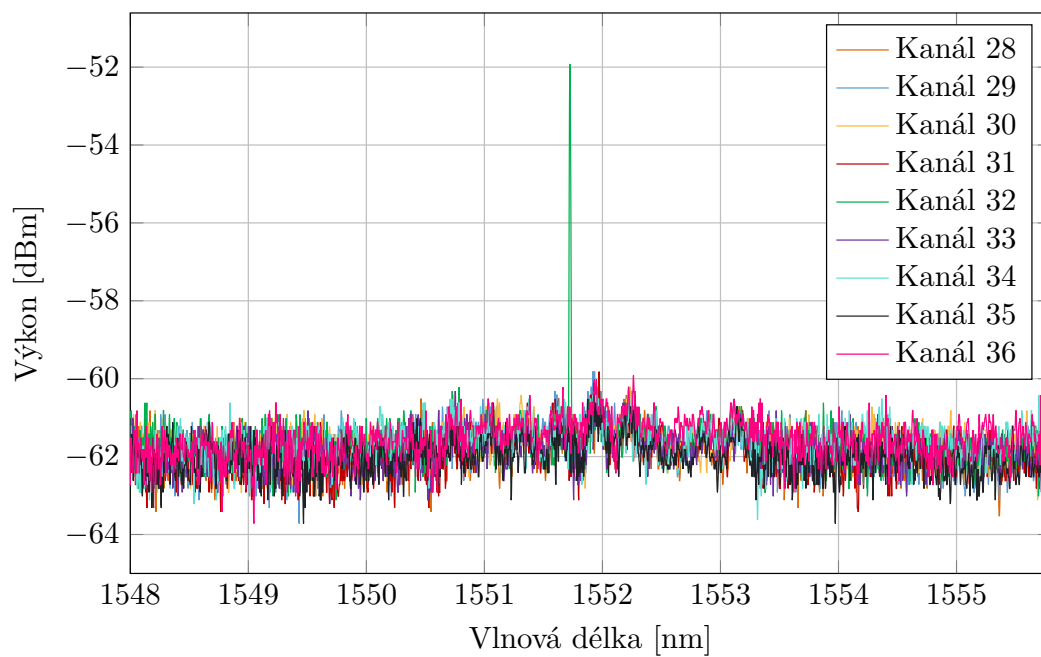
A.3 Směr PASS → REF

V ideálním případě by v tomto směru nemělo procházet žádné světlo. Jelikož mají ale filtry pouze omezenou účinnost, prochází v tomto směru malá část kanálu 32, která neprošla na port COM.



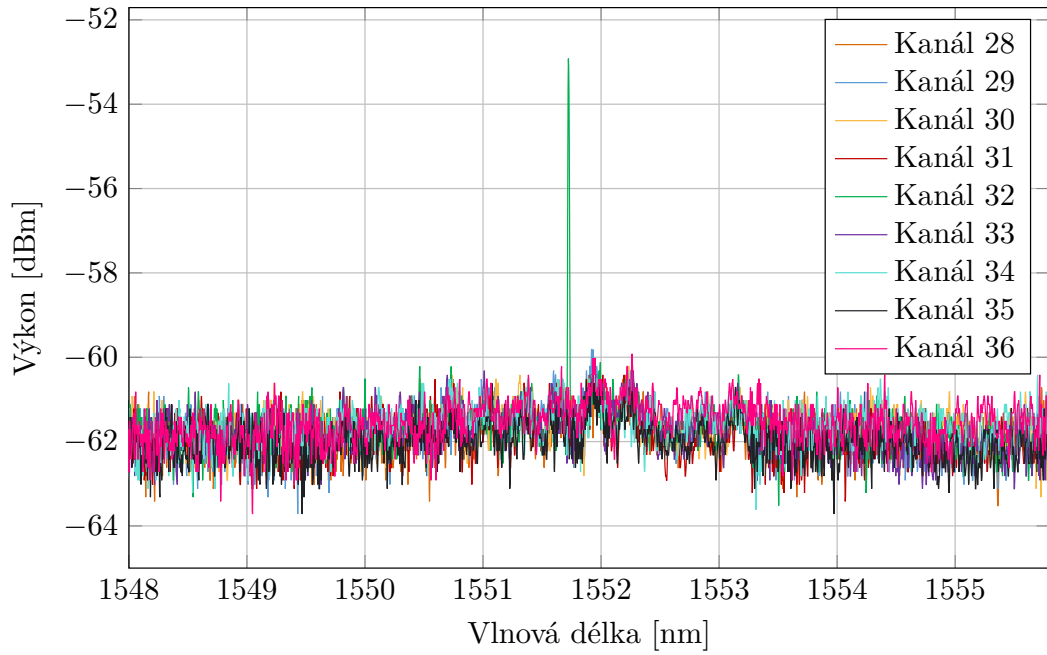
Obr. A.9: Zapojení trasy.

Spektrum pro zapojení: Filtr 1, PASS → REF



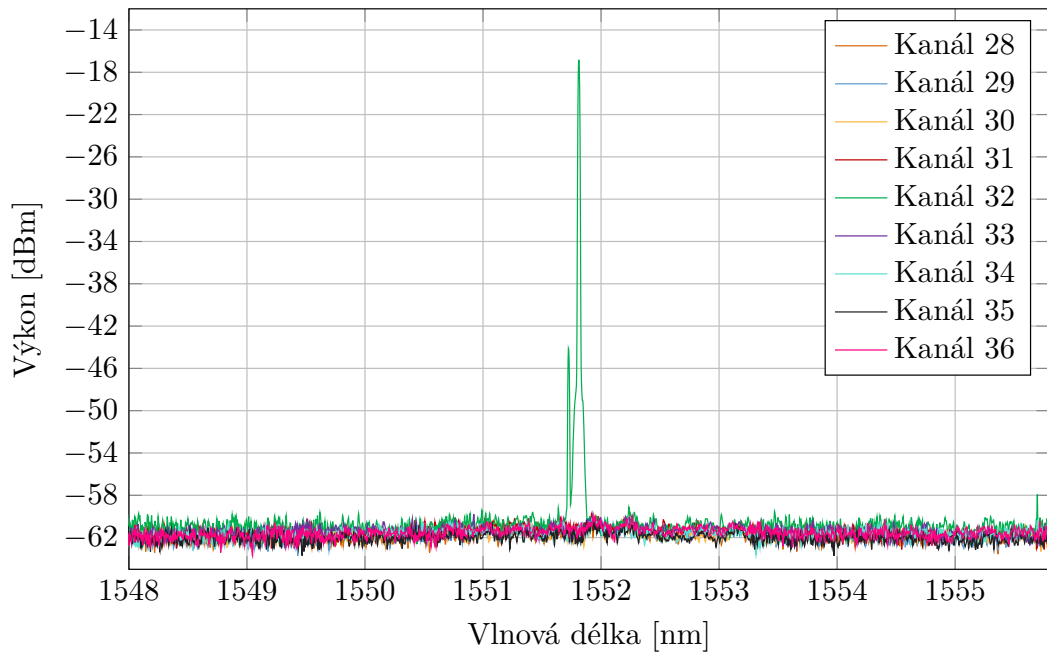
Obr. A.10: Charakteristika filtru 1 pro zapojení PASS → REF.

Spektrum pro zapojení: Filtr 2, PASS → REF



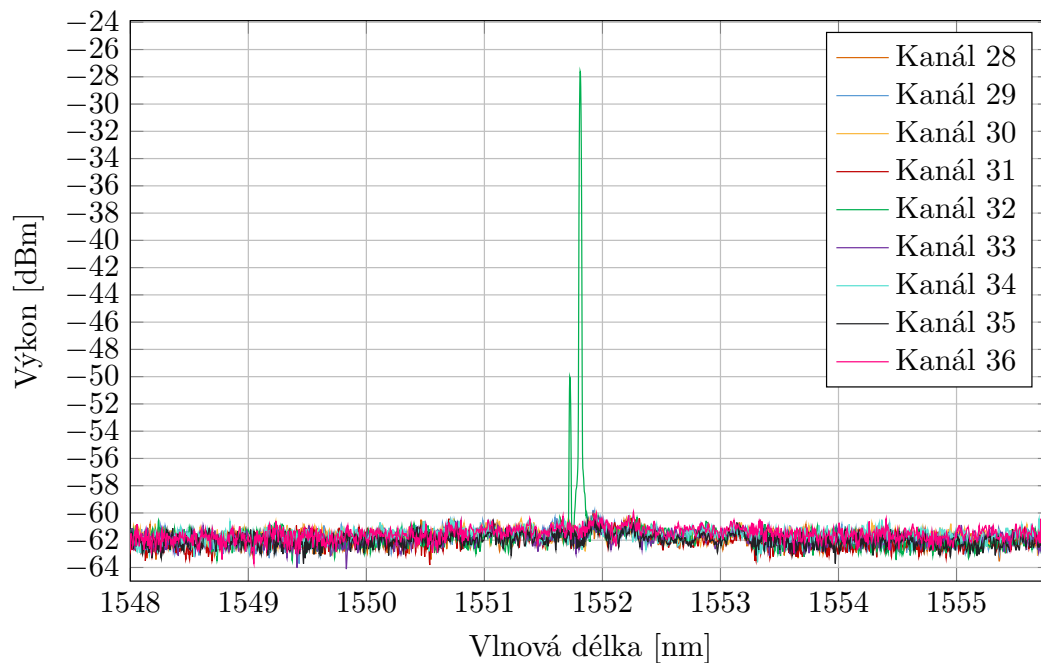
Obr. A.11: Charakteristika filtru 2 pro zapojení PASS → REF.

Spektrum pro zapojení: Filtr 3, PASS → REF



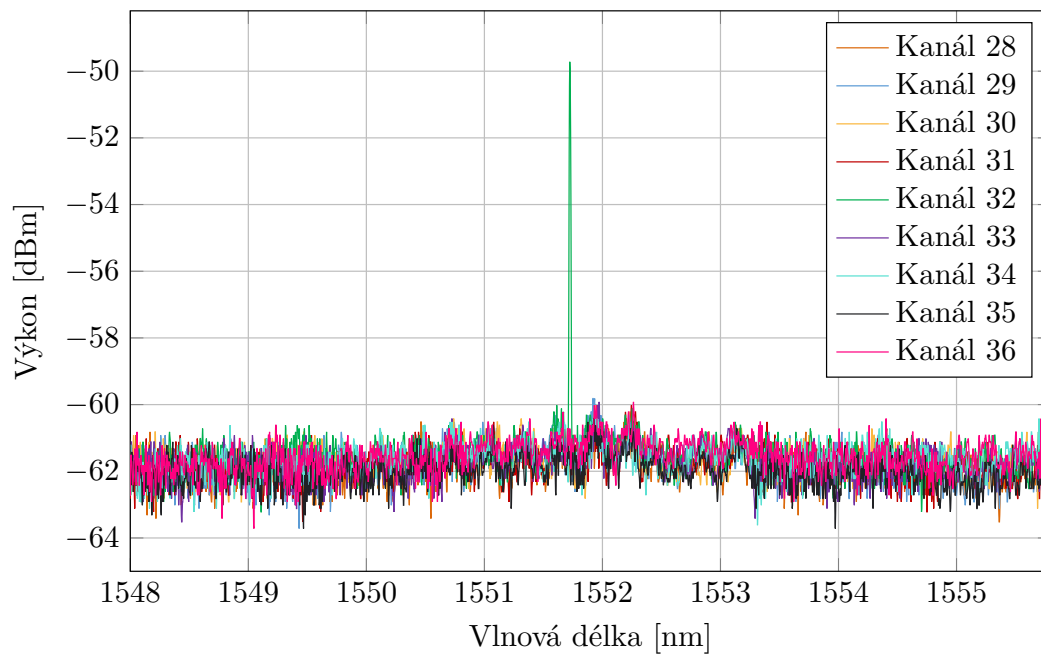
Obr. A.12: Charakteristika filtru 3 pro zapojení PASS → REF.

Spektrum pro zapojení: Filtr 4, PASS → REF



Obr. A.13: Charakteristika filtru 4 pro zapojení PASS → REF.

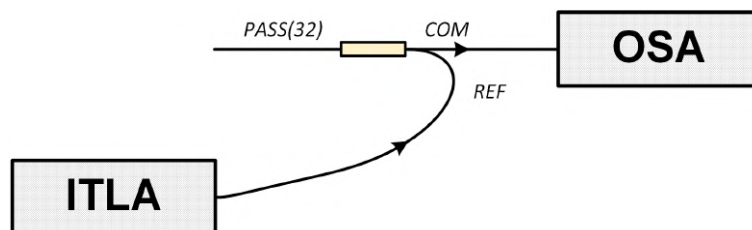
Spektrum pro zapojení: Filtr 5, PASS → REF



Obr. A.14: Charakteristika filtru 5 pro zapojení PASS → REF.

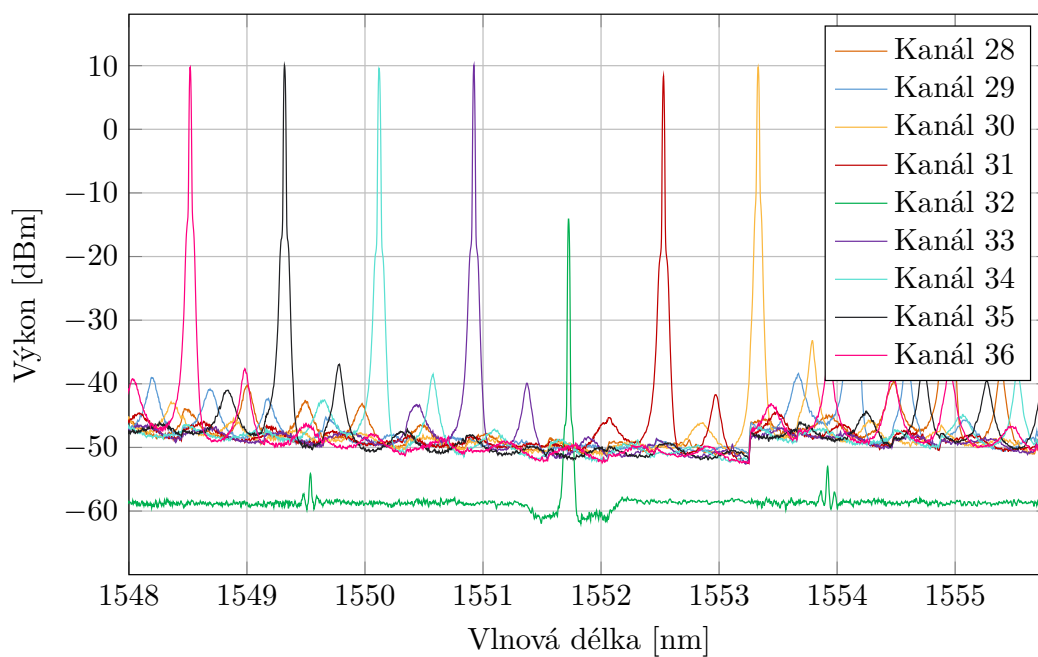
A.4 Směr REF → COM

Veškeré kanály, kromě kanálu průchozího, jsou odraženy s minimálním útlumem na port COM. V případě kanálu 32 dochází k výraznějšímu útlumu.



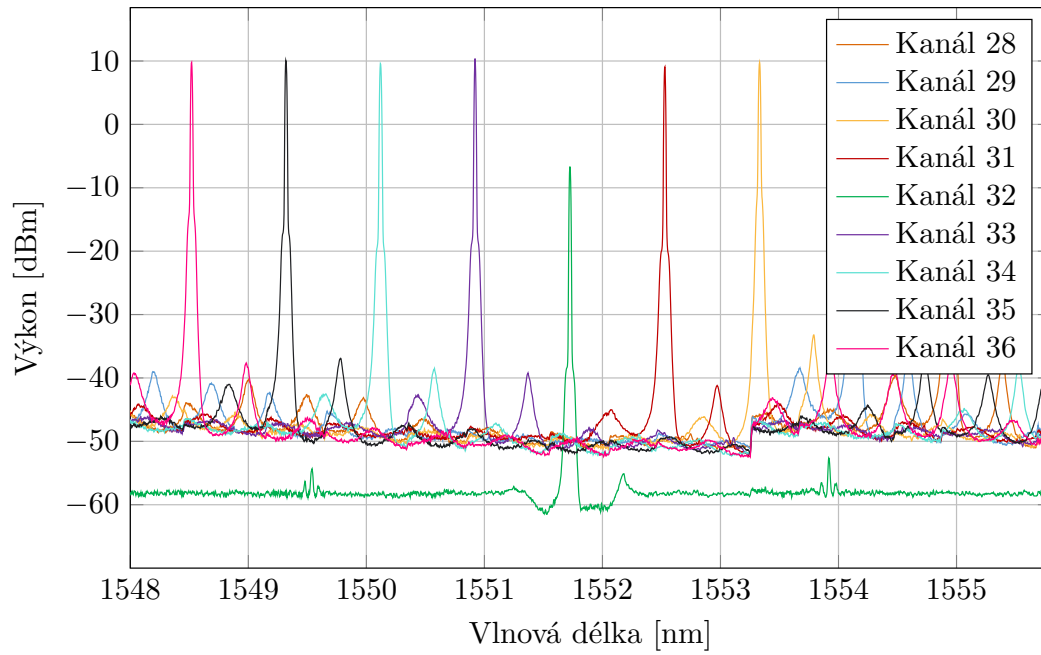
Obr. A.15: Zapojení trasy.

Spektrum pro zapojení: Filtr 1, REF → COM



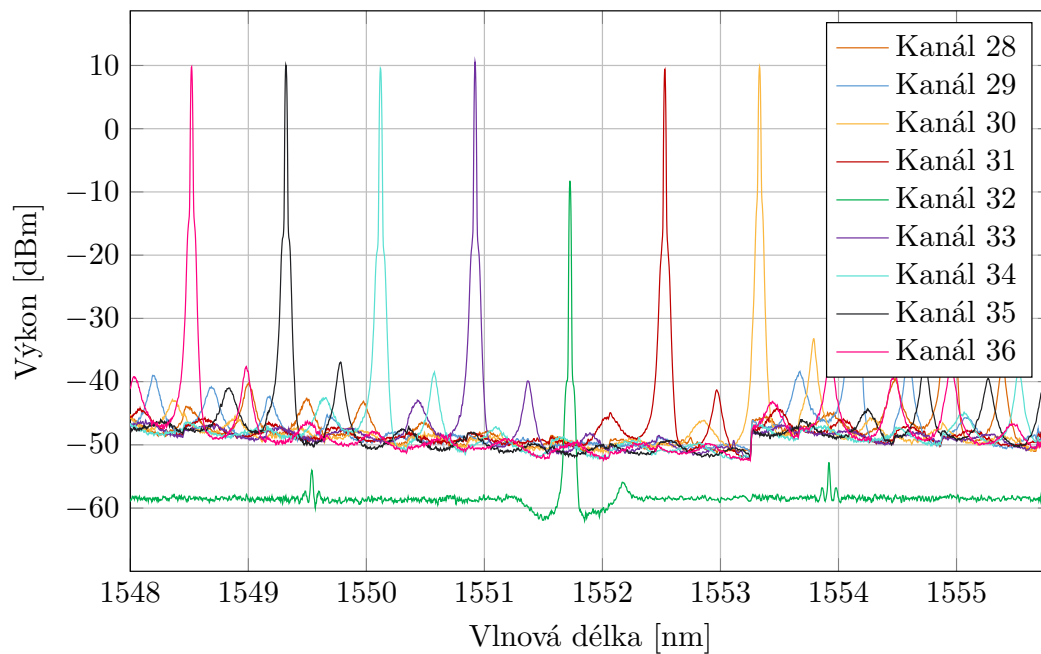
Obr. A.16: Charakteristika filtru 1 pro zapojení REF → COM.

Spektrum pro zapojení: Filtr 2, REF → COM



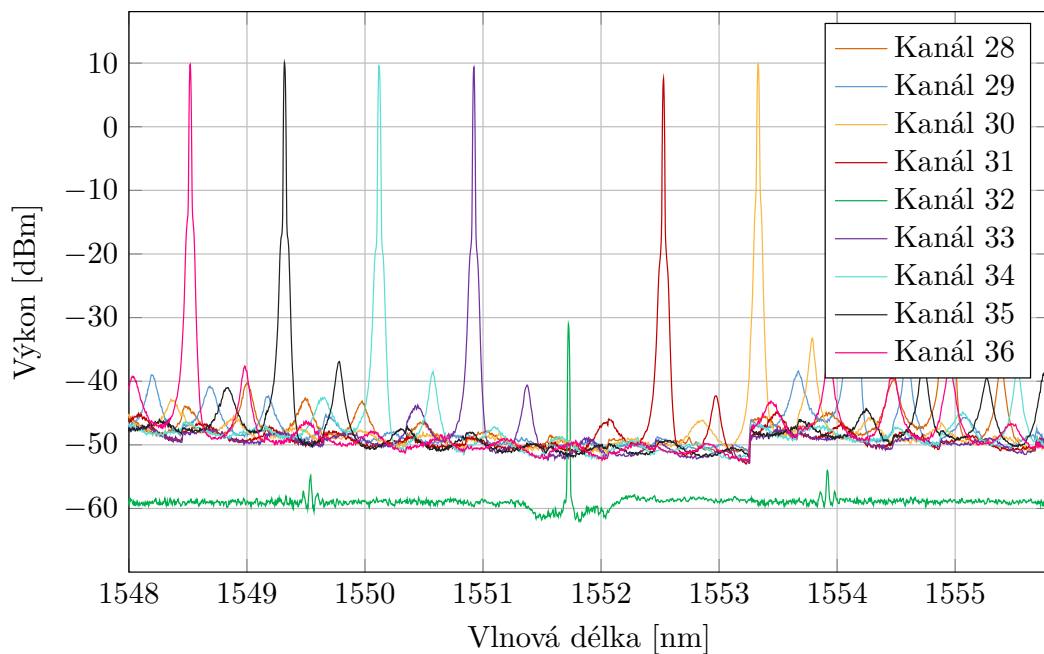
Obr. A.17: Charakteristika filtru 2 pro zapojení REF → COM.

Spektrum pro zapojení: Filtr 3, REF → COM



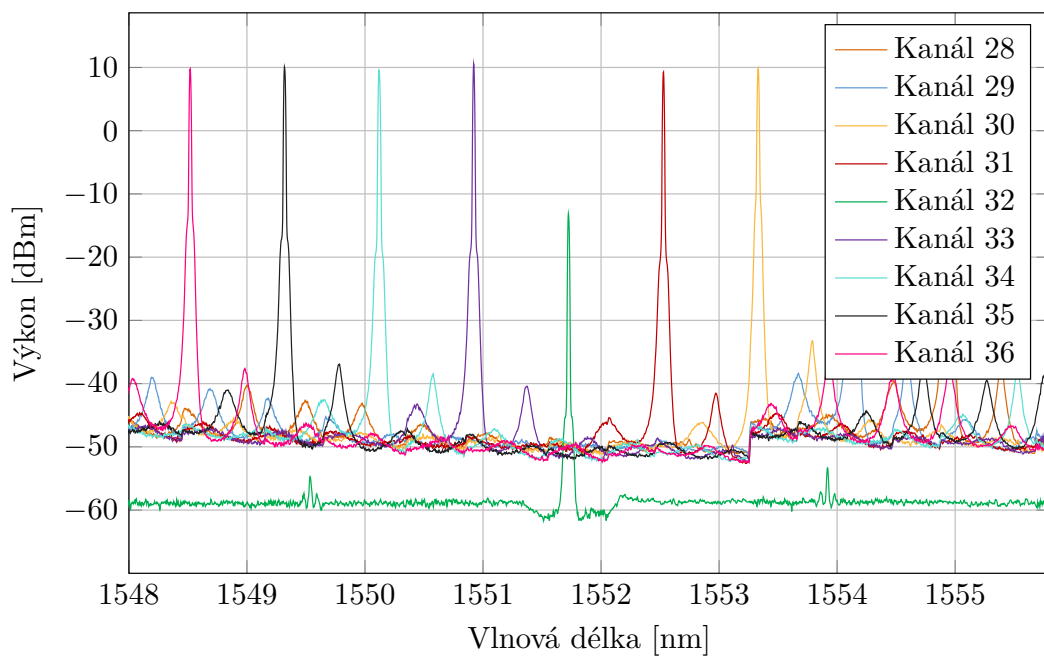
Obr. A.18: Charakteristika filtru 3 pro zapojení REF → COM.

Spektrum pro zapojení: Filtr 4, REF → COM



Obr. A.19: Charakteristika filtru 4 pro zapojení REF → COM.

Spektrum pro zapojení: Filtr 5, REF → COM



Obr. A.20: Charakteristika filtru 5 pro zapojení REF → COM.

A.5 Kvalita provedení filtrů

Pro vybrané kanály byly hodnoty z grafů výše přepsány do tabulek níže. Tabulka A.2 obsahuje hodnoty přímo na výstupu z laseru, které slouží jako referenční.

Tab. A.2: Referenční hodnoty kanálů naměřené přímo na výstupu laseru

| PASS → COM | CH31 | CH32 | CH33 |
|-------------------|-------------|-------------|-------------|
| Laser [dBm] | 11,08 | 11,08 | 9,78 |

Tab. A.3: Srovnání měřených filtrů pro směr PASS → COM.

| PASS → COM | CH31 | CH32 | CH33 |
|---------------------|---------------|--------------|---------------|
| Filtr 1 [dBm] | -29,98 | 10,48 | -33,62 |
| Filtr 2 [dBm] | -28,62 | 10,08 | -40,62 |
| Filtr 3 [dBm] | -32,72 | 10,88 | -30,42 |
| Filtr 4 [dBm] | -35,32 | 10,28 | -34,21 |
| Filtr 5 [dBm] | -29,72 | 10,18 | -33,42 |
| Průměr [dBm] | -31,27 | 10,38 | -34,46 |
| MAX-MIN [dB] | 6,70 | 0,80 | 10,20 |

Tab. A.4: Srovnání měřených filtrů pro směr PASS → REF.

| PASS → REF | CH31 | CH32 | CH33 |
|---------------------|---------------|---------------|---------------|
| Filtr 1 [dBm] | -59,82 | -51,92 | -59,92 |
| Filtr 2 [dBm] | -60,02 | -52,92 | -60,02 |
| Filtr 3 [dBm] | -59,72 | -16,82 | -59,82 |
| Filtr 4 [dBm] | -59,92 | -27,62 | -59,82 |
| Filtr 5 [dBm] | -60,02 | -49,72 | -59,92 |
| Průměr [dBm] | -59,90 | -39,80 | -59,90 |
| MAX-MIN [dB] | 0,30 | 36,10 | 0,20 |

Tab. A.5: Srovnání měřených filtrů pro směr REF → COM.

| REF → COM | CH31 | CH32 | CH33 |
|---------------------|-------------|---------------|--------------|
| Filtr 1 [dBm] | 8,38 | -14,12 | 10,08 |
| Filtr 2 [dBm] | 9,08 | -6,72 | 10,28 |
| Filtr 3 [dBm] | 9,38 | -8,32 | 10,58 |
| Filtr 4 [dBm] | 7,58 | -31,02 | 9,38 |
| Filtr 5 [dBm] | 9,28 | -13,12 | 10,58 |
| Průměr [dBm] | 8,74 | -14,66 | 10,18 |
| MAX-MIN [dB] | 1,80 | 24,30 | 1,20 |

Na základě těchto údajů je v dalších podkapitolách vypočtena izolace a útlum pro každý z filtrů. Podle nich jsou pak vybrané filtry zapojeny na jednotlivá místa v topologii 11.1.

A.6 Vložný útlum a izolace filtrů

A.6.1 Vložný útlum

Ve směrech, které jsou pro vybraný kanál průchozí, není kanál ovlivněn izolací filtru. Veškerý naměřený rozdíl mezi výkonem přímo z laseru a na výstupu z filtru je tak považován za vložný útlum. Ten je měřen ve směru PASS → COM na kanále 32. Pro směr REF → COM byl vybrán kanál 35, který je dostatečně vzdálený a izolace filtru tak na něj nemá velký vliv.

Tab. A.6: Hodnoty výkonu při výstupu z laseru a filtrů pro výpočet vložného útlumu.

| Kanály 32 a 35 | PASS → COM | | REF → COM | |
|------------------------|----------------|-------|----------------|-------|
| Kanál | CH32 | | CH35 | |
| Výstup z laseru | | | | |
| Laser [dBm] | $P_{l,32,PC}$ | 11,08 | $P_{l,35,RC}$ | 10,68 |
| Výstup z filtru | | | | |
| Filtr 1 [dBm] | $P_{f1,32,PC}$ | 10,48 | $P_{f1,35,RC}$ | 10,08 |
| Filtr 2 [dBm] | $P_{f2,32,PC}$ | 10,08 | $P_{f1,35,RC}$ | 10,18 |
| Filtr 3 [dBm] | $P_{f3,32,PC}$ | 10,88 | $P_{f1,35,RC}$ | 10,28 |
| Filtr 4 [dBm] | $P_{f4,32,PC}$ | 10,28 | $P_{f1,35,RC}$ | 9,98 |
| Filtr 5 [dBm] | $P_{f5,32,PC}$ | 10,18 | $P_{f1,35,RC}$ | 10,18 |

K výpočtu byly použity hodnoty z tabulky A.6. Ukázkový postup pro první filtr prezentuje rovnice A.1. Výsledky, včetně průměrné hodnoty a maximálního rozdílu, jsou pak uvedeny v tabulce A.7.

$$a_{f1,PC} = P_{l,32,PC} - P_{f1,32,PC} \quad (\text{A.1})$$

Tab. A.7: Vypočtený vložný útlum.

| Vložný útlum | PASS → COM | | REF → COM | |
|---------------------|-------------------|-------------|-------------------|-------------|
| Filtr 1 [dB] | $a_{f1,PC}$ | 0,60 | $a_{f1,RC}$ | 0,60 |
| Filtr 2 [dB] | $a_{f2,PC}$ | 1,00 | $a_{f2,RC}$ | 0,50 |
| Filtr 3 [dB] | $a_{f3,PC}$ | 0,20 | $a_{f3,RC}$ | 0,40 |
| Filtr 4 [dB] | $a_{f4,PC}$ | 0,80 | $a_{f4,RC}$ | 0,70 |
| Filtr 5 [dB] | $a_{f5,PC}$ | 0,90 | $a_{f5,RC}$ | 0,50 |
| Průměr [dB] | $\bar{a}_{f,PC}$ | 0,70 | $\bar{a}_{f,RC}$ | 0,54 |
| MAX–MIN [dB] | $\Delta a_{f,PC}$ | 0,80 | $\Delta a_{f,RC}$ | 0,30 |

A.6.2 Izolace sousedních kanálů

Ve směrech, které jsou pro kanály neprůchozí, dochází k výrazně většímu potlačení signálu. V tomto případě se hovoří o tzv. izolaci sousedních kanálů. Pro měření byl zvolen kanál 33 pro směr PASS → COM. Ve směru REF → COM byl zvolen kanál 32. V obou případech dochází k jejich odfiltrování (odražení).

Tab. A.8: Hodnoty výkonu při výstupu z laseru a filtrů pro výpočet izolace.

| Kanály 33 a 32 | PASS → COM | | REF → COM | |
|------------------------|----------------|--------|----------------|--------|
| Kanál | CH33 | | CH32 | |
| Výstup z laseru | | | | |
| Laser [dBm] | $P_{l,33,PC}$ | 11,08 | $P_{l,32,RC}$ | 11,08 |
| Výstup z filtru | | | | |
| Filtr 1 [dBm] | $P_{f1,33,PC}$ | -33,62 | $P_{f1,32,RC}$ | -14,12 |
| Filtr 2 [dBm] | $P_{f2,33,PC}$ | -40,62 | $P_{f2,32,RC}$ | -6,72 |
| Filtr 3 [dBm] | $P_{f3,33,PC}$ | -30,42 | $P_{f3,32,RC}$ | -8,32 |
| Filtr 4 [dBm] | $P_{f4,33,PC}$ | -34,21 | $P_{f4,32,RC}$ | -31,02 |
| Filtr 5 [dBm] | $P_{f5,33,PC}$ | -33,42 | $P_{f5,32,RC}$ | -13,12 |

Na výstupu z filtru je tak možné naměřit nižší výkon, což je dáno vlivem filtrace. Hodnotu izolace je tak možné spočítat jako rozdíl vstupního a výstupního výkonu.

$$I_{f1,PC} = P_{l,33,PC} - P_{f1,33,PC} \quad (\text{A.2})$$

Tab. A.9: Vypočtená izolace sousedních kanálů.

| Izolace | PASS → COM | | REF → COM | |
|---------------------|-----------------------|--------------|-----------------------|--------------|
| Filtr 1 [dB] | $I_{f1,PC}$ | 44,70 | $I_{f1,RC}$ | 22,20 |
| Filtr 2 [dB] | $I_{f2,PC}$ | 51,70 | $I_{f2,RC}$ | 17,80 |
| Filtr 3 [dB] | $I_{f3,PC}$ | 41,50 | $I_{f3,RC}$ | 19,40 |
| Filtr 4 [dB] | $I_{f4,PC}$ | 45,29 | $I_{f4,RC}$ | 42,10 |
| Filtr 5 [dB] | $I_{f5,PC}$ | 44,50 | $I_{f5,RC}$ | 24,20 |
| Průměr [dB] | $\overline{I_{f,PC}}$ | 45,54 | $\overline{I_{f,RC}}$ | 25,74 |
| MAX-MIN [dB] | $\Delta I_{f,PC}$ | 10,20 | $\Delta I_{f,RC}$ | 24,30 |

B Výpočet Ramanova rozptylu

V závislosti na vzdálenosti kvantového kanálu od kanálu klasického a jeho výstupním výkonu je možné odhadnout výkon Ramanova šumu v obou směrech. Jelikož se jedná o nelineární jev, je nutné počítat v základních jednotkách (nikoli v decibelech). Níže je uveden příklad pro trasu popsanou v kapitole 11.1. Pro výpočet jsou použity vzorce 7.17 a 7.18. K nim jsou potřeba následující parametry:

- **Výstupní výkon** – získán z nákresu 11.1 jako hodnota CH29 v bodě 3) a CH30 v bodě 4). Tento výkon je nutné přepočítat na mW podle příslušného vzorce v tabulce 7.1.

$$P_{výstup|29} = -32,7 \text{ dBm} = 5,37 \cdot 10^{-4} \text{ mW}$$

$$P_{výstup|30} = -32,5 \text{ dBm} = 5,62 \cdot 10^{-4} \text{ mW}$$

- **Průřez Ramanova rozptylu** – získán (odhadnut) z grafu 7.14 pro kanály vzdálené 2 a 3 pozice od kvantového kanálu v oblasti Stokesova rozptylu.

$$\rho(\lambda) = 1,85 \cdot 10^{-9} \frac{1}{\text{km} \cdot \text{nm}}$$

- **Šířka pásma** – oblast spektra, ve které je měřen výkon Ramanova rozptylu. DWDM kanál má šířku 100 GHz, což je nutné převést na nm.

$$\Delta\lambda = 0,8 \text{ nm} \approx \Delta\nu = 100 \text{ GHz}$$

- **Délka trasy** – část trasy, ve které dochází k Ramanovu rozptylu a dalším nelineárním jevům.

$$L = 20 \text{ km}$$

- **Měrný útlum** – dopočítán na základě rozdílu vstupního a výstupního výkonu v nákresu 11.1. Následně převeden na km^{-1} podle vzorce pro nelineární měrný útlum v tabulce 7.1.

$$\alpha = 0,325 \frac{\text{dB}}{\text{km}} = 7,48 \cdot 10^{-2} \text{ km}^{-1}$$

Výkon Ramanova šumu vyvolaného jedním klasickým kanálem v dopředném (\rightarrow) a zpětném (\leftarrow) směru je možné spočítat jako:

$$P_{\overrightarrow{SR\dot{S}}} = P_{výstup} \cdot \rho(\lambda) \cdot L \cdot \Delta\lambda$$

$$P_{\overleftarrow{SR\dot{S}}} = P_{výstup} \cdot \rho(\lambda) \cdot \frac{\sinh(L\alpha)}{\alpha} \cdot \Delta\lambda$$

Tab. B.1: Výkon SRS u obou servisních kanálů.

| CH29 $A \leftarrow B$ | | CH30 $A \rightarrow B$ | |
|--|-----------------------|----------------------------------|-----------------------|
| Výkon SRS v dopředném směru ($P_{\overrightarrow{SRS}}$) | | | |
| $1,66 \cdot 10^{-11} \text{ mW}$ | $-107,79 \text{ dBm}$ | $1,60 \cdot 10^{-11} \text{ mW}$ | $-107,99 \text{ dBm}$ |
| Výkon SRS ve zpětném směru ($P_{\overleftarrow{SRS}}$) | | | |
| $2,36 \cdot 10^{-11} \text{ mW}$ | $-106,27 \text{ dBm}$ | $2,25 \cdot 10^{-11} \text{ mW}$ | $-106,47 \text{ dBm}$ |

V souladu s očekáváním je zpětný Ramanův rozptyl mírně výkonnější, než rozptyl v dopředném směru. Tento rozdíl ve výkonu roste spolu s délkou trasy. Kvantový kanál je jednosměrný a vysílá ve směru $A \rightarrow B$. Celkový výkon Ramanova rozptylu, který jej ruší se tak určí jako součet dopředného Ramanova rozptylu kanálu 30 a zpětného Ramanova rozptylu kanálu 29. Stejný postup je použit i pro výpočty v dalších kapitolách.

$$P_{SRS|QKD} = P_{\overrightarrow{SRS}|30} + P_{\overleftarrow{SRS}|29} = 3,92 \cdot 10^{-11} \text{ mW} = -104,07 \text{ dBm}$$

C Standardy pro QKD

Příloha obsahuje seznam všech nalezených platných standardů, případně jejich návrhů. Seznam je prezentován formou tabulek obsahujících postupně standardy od ETSI, ITU-T, IEEE a ISO/IEC. Vypsane standardy pocházejí přímo z oficiálních stránek těchto organizací. Tedy [116], [117], [118], [119] a [120].

C.1 ETSI

Tab. C.1: Typy ETSI dokumentů.

| |
|--|
| European Standard (EN) |
| Dokument určený k převzetí do národních norem evropských zemí. Může být vypracován na základě žádosti Evropské komise. |
| ETSI Standard (ES) |
| Dokument obsahující technické požadavky. |
| ETSI Guide (EG) |
| Obecné pokyny pro ETSI při zpracování specifických technických standardizačních činností. |
| ETSI Technical Specification (TS) |
| Dokument obsahuje technické požadavky a je nutné, aby byl rychle k dispozici. |
| ETSI Technical Report (TR) |
| Dokument obsahuje vysvětlující materiál. |
| ETSI Special Report (SR) |
| Používá se k různým účelům, mimo jiné ke zpřístupnění informací veřejnosti. |
| ETSI Group Specification (GS) |
| Dokument obsahuje technické požadavky, vysvětlující materiál nebo obojí. |
| ETSI Group Report (GR) |
| Výstup ETSI obsahující pouze informativní prvky. |

Tab. C.2: Kompletní seznam ETSI dokumentů vztahujících se ke QKD.

| | |
|--|---------|
| ETSI GR QKD 003 | 3/2018 |
| Komponenty a interní rozhraní. | |
| ETSI GR QKD 007 | 12/2018 |
| Slovník QKD pojmů. | |
| ETSI GS QKD 002 | 6/2010 |
| Použití QKD. | |
| ETSI GS QKD 004 | 8/2020 |
| Aplikační rozhraní obecně. | |
| ETSI GS QKD 005 | 12/2010 |
| Důkazy bezpečnosti. | |
| ETSI GS QKD 008 | 12/2010 |
| Specifikace zabezpečení QKD modulu. | |
| ETSI GS QKD 010 | návrh |
| Implementace zabezpečení: Ochrana proti útokům trojským koněm u jednosměrných QKD systémů. | |
| ETSI GS QKD 011 | 5/2016 |
| Charakteristika komponent: optické komponenty pro QKD systémy. | |
| ETSI GS QKD 012 | 2/2019 |
| Parametry zařízení a komunikačního kanálu pro nasazení QKD. | |
| ETSI GS QKD 013 | návrh |
| Charakteristika optického výstupu vysílacích modulů QKD. | |
| ETSI GS QKD 014 | 2/2019 |
| Protokol a formát dat REST API rozhraní pro doručování klíčů. | |
| ETSI GS QKD 015 | 4/2022 |
| Rozhraní pro řízení QKD pomocí SDN. | |
| ETSI GS QKD 016 | návrh |
| Profil ochrany (PP). | |
| ETSI GS QKD 017 | návrh |
| Architektury sítí. | |
| ETSI GS QKD 018 | 4/2022 |
| Rozhraní pro orchestraci pomocí SDN. | |
| ETSI GS QKD 019 | návrh |
| Návrh QKD rozhraní s autentizací. | |
| ETSI GS QKD 020 | návrh |
| Protokol a formát dat REST API rozhraní pro interoperabilitu systémů správy klíčů (KMS). | |

Tab. C.3: Kompletní seznam ETSI dokumentů vztahujících se k PQC.

| | |
|---|---------|
| ETSI GR QSC 001 | 7/2016 |
| Kvantově bezpečné algoritmické frameworky. | |
| ETSI GR QSC 003 | 2/2017 |
| Případové studie a scénáře nasazení. | |
| ETSI GR QSC 004 | 3/2017 |
| Posouzení hrozeb v kvantově bezpečném systému. | |
| ETSI GR QSC 006 | 2/2017 |
| Limitace kvantových výpočtů aplikované na velikosti symetrických klíčů. | |
| ETSI TR 103570 | 10/2017 |
| Kvantově bezpečné výměny klíčů. | |

C.2 ITU-T

Tab. C.4: Typy ITU-T dokumentů.

| | |
|----------|---|
| A | Organizace práce ITU-T |
| B | Vyjadřovací prostředky: definice, symboly, klasifikace |
| C | Obecné telekomunikační statistiky |
| D | Obecné zásady tarifů |
| E | Celkový provoz sítě, telefonní služby, provoz služeb a lidské faktory |
| F | Netelefonní telekomunikační služby |
| G | Přenosové systémy a média, digitální systémy a sítě |
| H | Audiovizuální a multimediální systémy |
| I | Digitální síť integrovaných služeb |
| J | Kabelové sítě a přenos televizních, zvukových a jiných multimediálních signálů |
| K | Ochrana proti rušení |
| L | Výstavba, instalace a ochrana kabelů a dalších prvků vnějšího zařízení |
| M | TMN a správa sítě: mezinárodní přenosové systémy, telefonní okruhy, telegrafie, faxové a pronajaté okruhy |
| N | Údržba: mezinárodní zvukový program a televizní přenosové okruhy |
| O | Specifikace měřicích zařízení |
| P | Terminály a subjektivní a objektivní metody vyhodnocování |
| Q | Přepínání a signalizace |
| R | Telegrafní přenos |
| S | Koncová zařízení telegrafních služeb |
| T | Terminály pro telematické služby |
| U | Telegrafní přepínání |
| V | Datová komunikace prostřednictvím telefonní sítě |
| X | Datové sítě a otevřené systémové komunikace |
| Y | Globální informační infrastruktura a aspekty internetového protokolu |
| Z | Jazyky a obecné aspekty softwaru pro telekomunikační systémy |

Tab. C.5: Kompletní seznam ITU-T dokumentů vztahujících se ke QKD kategorie X.

| | |
|--|---------|
| ITU-T X.1702 | 10/2019 |
| Architektura generátoru náhodných čísel s kvantovým šumem. | |
| ITU-T X.1710 | 4/2020 |
| Bezpečnostní framework pro sítě pro kvantovou distribuci klíčů. | |
| ITU-T X.1712 | 12/2020 |
| Bezpečnostní požadavky a opatření pro QKDN – správa klíčů. | |
| ITU-T X.1714 | 12/2020 |
| Kombinování a doručování tajných klíčů pro QKDN. | |
| ITU-T X.1715 | 9/2020 |
| Bezpečnostní požadavky a opatření pro integraci QKDN a sítí pro bezpečné ukládání dat. | |
| ITU-T X.1811 | 12/2021 |
| Bezpečnostní pokyny pro použití kvantově bezpečných algoritmů v systémech IMT-2020. | |
| ITU-T X.sec-QKDN-TN | návrh |
| Bezpečnostní požadavky a opatření pro QKDN – důvěryhodný uzel. | |
| ITU-T X.sec-QKDN-CM | návrh |
| Bezpečnostní požadavky a opatření pro QKDN – kontrola a správa. | |
| ITU-T X.sec-QKDN-AA | návrh |
| Autentizace a autorizace v QKDN pomocí PQC. | |
| ITU-T X.sec-QKDni | návrh |
| Bezpečnostní požadavky na interoperabilitu QKDN (QKDni). | |
| ITU-T X.sec-QKD-profr | návrh |
| Framework protokolů pro kvantovou distribuci klíčů v QKDN. | |

Tab. C.6: Kompletní seznam ITU-T dokumentů vztahujících se ke QKD kategorie Y.

| | |
|---|---------|
| ITU-T Y.3800 | 10/2019 |
| Přehled sítí podporujících kvantovou distribuci klíčů. | |
| ITU-T Y.3801 | 4/2020 |
| Funkční požadavky na sítě pro kvantovou distribuci klíčů. | |
| ITU-T Y.3802 | 12/2020 |
| Funkční architektura. | |
| ITU-T Y.3803 | 12/2020 |
| Správa klíčů. | |
| ITU-T Y.3804 | 9/2020 |
| Kontrola a správa. | |
| ITU-T Y.3805 | 12/2021 |
| SDN kontrola. | |
| ITU-T Y.3806 | 9/2021 |
| Požadavky na zajištění kvality služeb. | |
| ITU-T Y.3807 | 2/2022 |
| Parametry kvality služeb. | |
| ITU-T Y.3808 | 2/2022 |
| Framework pro integraci sítě pro kvantovou distribuci klíčů a sítí pro bezpečné ukládání dat. | |
| ITU-T Y.3809 | 2/2022 |
| Model založený na rolích při nasazení sítí pro kvantovou distribuci klíčů. | |
| ITU-T Y.3810 | 9/2022 |
| QKDN interoperabilita – framework. | |
| ITU-T Y.3811 | 9/2022 |
| Funkční architektura pro zajištění kvality služeb. | |
| ITU-T Y.3812 | 9/2022 |
| Požadavky na zajištění kvality služeb na základě strojového učení. | |
| ITU-T Y.3813 | 1/2023 |
| QKDN interoperabilita – funkční požadavky. | |
| ITU-T Y.3814 | 1/2023 |
| Funkční požadavky a architektura pro podporu strojového učení. | |
| ITU-T ITU-T Y.Sup70 | 7/2021 |
| Uplatnění strojového učení v QKDN. | |
| ITU-T Y.Sup75 | 3/2023 |
| Budoucí sítě založené na kvantových technologiích. | |

| | |
|---|-------|
| ITU-T Y.QKDN-QOS-AUTO-RQ | návrh |
| Požadavky na autonomní zajištění kvality služeb. | |
| ITU-T Y.QKDN-QOS-IW-REQ | návrh |
| Požadavky na zajištění QoS pro interoperabilitu QKDN. | |
| ITU-T Y.QKDN-QOS-ML-FA | návrh |
| Vylepšení funkční architektury pro zajištění QoS na základě strojového učení. | |
| ITU-T Y.QKDN-QOS-MMQ | návrh |
| Metodika měření parametrů QoS v QKDN. | |

C.3 IEEE

Tab. C.7: Kompletní seznam IEEE dokumentů vztahujících se ke QKD.

| | |
|---|-------|
| IEEE P1913 | návrh |
| YANG model pro softwarově definovanou kvantovou komunikaci. | |

C.4 ISO/IEC

Tab. C.8: Kompletní seznam ISO/IEC dokumentů vztahujících se ke QKD.

| | |
|--|-------|
| ISO/IEC 23837-1 | návrh |
| Bezpečnostní požadavky, testovací a vyhodnocovací metody pro kvantovou distribuci klíčů. Část 1: Požadavky. | |
| ISO/IEC 23837-2 | návrh |
| Bezpečnostní požadavky, testovací a vyhodnocovací metody pro kvantovou distribuci klíčů. Část 2: Testování a vyhodnocovací metody. | |