VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

Fakulta elektrotechniky
a komunikačních technologií

BAKALÁŘSKÁ PRÁCE

Brno, 2021 Ondřej Klíčník

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 PŘES OPTICKOU VLÁKNOVOU INFRASTRUKTURU
QUANTUM KEY DISTRIBUTION OVER OPTICAL FIBRE INFRASTRUCTURE

BAKALÁŘSKÁ PRÁCE
BACHELOR'S THESIS

AUTOR PRÁCE
AUTHOR
Ondřej Klíčník

VEDOUCÍ PRÁCE
SUPERVISOR
doc. Ing. Petr Münster, Ph.D.

BRNO 2021

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

Bakalářská práce

bakalářský studijní program **Informační bezpečnost**

Ústav telekomunikací

Student: Ondřej Klíčník ***ID:*** 211259

Ročník: 3 ***Akademický rok:*** 2020/21

NÁZEV TÉMATU:

Kvantová distribuce klíčů přes optickou vláknovou infrastrukturu

POKYNY PRO VYPRACOVÁNÍ:

Cílem práce je detailní rozbor problematiky kvantové distribuce klíčů (QKD) a popis současného stavu. V rámci popisu současného stavu bude provedena rešerše komerčně nabízených řešení a bude provedeno jejich srovnání. V rámci praktické části bude proveden návrh testovacího optického vláknového polygonu pro přenos QKD. Návrh bude ověřen simulací. Na základě návrhu, bude realizován testovací polygon umožnující ověření základních parametrů QKD systému.

DOPORUČENÁ LITERATURA:

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

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

Termín zadání: 1.2.2021 ***Termín odevzdání:*** 31.5.2021

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

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

ABSTRAKT

Cílem této bakalářské práce je vytvoření uceleného pohledu na současné technologie kvantové distribuce klíčů (QKD) po optickém vlákně, v teoretické rovině tedy zcela bezpečné výměny klíčů. Práci lze rozdělit na část teoretickou a praktickou. Teoretická část osvětluje důvody použití těchto systémů a základy kvantové mechaniky potřebné pro pochopení funkce jednotlivých QKD protokolů. Dále jsou popsány principy fungování jak daných protokolů, tak souvisejících služeb, jako je postkvantová kryptografie (PQC) a kvantové generování čísel (QRNG). Poslední kapitola se věnuje architektuře QKD sítí a popisuje současné standardy QKD komunikací. V praktické části je provedena detailní analýza komerčně dostupných zařízení. Následně jsou předvedeny výsledky simulací vybraných QKD protokolů a je navržen, sestaven a otestován vlastní QKD polygon.

KLÍČOVÁ SLOVA

Clavis^3, CV-QKD, DV-QKD, ETSI Key Delivery API, komerční systém QKD, kvantová distribuce klíčů (QKD), kvantová mechanika, kvantové generování čísel (QRNG), postkvantová éra, postkvantová kryptografie (PQC), QKD síť (QKDN), QKD polygon, QVPN, simulace QKD protokolů

ABSTRACT

The aim of this bachelor thesis is to create a comprehensive view of the current technology of quantum key distribution (QKD) over optical fiber, in theoretical terms, a completely secure key exchange. The thesis can be divided into theoretical and practical parts. The theoretical part illuminates the reasons for the use of these systems and the fundamentals of quantum mechanics needed to understand the function of individual QKD protocols. Furthermore, the principles of operation of both the protocols and related services such as post-quantum cryptography (PQC) and quantum number generation (QRNG) are described. The last chapter is devoted to the architecture of QKD networks and describes current standards for QKD communications. In the practical part, a detailed analysis of commercially available devices is performed. Subsequently, simulation results of selected QKD protocols are presented and a custom QKD polygon is designed, built and tested.

KEYWORDS

Clavis^3, CV-QKD, DV-QKD, ETSI Key Delivery API, commercial QKD system, quantum key distribution (QKD), quantum mechanics, quantum random number generator (QRNG), post-quantum era, post-quantum cryptography (PQC), QKD network (QKDN), QKD polygon, QVPN, QKD protocol simulation

KLÍČNÍK, Ondřej. *Přenos kvantové distribuce klíčů přes optickou vláknovou infrastrukturu*. Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav telekomunikací, 2021, 170 s. Bakalářská práce. Vedoucí práce: doc. Ing. Petr Münster, Ph.D.

Prohlášení autora o původnosti díla

Jméno a příjmení autora:	Ondřej Klíčník
VUT ID autora:	211259
Typ práce:	Bakalářská práce
Akademický rok:	2020/21
Téma závěrečné práce:	Přenos kvantové distribuce klíčů přes optickou vláknovou infrastrukturu

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

Děkuji vedoucímu své bakalářské práce panu doc. Ing. Petru Münsterovi, Ph.D. za odborné vedení, konzultace a podnětné návrhy k práci. Za konkrétní konzultace bych také rád poděkoval pánům Ing. Michalu Křelinovi, Ph.D. z Fakulty jaderné a fyzikálně inženýrské ČVUT a Vladyslavu Usenkovi, Ph.D. z Přírodovědecké fakulty UPOL. V neposlední řadě pak své rodině, která mě v průběhu studia podporovala.

Obsah

Seznam obrázků

Seznam tabulek

Úvod

Protokoly kvantové distribuce klíčů (QKD) jsou v současnosti nejrozšířenější aplikací kvantové kryptografie. Tzn. odvětví kryptografie opírající se o principy kvantové mechaniky a nabízející tak tzv. bezpodmínečnou bezpečnost. Ačkoliv je dnes QKD záležitostí spíše státních institucí a velkých firem, díky hrozbě brzké existence kvantových počítačů lze očekávat jejich postupné nasazení i jinde.

Tato práce si klade za cíl objasnit principy a význam kvantové kryptografie v tzv. postkvanové době[1] a poukázat na nedostatky současných algoritmů asymetrické kryptografie, které jsou založeny na matematických problémech. Následně budou vysvětleny základy kvantové mechaniky v míře potřebné pro pochopení principu činnosti kvantových technologií.

Pro komplexní zabezpečení komunikace proti kvantovému počítači je nutné využívat tří základních technologií. Jedná se o kvantové generování čísel (QRNG), kvantovou distribuci klíčů (QKD) a postkvantovou kryptografii (PQC). Pozornost bude věnována zejména QKD protokolům. Technologie QRNG a PQC budou popsány jen stručně.

V rámci popisu QKD bude rovněž rozebrána problematika bezpodmínečné bezpečnosti a bude představen tzv. PNS útok a návnadové stavy. Tedy jeden ze základních útoků na praktické nedokonalosti QKD zařízení a následná záplata.

Komplexní QKD systémy se ovšem neskládají pouze ze zařízení implementujících daný protokol. Z tohoto důvodu je nutné seznámit se i s možným referenčním modelem QKD sítě (QKDN). Demonstrovány budou taktéž principy správy klíčů, jež jsou momentálně rozhodující pro budování jakýchkoliv komplexnějších topologií.

V neposlední řadě bude následovat rešerše organizací poskytujících komerčně dostupná řešení QKD. Spolu s nimi budou stručně popsány nabízené technologie. Nejperspektivnější budou následně srovnány pomocí tabulek.

V praktické části budou představeny výsledky simulací vybraných QKD protokolů, které byly uskutečněny v nástroji *VPI Photonics*. Závěrem je prezentován návrh a sestavení vlastního QKD polygonu s využitím zařízení *Clavis*[3], technologii společnosti *IDQ*.

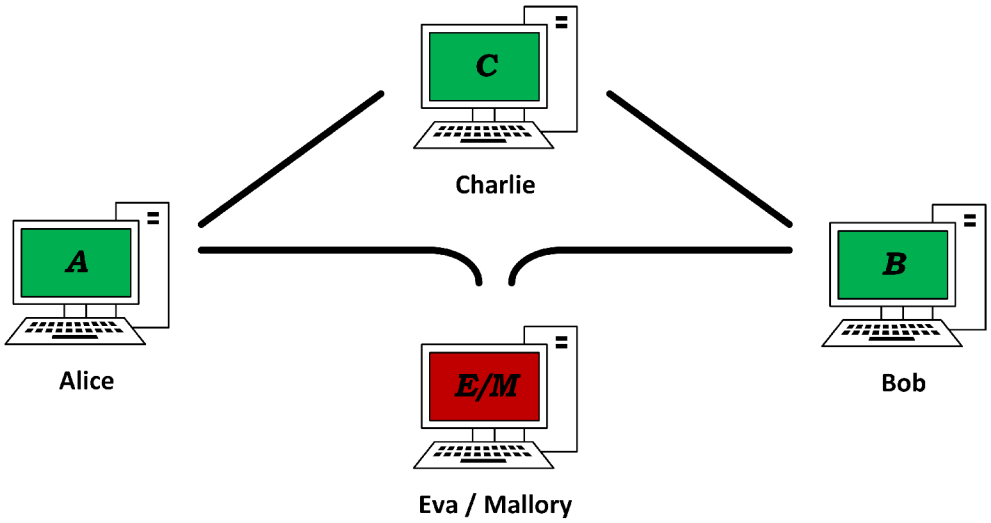
[1] Období po sestavení prvního dostatečně výkonného kvantového počítače.

1 Popis a notace

V první praktické kapitole této práce budou stručně vysvětleny základy šifrované komunikace a jejich souvislost s distribucí klíčů pro správné šifrování a dešifrování přenášených dat. Nejdříve však proběhne seznámení se s běžně používanou kryptologickou notací zvanou Alice a Bob.

1.1 Alice a Bob

Tato notace bývá používána pro lepší pochopení kryptografických protokolů. Jména jsou odvozena od počátečních písmen abecedy. Uzel A je tedy nazýván Alice, uzel B se jmenuje Bob. Tyto entity tvoří absolutní základ jakékoliv komunikace, často se však vyskytují i další uzly. Spolu s Alicí a Bobem lze tak narazit i na dalšího běžného účastníka – uzel C. Z tohoto důvodu se nazývá Charlie (nebo Carol). V případě, že by se jednalo o útočníka, bude se jmenovat Eva (eavesdropper – pasivní, nezasahuje do komunikace, pouze odposlouchává) případně Mallory (malicious – aktivní, zasahuje do komunikace). Takovýchto fiktivních postav existuje více. Pro potřebu této práce, však budou tyto více než dostatečné. Důležité je uvědomit si, že pod každým jménem se může skrývat libovolná komunikační entita (např. servery, směrovače atd.) [1].



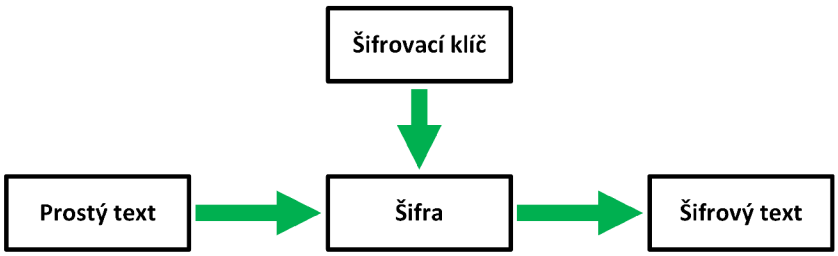
Obr. 1.1: Příklad notace Alice a Boba spolu s dalšími aktéry [1].

1.2 Distribuce klíčů

1.2.1 Důvody vzniku distribuce klíčů

Alice chce Bobovi poslat tajnou zprávu tak, aby si ji potenciálně odposlouchávající Eva nemohla přečíst. Aby tomuto zabránila, musí obsah této zprávy zašifrovat. K tomuto účelu slouží celá škála šifrovacích algoritmů (šifer) symetrické kryptografie. Ačkoliv není jejich detailnější charakteristika předmětem tohoto dokumentu, je nutné je alespoň stručně popsat [2].

Jak je možné vyčíst z obrázku 1.2, samotná šifra má 2 vstupy. Jedním z nich je prostý nezašifrovaný text, druhým potom symetrický šifrovací klíč. Kombinací šifrovacího postupu s šifrovacím klíčem je Alice schopná zprávu zašifrovat. Stejný klíč potom musí použít na druhé straně k dešifrování Bob. Zatímco dříve byl utajován samotný šifrovací postup, dnes převládá odlišný přístup. Postup většiny šifer je dnes veřejně známý, a tak je v současnosti tím, co chrání zašifrovanou zprávu před prozrazením výhradně tajný šifrovací klíč [2].



Obr. 1.2: Obecné schéma šifrovacího algoritmu [3].

1.2.2 Průběh

Jak již bylo řečeno, k samotnému šifrování zprávy je používána symetrická kryptografie. To znamená, že Alicin klíč pro šifrování i Bobův klíč pro dešifrování jsou shodné. Aby tedy mohla šifrovaná komunikace vůbec probíhat, musejí se nejdříve Alice s Bobem dohodnout na společném klíči. Tato výměna, respektive distribuce klíčů, ale musí být většinou provedena přes veřejný kanál, kde hrozí, že je bude odposlouchávat Eva. Ta by následně mohla se získaným klíčem rozšifrovat celou tajnou komunikaci mezi Alicí a Bobem. Je nutné rovněž předpokládat, že se Alice s Bobem nikdy dříve nesetkali a nemohli se tak dopředu na klíči domluvit.

V tuto chvíli je zřejmé, že klíč nejde prostě jednoduše symetricky zašifrovat. Z tohoto důvodu bylo třeba vyvinout jiné typy kryptografie. Dnešní distribuce klíčů jsou tedy postaveny na kryptografii asymetrické, která se opírá o dosud nevyřešené

matematické problémy. Z důvodů, které budou popsány později, se ale začíná objevovat i zcela odlišný způsob výměny klíčů, využívající fyzikálních vlastností částic a teorie kvantové mechaniky – tzv. kvantová distribuce klíčů, někdy též nepřesně zvaná kvantová kryptografie.

2 Současné techniky distribuce klíčů

Dnešní způsoby distribuce dešifrovacích klíčů staví na jednosměrných matematických funkcích. Jednosměrná funkce $f(x)$ je taková funkce, kterou lze na základě vstupu x snadno spočítat. Pro výpočet inverzní funkce $g(x)$, však dnes neexistuje algoritmus. Jedinou možností je tedy vyzkoušet všechny možnosti, což může být při použití dostatečně velkých čísel časově velmi náročné. Přesněji vyjádřeno, v tuto chvíli nelze tyto problémy řešit v polynomiálním čase. Aby bylo zajištěno, že bude existovat pouze jedna přípustná varianta $g(x)$, využívá asymetrická kryptografie výhradně kombinace prvočísel. Současná asymetrická kryptografie, a tedy i distribuce klíčů staví právě na těchto problémech. Níže jsou uvedeny dva nejčastěji používané protokoly. DH využívá problému diskrétního logaritmu, zatímco RSA staví na problému faktorizace.

2.1 RSA: Rivest & Shamir & Adleman

RSA je asymetrickou šifrou. To v praxi znamená, že pro šifrování (ověření podpisu) a dešifrování (podepsání) využívá dvou odlišných klíčů. Veřejný klíč (VK), jak již název napovídá, je obecně dostupný (např. v rámci PKI) a jakákoliv entita ním může zašifrovat svá data (případně ověřit podpis). Ta potom odešle příjemci, který vlastní soukromým klíčem. Tento soukromý klíč (SK) je naopak tajný a zná jej pouze ta entita, která ním data dešifruje (případně podepisuje). Podstatnou informací tedy je, že data zašifrovaná veřejným klíčem, nelze tímto klíčem zpětně dešifrovat. Obdobně data podepsaná pomocí SK, nelze pomocí tohoto klíče ověřit [2].

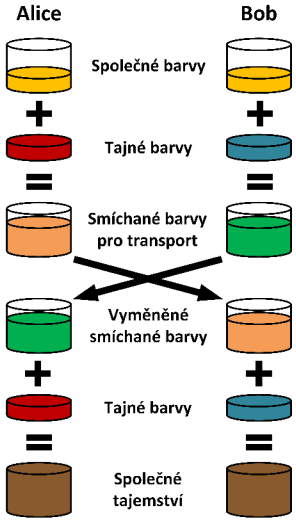
2.1.1 Faktorizace v RSA

Nechť je funkce $f(x) = 11x$, pokud je na vstupu např. $x = 7$, není žádným problémem zjistit výsledek. Funkce $f(x) = 11 \cdot 7 = 77$. Pro inverzní funkci $g(x) = 77$ však v současnosti neexistuje žádný algoritmický způsob, jak zjistit její podobu. I kdyby bylo známo, že číslo 77 vzniklo vynásobením dvou jiných přirozených čísel, nebude tato informace jakkoliv platná. V tomto stavu není možné určit, která kombinace čísel dá výsledek 77 a je tak nutné vyzkoušet všechny možnosti.

2.2 DH: Diffie & Hellman

U Diffieho-Hellmanova protokolu funguje koncept soukromého a veřejného klíče odlišně než u RSA. Soukromé klíče jsou dva a označují se tak tajné hodnoty vstupující do algoritmu jak ze strany Alice, tak ze strany Boba. Jako veřejný nebo sdílený klíč se potom označuje hodnota, která z algoritmu vystupuje, a i přes odlišný postup vychází na obou stranách stejně. Jelikož detailní popis těchto algoritmů není tématem této práce, je pro lepší pochopení použito přirovnání s barvami na přiloženém obrázku 2.1. Zde je možné SK připodobnit k tajným barvám (červená a zelená), zatímco VK symbolizuje hnědá barva dole [2].

Pokud je DH použit samostatně je náchylný na útoky typu Man-In-The-Middle (MITM). V tomto případě dojde kvůli absenci autentizace k navázání klíče s „mužem uprostřed“. Tzn., že se mezi Alicí a Bobem vyskytuje třetí entita – Eva. Eva tedy ustanoví dva sdílené klíče, jeden pro komunikaci s Alicí a druhý pro komunikaci s Bobem. To jí umožňuje odposlouchávat jejich vzájemnou komunikaci. Aby se tomuto předešlo, bývá DH používán v kombinaci s jinými protokoly zajišťujícími autentizaci jako TLS/SSL [2].



Obr. 2.1: Intuitivní pojetí Diffie-Hellmanova protokolu [4].

2.2.1 Diskrétní logaritmus v DH

Nechť je funkce $f(x) = 5^x \ (mod\, 23)$. Bude-li na vstupu např. $x = 2$, není podobně jako u faktorizace žádný problém rovnici vyřešit.

Tzn. $f(x) = 5^2 \ (mod\, 23) = 25 \ (mod\, 23) = 2$. Opět však ani v případě znalosti inverzní funkce $g(x) = 2 = 5^x \ (mod\, 23)$ nelze určit hodnotu x a je tak třeba postupně zkoušet všechny možnosti.

2.3 Problém P vs. NP

Problémem jednosměrných funkcí je však to, že není vůbec jasné, zda vůbec existují. Aby bylo možné na tuto otázku odpovědět, je v první řadě nutné vyřešit tzv. Problém P vs. NP. Tedy stručně řečeno platí, že P = NP? Pojmy jako P a NP třída definoval poprvé americký informatik Stephen Cook. Podle jeho teorie existuje třída P obsahující všechny úlohy, které je možné řešit pomocí deterministického Turingova stroje (DTM) v polynomiálním čase. Třída NP, je rozšířením P o ty úlohy, které lze algoritmicky řešit pouze na nedeterministickém Turingově stroji (NTM). Na DTM je jejich výpočet velmi časově náročný a prakticky spočívá v tom, že stroj zkouší postupně všechny možnosti tak, jak je vysvětleno na příkladech výše. Narozdíl od DTM, jehož reálnou implementací jsou prakticky všechny dnešní počítače, nic takového jako NTM v současnosti neexistuje [5].

Vyřešením problému P = NP by tedy byla současně zodpovězena otázka, zda jednosměrné funkce existují nebo ne. Respektive, zda pro dnešní počítače algoritmus pro výpočet jejich inverzní funkce neexistuje, nebo zda zatím pouze nebyl nalezen. Jedná se o jeden z největších matematických problémů 21. století, jehož vyřešení by mohlo mít fatální důsledky pro současnou asymetrickou kryptografii. Dnes se však spíše očekává, P $\neq$ NP, v případě opaku by bylo jasné, že nic jako jednosměrné funkce neexistuje a žádný NTM tedy není k jejich řešení potřeba [5].

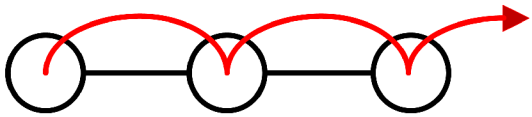
3 Důvody vzniku kvantové kryptografie

Ačkoliv již bylo v předchozí kapitole řečeno, že nic jako nedeterministický Turingův stroj momentálně neexistuje, a současně není pravděpodobné, že by šlo NP úlohy řešit na DTM, na obzoru se pomalu začíná objevovat další hrozba pro asymetrickou kryptografii. V této kapitole bude stručně vysvětlen rozdíl mezi DTM, NTM a kvantovým počítačem.

Nejdříve bude představena teorie vyčíslitelnosti, jedná se obor na pomezí matematiky a informatiky zabývající se tím, zda je možné problém řešit za pomoci algoritmu. Z pohledu teorie vyčíslitelnosti existuje několik výpočetních modelů. Každý Turingův stroj funguje na principu přechodu mezi stavy pomocí přechodové funkce. Jinak řečeno, problém je rozdělen na kroky a mezi těmito kroky je poté přepínáno pomocí přechodové funkce [6].

3.1 Deterministický Turingův stroj (DTM)

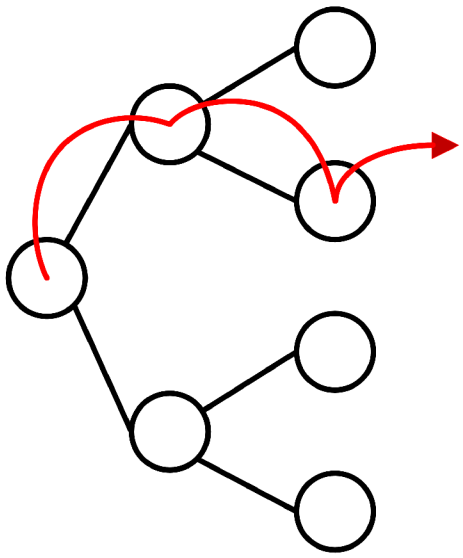
Jak již název napovídá, jeho chování je deterministické neboli dopředu určené. V praxi to znamená, že existuje pouze jedna varianta přechodové funkce a stroj si nemůže vybrat, kterým krokem bude pokračovat. Jedná se o téměř všechny dnešní počítače [6].



Obr. 3.1: Schéma stavů a přechodové funkce v DTM.

3.2 Nedeterministický Turingův stroj (NTM)

Druhou, ačkoliv zatím neexistující variantou Turingova stroje je NTM. Na rozdíl od předchozího se u něj vyskytuje několik možných přechodových funkcí. Kroky, kterými by se měl počítač řídit nejsou poskládány lineárně za sebou, ale tvoří strom. V něm se NTM snaží výběrem vhodných přechodových funkcí dostat ke správnému řešení [6].



Obr. 3.2: Schéma stavů a přechodové funkce v NTM.

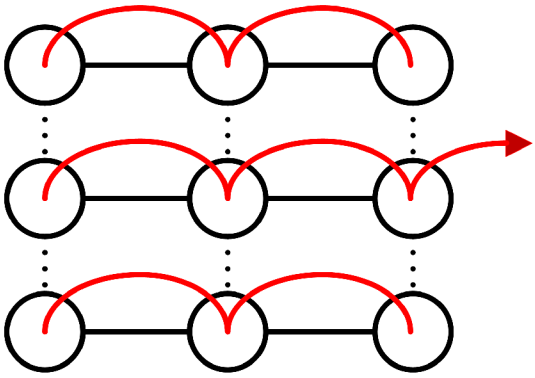
3.3 Kvantový Turingův stroj (QTM)

Běžně (nepřesně) také kvantový počítač je stroj, fungující na principech kvantové mechaniky. Na rozdíl od předchozích dvou, je schopen počítat ohromné množství operací současně (paralelně). To ale neznamená, že by měl stejné množství výstupů. Po provedení operací zkolabuje QTM s určitou pravděpodobností do jednoho ze stavů. To, s jakou pravděpodobností bude vrácen správný výsledek, závisí na povaze algoritmu. Z tohoto důvodu je výpočty třeba provádět vícekrát za sebou. Správný výsledek by se měl vyskytovat nejčastěji [7, 8, 9].

Kvantové počítače nepracují s bity nýbrž s qubity. To jim umožňuje exponenciálně zvýšit množství prováděných operací přidáním jen malého množství těchto qubitů. S množstvím pouze 1000 qubitů je možné současně provádět operaci nad 2^{1000} stavy současně. Jednotlivé stavy tak společně tvoří jeden vícequbitový systém, znázorněný na obrázku 3.3 tečkovanou čarou. V současnosti má však většina těchto strojů registr maximálně o několika desítkách qubitů [7, 8, 9].

Není ovšem pravda, že by kvantový počítač byl obecně rychlejší něž běžné počítače. Kvantové počítače jsou vhodné pro řešení specifických úloh. Typicky se jedná o hledání nejlepšího řešení, např problém obchodního cestujícího, lámání šifer, modelování molekul pro farmaceutický průmysl atp [7, 8, 9].

Neexistuje ovšem úloha, kterou by klasický počítač nemohl spočítat a kvantový ano. Rozdíl je však v efektivitě. Naopak se odhaduje, že třída problémů řešitelná pomocí QTM, není shodná se třídou, kterou řeší NTM. To znamená, že modely jsou určeny k řešení odlišných problémů. BQP je potom třída problémů, které je QTM schopen řešit s minimální pravděpodobností 66 %. Vztah mezi třídami BQP a NT, však není znám [7, 8, 9].



Obr. 3.3: Schéma stavů a přechodové funkce v QTM.

3.4 Shorův algoritmus

Jedná se o algoritmus částečně navržený pro kvantové počítače od Petera Shora z roku 1994 (velká část je ovšem klasický algoritmus). Pomocí něj je možné řešit problémy faktorizace a diskrétního logaritmu (včetně variant nad eliptickými křivkami) v polynomiálním čase. Z tohoto důvodu se jedná o hrozbu pro současnou asymetrickou kryptografii a spolu s kvantovými počítači je důvodem vzniku QKD systémů [6, 10, 11, 12].

3.4.1 Příklad

Pro rok 2020 byla minimální doporučená délka klíče u algoritmu RSA 2048. Na běžných počítačích by prolomení této šifry zabralo odhadem 300 trilionů let. Ačkoliv bude velmi záležet na samotných kvantových procesorech, odhaduje se, že na kvantových počítačích by tento problém mohl být vyřešen v řádu několika minut až hodin. Podle některých odhadů, by při použití kvantového počítače s cca 4000 qubity mohla být šifra prolomena dokonce do 10 sekund [13].

3.5 Groverův algoritmus

Jestliže Shorův algoritmus představuje hrozbu pro asymetrickou kryptografii, Groverův algoritmus lze s nadsázkou považovat za jeho protějšek vůči kryptografii symetrické. Navržen byl roku 1996 Lovem Groverem. Reálně je však tento algoritmus univerzálnější a nepřináší až takové zrychlení jako algoritmus Shorův. Jeho výsledkem je snížení náročnosti úlohy z $O(N)$ na $O(\sqrt{N})$. Na druhou stranu je tento algoritmus pro lámání symetrických šifer velmi náročný na počet qubitů. Z tohoto důvodu tak není jasné, zda se bude v blízké budoucnosti dát využít [9, 12, 14, 15, 16].

3.5.1 Příklad

Při použití šifry AES se 128bitovým klíčem existuje 2^{128} možných kombinací klíčů. To je v současnosti stále považováno za bezpečné. Groverův algoritmus ovšem zredukuje počet těchto možností pouze na $\sqrt{2^{128}} = 2^{64}$. Tato hodnota již ovšem bezpečná není (kvůli obtížné implementaci GA, by však měl být i 128bitový klíč stále bezpečný). Při 256bitovém klíči by po aplikaci Groverova algoritmu sice došlo k degradaci na klíč 128bitový, ten je však stále považován za bezpečný. Obecně je tedy symetrická kryptografie mnohem méně náchylná na hrozbu kvantových počítačů. Musí však být použity vhodné algoritmy s dostatečnou délkou klíče [16].

4 Základy kvantové mechaniky

Přestože není hlubší analýza kvantové mechaniky prioritním zaměřením této práce, je nutné si základní pojmy z tohoto oboru zavést alespoň intuitivně. Pojmy, jako např. qubit, jsou pro porozumění technologií QKD zásadní, proto budou ve stručnosti vysvětleny.

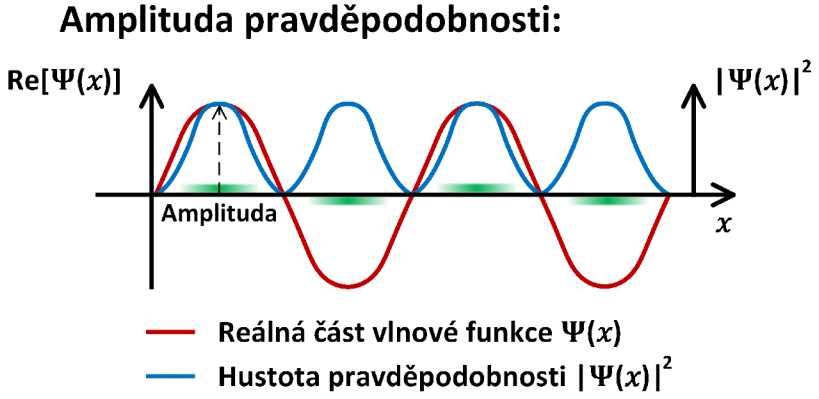
4.1 Intuitivní pojetí kvantové mechaniky částic

Principy kvantové mechaniky částic se značně liší od vlastností objektů, na které je člověk zvyklý z klasického makrosvěta. Zatímco v makrosvětě dochází ke striktnímu rozlišování vln a hmotných objektů, v mikrosvětě nic takového neplatí. Libovolná částice, ať už se jedná o světelný foton, nebo např. atom hmoty, má vlastnosti obou. Každá vlastnost se však projevuje výrazněji v odlišných případech. Zatímco někdy se částice projevuje spíše „vlnovitě“, jindy si ji pro zjednodušení člověk představuje jako jakýsi konkrétní míček s jasně danou polohou [17].

4.1.1 Vlna nebo částice?

Tato myšlenka, lépe vyjádřena jako dualita částice a vlnění, přiřazuje částicím vlnové vlastnosti. Jakým způsobem spolu tedy tyto vlastnosti souvisejí? Jednoduše řečeno, nelze jednoznačně říct, kde přesně se daná částice v určitém čase nachází. Lze to však vyjádřit pravděpodobnostně pomocí tzv. vlnové funkce $\Psi(x)$ [17, 18].

Je-li tedy částice opravdu objektem, není možné s jistotou sdělit, kde se momentálně nachází. Zde však přichází na řadu vlnové vlastnosti částice. Z obrázku 4.1 je zřejmé, že v rámci fáze vlny je největší pravděpodobnost výskytu částice (koncentrace zelené barvy) v takovém bodě x, kterým prochází i amplituda [17, 18].

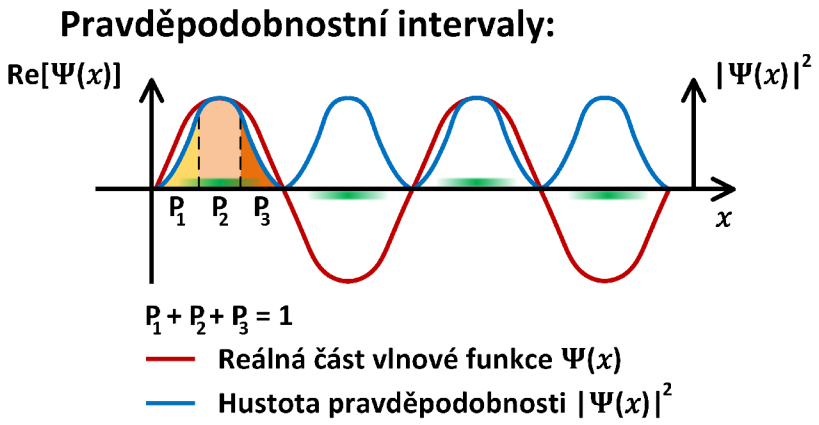


Obr. 4.1: Pravděpodobnost výskytu částice [17, 18].

Protože se však jedná o spojité rozdělení, je možné určit pouze pravděpodobnostní intervaly, ve kterých by se částice mohla nacházet. Přitom je jisté, že se zde někde částice vyskytuje se 100% pravděpodobností. První fázi lze rozdělit např. na 3 stejně velké intervaly podle osy x tak, jak lze vidět na obrázku 4.2. Pravděpodobnost, že se částice vyskytuje v určitém intervalu, je potom rovna obsahu tohoto intervalu pod funkcí hustoty pravděpodobnosti. Z vlnové funkce $\Psi(x)$ lze snadno vypočítat funkci hustoty jako $|\Psi(x)|^2$. Výsledná pravděpodobnost výskytu se následně spočítá jako:

$$P_{a \leq x \leq b} = \int_a^b |\Psi(x,t)|^2 \, dx \tag{4.1}$$

Tímto vzorcem lze následně dopočítat všechny tři vyznačené úseky. Není asi překvapující, že součet všech tří pravděpodobností musí být roven 1, tedy celková pravděpodobnost, že se částice vůbec někde vyskytuje musí být 100 % [17, 18].

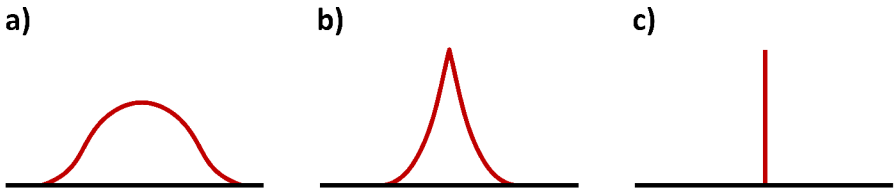


Obr. 4.2: Pravděpodobnostní intervaly [17, 18].

4.1.2 Kde tedy je?

Již dříve bylo řečeno, že částice má někdy spíše vlastnosti „objektu“ a někdy spíše vlny. Aby bylo možné přiblížit si, kdy se mění hranice mezi těmito dvěma stavy, je nutné nejdříve objasnit, co je vlastně měřením jejího výskytu. Měření v mikrosvětě se značně liší od měření ve světě makroskopických objektů, kde samotné měření nemá žádný vliv na existenci nebo změnu objektu. U mikroskopických částic je však měření aktem, kterým se z pravděpodobnostního vyjádření možné polohy částice (tzn. vlny) stává víceméně přesné určení její polohy (tzn. určí se poloha objektu). Tento jev je založen na Heisenbergově relaci neurčitosti, což je vztah mezi dvěma konjugovanými (propojenými) veličinami. Zde se jedná o polohu a hybnost. Tato relace říká, že čím více je možné určit jednu z veličin, tím méně přesně lze určit veličinu druhou. Jinými slovy, měření jedné z těchto vlastností částici ovlivní. Na této skutečnosti stojí například protokoly rodiny BB84 [17].

Tento přechod od vlny k „objektu“ je označován jako kolaps vlnové funkce a je znázorněn na obrázku 4.3. Ve chvíli, kdy částice letí a není měřena, nikdo neví, kde přesně se nachází a její vlnová funkce vypadá tak, jako v části *a*. Ve chvíli měření však dojde ke kolapsu vlnové funkce (část *c*). Je patrné, že určit pozici částice, je nyní mnohem jednodušší. Obecně platí, že vlnové funkce nehmotných částic jako např. foton mají tendenci vypadat spíše jako funkce na obrázku a, zatímco částice hmotné jako je atom jsou ostřejší jako v případě části *b*. To také umožňuje člověku vnímat polohu hmotné částice mnohem přesněji [17].

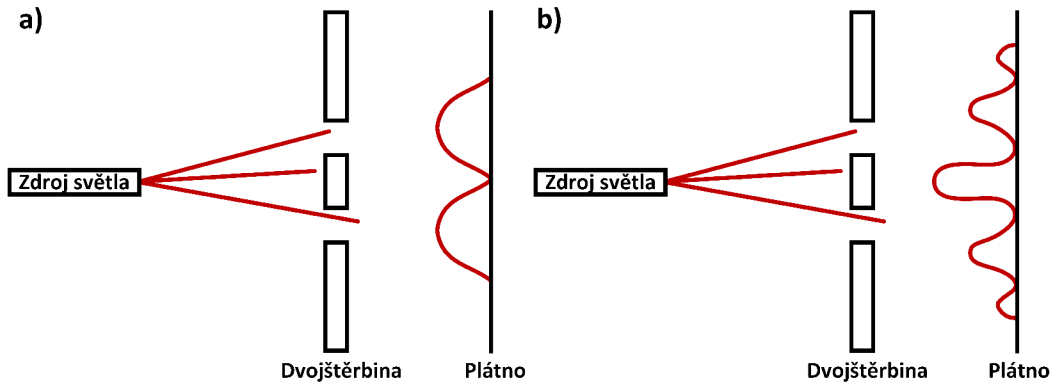


Obr. 4.3: Tvar grafu vlnové funkce udávající pravděpodobnosti výskytu částice [17].

V praxi ale není nikdo schopen změřit polohu částice s nulovou chybovostí. Zcela přesnou polohu částice je však možné odhadnout pomocí transformace její vlnové funkce na tzv. Diracovu delta funkci. Ta je znázorněna v části *c*. Její význam bude stručně nastíněn později [17, 19].

4.1.3 Youngův dvojšterbinový experiment

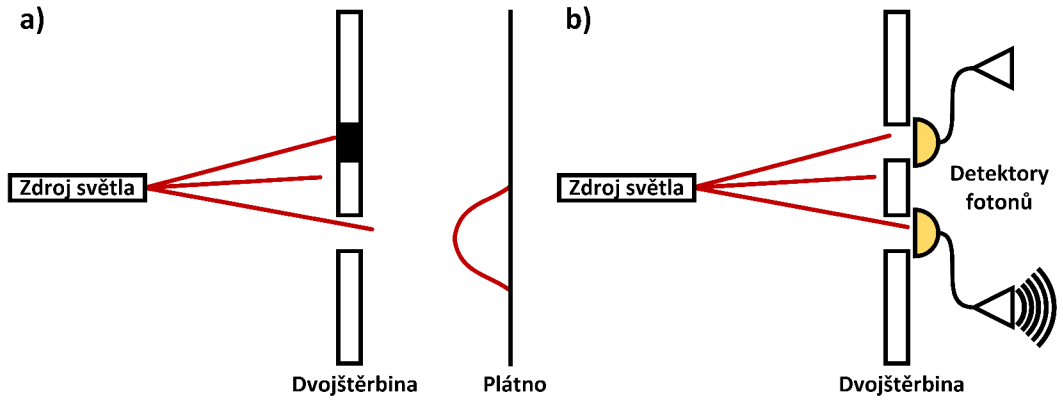
Jedná se o experiment, kterým Thomas Young roku 1801 prokázal, že světlo je vlněním. Francouzský fyzik Louis de Broglie následně dokázal platnost tohoto tvrzení i pro hmotné částice. Zde ovšem Youngův pokus poslouží i k vysvětlení dalších jevů. Základním předpokladem pro Youngův experiment je znalost rozložení dopadu hmotných objektů a vln po průletu dvojštěrbinou. Zatímco hmotné objekty se budou chovat podle rozložení *a* na obrázku 4.4, u světla dochází vlivem interferencí k rozložení pro vlny podobnému tomu v části *b* [17].



Obr. 4.4: Rozdíl rozložení dopadu u hmotných objektů a vln [17].

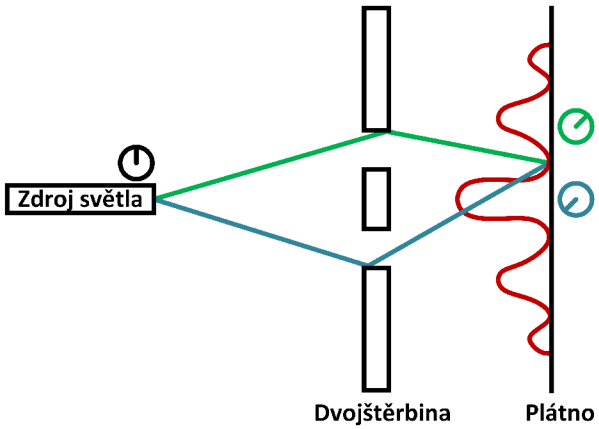
Nyní bude tento experiment dán do souvislosti s výše zmíněnou vlnovou funkcí a měřením tak, jak je zobrazeno na obrázku 4.5 na následující straně. Foton bude vystřelen z laseru a jedna ze štěrbin bude zakryta. Nemá tedy na výběr a musí projít jedinou možnou štěrbinou (případy, kdy foton neprojde vůbec, nebudou brány v potaz). Současně tak nemá s čím interferovat. Pokud bude vystřeleno více částic, pravděpodobné místo jejich dopadu na plátno bude reprezentováno rozložením, jenž bude podobné tomu v části *a* [17].

Nyní bude pokus zopakován s oběma štěrbinami odkrytými, plátno bude ovšem zaměněno za dva detektory tak, jako v části *b*. To, kterou štěrbinou foton prolétl bude známo podle toho, zda se ozve kliknutí na horním nebo spodním detektoru. Realita je ovšem od běžného uvažování odlišná. Foton totiž proletí oběma štěrbinami současně a vždy tak dopadne na odlišný detektor (existují tedy dva stavy v superpozici). Jak je něco takového možné, vysvětluje tzv. Kodaňská interpretace kvantové mechaniky, případně teorie multivesmíru (ang. multiverse) tak, že foton proletí oběma štěrbinami současně, vždy však v jiném vesmíru (realitě). Tyto vesmíry jsou zcela shodné, liší se pouze pozorovatelovou realitou toho, zda foton dopadl na horní nebo spodní štěrbinou [17].



Obr. 4.5: Rozdíl rozložení dopadu částic u jedné štěrbiny a dvojštěrbiny s detektory [17].

Ačkoliv se může zdát tato teorie těžko uchopitelná, má jeden velmi praktický důsledek – interferenci světla. Detektory budou nyní odstraněny a bude vráceno plátno tak, jak bylo naznačeno na obrázku 4.4 v části *b*. Již bylo řečeno, že foton proletí oběma štěrbinami. Teď ovšem obě jeho kopie dopadnou na stejné místo. Struktura na plátně tedy říká, jak je pravděpodobné, že existuje vesmír, ve kterém by existovaly dva stavy fotonu v takové superpozici, aby foton dopadl na dané místo na plátně. Richard Feynman ve své knize Neobyčejná teorie světla a látky uvádí intuitivní vysvětlení průběhu tohoto jevu s jeho vlivem na interferenci [17, 20].



Obr. 4.6: Vysvětlení interference podle Richarda Feynmana [17, 20].

Nechť zelená verze fotonu proletí horní štěrbinou, zatímco modrá verze fotonu proletí štěrbinou spodní. Pro představu bude nyní uvažováno, že oba fotony k sobě mají připevněny jakési stopky, tak jako na obrázku 4.6. Nyní bude pozornost věnována místům s destruktivní interferencí. Ve chvíli, kdy by fotony opustily laser, by stav na stopkách byl shodně 12 hodin. Protože zelený foton musí urazit kratší

vzdálenost, otočila by se rafička pouze na 2 hodiny. Modrý foton však dopadá se stavem 8 hodin. Jak je vidět, rafičky na ciferníku jsou přesně naproti sobě [17, 20].

Dále je známo, že oba vesmíry jsou shodné a k jejich rozdělení dochází až při průchodu dvojštěrbinou. Příčinou tohoto rozdělení jsou dvě nově vzniklé verze fotonu. Oba nové vesmíry tedy budou zcela shodné až na daný foton, který bude mít vždy jiné znaménko. To lze vyjádřit též matematicky. Zde A je stavem vesmíru, a stavem částice:

$$|A_1\rangle |a_1\rangle + |A_2\rangle |a_2\rangle = ?$$

Oba vesmíry jsou však shodné:

$$|A_1\rangle = |A_2\rangle = |A\rangle$$

Částice jsou shodné, mají pouze opačná znaménka:

$$|a_1\rangle = -|a_2\rangle$$

Z toho tedy vyplývá:

$$|A_1\rangle |a_1\rangle + |A_2\rangle |a_2\rangle = |A\rangle (|a_1\rangle - |a_1\rangle) = 0 \tag{4.2}$$

Místa s maximální destruktivní interferencí tedy znamenají, že neexistuje vesmír (je nulová pravděpodobnost jeho existence), ve kterém by foton do takové oblasti dorazil. Jinak řečeno, neexistuje vesmír, který by odpovídal takové superpozici. Případ opačných znamének je však velmi specifická varianta. Ve všech ostatních případech se hodnoty částic pouze částečně sčítají nebo odčítají, tzn. pravděpodobnost existence vesmíru s takovou superpozicí fotonu existuje. Maximální konstruktivní interference je potom dosaženo přesně ve středu plátna (mezi štěrbinami). Shrne-li se výše uvedené, je interference důkazem, že částice současně v různých vesmírech na sebe jsou schopny působit. Této vlastnosti se využívá například u kvantových počítačů a některých QKD protokolů [17, 20].

4.1.4 Kterou štěrbinou?

Jaká je ale pravděpodobnost průletu horní nebo spodní štěrbinou. Tuto otázku lze položit i jinak. Ocitne se pozorovatel po rozdělení tam, kde foton proletěl horní štěrbinou nebo v tom vesmíru, kde foton proletěl spodem. To, kterou štěrbinou foton prolétne, je zcela náhodná událost vždy s 50% pravděpodobností. To znamená, že ji nelze deterministicky jakkoliv určit. Zobecnění tohoto tvrzení znamená, že jsou-li dva stavy v takto vhodné superpozici dané vlnovou funkcí, je šance přesně poloviční, že zkolabuje do jednoho nebo do druhého z těchto stavů. Jedná se o skutečnou náhodnost, které se využívá například v kvantovém generování čísel (QRNG). Tímto se

výrazně liší od pseudonáhodného (PRNG), ale i „skutečného“ (TRNG) generování, které je založené na deterministickém chaosu. Zde podstata spočívá v tom, že člověk není schopen znát všechny proměnné k vypočítání výstupního čísla [17, 21].

4.2 Qubit

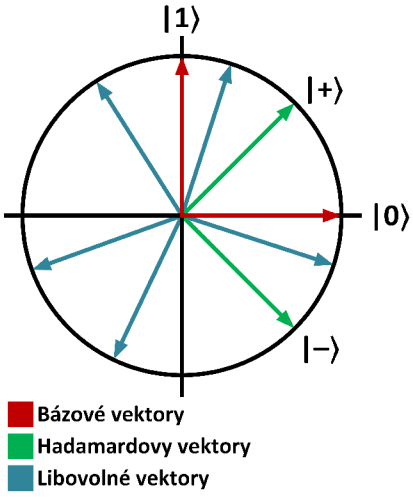
Zatímco klasický bit může nabývat jedné ze dvou hodnot, tj. 0 a 1, qubit může nabývat jak těchto stavů, tak jejich libovolné kombinace – superpozice. Samotný qubit je definován matematicky pomocí vektorů. Tato matematická abstrakce je tak nezávislá na libovolné fyzikální implementaci. Lze využít například spinu elektronu, spinu jádra atomu, nebo polarizace fotonu. Poslední varianta se u QKD systémů v praxi používá nejčastěji, proto bude spolu s matematickým modelem vysvětlena.

4.2.1 Matematický model

Z matematického hlediska je qubit jakýmkoliv systémem s dvojstavovým prostorem, tj. jedná se o dvojdimenzionální Hilbertův vektorový prostor. Tento prostor je určen ortonormální bází tj. z ortogonálních (vzájemně kolmých) normovaných (s délkou 1) vektorů $|0\rangle$ a $|1\rangle$. Jedná se o dva základní stavy celého systému, jejichž lineární kombinací (pouze pomocí sčítání vektorů a násobení skalárem) je možné vygenerovat jakýkoliv jiný vektor, tzn. jakýkoliv jiný stav sestávající ze superpozice vektorů $|0\rangle$ a $|1\rangle$. Matematicky je stav qubitu dán vzorcem:

$$|\Psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle \tag{4.3}$$

Zde $|\Psi\rangle$ je vektorem neboli libovolným kvantovým stavem. Koeficienty α a β určují poměr obou bázových stavů na dané superpozici. Matematický model je znázorněn na obrázku 4.7. Qubit bývá často zobrazován jako tzv. Blochova koule. Pro jednoduchost a lepší srovnání s polarizací fotonu bude ale nyní představena pouze dvourozměrná varianta tak, jako na obrázku 4.7 [17, 22, 23].



Obr. 4.7: Dvojrozměrný qubit vytvořený pomocí polarizace fotonu [17].

Qubit je zde znázorněn jako kružnice s červeně vyznačenou bází danou vektory $|0\rangle$ a $|1\rangle$. Může ovšem nabývat libovolného stavu. Na zmíněné kružnici je možné si takový stav představit jako libovolný jednotkový vektor. To znamená takový vektor, který začíná ve středu kružnice a končí na kružnici. Báze zelených vektorů $|+\rangle$ a $|-\rangle$ bývá využívána v kombinaci s bází červenou u QKD protokolů rodiny BB84. Zelený stav qubitu má při měření v červené bázi 50% šanci zkolabovat do stavu $|0\rangle$ i $|1\rangle$, stejně to potom platí i obráceně [17, 22, 23].

4.2.2 Souvislost vlnových funkcí vektorů

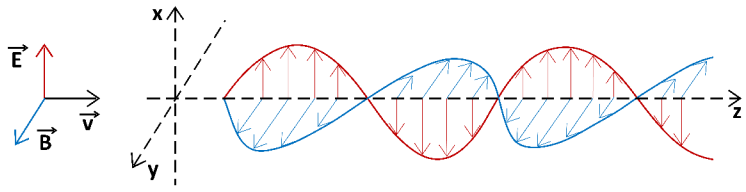
Zde bude vysvětleno, jakým způsobem souvisí qubit a kvantové stavy s vlnovou funkcí částice. Jak již bylo uvedeno výše, vlnové vlastnosti částice jsou reprezentovány její vlnovou funkcí (jedná se o funkce integrovatelné s kvadrátem v L^2 prostoru). Je-li nutné zcela bezchybně určit polohu takové částice, využívá Diracovy delta funkce. Ačkoliv delta funkce samy nejsou součástí L^2 prostoru, jedná se o bázové funkce určující celý prostor [17, 24].

Tab. 4.1: Porovnání matematických a fyzikálních pojmů [17].

Dvojdimenzionální vektorový prostor	Dvojstavový prostor	L^2 prostor
Vektor	Kvantový stav	(Vlnová) funkce integrovatelná s kvadrátem
Bázové vektory	Stavy $\|0\rangle$ a $\|1\rangle$	Delta funkce vlnové funkce

4.2.3 Polarizace fotonu

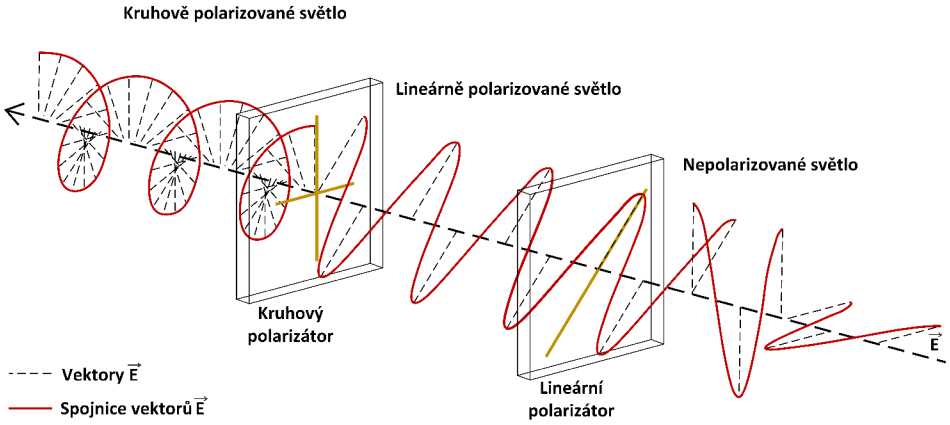
Fotonem se obecně rozumí libovolná elementární částice popisující kvantum elektromagnetického záření. V případě QKD se většinou využívá infračervené části světelného spektra. Tzn. elektromagnetických vln s frekvencí cca 430 THz až 300 GHz. Pojem elektromagnetická vlna bude přiblížen pomocí obrázku 4.8 níže [25].



Obr. 4.8: Zobrazení vektorů elektromagnetické vlny [26].

Jak je z obrázku patrné elektromagnetická vlna sestává 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 $\vec{E}$ [26].

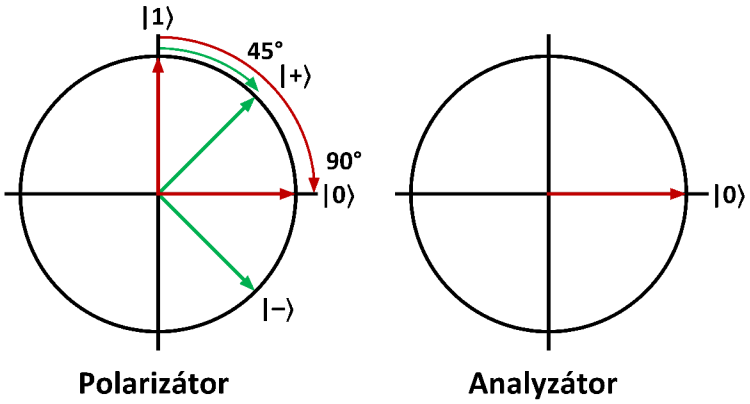
V případě, že vektor $\vec{E}$ rotuje kolem osy z náhodně (vždy je na ni ale kolmý), jedná se o světlo nepolarizované, to lze vidět v pravé části obrázku 4.9 níže. Pomocí půlvlnné destičky je možné světlo lineárně polarizovat, jak je znázorněno uprostřed. To znamená, že vektor $\vec{E}$ nyní kmitá v jedné rovině. Pomocí čtvrtvlnné destičky je možné světlo polarizovat kruhově (případně elipsovitě). V tomto případě bude vektor opisovat kružnici kolem osy z. Polarizace je reprezentována skládáním dvou lineárně polarizovaných vzájemně kolmých vln. Je-li jejich fázový posun nulový je vlna polarizována lineárně, je-li posun $\frac{\pi}{2}$ dojde k polarizaci kruhové. Jakýkoliv jiný posun vyústí v obecnou eliptickou polarizaci [27, 28].



Obr. 4.9: Zleva kruhová a lineární polarizace, vpravo nepolarizované světlo [26].

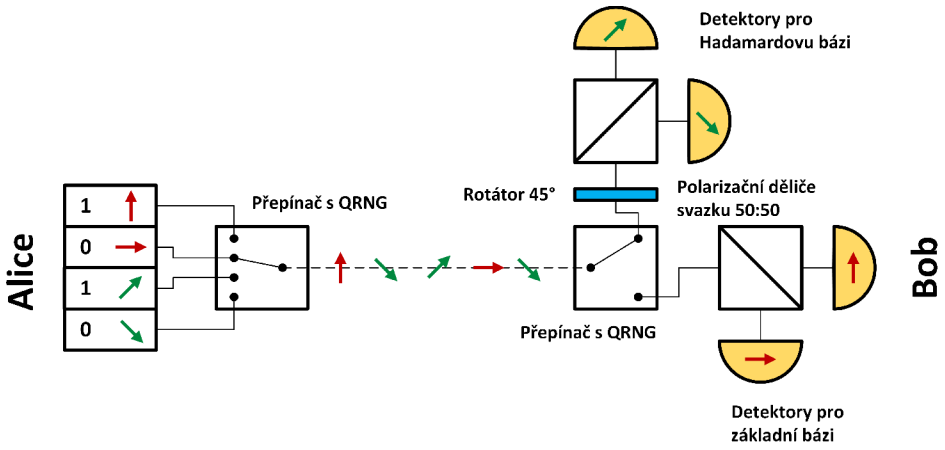
Pro srovnání matematického a fyzikálního qubitu bude nyní pozornost upřena výhradně na lineární polarizaci fotonu pomocí dvou polarizačních filtrů. Filtr, kterým světlo do sestavy vstupuje se nazývá polarizátor. Filtru, ze kterého světlo potom vystupuje, analyzátor [29, 30, 31, 32].

Na polarizátoru z obrázku 4.10 je vyznačena stejná základní báze jako u matematického modelu (červená). To znamená, že budou vysílány dvě varianty polarizovaného světla. Např. vodorovně polarizované ($\rightarrow$) odpovídající stavu $|0\rangle$ a svisle polarizované ($\uparrow$) fotony reprezentující stav $|1\rangle$. Mezi těmito stavy se bude přepínat pootočením polarizátoru o 90°. Stejně tak je ale možné vyslat libovolnou superpozici těchto dvou stavů. Vektor $|+\rangle$ lze získat jako zkosenou polarizaci ($\nearrow$) pootočením pouze o 45° doprava ze stavu $|1\rangle$. Obdobně potom vektor $|-\rangle$ neboli ($\searrow$) [17].



Obr. 4.10: Vlevo polarizátor, se střídajícími se stavy, vpravo analyzátor nastavený pevně na stav $|0\rangle$ [17].

Analyzátorem se neotáčí. Místo toho je např. trvale nastaven tak, aby byl ve stavu $|0\rangle$ neboli ($\rightarrow$). To znamená, že přilétající foton polarizovaný vodorovně ($\rightarrow$), vždy bez problému projde, zatímco foton ve svislém stavu ($\uparrow$) bude 100% odražen. Při použití dvou bází se v praxi využívá polarizačních děličů svazku. Ty určí následující „dráhu“ fotonu podle jeho polarizace. Na konci každé takovéto dráhy je jeden ze 4 fotonových detektorů. Možná implementace zdroje a soustavy detektorů je znázorněna na obrázku 4.11 na následující straně [17].



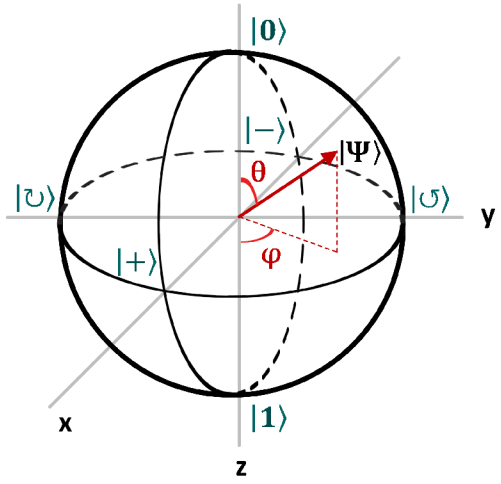
Obr. 4.11: Možná implementace zdroje a soustavy detektorů k rozlišení 4 stavů (protokol BB84) [33].

Jaký ale bude výsledek v případě, že přiletí jeden foton polarizovaný pro stav $|+\rangle$ nebo $|-\rangle$, případně jakákoliv jiná superpozice stavů. V tuto chvíli foton projde jen s určitou pravděpodobností. Jak již bylo nastíněno v matematické části, stavy $|+\rangle$ a $|-\rangle$ jsou výjimečné tím, že je u nich v „červené“ bázi přesně 50% šance na průchod. Jinak řečeno 50% šance na kolaps superpozice do stavů $|1\rangle$ nebo $|0\rangle$ [17, 33].

4.2.4 Blochova koule

V této části bude představena tzv. Blochova koule. Jedná se o alternativní grafické znázornění qubitu, nyní však trojrozměrné. Je důležité uvědomit si, že nemá fyzikální význam. Základním rozdílem oproti představě s polarizátory je vztah mezi dvěma ortogonálními vektory (např. $|0\rangle$ a $|1\rangle$). Zatímco u polarizátoru byly vzájemně pootočeny o 90°(kolmé), v Blochově kouli jsou posunuty o 180°.

Jak je vidět k původním čtyřem vektorům přibyl ještě levotočivý $|\circlearrowleft\rangle$ a pravotočivý $|\circlearrowright\rangle$ vektor na ose y. Tyto dva vektory tvoří tzv. rotační bázi, která je dána kruhovou polarizací fotonu. Pokud by jeden z vektorů $|\circlearrowleft\rangle$ nebo $|\circlearrowright\rangle$ byl změřen jinou než rotační bází, budou výsledky zcela náhodné stejně, jako to platí u lineárních bází. Příkladem využití této báze je např. Six State protocol (SSP), jinak se ale příliš často nevyužívá, proto se jí tento dokument blíže nevěnuje [12, 17, 34].



Obr. 4.12: Blochova koule [17].

Problém lze vyjádřit i matematicky. Za předpokladu, že je známo, že koeficienty α a β jsou komplexní čísla, lze výraz postupně upravit následovně:

$$\begin{aligned} |\Psi\rangle &= \alpha\,|0\rangle + \beta\,|1\rangle \\ |\Psi\rangle &= \cos\frac{\theta}{2}\,|0\rangle + e^{i\varphi}\sin\frac{\theta}{2}\,|1\rangle \end{aligned} \tag{4.4}$$

Jak možno vidět, polarizace fotonu ve stavovém prostoru je definována dvěma reálnými hodnotami – úhly θ a φ. To odpovídá pohybu po povrchu sférické (kulové) soustavy souřadnic [17].

4.3 Systémy s více qubity

Aby mohly být s qubity prováděny nějaké výpočty, bude jich pravděpodobně potřeba více než pouze jeden. Zde bude stručně vysvětlena, jejich výpočetní síla a budou představeny základní kvantové operace a pojmy. Jak již bylo zmíněno, jeden qubit může nabývat buďto stavů $|0\rangle$ a $|1\rangle$, nebo jejich libovolné lineární kombinace. V případě většího množství qubitů počet jejich stavů roste exponenciálně. To znamená, že při množství n qubitů, vznikne 2^n stavů. Nechť jsou tedy qubity dva. Jejich společný systém tak bude obsahovat 2^2 bázových stavů, tedy: $|00\rangle$, $|01\rangle$, $|10\rangle$ a $|11\rangle$. Stav systému o dvou qubitech lze pak popsat následovně:

$$|\Psi\rangle = \alpha\,|00\rangle + \beta\,|01\rangle + \gamma\,|10\rangle + \delta\,|11\rangle \tag{4.5}$$

Protože výpočetní síla kvantového počítače roste s počtem qubitů exponenciálně, je kvantový počítač schopen řešit ohromné množství operací současně. Například již při velikosti registru 1000 qubitů je schopen v jeden okamžik paralelně reprezentovat $2^{1000} \approx 10^{300}$ stavů a řešit nad nimi stejný počet operací [17].

4.3.1 Kvantová hradla a logické operace

Kvantové logické operace, případně brány nebo hradla se u qubitů vyskytují podobně jako v systémech s běžnými bity. Základem pro to, aby mohla být nějaká operace použita při kvantových výpočtech, je unitárnost z níž vyplývá normalizace a reverzibilnost. To znamená, že z výstupu musí být jednoznačně možné určit vstup. Samotné operace budou popsány pouze stručně, přehled o nich je však nutný pro porozumění pojmům jako kvantové provázání nebo kvantová teleportace. Při aplikaci kvantové operace na qubit nedochází k měření jeho stavu. Pokud je tedy qubit v superpozici, nedojde k jeho náhodnému kolapsu do jednoho z bázových stavů [17, 35].

4.3.2 Hadamardova operace

Jedna ze základních kvantových operací. Jedná se o kvantovou Fourierovu transformaci nad jedním qubitem. Stručně řečeno, v případě bázových stavů $|0\rangle$ a $|1\rangle$ dochází k jejich konverzi na superpoziční stavy $|+\rangle$ a $|-\rangle$. Hadamardova brána je definována pomocí následující matice [35, 36].

$$\hat{H} = \sigma_H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \tag{4.6}$$

$$\hat{H}\,|0\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} = |+\rangle$$

$$\hat{H}\,|1\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}} = |-\rangle$$

Nyní je zřejmé, jaký význam stavy $|+\rangle$ a $|-\rangle$ vlastně mají. Z tohoto důvodu lze někdy bázi těchto vektorů najít pod pojmem Hadamardova báze.

4.3.3 Operace identita

Tato operace znamená jednoduše to, že výstupem je stejný stav, jakým byl stav vstupní. Využita bude níže spolu s Pauliho operacemi [35].

$$\hat{I} = \sigma_I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \tag{4.7}$$

Pro Pauliho operace a identitu platí následující:

$$\hat{I} = \hat{X}\hat{X} = \hat{Y}\hat{Y} = \hat{Z}\hat{Z} = \hat{X}^2 = \hat{Y}^2 = \hat{Z}^2 = -i\hat{X}\hat{Y}\hat{Z}$$

To znamená, že pokud je operace použita dvakrát za sebou výsledkem je opět původní stav. Z tohoto vztahu je tedy možné určit i následující operace. Např. operace iY se spolu s I využívá u popisu protokolu LM05.

$$i\hat{X} = \hat{Y}\hat{Z} = -\hat{Z}\hat{Y}$$

$$i\hat{Y} = \hat{Z}\hat{X} = -\hat{X}\hat{Z}$$

$$i\hat{Z} = \hat{X}\hat{Y} = -\hat{Y}\hat{X}$$

4.3.4 Pauliho operace

Jedná se o základní operace nad qubity. Lze si je představit jako rotace Blochovi koule o 180° podle jednotlivých os. Protože jsou v Blochově kouli osy tři, existují i tři Pauliho operace. Pro potřebu této práce je nedůležitější Pauliho X-brána, tedy rotace Blochovy sféry kolem osy x o 180°. Tato operace je ekvivalentem klasické operace NOT. Využívá se však i Z-brána a pro úplnost je uvedena i Y-brána [35].

Pauliho X-brána (Prohození bitu / bit flip) je definována pomocí matice:

$$\hat{X} = \sigma_X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \tag{4.8}$$

$$\hat{X}\,|0\rangle = |1\rangle$$
$$\hat{X}\,|1\rangle = |0\rangle$$

Příklad:

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

Pauliho Y-brána je definována pomocí matice:

$$\hat{Y} = \sigma_Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \tag{4.9}$$

$$\hat{Y}\,|0\rangle = i\,|1\rangle$$
$$\hat{Y}\,|1\rangle = -i\,|0\rangle$$

Příklad:

$$\begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} = i \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

Pauliho Z-brána (Prohození fáze / phase flip) je definována pomocí matice:

$$\hat{Z} = \sigma_Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \tag{4.10}$$

$$\hat{Z}\,|0\rangle = |0\rangle$$
$$\hat{Z}\,|1\rangle = -\,|1\rangle$$

Příklad:

$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

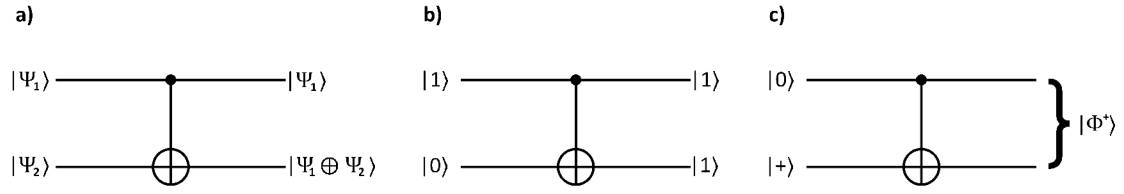
Fázový posun nemá vliv na stavy $|0\rangle$ a $|1\rangle$. Tzn. z tohoto pohledu je hodnota $|1\rangle$ ekvivalentní hodnotě $-\,|1\rangle$. Stav $|0\rangle$ je samozřejmě stejný vždy.

4.3.5 CNOT brána

Jedná se o „podmíněnou“ verzi Pauliho X-rotace (controlled NOT) a je ji možno použít ke kvantovému provazování částic. Tato operace již probíhá nad dvěma qubity. Obecné schéma operace lze najít na obrázku 4.13 v části a. Pokud je kontrolní qubit nastaven na $|1\rangle$ dojde k prohození stavu na cílovém qubitu. To demonstruje část b na stejném obrázku. V případě, kdy není ani jeden z qubitů v superpozici stavů $|0\rangle$ a $|1\rangle$, je určení výstupů prosté:

$$\begin{aligned} CNOT\,|00\rangle &= |00\rangle \\ CNOT\,|01\rangle &= |01\rangle \\ CNOT\,|10\rangle &= |11\rangle \\ CNOT\,|11\rangle &= |10\rangle \end{aligned} \tag{4.11}$$

Může se však vyskytnout i příklad, kdy je libovolný qubit v superpozici tak, jako v části c na obrázku. Zde nabývá kontrolní qubit stavu $|+\rangle$. V tomto případě dojde ke kvantovému provázání (propletení) obou částic. Tento nyní dvouqubitový systém má pak jeden společný stav, kterému se říká Bellův stav. V něm není možné rozlišit samostatné stavy daných částic. Bellovy stavy jsou maximálně korelovány. Tzn., že měření jedné z částic definuje výsledek měření druhé částice [37].



Obr. 4.13: Operace CNOT s různými vstupy [37].

Tyto stavy jsou čtyři a tvoří bázi dvouqubitového prostoru. Souhrnně jsou vyjádřeny níže:

$$\begin{aligned} |\Phi^{\pm}\rangle &= \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle) \\ |\Psi^{\pm}\rangle &= \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle) \end{aligned} \tag{4.12}$$

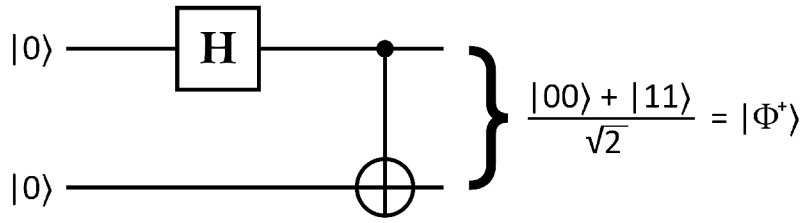
Každý z Bellových stavů se při dvou nezávislých měřeních (nad každým qubitem) chová mírně odlišným způsobem. Výsledné stavy obou částic závisí na daném Bellově stavu a na úhlu, který svírají Alicin a Bobův detektor. Podmínky, za kterých mají Bellovy stavy tendenci vždy kolabovat do stejných (korelace) a opačných (antikorelace) stavů, jsou uvedeny v tabulce 4.2.[1]

[1] Úhly odpovídají znázornění v Blochově kouli, nikoliv úhlům na polarizátoru. Např. úhel 180° v Blochově kouli tak znamená v případě polarizátoru pootočení jen o 90°.

Tab. 4.2: Tabulka chování Bellových stavů v závislosti na úhlu mezi detektory.

Bellův stav	**Úhel – korelace**	**Úhel – antikorelace**
$\|\Phi^+\rangle$	0°	180°
$\|\Phi^-\rangle$	0° a 180°	90° a 270°
$\|\Psi^+\rangle$	180°	0°
$\|\Psi^-\rangle$	90°a 270°	0°a 180°

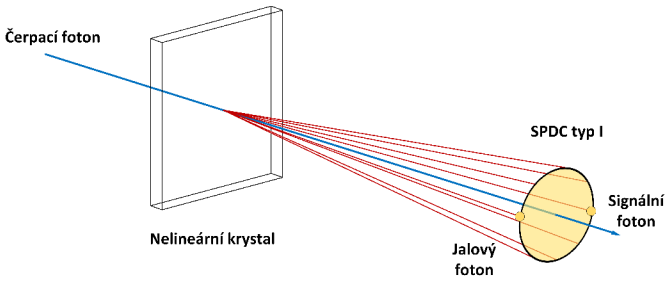
Kompletní kvantový obvod používaný ke kvantovému provázání dvou částic (vznik Bellových stavů) potom vypadá tak, jak je vidět na obrázku 4.14 níže. Vstupující stavy přímo určují výsledný Bellův stav. V tomto daném případě byl vytvořen Bellův stav $|\Phi^+\rangle$ [12, 37, 38].



Obr. 4.14: Kvantový obvod sloužící k vytvoření Bellova stavu $|\Phi^+\rangle$ [38].

4.3.6 Spontánní sestupná parametrická konverze (SPDC)

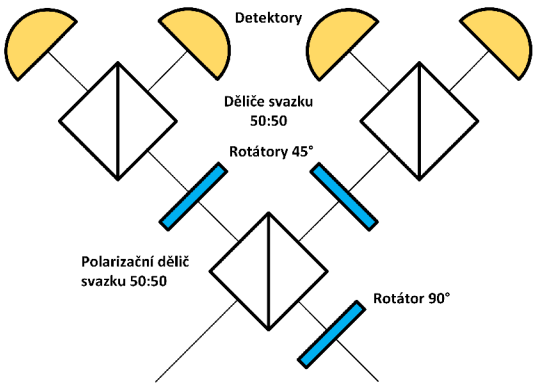
Operace CNOT však není jediným způsobem, jak vytvářet provázané částice. U fotonů se v praxi využívá tzv. spontánní sestupná frekvenční parametrická konverze. Její princip spočívá v tom, že je za pomoci speciálního krystalu zapříčiněn rozpad jednoho vysokoenergetického čerpacího fotonu (pump) na korelovaný fotonový pár. Tyto fotony jsou označovány jako signální (signal) a jalový (idle). Rozlišují se dva typy SPDC. SPDC lze dosáhnout pomocí Kwiatova zdroje, jehož zjednodušené schéma je naznačeno na obrázku 4.15 [39, 40].



Obr. 4.15: Kwiatův zdroj a SPDC typu I.

4.3.7 Měření Bellových stavů (BSM)

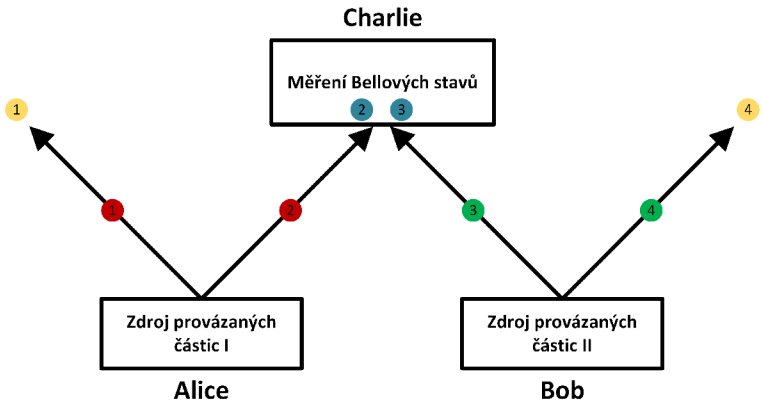
V kvantové informatice velmi používaná technika, sloužící k rozpoznávání Bellových stavů. V praxi však zatím není možné měřit současně všechny Bellovy stavy. Jedná se tedy o částečné BSM. Použitím tohoto měření dochází nejdříve k interferenci na děliči svazků (tím dojde k provázání, pokud částice provázány nebyly) a následně ke kolapsům na dva samostatné stavy, jako je tomu u běžného měření. Této vlastnosti se často využívá například u prohození provázání (entanglement swap). K tomuto účelu je BSM typicky využíváno například u MDI-QKD protokolů [41, 42, 43, 44].



Obr. 4.16: Schéma sloužící k měření Bellových stavů [41].

4.3.8 Prohození provázání (Entanglement SWAP)

K demonstraci fenoménu slouží obrázek 4.17. Nechť jsou dva zdroje provázaných párů. Alice vytvoří provázané fotony 1 a 2, Bob zase fotony 3 a 4. Jeden z fotonů (2 a 3) odešle každý z nich k detektoru Bellových stavů v uzlu Charlie. Tyto dva fotony spolu ovšem nejsou provázány. Jednoduše řečeno, BSM přehodí provázání fotonů takovým způsobem, že nyní budou provázány fotony 2 a 3 stejně jako pár 1 a 4. Jedná se o pozoruhodnou techniku, protože tyto fotony nepřišly nikdy do kontaktu a byly vzájemně provázány na dálku. Toho se využívá např. u některých DI-QKD protokolů [45].



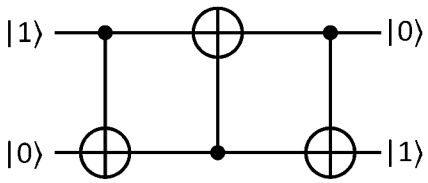
Obr. 4.17: Intuitivní znázornění prohození provázání [45].

4.3.9 Věta o zákazu klonování a operace SWAP

Tato věta říká, že není možné vytvořit nezávislou kopii neznámého kvantového stavu. Aby bylo možné něco takového udělat, musel by se nejdříve daný kvantový stav zjistit, což znamená provést měření, při kterém ovšem dojde ke kolapsu. Druhou možností je nechat daný stav „pozorovat“ jiným kvantovým systémem, podobně jak je popsáno u brány CNOT. Taková operace klonování by ovšem nebyla unitární a z tohoto důvodu není možná [17].

Zatímco kopírování qubitů není možné, existuje funkce, která dokáže jejich stavy prohodit. Toho je využíváno u některých QKD protokolů popsaných níže. Tato operace se nazývá SWAP a sestává ze tří za sebou střídavě zapojených CNOT operací. Funkčnost lze ověřit pomocí schématu 4.18 pro dvě libovolné kombinace qubitů [17].

$$\begin{aligned} SWAP\,|00\rangle &= |00\rangle \\ SWAP\,|01\rangle &= |10\rangle \\ SWAP\,|10\rangle &= |01\rangle \\ SWAP\,|11\rangle &= |11\rangle \end{aligned} \tag{4.13}$$



Obr. 4.18: Schéma operace SWAP využívající tři CNOT brány [17].

4.3.10 Kvantová teleportace

Pod tímto termínem se nerozumí samotný přenos částice, nýbrž přenos naměřeného stavu mezi dvěma provázanými částicemi. Jak již bylo uvedeno výše, měří-li detektory vzájemně svírající 0° dvě kvantově provázané částice ve stavu $|\Psi^+\rangle$, dojde změřením stavu $|0\rangle$ na jedné z nich k okamžitému kolapsu druhé částice do stavu $|1\rangle$ a naopak. Přitom nezáleží, jak daleko od sebe obě částice jsou. Albert Einstein popsal tuto akci jako „strašidelné působení na dálku“ a byl přesvědčen o neúplnosti nebo chybě v teorii kvantové mechaniky, což vyústilo v jeho spor s Nielsem Bohrem. Detailněji bude tato problematika popsána níže [46].

Na kvantovou teleportaci se však dá dívat i jako na kvantový algoritmus nad třemi částicemi, sestávající ze základních kvantových operací jako jsou Hadamardova hradla, nebo podmíněné X a Z rotace. Je však důležité podotknout, že pomocí kvantové teleportace nelze okamžitě komunikovat na dálku, jak se někdy mylně uvádí [17].

4.4 Kvantové provázání

Všechny zbývající principy v tomto dokumentu budou demonstrovány výhradně pomocí Bellova stavu $|\Psi^+\rangle$. To platí i v případě popisu jednotlivých protokolů.

Jak již bylo nastíněno výše, kvantové provázání je situace, kdy není možné rozlišit stavy dvou samostatných částic. Jedinou možností, jak jejich stav zjistit je měření, které je donutí zkolabovat do jednoho ze samostatných stavů. Kompletní měření tak provázání obou částic rozbije a výsledkem jsou opět dvě samostatné částice. Měření částic může probíhat různě. Nechť je například Alice a Bob, k nimž oběma letí jeden ze vzájemně provázaných fotonů. Alice je však se svým detektorem ke zdroji fotonů blíže, a tak k ní foton doletí dříve než k Bobovi. Pokud vlnová funkce Alicina fotonu při měření zkolabuje např. do stavu $|0\rangle$, zkolabuje vlnová funkce Bobova fotonu vždy do stavu $|1\rangle$ ještě před vlastním měřením [47, 48].

V tuto chvíli ještě nedochází k problémům. Platí-li speciální teorie relativity, není možné komunikovat rychlostí vyšší, než je rychlost světla. Jestliže tedy mezi sebou fotony komunikují, musí to stihnout před tím, než bude změřen i Bobův foton. Pokud by to nestihly, Bobův foton by „netušil“, do kterého stavu zkolabovat a výsledek by tak nebyl vždy 100% opačný [47, 48].

Problém však nastává ve chvíli, kdy jsou jak Alice, tak Bob od zdroje provázaných párů vzdáleni stejně. Logicky to znamená, že obě měření proběhnou ve stejnou chvíli. Pokud by tedy byly oba fotony změřeny ve stejnou chvíli, nemají žádný čas na komunikaci. Jinak řečeno, musela by podle Einsteina existovat jakási nadsvětelná (okamžitá) komunikace. To by znamenalo, že pokud se něco stane na libovolném místě, může to okamžitě ovlivnit situaci na úplně odlišné straně vesmíru, což by odporovalo speciální teorii relativity [47, 48].

4.4.1 EPR paradox

Alberta Einsteina tato myšlenka provokovala natolik, že v roce 1935 sestavil spolu s Borisem Podolskym a Nathanem Rosenem myšlenkový experiment, který později vešel ve známost jako EPR paradox. Ten představoval alternativu k Bohrově kvantové teorii, podle níž jsou propletené částice v obou stavech současně a stavy, které jsou později zjištěny před samotným měřením ještě neexistují [49].

Podle Einsteina byly obě částice již dopředu „domluveny“ na tom, do kterého stavu zkolabují. Tato informace měla být podle Einsteina uložena u každé částice v určitých skrytých proměnných. Tím pádem by tedy bylo již dopředu deterministicky určeno, jak situace dopadne [49].

4.5 Bellův teorém

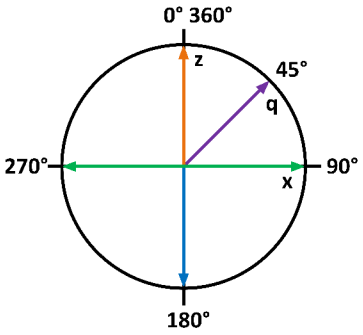
Až do roku 1964 byly obě teorie považovány za rovnocenné. S řešením následně přišel severoirský fyzik John Stewart Bell, kterému se nakonec podařilo prokázat platnost kvantové teorie a omyl EPR paradoxu. Bell sestavil nerovnici založenou na výsledcích opakovaných měření. Pro vesmír, ve kterém by platila EPR teorie o skrytých proměnných, musí tato nerovnice bezpodmínečně platit. Zatímco v případě, kdy platí kvantová teorie, dojde k porušení této nerovnosti.

$$P(Z_+, X_+) \leq P(Z_+, Q_+) + P(Q_+, X_+) \tag{4.14}$$

Pro lepší pochopení této nerovnice je nutné se nejdříve seznámit s níže popsanými pojmy, ty budou následně dány s rovnicí do souvislosti [49].

4.5.1 Korelace a Bellovy testy

Samotné slovo korelace vyjadřuje jakýsi vzájemný vztah mezi dvěma veličinami. Vztáhne-li se konkrétně na měření v kvantové mechanice, říká, jaký vliv má měření Alice na měření Boba. Může dojít k různým výsledkům na základě úhlu mezi detektory znázorněné v Blochově kouli na obrázku 4.19.[2]



Obr. 4.19: Zredukovaná Blochova koule bez rozměru Y [49].

Nyní bude opět uvažována Blochova koule, rozměr zadaný osou y však bude zanedbán. Bude tedy zredukována do polohy, kterou je možné najít na obrázku 4.19. Stav Alicina detektoru je zde ve stavu označeném oranžovou šipkou. Pootočení Bobova detektoru proti jejímu lze potom znázornit všemi třemi barvami tak, jak je znázorněno v tabulce 4.3.

Nechť tedy existuje kvantově provázaná dvojice fotonů tak, aby každý foton letěl opačným směrem. Jeden k Alici a druhý k Bobovi. V případě, že budou oba detektory nastaveny ve stejném úhlu (0° a 360°). Pak je vždy 100% pravděpodobnost, že jeden

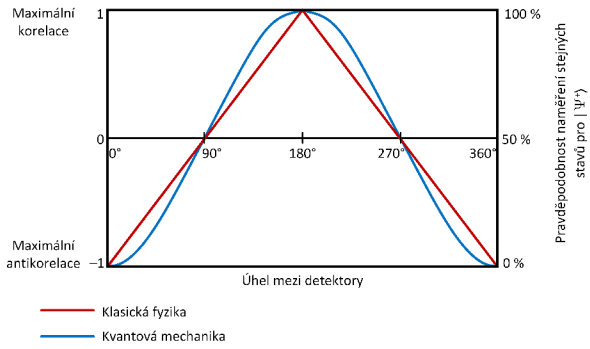
[2]Pozor, nejedná se o polarizátor.

ze stavů bude změřen jako $|0\rangle$ a druhý jako $|1\rangle$. Jedná se o maximální antikorelaci. Budou-li oba detektory pootočeny o 90°, pak je šance na naměřený opačný stav přesně 50 %. Korelace je zde nulová, to znamená, že měření na jednom z detektorů nějak neovlivní měření na detektoru druhém. Oba výsledky budou 100% stejné za předpokladu pootočení o 180°. Nyní se jedná se o maximální korelaci. Tyto výsledky očekává jak klasická fyzika, tak kvantová mechanika [49].

Tab. 4.3: Vliv úhlů mezi detektory na korelaci částic v Bellově stavu $|\Psi^+\rangle$. Uvedené barvy odpovídají vektorům zobrazeným na obrázku 4.19.

Úhel mezi detektory		**Opačné/shodné výsledky**	**Korelace**
0° a 360°		100% opačné	-1 (max. antikorelace)
90° a 270°		50% shodné, 50% opačné	0
180°		100% shodné	+1 (max. korelace)

Potíž však nastává, při pootočení detektorů o jiný úhel. Podle klasické fyziky by měl vztah mezi detektory být vyjádřen lineárně, jak je znázorněno červeně na obrázku 4.20. Podle kvantové mechaniky je ale tímto vztahem sinusová vlna vyvedená modře. Pokud tak například došlo k natočení detektorů vzájemně o 45° tak, jak ukazuje fialová šipka na obrázku 4.19, klasická fyzika bude očekávat opačný výsledek v 75 % případů (25 % případů bude shodný výsledek), zatímco podle kvantové mechaniky lze očekávat 85,4 % (14,6 % bude opačných) případů [49].



Obr. 4.20: Platnost klasické fyziky a kvantové mechaniky [50].

Výše uvedené je základem tzv. Bellova testu neboli praktického ověření platnosti Bellových nerovnic. V QKD protokolech se nejčastěji využívá konkrétní podoby, tohoto testu známé jako CHSH, k ověření provázanosti částic. Jsou-li částice provázané, budou výsledky měření při „nestandardních“ úhlech (45°, 22,5°, 67,5° atp.) odpovídat modré křivce. Pokud by však částice provázány nebyly (Eva je mohla vyměnit za předpřipravené oddělené stavy), budou výsledky odpovídat křivce červené [49, 50, 51].

4.6 Shrnutí

Nyní bude tedy detailněji popsána Bellova nerovnice, jež bude dána do souvislosti s praktickými výsledky měření, zmíněnými výše. Nechť je tedy nerovnice:

$$P(Z_+, X_+) \leq P(Z_+, Q_+) + P(Q_+, X_+)$$

Jednotlivé výrazy představují pravděpodobnost, že Alice i Bob naměří shodně stav $|1\rangle$ (index + v daných výrazech značí korelaci)...

$P(Z_+, X_+)$ ... pokud jsou oba detektory pootočeny o 90° (A: osa z, B: osa x)
$P(Z_+, Q_+)$ ... pokud jsou oba detektory pootočeny o 45° (A: osa z, B: osa q)
$P(Q_+, X_+)$ ... pokud jsou oba detektory pootočeny o 45° (A: osa q, B: osa x)

Nechť je uvažována platnost EPR paradoxu. Z grafu výše tedy lze předpokládat lineární průběh. Podle tabulky je zřejmé, že pravděpodobnost naměření shodných stavů, je při vzájemném natočení detektorů o 90° 50 %. Pravděpodobnost naměření shodných hodnot v případě druhém a třetím je 25 %. Jak lze tedy vidět nerovnice platí [49].

$$\begin{aligned} P(Z_+, X_+) &\leq P(Z_+, Q_+) + P(Q_+, X_+) \\ 0,5 &\leq 0,25 + 0,25 \\ 1 &\leq 1 \end{aligned}$$

V tomto případě bude naopak uvažována platnost kvantové teorie. V prvním případě, je pravděpodobnost opět 50 %. Druhý a třetí výraz odpovídají shodně pravděpodobnosti 14,6 %. V tomto případě dochází ke zřejmému porušení nerovnice [49].

$$\begin{aligned} P(Z_+, X_+) &\leq P(Z_+, Q_+) + P(Q_+, X_+) \\ 0,5 &\leq 0,146 + 0,146 \\ 0,5 &\leq 0,292 \end{aligned}$$

Závěrem se však ještě hodí podotknout, že ačkoliv byly Bellovy / CHSH testy považovány za důkaz správnosti Bellových nerovnic a tím i kvantové teorie, až donedávna se v těchto testech objevovaly (zejména dvě) díry (loopholes), díky kterým stále existovala možnost (ačkoliv velmi nepravděpodobná), že kvantová teorie není správná. Jedná se o:

- **Detekční díra** (Detection loophole) – Možnost, kdy došlo k chybě detektoru. Částice buďto změřena nebyla, nebo mohlo dojít k falešnému naměření.
- **Lokalitní díra** (Locality loophole) – Neznámá možnost, kdy by částice nebo detektory byly příliš blízko a mohly by tak spolu vzájemně komunikovat.

Při testech se tyto dvě díry dlouhou dobu nedařilo uzavřít obě současně. S prvním zaznamenaným případem přišli v roce 2015 výzkumníci z nizozemské Technologické univerzity v Delftu. Jedná se příčinu malého používání DI-QKD protokolů, které budou popsány později [48, 52].

5 Generování náhodných čísel

Pro kryptografii je generování skutečně náhodných čísel velmi důležité. Nechť je jako šifrovací klíč použit řetězec náhodně vygenerovaných čísel. Pokud by ho Eva byla schopna nějakým způsobem určit nebo odhadnout, byla by prolomena veškerá bezpečnost šifrování. Z tohoto důvodu je nutné zajistit dokonalý zdroj entropie. Od něj se očekává:

- **Rovnoměrné rozdělení** – generování všech možností probíhá se shodnou pravděpodobností
- **Nulová korelace mezi hodnotami** – nesmí existovat vztah mezi žádnými dvěma vygenerovanými hodnotami
- **Nemožnost predikce hodnoty** – neexistuje způsob jakým určit nebo odhadnout hodnotu
- **Rychlost** – nejedná se vyloženě o nutnost, v praxi však musí generování náhodných čísel stíhat poptávce odebírající aplikace (např. QKD)

Generátory náhodných čísel lze rozdělit do dvou základních kategorií: PRNG a TRNG (případně kombinace). Specifickým typem je pak tzv. QRNG založené na průchodu fotonu děličem svazku. Otázka skutečné náhodnosti je však v mnoha případech problematická [21].

5.1 Generátor pseudonáhodných čísel (PRNG)

Algoritmicky řešené generátory, využívající výpočetních / softwarových metod. Základním problémem ovšem je, že jakýkoliv v současnosti existující program je deterministický. To znamená, že existuje pouze jedna možnost, jak k výsledné hodnotě dojít. Ta, ač se člověku může jevit jako náhodná, ve skutečnosti náhodná není. Pro člověka pouze není snadné zjistit jakým způsobem byla vytvořena. Z tohoto důvodu je považuje za náhodné [17, 21].

5.2 Generátory skutečně náhodných čísel (TRNG)

Generátory využívající fyzikální / hardwarové metody. Zdrojem entropie je tedy nějaký klasický nebo kvantový fyzikální jev.

5.2.1 Klasická náhodnost

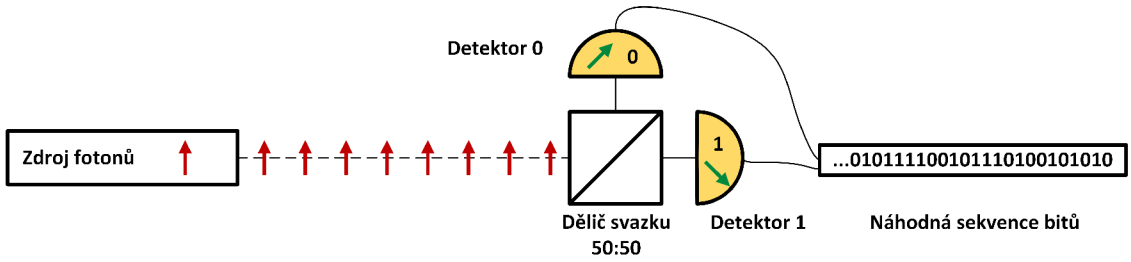
Klasický RNG systém, který je možné popsat klasickou fyzikou. Ta je však z podstaty deterministická, a tak v pravém slova smyslu nelze hovořit o náhodnosti. Jedná se spíše o tzv. deterministický chaos. Pro představu lze použít hod kostkou. Jak již bylo řečeno výše, systém, v němž se člověk nachází je zcela deterministický. To znamená, že při hodu kostkou není schopen určit výsledek, pouze z toho důvodu, že nemá dostatek informací o jevech, které na kostku působí (např. zcela přesné vlastnosti vzduchu atp.). Celkový systém však tyto informace zná. To znamená, že již před samotným hodem je určeno, jaký bude výsledek. V praxi se využívá např. tepelného či atmosférického šumu [17, 21].

5.2.2 Kvantová náhodnost

Kvantové RNG systémy (jevy) jsou však náhodné již z principu a nelze tedy žádným způsobem jejich výsledek předpovědět. Pro generování skutečně náhodných čísel je třeba použít generování opírající se o kvantovou teorii. To je činí v této realitě zcela nedeterministickými. Využít lze např. radioaktivního rozpadu (nelze určit, které jádro se přemění). Nevýhodou této metody je ovšem nerovnoměrné rozdělení. Druhou zásadní technikou je průchod fotonu děličem svazku 50:50 (polopropustné zrcadlo). Tuto techniku lze také nejčastěji najít pod zkratkou QRNG a bude dále detailněji popsána [17, 21].

5.3 Kvantové generování náhodných čísel (QRNG)

V teoretické části byl již zmíněn Youngův experiment s dvojštěrbinou. Jak bylo uvedeno, vystřelený foton prochází oběma štěrbinami současně a následně jeho vlnová funkce zcela náhodně zkolabuje pouze za jednou ze štěrbin. Tím vlastně rozdělí tuto realitu na dvě. To, jestli se člověk ocitne v realitě s fotonem „nahoře“ nebo „dole“ je pro něj zcela náhodné s pravděpodobností přesně 50 %. Řečeno jinak, z pohledu pozorovatele, je naprosto náhodné, zda se mu foton zjeví „nahoře“, nebo „dole“. Podobně jako na dvojštěrbinu reaguje foton i na děliče svazků. Právě ten se využívá k sestavení nejjednodušších kvantových generátorů. Jeden takový je možné najít na obrázku 5.1 níže.



Obr. 5.1: Jednoduchý kvantový generátor náhodných čísel [53].

Foton vychází ze zdroje vlevo, následně na děliči „rozdělí“ realitu na dvě části. V každé prochází jiným směrem. To, ve které realitě se pozorovatel nachází, zjistí ve chvíli kolapsu vlnové funkce na jednom z detektorů. Tedy jestli se nachází v realitě s bitem 1 nebo 0. V praxi tak dochází ke zcela náhodnému generování.

Právě toto generování by mělo být použito u QKD systémů, existují však i sofistikovanější implementace této metody. Například Toshiba využívá integrovaných světelných obvodů (čipy) [17, 54].

6 Protokoly kvantové distribuce klíčů (QKD)

Podle zdroje fotonů lze kvantovou distribuci klíčů rozdělit na dva základní přístupy. Původním řešením bylo využívat samostatné fotony a do jejich fyzikálních vlastností (většinou polarizace) zakódovat přenášenou informaci. Tato skupina, známá nejčastěji pod zkratkou DV-QKD, zahrnuje téměř všechny v současnosti známé a používané protokoly. Jejím specifickým typem jsou potom protokoly ukládající informaci do fázového posunu mezi dvěma pulzy. Druhá, novější skupina, známá jako CV-QKD, naopak ukládá informaci do mnohafotonových pulzů pomocí modulací. V této práci budou popsány následují kategorie protokolů [55].

- **QKD s diskrétní proměnnou (DV-QKD)**
  - Jednocestné DV-QKD protokoly (PM ONE-WAY)
  - DV-QKD protokoly založené na kvantovém provázání (EB)
  - Dvoucestné DV-QKD protokoly (PM TWO-WAY)
  - DV-QKD protokoly distribuované fázové reference (DPR)
- **QKD se spojitou proměnnou (CV-QKD)**
- **Speciální protokoly založené na modelech bezpečnosti**

V současnosti existuje nepřeberné množství nejrůznějších protokolů v různých fázích vývoje a komerční dostupnosti. Přesto snad téměř všechny stojí na dvou základních principech kvantové mechaniky.

V první řadě se jedná o Heisenbergův princip neurčitosti spolu se superpozicí kvantových stavů. Tento jev je základem tzv. Prepare-and-Measure (PM) protokolů, kam spadají jak jednocestné a dvoucestné DV-QKD protokoly, tak některé protokoly CV-QKD. Níže budou vysvětleny jednocestné protokoly BB84, SARG04 a B92. Z dvoucestných protokolů jsou zmíněny protokoly LM05 a Ping-pong protokol. Z CV-QKD je pak nastíněn protokol CV-B92 a GG02.

Druhým jevem je potom kvantová provázanost spolu s kvantovou teleportací. Tyto protokoly bývají také nazývány Entanglement-Based (EB). Z nich se bude pozornost věnována protokolu E91 a okrajově též BBM92. Někdy mezi ně bývají řazeny také protokoly založené na distribuované fázové referenci, neboli Distributed-Phase-Reference (DPR). V dokumentu jsou popsány protokoly DPS a COW.

Specifickou skupinu potom tvoří protokoly založené na specifických modelech bezpečnosti. Ty jsou speciálně uzpůsobeny proti některým typům útoků a jsou v některých ohledech specifické. Jedná se například o protokoly založené na modelech DI-QKD a MDI-QKD. Stručně bude popsán princip MDI-QKD protokolů.

6.1 Obecný princip QKD komunikace

U QKD probíhá komunikace mezi dvěma entitami odlišným způsobem než u klasické kryptografie. Zatímco u asymetrické kryptografie se data i klíč přenášejí po libovolném společném kanále, QKD využívá speciální kvantový kanál pro ustanovení klíče pomocí posílaných qubitů a klasický kanál, zajišťující režii při přenosu. Celou problematiku kvantové distribuce lze připodobnit k referenčním modelům ISO-OSI nebo TCP/IP.

Samotná QKD komunikace by totiž měla tvořit jednu nezávislou vrstvu celé QKD sítě (QKDN) podobným způsobem, jako se u referenčních modelů objevují vzájemně nezávislé vrstvy. Ačkoliv může docházet ke specifickým případům, níže bude vysvětlen obecný model této komunikace.

Komplexní QKD komunikace sestává ze tří základních kroků. Samotný QKD protokol však definuje pouze první dva. Proces destilace je zajištěn dodatečnými protokoly. Tyto kroky budou podrobněji vysvětleny na protokolu BB84.

- **Výměna hrubého klíče** (Raw key exchange)
  - Výměna qubitů po kvantovém kanále (Quantum transmission)
  - Veřejná diskuze po klasickém kanále (Public discussion)
- **Prosévání klíče** (Key sifting)
- **Destilace klíče** (Key destilation)
  - Oprava chyb (Error correction)
  - Zesílení bezpečnosti (Privacy amplification)
  - Autentizace (Authentication)

Fotony neobsahují informaci o pořadí, ve kterém byly vyslány. Z tohoto důvodu dochází mezi Alicí a Bobem k časové synchronizaci. Pomocí ní je Bob schopen rozlišovat jednotlivé fotony, případně určit, zda došlo k jejich ztrátě [56].

7 QKD s diskrétní proměnnou (DV-QKD)

Jedná se o původní přístup ke kvantové distribuci klíčů, jenž vznikl spolu s protokolem BB84. Cílem je zakódovat informaci do fyzikálních vlastností jedné částice. V případě QKD se využívá zejména polarizace fotonu. Vytváření takovýchto „osamocených“ částic však není jednoduchou záležitostí, proto v praxi dochází k aproximaci za použití slabých koherentních pulzů [57, 58].

Tab. 7.1: Tabulka obsahující výčet klíčových technologií DV-QKD [58].

Technologie DV-QKD	
Zdroj	**Detektor**
Jednofotonový zdroj (SPS)	Jednofotonový detektor
Slabý koherentní laser (WCP)	Jednofotonový detektor

7.1 Jednofotonové DV-QKD protokoly

Původní a ideální varianta, dříve však nedostupná z důvodu neexistence dostatečně kvalitních světelných zdrojů, které by byly schopny vysílat výhradně jednofotonové pulzy. Tato varianta je z podstaty bezpečná, dodnes je však většina technologií založena spíše na aproximované variantě [59].

7.2 Aproximované DV-QKD protokoly

Tato varianta využívá slabých koherentních pulzů. V praxi to znamená, že zdroj světla není schopen vždy vygenerovat pouze jeden foton, jak by bylo záhodno. Místo toho generuje pulzy o průměrně velmi malém počtu fotonů. Jejich počet je určen pomocí Poissonova rozložení:

$$P(X = x) = \frac{\mu^x e^{-\mu}}{x!} \tag{7.1}$$

μ – Průměrné množství fotonů na pulz
x – Diskrétní množství fotonů na pulz

Nechť jeden pulz tedy průměrně obsahuje 0,65 fotonu ($\mu = 0,65$). To podle vzorce pro Poissonovo rozdělení znamená, že 52 % pulzů neobsahuje žádný foton ($x = 0$), respektive 52 % pulzů se neuskuteční (vakuové pulzy). Dalších 34 % pulzů obsahuje jeden foton ($x = 1$). Zbylých 14 % procent pulzů obsahuje dva a více fotonů. Pulzy obsahující foton jsou označovány jako slabé koherentní pulzy [60].

Zatímco jednofotonová varianta je prokazatelně bezpečná, v případě, kdy dochází k aproximaci fotonů je systém náchylný na tzv. útok dělením počtu fotonů (PNS). Z tohoto důvodu jsou protokoly využívající fotonové aproximace zabezpečeny např. pomocí tzv. návnadových stavů (decoy states). Jejich princip bude i s PNS útokem podrobně vysvětlen na aproximované variantě protokolu BB84.

8 Jednocestné DV-QKD protokoly

Jak již bylo uvedeno výše, jednocestné protokoly (ONE-WAY) patří do skupiny tzv. Prepare-and-Measure (PM) protokolů. Název vychází z faktu, že Alice fotony připravuje (prepare) a Bob je měří (measure).

Všechny PM protokoly vycházejí z Heisenbergovy relace neurčitosti. Jednocestné DV-QKD protokoly jsou vůbec nejstarší a jak již název napovídá, kvantová informace je přenášena pouze jedinou cestou. Tzn. většinou od Alice k Bobovi. Tímto se liší od dvoucestných protokolů, které budou popsány později [61, 62].

8.1 BB84: Bennett & Brassard (1984)

Jedná se o vůbec první QKD protokol, na jehož základě staví velké množství dalších odvozených protokolů. V ideálním stavu je prokazatelně bezpodmínečně bezpečný. Nedokonalost používaných zařízení však otevírá dveře několika možným útokům. BB84 využívá lineární polarizace fotonu [63].

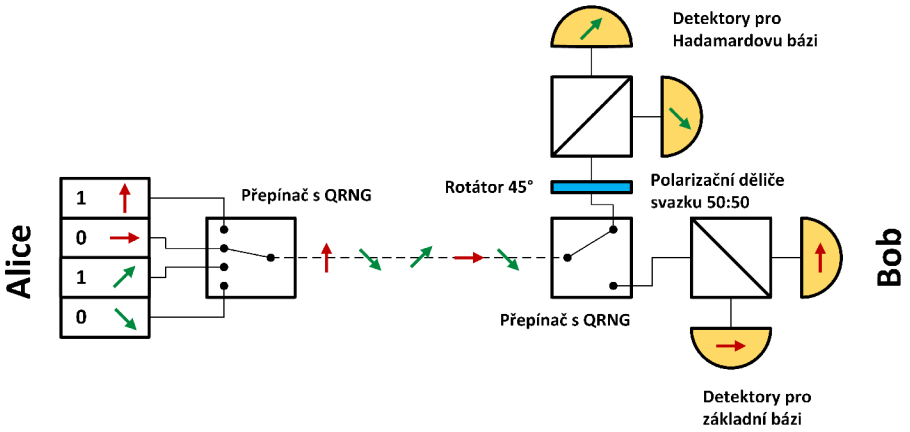
8.1.1 Výměna hrubého klíče (Raw key exchange)

Výměna qubitů po kvantovém kanále

Nechť jsou dva uzly Alice a Bob, mezi kterými musí proběhnout výměna klíčů pomocí protokolu BB84. Protokol využívá dvou bází. Ty jsou na polarizátoru vzájemně pootočeny o 45°(pootočení o 90° na Blochově kouli). Celkem se používají čtyři stavy. Používá se tedy vertikálně-horizontální báze stavů $\{|\uparrow\rangle, |\rightarrow\rangle\}$ a diagonální báze $\{|\nearrow\rangle, |\searrow\rangle\}$. Tyto báze bývají také často reprezentovány symboly $\oplus$ a $\otimes$ [63].

Nejdříve si Alice vygeneruje pomocí QRNG náhodnou sekvenci bitů s hodnotami 0 a 1. Například v bázi $\oplus$ by bitu 0 odpovídal stav $|\rightarrow\rangle$, zatímco bitu 1 stav $|\uparrow\rangle$. Obdobně v bázi $\otimes$ by bitu 0 odpovídal $|\nearrow\rangle$ a bitu 1 $|\searrow\rangle$. Existují tedy dva způsoby, jak daný bit reprezentovat. Alice pomocí dalšího QRNG náhodně volí báze a tím pro každou hodnotu bitu vybírá ze dvou polarizací fotonu (celkem 4 stavy) [63].

Na straně druhé čeká Bob vybaven stejnými dvěma bázemi jako Alice. Bob pro každý přijatý foton náhodně vybere bázi, se kterou bude měřit. K výběru báze je opět použit kvantový generátor. Vybere-li Bob stejnou bázi, jakou vybrala Alice, získá vždy správnou hodnotu bitu. Pokud ale vybere bázi opačnou, bude výsledné měření správné v 50 % případů. Vlnová funkce totiž zkolabuje náhodně do jednoho ze základních stavů Bobem vybrané báze. Bob však v tuto chvíli netuší, které bity v jeho řetězci neodpovídají původním Aliciným hodnotám [63].



Výměna klíče	Aliciny bity	0	1	0	1	1	1	0	1
	Aliciny fotony	↘	↗	→	↑	↑	↗	↘	↑
	Bobem vybraná báze	+	×	×	+	×	×	×	×
	Bobovy výsledky	↑	↗	↘	↑	↗	↗	↘	↘
	Bobovy bity	1	1	0	1	1	1	0	0
Veřejná diskuze	Bob oznámí báze	+	×	×	+	×	×	×	×
	Alice oznámí shody	✗	✓	✗	✓	✗	✓	✓	✗
	Hrubý klíč	-	1	-	1	-	1	0	-

Obr. 8.1: Základní schéma protokolu BB84 s tabulkou [33].

Veřejná diskuze po klasickém kanále

Z tohoto důvodu odešle Bob Alici po libovolném nezabezpečeném kanálu pořadí bází použitých k měření. Alice porovná Bobovy báze s vlastními. Bity, u kterých se Aliciny i Bobovy báze shodují, prohlásí Alice za klíč, ostatní bity jsou zahozeny. Bobovi následně pošle pořadí vyhovujících bitů. Tak získá klíč i Bob. Klíč, který nyní oba znají je označován jako tzv. surový, případně hrubý klíč (raw key). Tento klíč však ještě nemusí být zcela shodný, kvůli přítomným chybám [56, 63, 64].

8.1.2 Prosévání klíče (Key sifting)

Surový klíč je nyní potřeba „prosít“. Aby Alice s Bobem zjistili, zda nejsou odposlouchávání. Z tohoto důvodu obětují (zveřejní) část hrubého klíče. Takto jsou schopni určit chybovost přenosu, neboli QBER (Quantum-Bit Error Rate) a tím detekovat odposlouchávající Evu. Pokud by se zde totiž Eva vyskytovala, byla by nucena stavy přicházejících fotonů měřit a volbou bází by sama dělala chyby. Ty by se zde následně projevily. V ideálním případě by jediným zdrojem chyb byla Eva. Kvůli nedokonalostem přístrojů vznikají chyby i jiným způsobem (zdroje, přenosová soustava, detektory). Z tohoto důvodu je nízká chybovost tolerována. Většinou se uvádí bezpečná hranice cca 11 %. Výsledkem tohoto procesu je potom tzv. prosetý klíč (sifted key) [65, 66, 67].

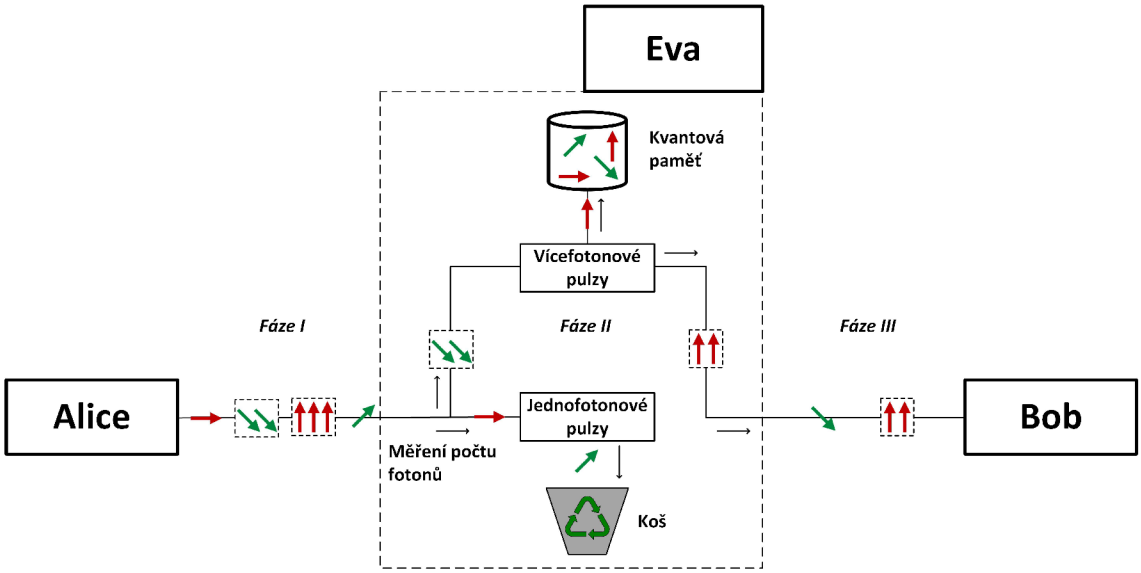
8.1.3 Destilace klíče (Key destilation)

Prosetý klíč následně prochází procesem tzv. destilace sestávající ze tří fází. Nejdříve dochází k **opravě chyb** (error correction), které mohly v prosetém klíči zůstat. Druhou fází je **zesílení bezpečnosti** (privacy amplification) spočívající v kompresi klíče za účelem snížení informací, které Eva zná. Poslední částí je **autentizace**, nutná k vyloučení MITM útoku. Tato autentizace probíhá pomocí předsdíleného klíče na klasickém kanálu. Tento klíč se používá pouze pro první výměnu, následně bývá vždy odvozován od dohodnutého „kvantového“ klíče.

Po dokončení procesu destilace získávají obě strany finální shodný a bezpečný klíč, kterým je následně šifrována komunikace v uživatelské síti. Tento protokol bývá považován za bezpodmínečně bezpečný [68, 69].

8.1.4 Aproximace, útok PNS a návnadové stavy

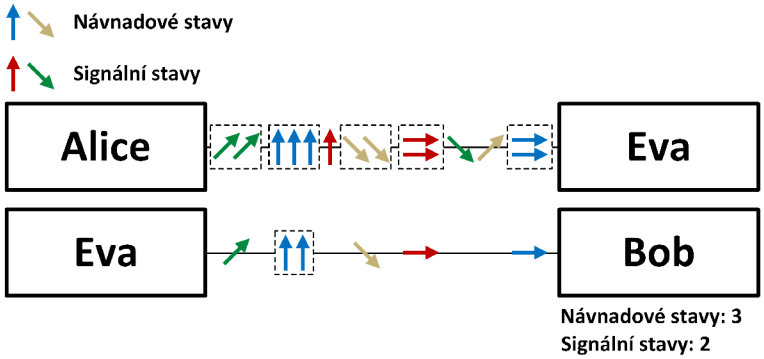
Až dosud byla popisována dokonalá jednofotonová verze protokolu. Reálně se však využívá aproximovaná verze. Alice tedy není schopna odesílat přesně jednofotonové pulzy. Toto ovšem představuje příležitost pro Evu. V případě, kdy by zachytila pulz o více fotonech, jeden si ponechá a zbytek pošle dále Bobovi. Pulzy obsahující jeden foton Eva zahodí a Bob se k nim tak nikdy nedostane. Výhodou je pro Evu ztrátový kanál, který by v nejhorším případě mohla nahradit kanálem bezztrátovým. V tomto případě není jednoduché Evu detekovat. Jakmile začnou Bob s Alicí zveřejňovat informace o bázích k ustanovení hrubého klíče, získá Eva informace, podle kterých je schopna si klíč sama odvodit. Jedná se o tzv. útok dělením počtu fotonů, lépe známý jako **PNS útok** (Photon-Number-Splitting Attack). Tento PNS útok je zobrazen na obrázku 8.2 [70].



Obr. 8.2: Schéma zachycující PNS útok [70].

K obraně před touto zlovolností slouží tzv. návnadové stavy (decoy states). Nedokážou Evu sice zastavit, zato ji pomohou detekovat. Princip je takový, že Alice posílá Evě kromě běžných stavů i stavy návnadové. Tyto návnadové stavy mají vyšší průměrné množství fotonů na pulz. Eva nedokáže rozlišit, jestli se jedná o signální, nebo návnadový pulz, 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. Tento systém byl poprvé navržen na Severozápadní univerzitě v USA a poprvé prakticky implementován v Kanadě pod názvem Vacuum + Weak decoy state protocol. Nyní však již existuje

v mnoha variantách a modifikacích, které je možné najít pod názvy jako Decoy state BB84, Decoy state protocol atp. [57, 71, 72].



Obr. 8.3: Schéma zachycující důsledky návnadových stavů na PNS útok [70].

Ačkoliv se to nemusí na první pohled zdát, je i tento protokol bezpodmínečně bezpečný (budou-li pominuty chyby detektorů). Kromě toho však dokáže razantně zvýšit vzdálenost, na kterou lze komunikovat. Tyto návnady se nepoužívají pouze u BB84, ale mohou se vyskytovat i u mnoha dalších protokolů [55, 71].

8.2 SARG04: Scarani & Acin & Ribordy & Gisin (2004)

Jeden z protokolů odvozených od BB84. Využívá slabých koherentních pulzů a představuje alternativní obranu před PNS útoky. Výměna qubitů probíhá stejně jako u BB84 s tím rozdílem, že stavy $|\rightarrow\rangle$ a $|\uparrow\rangle$ budou nyní symbolizovat bit 1 a stavy $|\nearrow\rangle$ a $|\searrow\rangle$ bity s hodnotou 0. Veřejná diskuse však již neprobíhá tak, že by Alice poslala Bobovi použité báze. Místo toho pošle Bobovi ke každému přijatému fotonu další dvojici fotonů. Tyto dva fotony nesmějí být vzájemně ortogonální. To znamená, že může odeslat následující páry:$|\rightarrow\rangle + |\nearrow\rangle$, $|\rightarrow\rangle + |\searrow\rangle$, $|\uparrow\rangle + |\nearrow\rangle$ a $|\uparrow\rangle + |\searrow\rangle$. Jeden z těchto stavů odpovídá polarizaci fotonu podle Alice [55, 63, 73].

Pokud tedy Alice odeslala foton ve stavu $|\rightarrow\rangle$ a Bob jej měřil pomocí diagonální báze $\otimes$, může mu při měření zkolabovat $|\rightarrow\rangle$ do jednoho ze stavů $|\nearrow\rangle$ a $|\searrow\rangle$. Uvažován nyní bude tedy stav $|\searrow\rangle$. Alice dále pošle pár fotonů polarizovaných takto $|\rightarrow\rangle + |\nearrow\rangle$. Protože si diagonální stavy neodpovídají, ví Bob, že použil špatnou bázi a je tedy jasné, že Alice polarizovala foton na stav $|\rightarrow\rangle$. Bob tedy ví, že přijatý qubit odpovídá bitu s hodnotou 1 [55, 63, 73].

Pokud by Alice poslala pár $|\rightarrow\rangle + |\searrow\rangle$ existují z pohledu Boba dvě možnosti. Buď použil správnou bázi a foton je skutečně ve stavu $|\searrow\rangle$, nebo zvolil bázi nesprávně a foton do tohoto stavu náhodně zkolaboval. Bob není schopen určit, která z možností je správná, a tak qubit zahodí [55, 63, 73].

Poslední možností je, že Bob vybere správnou bázi, tzn. horizontálně-vertikální $\oplus$. S její pomocí určí stav fotonu správně jako $|\rightarrow\rangle$. Tento stav bude samozřejmě odpovídat i jednomu ze stavů ve dvojici $|\rightarrow\rangle + |\searrow\rangle$ nebo $|\rightarrow\rangle + |\nearrow\rangle$ (nezáleží na tom, který Alice pošle). Bohužel Bob opět neví, zda měřil správně, nebo se jedná o náhodný kolaps. Z tohoto důvodu qubit opět zahodí. Obdobně se postupuje u každého ze čtyř stavů [55, 63, 73].

Postupně se tímto způsobem značná část qubitů zahodí. Zbývající qubity vytvoří následně surový klíč, postupující do další fáze [55, 63, 73].

8.3 B92: Bennett (1992)

V roce 1992 představil Charles Bennet svoji zjednodušenou verzi protokolu BB84. Protokol B92 (někdy též BB92) využívá pouze dvou vzájemně neortogonálních stavů. Například pro bit s hodnotou 0 bude využit horizontální stav $|\rightarrow\rangle$, zatímco pro bit s 1 diagonální stav $|\nearrow\rangle$. Alice nyní musí vybírat báze podle hodnoty bitu. Na druhou stranu Bob netuší, jaký qubit dostane, a tak volí báze náhodně [74, 75].

Pokud tedy Alice odeslala qubit $|\rightarrow\rangle$ a Bob pro měření použije horizontálně-vertikální bázi $\oplus$, potom získá se 100% pravděpodobností výsledek $|\rightarrow\rangle$. V tomto případě ovšem Bob neví, zda použil správnou bázi, nebo došlo k náhodnému kolapsu. Pokud by použil bázi diagonální $\otimes$, může stav $|\rightarrow\rangle$ zkolabovat dvěma způsoby. Buď do stavu $|\nearrow\rangle$ nebo do stavu $|\searrow\rangle$. U stavu $|\nearrow\rangle$ nastává z Bobova pohledu stejný problém jako před chvílí. Tzn. opět netuší, zda měřil správně nebo se jedná o náhodný kolaps. Jediným stavem s vypovídací hodnotou je tak stav $|\searrow\rangle$. Bob ví, že tento stav by Alice nikdy neposlala, proto si může být jistý, že bázi zvolil špatně. Alice tedy neodeslala $|\nearrow\rangle$, ale $|\rightarrow\rangle$ a bit tak může bezpečně interpretovat jako 0. V případě, že Alice odešle stav $|\nearrow\rangle$, je postup shodný, vypovídajícím stavem je tak $|\uparrow\rangle$ (bit 1). Bob následně oznámí Alici, která měření považuje za použitelná. Tak dojde k sestavení hrubého klíče. Využito je tak jen 25 % všech qubitů, zbytek je zahozen [55, 63, 64, 74, 75, 76].

8.4 Shrnutí

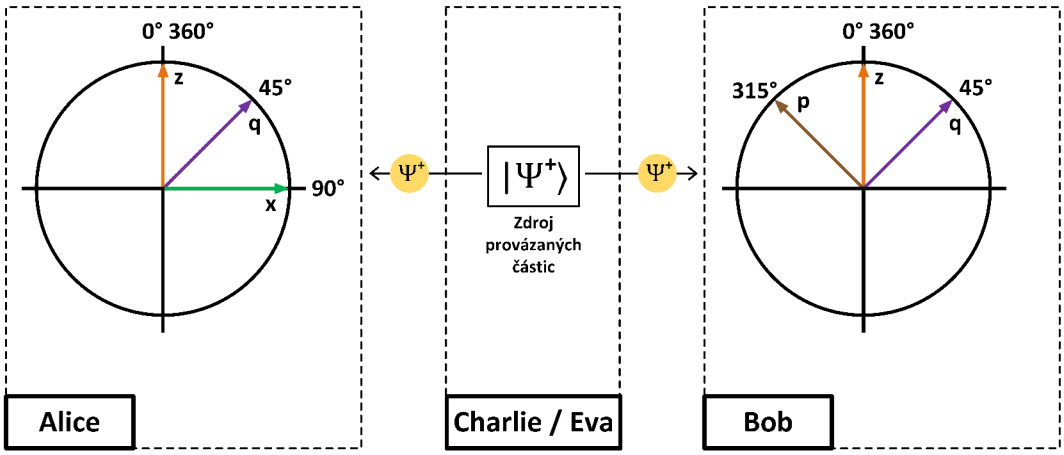
Existuje mnoho dalších protokolů pracujících na podobném principu. Nejčastěji se jedná o různé modifikace protokolu BB84 jako SSP (využívá 6 stavů a 3 báze, horizontálně-vertikální $\oplus$, diagonální $\otimes$ a rotační $\odot$ (báze vektorů $|\circlearrowleft\rangle$ a $|\circlearrowright\rangle$), S13 nebo KMB09. Tyto protokoly se nacházejí v nejrůznějších fázích (od návrhů, přes experimentální fáze, až po v současnosti komerčně využívaná řešení). Svoje modifikace však mají i tyto odvozené protokoly. Příkladem budiž třeba I-SARG04, SARG04 s návnadami atd. Existují např. i verze protokolu BB84 pracující s qudity, využívající kvantového provázání (BBM92) nebo fázového kódování místo polarizace. Do této kategorie patří např. protokol T12 (může však využívat i polarizace), vyznačující se neshodnými pravděpodobnostmi pro výběr bází. Např. báze $\oplus$ je vybírána Alicí častěji než $\otimes$. Tento protokol je považován za efektivnější než klasický BB84 [55, 77, 78, 79, 80, 81].

9 DV-QKD protokoly založené na Kvantovém provázání

Jak již bylo několikrát zmíněno druhou skupinou jsou protokoly založené na kvantovém provázání a kvantové teleportaci. Známé jsou také pod anglickým názvem Entanglement-Based (EB). Prvním a zároveň nejvýznamnějším protokolem z této kategorie je E91. Podobně jako BB84, existuje v několika modifikacích. Jak bude vysvětleno, v některých případech se jedná o jakousi „kvantově provázanou nástavbu“ nad protokolem BB84.

9.1 E91: Ekert (1991)

E91 je první protokol založený na kvantovém provázání. Jeho hlavní výhodou je možnost Alice delegovat generování a distribuci qubitů třetímu uzlu – Charliemu. Pod Charliem si lze představit například centrum, podnikající v oblasti generování a distribuce klíčů. Za maskou Charlieho může být paradoxně schována i Eva. Její kontrola nad tímto uzlem nějak neovlivní bezpečnost protokolu. Originální E91 využívá 3 báze. Ty budou nyní představeny na zredukované Blochově kouli (nikoliv na polarizátorech) tak, jako na obrázku 9.1 [83].



Obr. 9.1: Schéma protokolu E91 se vzájemným natočením detektorů [82, 83].

Protokol začíná tím, že Charlie, na Alicinu žádost, vygeneruje propletené páry fotonů, ty rozdělí a po jednom pošle jak Alici, tak Bobovi. Tyto dvě částice se nacházejí v Bellově stavu, což znamená, že budou-li Alice i Bob měřit foton detektory ve stejném úhlu, získají přesně opačné stavy (uvažován je stav $|\Psi^+\rangle$, běžně však bývá využíván stav $|\Psi^-\rangle$, který se chová mírně odlišně). S těmito částicemi je nakládáno dvěma různými způsoby [83].

9.1.1 Sestavení klíče

Bob s Alicí měří polarizaci přicházejících fotonů pomocí detektorů, jenž jsou vůči sobě v různých úhlech. Je-li tento úhel 0° získají přesně antikorelované výsledky. Jednomu pak pouze stačí invertovat daný bit. Budou-li jejich detektory natočeny o 90°, je 50% šance, že dostanou odpovídající si výsledky. Třetí možností je úhel 45° a 135°, tyto úhly jsou kritické při ověřování platnosti Bellovy rovnice [83].

Aby zjistili, v jakém případě se jejich směry shodovali musejí si záznamy o nich pro daný foton vzájemně vyměnit. Bity z fotonů, které měřili oba shodně, nyní tvoří hrubý klíč. Ostatní qubity jsou využity k detekci Evy, tedy odposlechu [83].

9.1.2 Kontrola Bellovy nerovnice

Za předpokladu, že se Evě podaří infiltrovat uzel Charlie a bude pouze pasivně naslouchat na kvantovém kanále, nějak jí to nepomůže. Obě částice jsou provázané a jejich stavy budou známy až po měření. Eva se však může pokusit do distribuce klíčů zasáhnout. Buď může Bellovy stavy měřit nebo může místo toho rovnou donutit Charlieho, aby neodesílal provázané fotony, ale již připravené stavy částic [83].

Vyřazené qubity z předchozího kroku tak poslouží k ověření Bellovy nerovnice. Použitím odlišných bází Alice s Bobem provedli měření s úhlem mezi detektory buď 90°, 45° nebo 135°. Právě druhé dva „nestandardní“ úhly lze použít k ověření platnosti Bellovy nerovnice tak, jak bylo popsáno v kapitole 4.5.1 [82, 83, 84, 85].

V takovém případě se výsledky korelací pro kvantovou teorii a klasickou fyziku liší. Tímto dojde k porušení Bellovy nerovnice a Eva je odhalena. Z pohledu Bellova teorému je Eva považována za skrytou proměnnou, která se v provázaném stavu nemůže vyskytovat [55, 64, 82, 83, 84, 85].

9.2 BBM92: Bennett & Brassard & Mermin (1992)

Protokol BBM92 z E91 vychází, a vznikl jako kritická reakce na něj. Protokoly BBM92 a E91 však bývají často zaměňovány. Stejně jako E91 využívá BBM92 uzlu Charlie, který distribuuje propletené páry. Rozdílem je ovšem použití dvou bází podobně jako u protokolu BB84 [55, 64, 86, 87].

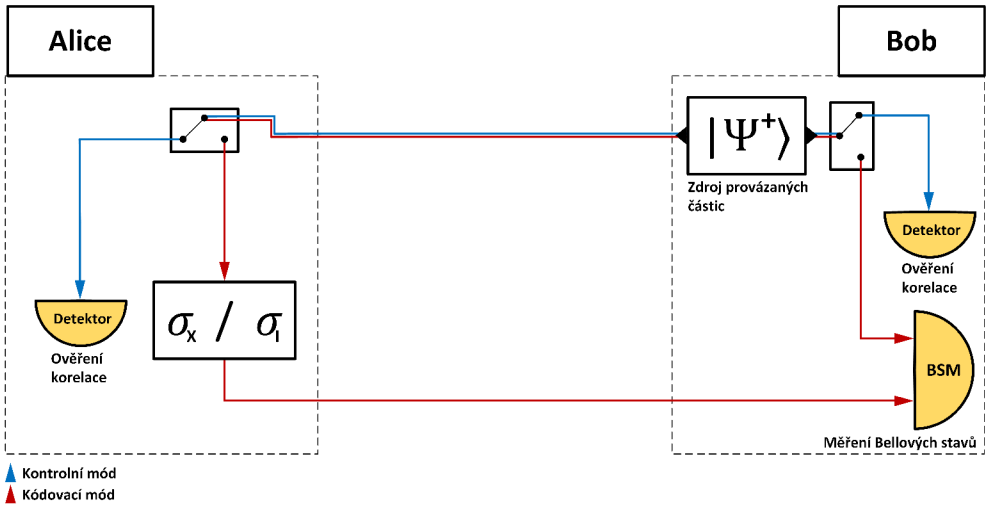
Aby protokol dával smysl je nutné použít stav $|\Psi^-\rangle$. Charlie produkuje propletené fotony a Alice s Bobem je náhodně měří v bázích $\bigoplus$ a $\bigotimes$. Pokud se báze shodují, bude docházet k antikorelaci (vizte tabulku 4.2). Ostatní fotony jsou zahozeny. Veřejná diskuze a ostatní operace probíhají podobně jako u protokolu BB84. Z tohoto důvodu bývá protokol BBM92 často považován za jakousi propletenou verzi PM protokolu BB84 [55, 64, 86, 87].

10 Dvoucestné DV-QKD protokoly

Tyto protokoly označované také jako TWO-WAY jsou druhou variantou tzv. Prepare-and-Measure protokolů, tj. protokolů stavících na Heisenbergově relaci neurčitosti. Původním obousměrným schématem však byl tzv. ping-pong protokol, využívající kvantového provázání (to se však u dalších TWO-WAY protokolů nepoužívá). Z tohoto důvodu je tato skupina protokolů představena až nyní. U jednocestných DV-QKD protokolů docházelo ke konverzaci po kvantovém kanále pouze v jednom směru, většinou od Alice k Bobovi. Bob již dále komunikoval pouze po klasickém kanále (např. zveřejnění bází u BB84). U dvoucestných protokolů kvantovou komunikaci naopak většinou iniciuje Bob, kterému Alice po kvantovém kanále odpovídá zpět.

10.1 Ping-Pong protokol: Boström & Felbinger (2002)

Ping pong protokol (PP) je původním protokolem využívající dvoucestné schéma. Protokol začíná tím, že si Bob vygeneruje dvojici fotonů v Bellově stavu (uvažován je stav $|\Psi^+\rangle$). Jeden z fotonů si ponechá a druhý odešle Alici. Novinkou oproti předchozím protokolům je, že si Alice může náhodně vybrat, jak s fotonem naloží. Na výběr má ze dvou tzv. módů. Kontrolní mód (modře) slouží k odhalení Evy, zatímco kódovací mód (červeně) slouží k přenosu klíče. Schéma protokolu lze najít na obrázku 10.1 [55].



Obr. 10.1: Schéma Ping-Pong protokolu [55].

10.1.1 Kontrolní mód (CM)

Pokud si Alice vybere kontrolní mód, změří příchozí foton v Z-bázi $\{|0\rangle,|1\rangle\}$ (tím dojde k rozvázání propletení), následně o výsledku měření informuje Boba. Pokud Bob změří svůj foton ve stejné bázi, měl by jeho výsledek být vždy opačný (antikorelace). Pokud bude Eva odposlouchávat, dojde k narušení korelací mezi měřeními [88].

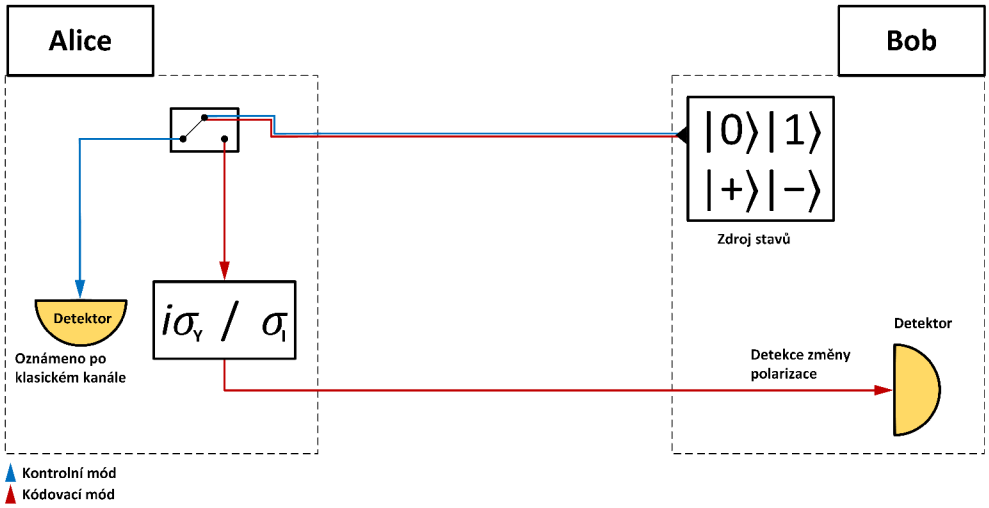
10.1.2 Kódovací mód (EM)

V případě tohoto módu provádí Alice nad přijatým fotonem jednu ze dvou operací. Jednou z možností je použít Z-rotaci. Pomocí ní změní Bellův stav z $|\Psi^+\rangle$ na $|\Phi^-\rangle$, reprezentující např. bit 0. Druhou možností je nedělat nic (operace identita). V tomto případě zůstane Bellův stav částic shodný, což reprezentuje např. stav 1. Následně Alice odešle foton zpět k Bobovi, který provede měření Bellových stavů. Z výsledku následně ví, jakou informaci Alice zakódovala. Ve výsledku tedy oba znají sdílený klíč [88, 89].

Takováto přímá komunikace je ovšem v reálných podmínkách, kvůli rušení, problematická. Současně je PP v základním režimu náchylný na DOS útoky. Existuje však mnoho modifikací, které se tyto problémy snaží řešit [88, 90].

10.2 LM05: Lucamarini & Mancini (2005)

Dvoucestné QKD protokoly ovšem provázané páry nepotřebují. Jedním z takových protokolů je LM05. Ten v mnoha věcech vychází z PP. Rozdíly jsou následující. Na začátku si Bob náhodně připraví stav pomocí bází Z $\{|0\rangle,|1\rangle\}$ nebo X $\{|+\rangle,|-\rangle\}$. Tento foton následně odešle Alici, ta opět používá 2 módy [55].



Obr. 10.2: Schéma LM05 protokolu [91].

10.2.1 Kontrolní mód (CM)

V kontrolním módu změří Alice stav fotonu náhodně vybranou bází. Výsledky jsou následně po klasickém kanálu porovnány s Bobem podobně, jako je tomu u protokolu BB84. Na základě výsledků je následně možné odhalit Evu [81, 91, 92].

10.2.2 Kódovací mód (EM)

Jako u PP Alice opět provádí nad qubitem 2 možné operace. Pokud chce, aby byl foton interpretován Bobem jako 0, nedělá nic. Respektive použije operaci identita σ_I. Pro logickou hodnotu 1 je provedena operace $i\sigma_Y = \sigma_Z\sigma_X$, neboli prohození bitu a fáze (rotace Z a X). Ta prohodí stav qubitu na opačný (ortogonální), na fázi (znaménku) přitom nezáleží. Prohození jsou tedy:

$$
\begin{aligned}
i\sigma_Y |0\rangle &= -|1\rangle \\
i\sigma_Y |1\rangle &= |0\rangle \\
i\sigma_Y |+\rangle &= |-\rangle \\
i\sigma_Y |-\rangle &= -|+\rangle
\end{aligned}
$$

Protože Alice netuší, v jaké bázi byl foton polarizován, nemůže si jednoduše vybrat jen jednu z rotací. Musela by totiž stav změřit, čímž by došlo ke kolapsu. Z tohoto důvodu používá kombinaci těchto rotací, kdy se σ_X používá k rotaci v bázi $\{|0\rangle,|1\rangle\}$, zatímco σ_Z pro bázi $\{|+\rangle,|-\rangle\}$. Následně Alice odešle foton zpět Bobovi. Ten qubit měří ve stejné bázi, ve které jej odeslal. Tímto způsobem získá tajný klíč i on [81, 91, 92].

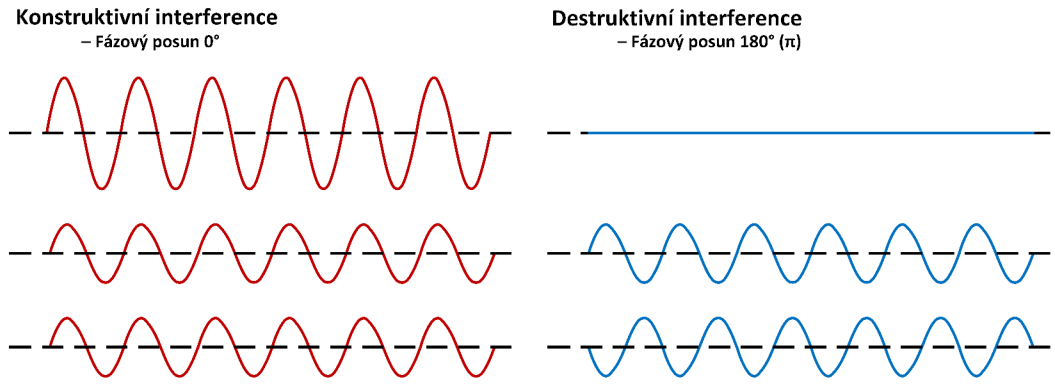
11 Protokoly distribuované fázové reference

Zatímco všechny předchozí protokoly využívají k reprezentaci qubitu polarizaci fotonu, existuje skupina protokolů, založených v tomto ohledu na zcela odlišné technice. Kódování informace do polarizace totiž není pro přenosy na dlouhé vzdálenosti vhodné. Z tohoto důvodu je využíváno fázového kódování pro DPS, případně time-bin kódování pro COW. Obě techniky jsou blízce příbuzné [93].

U fázového kódování je qubit reprezentován fázovým posunem mezi dvěma pulzy, zatímco u time-bin kódování je stav qubitu určen časem jeho přijetí. Podrobněji budou tyto techniky popsány u jednotlivých protokolů. Existují WCP i SPS verze protokolu DPS, protokol COW je vystavěn výhradně na slabých koherentních pulzech [93].

11.1 Koherence a interference

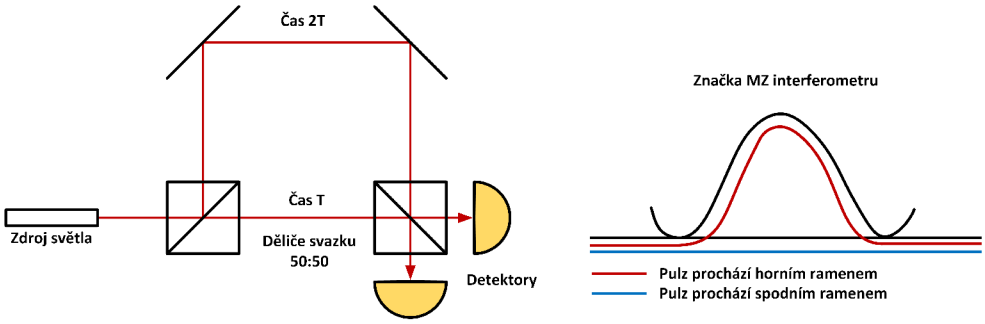
Jedná se o vzájemnou souvislost fáze a amplitudy vlnění. To může vycházet buď ze dvou různých míst (prostorová koherence), nebo z místa stejného, avšak s určitým časovým posunem (časová koherence). Za koherentní je světlo považováno, má-li stejnou frekvenci, směr a stejnou fázi, případně konstantní fázový posun. Koherence dvou vln má vliv na jejich vzájemnou interferenci [94].



Obr. 11.1: Konstruktivní interference vlevo a destruktivní interference vpravo [94].

11.2 Machův-Zehnderův interferometr

Podle fázového posunu totiž dochází ke konstruktivní (0°), nebo destruktivní (180°) interferenci. Koherenci dvou pulzů tak lze měřit pomocí interferometrů. U těchto QKD protokolů se využívá konkrétně tzv. asymetrický Machův-Zehnderův interferometr, jenž je zobrazen na obrázku 11.2 [95].

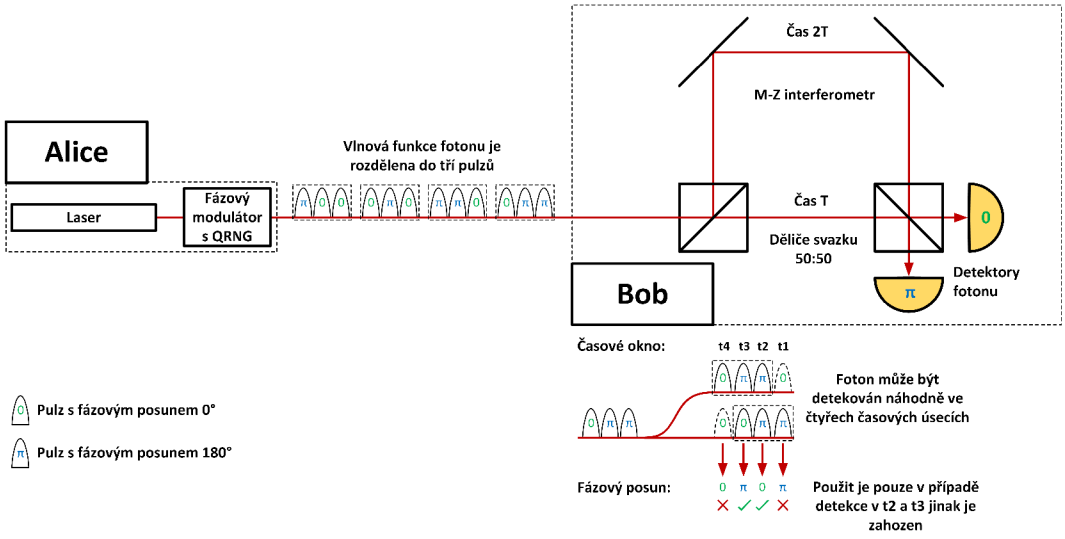


Obr. 11.2: Schéma Machova-Zehnderova interferometru spolu se značkou [95].

11.3 DPS: Waks & Yamamoto (2002)

Protokol založený na diferenciálním fázovém posunu, tzn. rozdílu fázového posunu mezi dvěma pulzy. Demonstrace protokolu je na obrázku 11.3 níže. Alice rozdělí vlnovou funkci fotonu do několika pulzů (zde do 3). Následně je mezi každými dvěma těmito pulzy náhodně vybrán fázový posun. Například 0° pro bit 0, nebo 180° (π) pro bit 1. Sekvence pulzů je nyní přenesena k Bobovi [95].

Zde každý pulz nejdříve narazí na dělič svazku (50 : 50), který jej rozdělí současně do dvou větví (podobně jako u Youngova experimentu). V dolní větvi prochází pulz přímo. Horní větev je přesně tak dlouhá, aby pulz zbrzdila na úroveň pulzu následujícího. Poté dochází k interferenci dvou posunutých pulzů. Tzn. pulz 1 interferuje s pulzem 2, pulz 2 následně s pulzem 3 atd. Z jejich interference je možné následně určit fázový posun mezi danými pulzy [95].



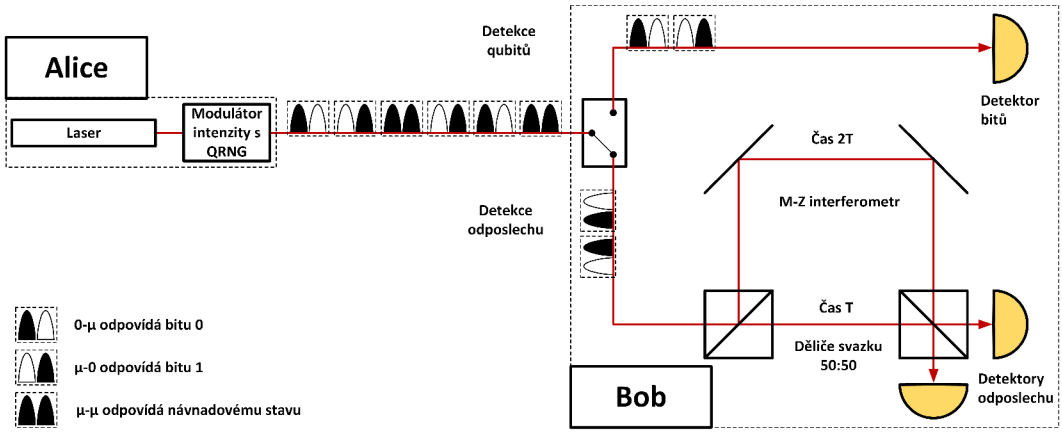
Obr. 11.3: Schéma protokolu DPS [95].

Foton se může náhodně nacházet v libovolném časovém okně (*t1*-*t4*). Pokud jeden z pulzů v okně obsahuje foton, je na základě interference zaznamenám jedním z detektorů. Je-li foton detekován v oknech *t1* a *t4* je zahozen. Při detekci v oknech *t2* a *t3* si Bob toto okno uloží spolu s naměřeným fázovým posunem. Po dokončení kvantové komunikace pošle Bob Alici seznam časových oken s naměřenými fotony. Alice ví, který pulz byl jak modulován a snadno tak určí klíč i ona [55, 61, 95, 96, 97, 98, 99, 100].

11.4 COW: Gisin & Ribordy & Zbinden & Stucki & Brunner & Scarani (2004)

V komerční sféře se jedná se o jeden z populárnějších protokolů. Oblíbený je hlavně díky své jednoduchosti a snadné implementaci. Na rozdíl od předchozího využívá tzv. time-bin kódování.

COW protokol využívá slabě koherentních pulzů (Coherent One-way protocol). Jednotlivé bity jsou reprezentovány časovým oknem obsahujícím dva pulzy. Například bit s logickou hodnotou 0 je reprezentován pulzem obsahujícím fotony a pulzem prázdným. Značí se *0-μ*. Logická 1 má opačné pořadí pulzů, tedy *μ-0*. To znamená, že pro bit 1 je pulz v daném časovém okně změřen „dříve“ než pulz reprezentující 0. Poslední přenášenou hodnotou jsou návnadové stavy (decoy states). Ty jsou reprezentovány dvěma plnými pulzy *μ-μ*. Průměrné množství fotonů na pulz je typicky $\mu = 0,5$. U protokolu je důležitá časová synchronizace. Základní princip je znázorněn na obrázku 11.4 [55, 101].



Obr. 11.4: Schéma protokolu COW [101].

Alice odesílá za sebou dvojice pulzů, které Bob měří pomocí detektoru bitů v horní části obrázku. Aby však byla zajištěna bezpečnost, obětuje Bob náhodně dva qubity, které spolu sousedí nenulovými pulzy. Pomocí interferometru a detektorů dole hledá změny interferenčních obrazců, způsobené změnou fázového posunu dvou qubitů. Pokud by chtěla Eva provést například PNS útok, dojde k posunutí fází dvou qubitů a k narušení systému. Tímto způsobem bude detekována. Návnadové stavy zde slouží pro ochranu před jiným typem útoků [63, 102, 103, 104].

12 QKD se spojitou proměnnou (CV-QKD)

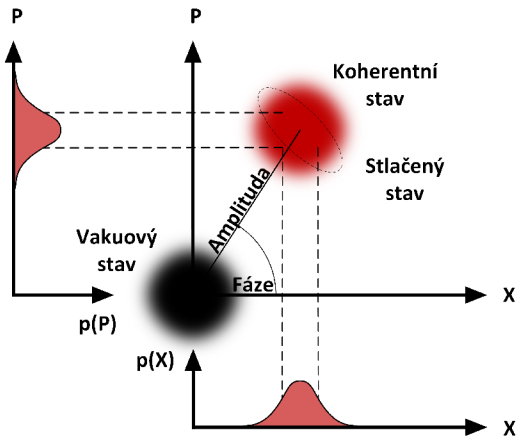
Základním rozdílem CV-QKD protokolů a jejich diskrétních protějšků je větší množství fotonů na pulz. Informace tedy již není přenášena jediným polarizovaným fotonem, ale je namodulována do světelných pulzů pomocí fáze a amplitudy. Na rozdíl od DV-QKD bývá používán modulovaný laser spolu s koherentními detektory. Většinou se jedná o homodynní detekci. CV-QKD protokoly nejsou v současnosti příliš rozšířeny. Z tohoto důvodu bude jejich princip nastíněn jen velmi stručně [58].

Tab. 12.1: Tabulka obsahující výčet klíčových technologií CV-QKD [58].

Technologie CV-QKD	
Zdroj	**Detektor**
Slabě modulovaný laser	Homodynní detektor
Slabě modulovaný laser	Heterodynní detektor

12.1 Koherentní a stlačený stav světla

Opět existují PM a EB protokoly. Zde budou pro orientaci uvedeny pouze zástupci první kategorie. Tyto protokoly obecně staví na Heisenbergově relaci neurčitosti mezi kvadraturami P a X. Kdy je možné přesněji určit polohu částice (X) pouze na úkor přesnosti její hybnosti (P). Měření kvadratur totiž vyvolává šum, který znemožňuje učinit druhé měření se stejnou přesností [105].



Obr. 12.1: Grafické znázornění koherentního (kulatého) a stlačeného (eliptického) stavu světla. Vakuový stav (černý) je koherentním stavem v počátku soustavy souřadnic [105].

Pomocí této neurčitosti se rozlišují speciální stavy světla. CV-QKD využívá koherentního stavu světla (coherent state) a stlačeného stavu světla (squeezed state). Speciálním případem koherentního stavu, je pak vakuový stav (vacuum state), jenž neobsahuje částice. Výše popsané je možné najít na obrázku 12.1. Jak koherentní, tak vakuový stav byl již zmíněn v části 7.2 [105, 106, 107, 108].

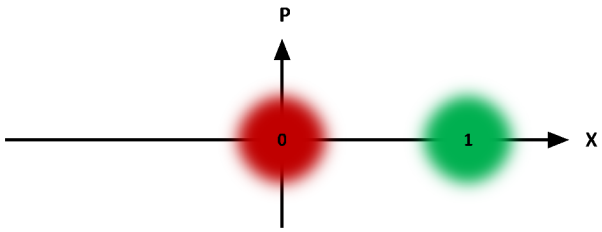
Měření následně probíhá pomocí homodynní nebo heterodynní detekce. Homodynní detekce umožňuje měřit jednu kvadraturu relativně přesně, na úkor, kvadratury druhé. Heterodynní detekce je schopná měřit obě kvadratury současně, oba výsledky jsou ovšem méně přesné. Heterodynní detekce v této práci probírána nebude [105, 106, 107, 108].

Nechť je tedy světlo v koherentním stavu, kde $p(X)$ je pravděpodobnost, že se světlo nachází na určitém místě a $p(P)$ je pravděpodobnost, že má danou hybnost. Koherentní stav je tedy takový, kdy bylo dosaženo hranice, kde již nejde dále zpřesňovat měření (minimální nejistota) ani jedné z kvadratur. Tato „neznalost“ je však u obou stejná (kruh). To znamená, že pravděpodobnosti $p(X)$ a $p(P)$ jsou obě dány Gaussovým (normálním) rozložením [105, 106, 107, 108].

Stlačený stav se liší tím, že umožňuje zjistit jednu veličinu přesněji, ovšem pouze na úkor znalosti veličiny druhé (elipsa). V této kapitole však budou probrány pouze protokoly využívající koherentních stavů [105, 106, 107, 108].

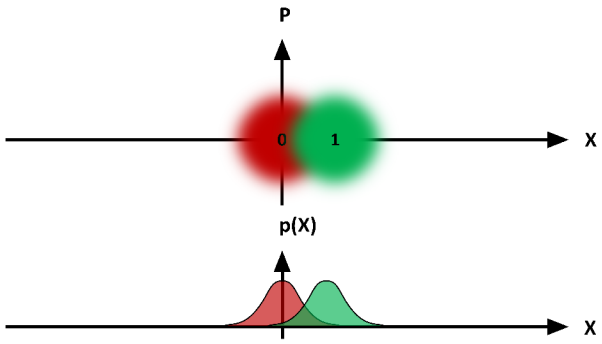
12.2 Spojitý protokol B92 neboli CV-B92

Jak bylo možno vidět na obrázku 12.1, pomocí fáze a amplitudy je možné vytvářet různé koherentní stavy světla. Nyní budou tímto způsobem zakódovány hodnoty 0 a 1. Pro hodnotu 0 se použije koherentní stav v samém počátku soustavy souřadnic (vakuový stav). Pro hodnotu 1 zase stav s větší amplitudou (fáze se zde měnit nebude), to znamená, že bude více vpravo na ose X, a Bob bude měřit pouze polohu částice (kvadraturu X). V tomto stavu není ani pro Boba, ani pro Evu problém oba stavy rozlišit, protože rozdíl jejich amplitud je dostatečně velký. To je ovšem problém, protože Eva může stav jednoduše změřit a přeposlat jej Bobovi [105].



Obr. 12.2: Princip reprezentace hodnot pomocí amplitudové modulace [105].

Řešením je snížení amplitudy tak, aby došlo k překrytí obou stavů tak, jak je prezentováno na obrázku 12.3. Pokud budou Eva s Bobem měřit, část jejich měření se bude vyskytovat v překrývajících se částech normálních rozložení. Pokud se tak stane, nejsou schopni určit, jedná-li se o stav 0 nebo 1. Eva bude chtít stav změřit a jeho kopii odeslat Bobovi. V případě, že bude Eva takto odposlouchávat, bude v tomto případě dělat chyby při určování stavů. Tzn., že bude Bobovi odesílat špatné stavy. To se promítne na Bobově rozložení [105].



Obr. 12.3: Princip zajištění bezpečnosti pomocí CV-QKD [105].

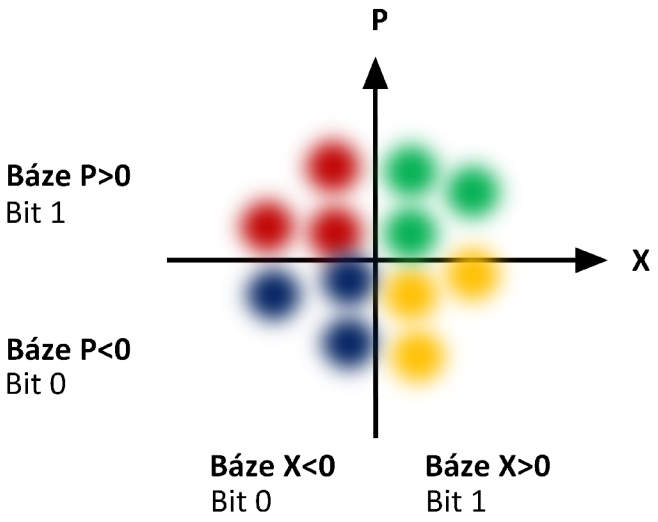
Bob se však může náhodně zeptat Alice, který stav odeslala. V případě, že by Alice odeslala např. hodnotu 0 a Bob ji naměřil jako jasnou 1 (tzn. čistě v zelené

nepřekrývající části) je jasné, že Eva odposlouchávala a určila špatně stav. Takto dojde k jejímu odhalení. Tyto testovací stavy jsou pak vyřazeny z tvorby klíče [105].

Bob však ještě stále nemusí mít stejný klíč jako Alice kvůli neobjeveným chybám. Z tohoto důvodu bývá přítomna ještě oprava chyb. Tento protokol bývá také někdy označován jako CV-B92, neboli spojitá varianta diskrétního protokolu B92 [105, 109].

12.3 GG02: Grosshans & Grangier (2002)

GG02, jinak známý též jako Coherent State Protocol, využívá kromě změn amplitudy i změny fáze. Alice náhodně generuje koherentní stavy, kdekoliv v rovině určené osami P a X. Do fáze a amplitudy tak kóduje hodnoty 0 a 1 (tzn. do X a P). Jejich interpretace může být různá, např. může být stanovena hranice pro fázi a amplitudu tak, jako na obrázku 12.4. Zda stav odpovídá bitu 0 nebo 1 se určí podle toho, zda daná hranice byla překročena nebo nikoliv. Bob si vybere, kterou kvadraturu (X nebo P) bude měřit homodynním detektorem [62, 101, 110, 111].

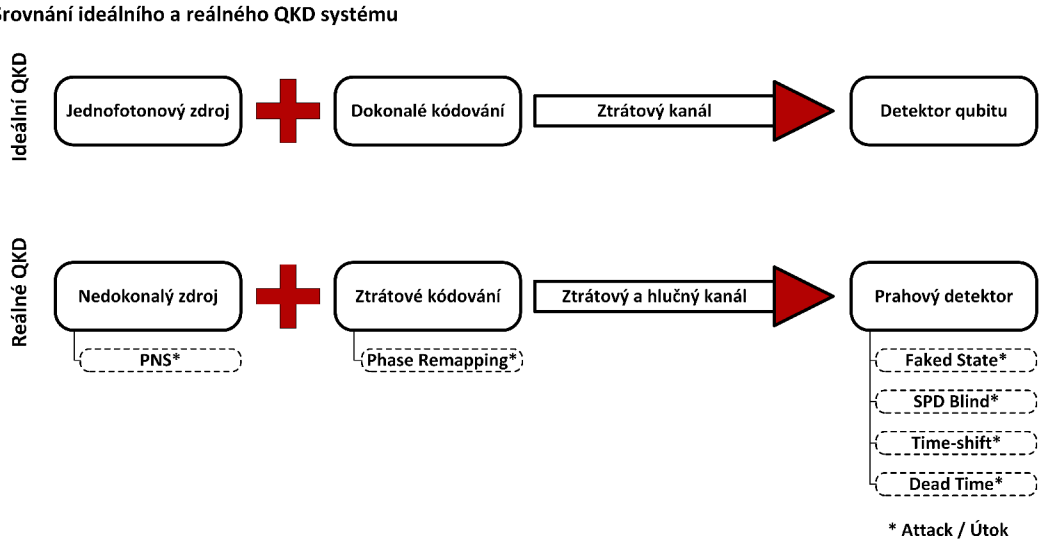


Obr. 12.4: Příklady různých koherentních stavů a jejich možné interpretace.

Jedno takové měření může provést přesně. Tím získá hodnotu bitu. To znamená, že polovina informace zůstane nevyužita. Alici následně sdělí, kterou kvadraturu měřil, respektive jakou použil bázi. (jako u BB84). Z toho Alice zjistí, jaký klíč Bob získal. Pokud poslouchá Eva, měřením bude vytvářet šum, který u Boba opět vyvolává chyby v měření. Ty budou následně Alicí a Bobem objeveny zveřejněním části klíče [62, 101, 110, 111].

13 Kvantový hacking a modely bezpečnosti

Ačkoliv se o QKD, často mluví jako bezpodmínečně bezpečné a zcela neprolomitelné kryptografii, v praktických implementacích se často nachází mnoho nedokonalostí. Ty mohou sloužit jako bezpečností díra ke kvantovému hackingu. Je nutné si uvědomit, že tzv. bezpodmínečná bezpečnost QKD se opírá o ideální (dokonalý) matematický model. Jak demonstruje obrázek 13.1, reálný QKD systém může nabízet mnoho příležitostí k útokům. PNS útok cílící na nedokonalost zdroje fotonů byl popsán již dříve. Jak je však z obrázku patrné, nejproblematičtější částí QKD systému bývá měření [112, 113].



Obr. 13.1: Grafika zobrazující vybrané útoky na nedokonalosti QKD systémů [113].

13.1 Modely bezpečnosti

Z pohledu obrany proti kvantovému hackingu existují v současné době minimálně 4 možné přístupy (modely bezpečnosti) [112].

13.1.1 Ideální QKD síť

Jedná se o čistě matematický model, který je sice zcela bezpodmínečně bezpečný, nepočítá ovšem s nedokonalostmi jednotlivých zařízení. Dá se také říct, že všechna zařízení v QKD systému jsou považována za důvěryhodná. To znamená, že neexistuje možnost, jak by se Eva mohla pomocí nich zmocnit distribuovaného klíče. Jako příklad lze uvést jednofotonovou variantu protokolu BB84 (samozřejmě bez dalších chyb) [112].

13.1.2 Opravování jednotlivých chyb

V praxi je zřejmé, že není vždy možno zcela naplnit očekávání, která jsou vyvíjena na ideální model. Jedná se o jakýsi responzivní systém, kdy je každá odhalená slabina následně záplatována. Příkladem může být aproximovaný protokol BB84, využívající WCP. Jeho slabinou je jasná nedokonalost zdroje fotonů, které využívá PNS útok. Jako záplata byl následně navržen systém návnadových stavů [112].

13.1.3 DI-QKD (Device-independent QKD)

Představuje principiálně odlišný přístup. Bezpečnost DI-QKD je postavena na porušení Bellovy nerovnosti, musejí však být uzavřeny obě dříve popsané díry. Alice s Bobem nemusejí vědět, jakým způsobem jejich zařízení fungují (black box). Případně, zda jsou vůbec správně a bezpečně nastavena. Aby ale bylo možno k zařízením takto přistupovat je nutné splnit několik předpokladů. Ty lze najít v tabulce níže. Ve srovnání s dále popsaným MDI-QKD se jedná např. o spolehlivost měřících zařízení, u kterých nesmí docházet k únikům informací. To neplatí pouze u Alice a Boba, ale typicky i u třetího uzlu Charlie. Jinak řečeno musejí být použita důvěryhodná zařízení. Protože bylo až do nedávna uzavření obou děr v Bellových testech nemožné, nejsou DI-QKD protokoly příliš rozšířené. Teoreticky však existuje mnoho různých variant. Zástupcem by mohl být například Spot-checking CHSH QKD protokol, dále existují například verze využívající prohození stavového provázání. K tomu bývá využíváno tzv. ESR (entangelement SWAP relay) [114, 115, 116].

Tab. 13.1: Srovnání požadavků na DI-QKD a MDI-QKD [112].

Vyžadováno	**DI-QKD**	**MDI-QKD**
QRNG	Ano	Ano
Autentizovaný klasický kanál	Ano	Ano
Bezpečné odvození klíčů	Ano	Ano
Důvěryhodný zdroj fotonů	Ne	Ano
Nulový únik informací z měření	Ano	Ne

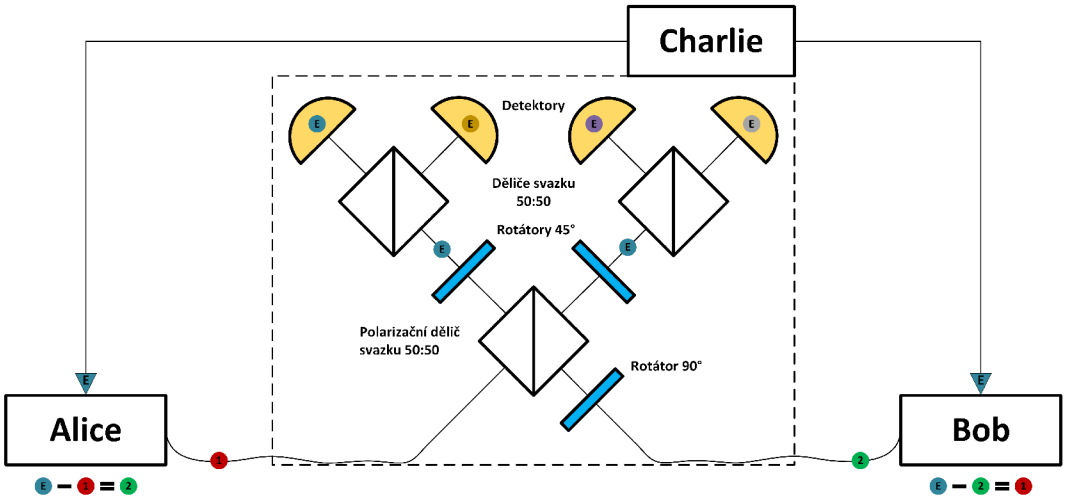
13.1.4 MDI-QKD (Measurement-device independent)

MDI-QKD využívá v podstatě opačný přístup, než DI-QKD. Na rozdíl od předchozího vyžaduje důvěryhodný zdroj fotonů (tzn. decoy state WCP, nebo jednofotonový zdroj). Nejsou však kladeny žádné nároky na měřící části zařízení, které tak mohou být nedůvěryhodné. To je obzvláště výhodné z toho důvodu, že většina útoků proti

QKD využívá právě chyb a nedokonalostí při měření. Z toho také vyplývá, že prostřední měřící uzel Charlie nemusí být důvěryhodný [117, 118, 119].

Princip MDI-QKD protokolů

Typickou topologii MDI-QKD protokolu lze vidět na obrázku 13.2 níže. Nechť je tedy Alice, Bob a Charlie, který ovšem může být klidně infiltrován Evou. To znamená, že MDI-QKD nevyžaduje, aby Charlie byl důvěryhodným uzlem. Alice a Bob mají pouze zdroje fotonů, Charlie naopak slouží k měření Bellových stavů (BSM) [119].



Obr. 13.2: Typická topologie MDI-QKD protokolů. Uprostřed uzel Charlie provádějící BSM [119].

Samotná podstata protokolu je potom následující. Alice i Bob odešlou foton v jednom ze dvou možných stavů. Oba fotony dorazí k Charliemu a vlivem BSM dojde k jejich provázání. Následně je zjištěn Bellův stav. To, který Bellův stav se získá je dáno stavy vyslaných fotonů. Charlie (ani Eva) původní stavy neznají a získají pouze tento výsledný Bellův stav. Eva je tedy schopna určit pouze to, zda byly odeslány shodné, nebo opačné fotony. Případ, kdy oba odeslali stejné fotony, není považován za bezpečný. V případě opačných fotonů, však není Eva schopna určit, z jakého směru, který foton přišel. Charlie následně ohlásí Alici a Bobovi změřený Bellův stav. Oba znají stav jimi vyslaného fotonu a z Bellova stavu jsou schopni určit foton odeslaný protistranou. Z bezpečných případů je následně sestavován klíč [119].

Jako u DI-QKD existuje opět několik dalších protokolů, vycházejících z daného principu. Mezi „odnože“ MDI-QKD patří například protokoly TF-QKD (Twinfield QKD) nebo DDI-QKD (Detector-device independent QKD) [120, 121, 122].

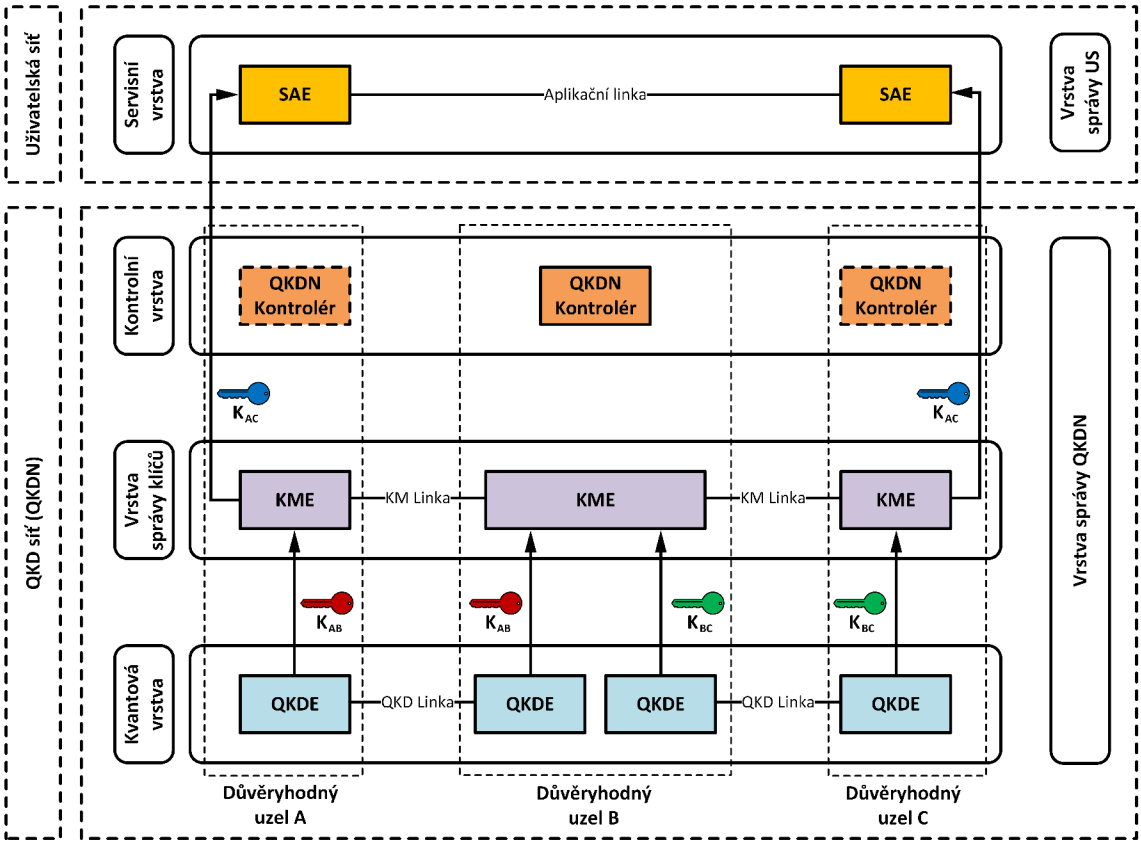
13.2 Shrnutí QKD technologií

V současnosti dochází na poli QKD protokolů k velmi rychlému vývoji, čehož výsledkem je nepřeberné množství různých protokolů a jejich nejrůznějších modifikací. V komerční sféře se však zatím uplatnila jen hrstka. Nejčastěji lze narazit na BB84 s návnadovými stavy a COW protokol. Naprostá většina protokolů je v současnosti pouze v experimentálním stádiu. Cílem tohoto dokumentu bylo sestavit přehled nejčastěji se vyskytujících fyzikálních principů a předvést jejich princip na konkrétním protokolu.

14 Topologie QKD sítí (QKDN)

V současnosti není schválen standard pro infrastrukturu kvantových sítí. Tzn. sítí, které existují společně s uživatelskou sítí, po které jsou posílána zašifrovaná data. Přesto však již byly navrženy referenční modely, vycházející např. z ISO-OSI nebo TCP/IP. Níže lze vidět návrh ITU-T z října roku 2019 na obrázku 14.1. Základem je rozdělení celé topologie do dvou nezávislých sítí [123].

Jak je možné vidět, rozlišuje se mezi uživatelskou sítí a kvantovou. Uživatelskou sítí může být například internet, ale i jakákoliv jeho část nebo zcela odlišná síť, na které dochází k šifrování dat pomocí QKD. Správnou funkci v dané síti zajišťuje specifická SAE. QKD síť je tvořena třemi základními vrstvami. Uživatelská představuje z pohledu QKD jedinou, tzv servisní vrstvu. Obě sítě dále obsahují vrstvy zajišťující celkový management sítě [123].



Obr. 14.1: Referenční model kvantových sítí navržený na standardizaci [123].

14.1 Základní pojmy

- **Bezpečná oblast** – oblast, ve které nemůže dojít ke zneužití QKD zařízení (budova, laboratoř atd.). V ní by se měla nacházet všechna zařízení současných QKD systémů (SAE a TN).
- **Trusted Node (TN)** – Důvěryhodný uzel – samostatné zařízení obsahující QKDE, KME a QKDN řadič (kontrolér). Může se vyskytovat i jako třetí opakovací uzel. V tomto případě se hovoří o tzv. důvěryhodném opakovači.
- **Quantum Key Distribution Entity (QKDE)** – QKD entita – část zařízení zodpovědná za ustanovení společného klíče, jeho součástí je kvantový generátor.
- **Key Management Entity (KME)** – Entita pro správu klíčů – softwarová entita / vrstva sloužící k ukládání vygenerovaných klíčů a jejich následné distribuci SAE. V rámci sítě má své jedinečné ID sloužící k autentizaci. Pomocí správy klíčů je možné budovat složitější topologie QKDN jako například kruh či hvězda.
- **Secure Application Entity (SAE)** – Entita bezpečnostní aplikace – samostatné šifrovací zařízení, pracující na libovolné vrstvě referenčního modelu. Podobně jako KME má své jedinečné ID [123, 124].

14.2 Vrstvy referenčního modelu

Navrhovaný referenční model přiřazuje QKD sítím v základu tři horizontální vrstvy. Uživatelská síť je potom z pohledu tohoto modelu tvořena jedinou servisní vrstvou. Model dále specifikuje vertikální vrstvy pro management jednotlivých sítí. Těmi se ovšem tato práce nebude hlouběji zabývat [123].

14.2.1 Kvantová vrstva (Quantum layer)

Kvantová vrstva sestává z QKDE modulu a QKD logické linky. Jejím úkolem je ustanovit kvantový klíč mezi dvěma sousedními moduly pomocí protokolů popsaných výše. Každý důvěryhodný uzel musí obsahovat minimálně jeden QKD modul. Dva sousední moduly jsou propojeny QKD linkou, tu lze dále rozložit na tzv. klasický[1] (servisní) kanál a kvantový kanál [123].

[1] Obzvlášť v praktické části, se pod pojmem klasický kanál myslí veškeré „nekvantové“ signály. Z tohoto důvodu je pro „nekvantový“ kanál z QKD serveru preferováno označení servisní kanál. Oba pojmy jsou ovšem zaměnitelné.

14.2.2 Vrstva správy klíčů (Key management layer)

V každém uzlu musí být přítomna správa klíčů, tzn. KME modul. Jednotlivé moduly jsou propojeny KM logickou linkou. Správa klíčů odebírá od QKD modulu bitové posloupnosti, které formátuje do podoby klíče. Využíván je formát json. Klíče jsou zde následně uloženy a na vyžádání jsou poskytovány SAE skrze nainstalovaná softwarová rozhraní. Po použití musí být bitová kopie klíče uložená v KME paměti bezpečně skartována. V případě, že má být klíč ustanoven mezi uzly, které spolu nesousedí (A a C), je pomocí QKDN kontroléru vyšší vrstvy nalezena cesta, kterou je klíč distribuován, skrze důvěryhodné opakovače (uzel B) [123].

Důvěryhodný opakovač (Trusted repeater)

Důvěryhodným opakovačem (TR) se rozumí zařízení, které není koncovým bodem. V současnosti nejsou dostupné kvantové paměti. Z tohoto důvodu nelze signál replikovat již na kvantové vrstvě při samotném přenosu klíče. Proto je složitější distribuce klíčů zajišťována pomocí správy klíčů, avšak již v klasické podobě (bity). To je důvodem proč se TR musejí nacházet v bezpečné oblasti stejně jako koncové body.

Princip přenosu klíče přes TR je následující. Chce-li uzel A komunikovat se uzlem C, budou mezi uzly A a B a uzly B a C ustanoveny dva rozdílné klíče K_{AB} a K_{BC}. Uzel A následně vygeneruje třetí klíč K_{AC}, jenž zašifruje pomocí K_{AB} (používá se OTP, popsáno dále) a odešle opakovači B. Ten klíč K_{AC} dešifruje, opět jej zašifruje pomocí K_{BC} a odešle konečnému uzlu C. Ten jej následně opět dešifruje. Výsledkem je bezpečný klíč sdílený mezi dvěma nesousedícími uzly [123].

14.2.3 QKDN kontrolní vrstva (QKDN control layer)

Funkce této vrstvy jsou zprostředkovávány pomocí kontrolérů. Jedná se zejména o směrování mezi TR při distribuci klíče, dohled nad nižšími vrstvami, QoS atd. [123]

14.2.4 Servisní vrstva (Service layer)

Tato vrstva není součástí QKD sítě, nýbrž sítě uživatelské. Pracují na ní specifické SAE, tedy kryptografické aplikace, šifrátory atp. Z QKD sítě odebírá pomocí ETSI API kvantové klíče, kterými šifruje komunikaci, která mezi SAE uzly probíhá po libovolné aplikační lince [123].

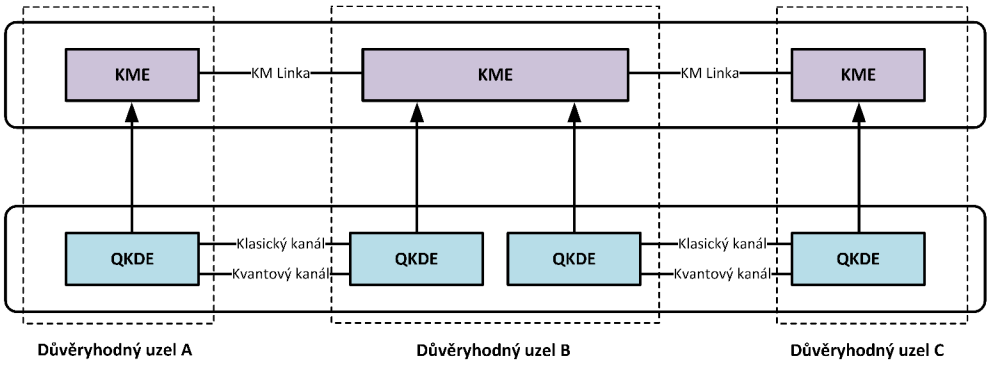
14.2.5 Management

Obě sítě, obsahují ještě vrstvy zajišťující správu sítě jako celku. Jedná se o vrstvu správy uživatelské sítě a QKDN (User network / QKDN management layer). [123].

14.3 Horizontální spoje v QKD síti

Jak již bylo uvedeno jednotlivé uzly mezi sebou udržují několik logických kanálů. Povinně musí existovat KM linka, klasický kanál a kvantový kanál. V některých případech jsou ale přítomny i další spoje sloužící např k časové synchronizaci atp. Fyzická implementace těchto logických kanálů může být různá. Kvantový kanál musí být vždy optické vlákno (to neplatí pro tzv. Free-space protokoly) [123].

- **KM linka** – logická linka sloužící ke komunikaci mezi KME, např. distribuci klíče mezi vzájemně nesousedícími uzly.
- **QKD linka** – logická linka spojující dva sousední QKD uzly. Jedná se o označení sdružující klasický a kvantový kanál.
  - **Klasický kanál** – logická linka zajišťující režii při přenosu qubitů a vytváření klíče, může se skládat z několika dalších logických (případně i fyzických) spojů, zajišťující např. destilaci klíče nebo synchronizaci.
  - **Kvantový kanál** – logická i fyzická linka sloužící k samotnému přenosu qubitů.



Obr. 14.2: Schéma horizontálních logických linek [123].

Aby bylo nasazení QKD technologií co nejefektivnější, navrhuje se používat pro několik logických kanálů jeden společný fyzický kanál. Doporučují se kombinace:

Tab. 14.1: Možná agregace logických linek [123].

KM linka	**Klasický QKD kanál**	**Kvantový QKD kanál**
Libovolná technologie		Optický kanál
Optický kanál s WDM		

14.4 Vertikální spoje v QKD síti

Z tohoto pohledu se rozlišují dva základní způsoby komunikace. V první řadě odebírá KM modul kvantové klíče z QKD modulu. K této komunikaci však dochází v rámci jednoho zařízení (důvěryhodného uzlu, TN). Z tohoto pohledu tak pro uživatele není příliš zajímavá. Druhým spojem je komunikace mezi TN a SAE, tedy mezi dvěma samostatným zařízeními. Má-li uživatel celý QKD systém v rámci jednoho zařízení nemusí nic řešit. V tomto případě putuje vygenerovaný společný klíč rovnou do šifrátoru/dešifrátoru přes společné vnitřní rozhraní. Většina pokročilých systémů ovšem sestává z více zařízení, jak bude popsáno níže [123].

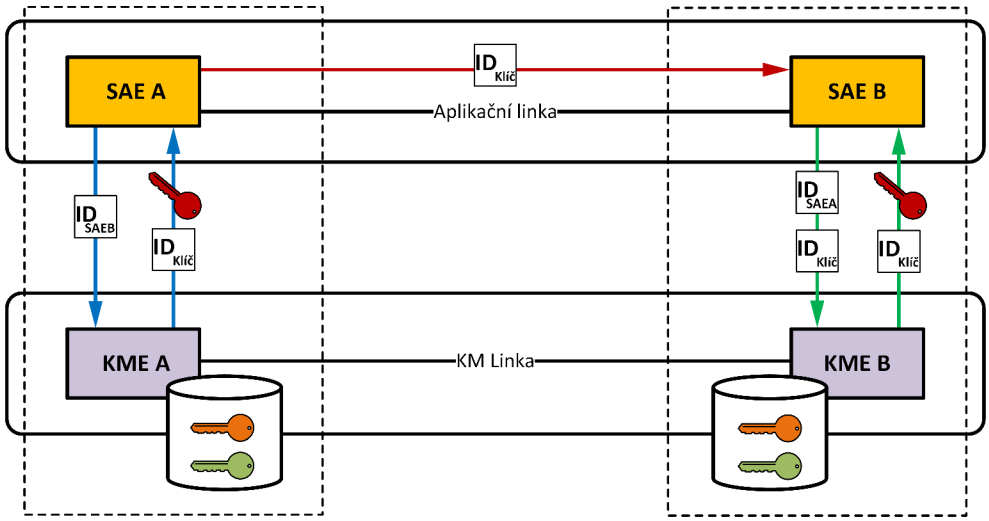
14.4.1 ETSI API

Pokud je tedy TN a SAE zvlášť, jsou tato dvě zařízení propojena společným rozhraním a musejí se nacházet v jedné zabezpečené oblasti. Aby bylo možné používat QKD servery a šifrátory vzájemně od různých výrobců, existuje standardizované rozhraní zvané ETSI Key delivery API[2]. Při použití některých zařízení umožňuje toto rozhraní i sofistikovanější zacházení s klíči. Česky by se dalo doslova přeložit jako aplikační (programovací) rozhraní pro doručování klíčů. Jedná se o rozhraní mezi dvěma softwarovými programy, sloužící k jejich vzájemné komunikaci (programy v SAE a KME v TN). Je založeno na REST API, z čehož vplývá, že veškerá komunikace mezi SAE a KME je založena na protokolu HTTPS, tj. zabezpečené verzi protokolu HTTP [124, 125].

Každý klíč má v KME paměti přiřazeno své ID. Stejně tak mají identifikátory přiděleny i SAE a KME. V případě složitějších topologií slouží všechna zmíněná ID k rozeznávání vzájemně komunikujících entit a klíčů.

SAE A (master) se nyní chystá odeslat šifrovanou zprávu SAE B (slave). Průběh komunikace z obrázku 14.3 je následující:

1. SAE A, sdělí KME A identifikátor cílové SAE, čímž si vyžádá klíč. KME A jí klíč poskytne spolu s jeho identifikátorem.
2. SAE A informuje SAE B o ID vybraného klíče přes uživatelskou síť.
3. SAE B si vyžádá tentýž klíč od své KME B. Po jeho poskytnutí jsou obě SAE připraveny k šifrovanému přenosu dat [124, 125].



Obr. 14.3: Průběh komunikace mezi KME a SAE pomocí ETSI API [124].

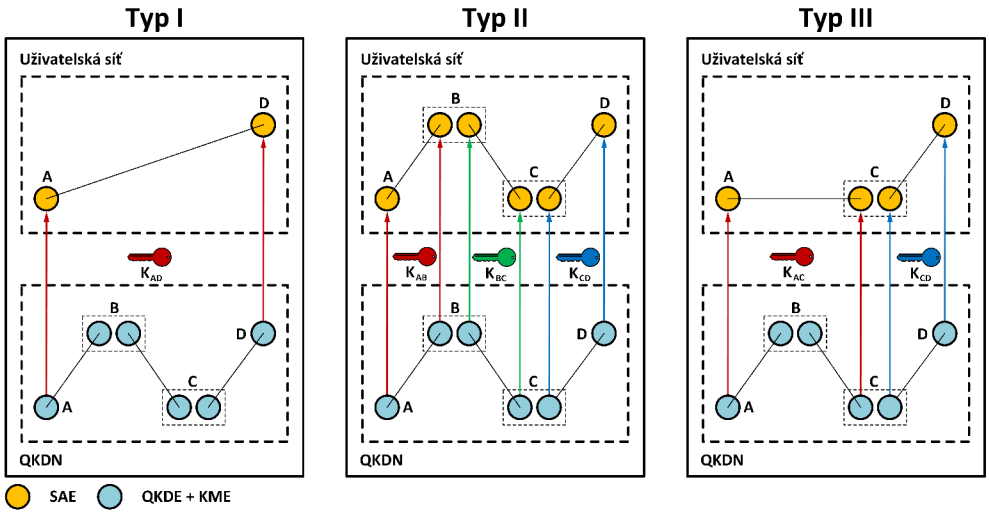
[2]Zkráceně pouze ETSI API.

14.4.2 Ostatní rozhraní

ETSI zvažovala použití tzv. konvenčního protokolu **KMIP** (Key Management Interoperability Protocol), ten však nebyl zcela vyhovující a proto pro něj byla vydána doporučení. Přesto je KMIP používán např. firmou QuintessenceLabs. Další společností nevyžívající ETSI API je i firma Qubitekk s protokolem **Modbus** [125].

14.5 Vztah mezi QKDN a uživatelskou sítí

Kvalitní správa klíčů dnes umožňuje stavbu QKD sítí s mnohem složitějšími topologiemi než jen bod-bod. V komerční sféře se dnes již běžně vyskytují sítě s důvěryhodným opakovačem nebo kruhové a hvězdicové topologie. Důležité ovšem je, že uživatelské sítě nemusejí přesně kopírovat topologie dané QKD sítí. Rozdíl je patrný z obrázku 14.4. Sítě využívající TR např. nepotřebují stejný počet šifrátorů jako QKD modulů, příkladem jsou typy I a II. Typ III potom představuje kombinovanou variantu [123].



Obr. 14.4: Možné vztahy mezi QKDN a uživatelskou sítí [123].

15 Šifrování uživatelské sítě

Přes klíčovou infrastrukturu se společný klíč dostává do šifrátoru. Nyní je ovšem třeba zvolit správný algoritmus pro šifrování dat přenášených po klasickém kanále. V opačném případě by celá tato snaha přišla vniveč. Šifrování je možné provádět na libovolné vrstvě referenčního modelu.

15.1 Postkvantová kryptografie (PQC)

Jinak též kvantově bezpečná kryptografie, neboli QSC (Quantum-safe Cryptography). Jedná se o takovou formu šifrování, jenž je odolná nejen vůči útokům pomocí běžných počítačů, ale i počítačů kvantových. To znamená, že není znám takový kvantový algoritmus, který by šifru prolomil, případně snížil složitost úlohy pod bezpečnou hranici.

Momentálně existuje několik hlavních směrů, kterými se výzkum PQC ubírá. Jedná se hlavně o kryptografii založenou na hashech, mřížích, teorii kódování a polynomiálních rovnicích. Popis těchto principů je však nad rámec této práce [12, 126].

V současnosti (2020) probíhá výběrové řízení NIST pro standard postkvantové kryptografie. Většina navrhovaných šifrovacích algoritmů je založena na mřížích. Konkrétně se jedná o šifry CRYSTALS-KYBER, NTRU a SABER. Posledním postupujícím algoritmem je Classic McEliece, který je založen na Goppových kódech [127].

Jak bylo uvedeno u popisu Groverova algoritmu, za splnění určitých podmínek lze za PQC považovat i některé současné symetrické algoritmy. Typicky se jedná o AES-256, užívá se ale i jihokorejský algoritmus LEA. Právě tyto algoritmy jsou nejčastěji zastoupeny u současných šifrátorů pracujících s QKD [15, 128, 129].

15.2 Vernamova šifra

Anglicky one-time pad (OTP), jinak také známá jako dokonalá šifra. Důvodem je fakt, že za dodržení základních požadavků, které jsou na šifru kladeny, neexistuje způsob, jak ji zlomit. Patentována byla v roce 1917 a ačkoliv si byl G. Vernam její neprolomitelností jistý, důkaz byl podán až v roce 1949 C. Shannonem. Princip spočívá v tom, že každý znak je posunut o náhodný počet míst v abecedě. To je prakticky stejná operace, jako kdyby byl každý znak nahrazen libovolným jiným znakem. I kdyby tedy útočník měl neomezený výpočetní výkon, výsledkem by mu byly úplně všechny možnosti o dané délce zprávy. Která ze zpráv je ta správná není možné určit. Digitální bitová verze je popsána níže [130, 131].

Požadavky na OTP:

- Skutečně náhodný tajný klíč
- Klíč je stejně dlouhý jako přenášená zpráva
- Klíč nesmí být opakovaně použit

U současné kryptografie je hlavní nevýhodou této šifry distribuce dlouhého klíče. Přesto se však již delší dobu používá v diplomatickém a vojenském prostředí. QRNG a QKD jsou ovšem pro OTP ideálním řešením. Bohužel, rychlost generování klíčů u těchto systémů stále není dostatečná. Současné QKD systémy pracují s rychlostmi v řádu kb/s. Při poměru klíče a zprávy 1:1, by tak došlo k degradaci klasického kanálu na stejnou rychlost, což jistě není žádoucí [130, 131].

Princip digitální verze, používající pouze bity s hodnotami 0 a 1 je znázorněn v tabulce 15.1. Nechť na bity převedená zpráva proudem vchází do šifry. Spolu s ní je druhým vstupem zcela náhodný klíč. Ten je taktéž v bitové formě. Oba proudy budou nyní seřazeny nad sebou, tak aby první bity vzájemně korespondovaly. Následně je nad každou dvojicí těchto bitů provedena operace XOR (exkluzivní disjunkce). Stejným klíčem a operací se šifrový text opět rozšifruje [130, 131].

Tab. 15.1: Využití operace XOR ve Vernamově šifře [131].

Šifrování					
Zpráva	$\oplus$	0	1	0	1
Klíč		0	0	1	1
Šifrový text	=	**0**	**1**	**1**	**0**

Dešifrování					
Šifrový text	$\oplus$	0	1	1	0
Klíč		0	0	1	1
Zpráva	=	**0**	**1**	**0**	**1**

15.3 Možné scénáře využití QKD podle vrstev

15.3.1 Virtuální privátní síť (VPN)

VPN je obecné označení pro technologie umožňující propojení dvou vzdálených bodů (bod-bod) do jediné společné virtuální sítě. Typicky se jedná o šifrované tunelové spojení zajišťující bezpečnost dat přes nedůvěryhodnou síť (např. internet). Nejběžněji se s ní lze setkat na síťové vrstvě (L3), kde je využíváno IPSec protokolu. VPN lze ovšem použít i na dalších vrstvách. Řadí se sem tak i protokoly jako SSL/TLS (L4), SSH (L7) atp. [132]

15.3.2 Kvantová virtuální privátní síť (QVPN)

Kvantová VPN (QVPN), někdy též pouze QPN je „kvantovým“ rozšířením standardní virtuální privátní sítě. Problematika bude vysvětlena na protokolu IPSec. Ten slouží jako zabezpečená VPN na síťové vrstvě ISO-OSI modelu. Pro ustanovení společného klíče využívá IPSec podprotokolu IKE (Internet Key Exchange) s implementovanou Diffie-Hellmanovou výměnou. Jako QVPN je tak možné si představit takovou variantu IPSecu, kde modifikované IKE využívá místo DH jeden z QKD protokolů [133].

Šifrátory však mohou pracovat na libovolné vrstvě ISO-OSI modelu (zahrne-li se L5 a L6 do aplikační vrstvy). V této sekci budou formou stručného seznamu uvedena možná využití QKD systémů v kombinaci s dnes běžnými bezpečnostními protokoly [133, 134].

- **Fyzická vrstva (L1)**
  - Libovolná technologie – elektrické, optické sítě, bezdrátový přenos
- **Spojová vrstva (L2)**
  - MACSec (Medium Access Control Security)
  - PPP (Point to Point Protocol)
    - ECP (Encryption Control Protocol)
- **Síťová vrstva (L3)**
  - IPSec (Internet Protocol Security)
    - IKE (Internet Key Exchange)
- **Transportní vrstva (L4)**
  - TLS/SSL (Transport Layer Security / Secure Socket Layer)
- **Aplikační vrstva (L7)**
  - Libovolná aplikační funkce např. SSH (Secure Shell)

16 Komerčně dostupná řešení

16.1 Komplexnost zabezpečení sítě

Za QVPN lze tedy považovat komplexní řešení kombinující jak QKD síť (QKDN), tak síť uživatelskou s libovolným zabezpečeným tunelem. Různé společnosti nabízejí různě komplexní kvantové zabezpečení. Popis možného modelu QKD systému byl již zmíněn výše. V komerční sféře ovšem bývají zařízení nazývána odlišně. Aby mohl takovýto systém fungovat, potřebuje v základu dále uvedené komponenty / zařízení.

Kvantový generátor náhodných čísel – pro kvantovou distribuci klíčů je nejdříve nutné vygenerovat, skutečně náhodnou posloupnost qubitů, tj. základ pro budoucí klíč. Takovýto generátor bývá označován jako QRNG modul. Vygenerované posloupnosti bývají následně nejčastěji aplikovány na polarizované fotony. QRNG moduly však bývají přímo integrovány do QKD serverů.

QKD server – základní komponenta, zprostředkovávající samotný protokol kvantové výměny klíčů. Z pohledu možného referenčního modelu obsahuje QKDE, KME a kontroléry. Výstup pro šifrátor bývá opatřen ETSI API.

Správa klíčů – v tomto případě nejde pouze o KME v rámci QKD serveru. V současnosti již existují speciální zařízení pracující mezí QKD serverem a šifrátorem. Pro vstup i výstup využívají ETSI API a jejich účelem je ještě komplexnější distribuce klíčů mezi jednotlivými uzly, než umožňuje standardní správa klíčů.

Šifrátor – zařízení, pracující na různých vrstvách ISO-OSI modelu. Z tohoto pohledu se může jednat o různé brány, přepínače, multiplexory atp. Tento šifrátor představuje SAE, do které klíč vstupuje pomocí ETSI API. Tímto symetrickým klíčem je potom standardním způsobem zašifrována komunikace v uživatelské síti. Měl by být použit kvantově bezpečný šifrovací algoritmus (PQC).

16.2 Sestavy QVPN

Jednotlivá zařízení lze mnohdy koupit samostatně, v takovém případě bývají kompatibilní s ostatními zařízeními od stejného výrobce a v mnoha případech i se zařízeními jiných výrobců. V tomto případě se jedná hlavně o kompatibilitu mezi QKD serverem a šifrátorem. QRNG modul bývá většinou součástí QKD serveru. Mezi samostatně fungující zařízení lze zařadit např. řadu „qProduktů“ australského výrobce Quintessence Labs[1].

Někteří prodejci nabízejí **jediné samostatné QVPN zařízení**, obsahující veškeré komponenty. Tento přístup využívá třeba americká společnost MagiQ, jejíž výrobek se jmenuje QPN.

Další možností je **modulární řešení** – jednotlivé komponenty jsou často umisťovány do 19palcového Blade systému. Takováto řešení představují např. systémy Clavis^{300} a Cerberis^{3} švýcarské firmy IDQ.

Implementace QKD se pomalu začínají objevovat i v **čipové podobě** fotonických integrovaných obvodů. Těmito technologiemi se zabývá např. britský startup |KETS>.

[1] Zmíněné společnosti a jejich zařízení budou popsány v další kapitole.

16.3 Společnosti zabývající se QKD

Nyní bude prezentován výčet společností a organizací zabývající se jak výrobou QKD systémů samotných, tak výrobou kompatibilních šifrátorů. Výrobky většiny firem ovšem nejsou v současné době z různých důvodů dostupné [135, 136].

16.3.1 ID Quantique (IDQ)

Švýcarská soukromá společnost, zabývající se jak výrobou kvantových generátorů, tak QKD serverů a šifrátorů. Spolu s nimi však nabízí i další specializované komponenty a přístroje. Následuje stručná charakteristika vybraných zařízení. Detailnější informace budou však přehledně uvedeny níže v tabulkách [137, 138].

- **QKD servery**
  - **Clavis**^{3} – otevřená a upravitelná QKD platforma pro výzkum; umožňuje pouze přímou komunikaci; využívá COW protokol
  - **Clavis**^{300} – modulární řešení, jehož součástí může být i LEA šifrátor; lze použít jako důvěryhodný opakovač; využívá návnadový protokol BB84
  - **Cerberis**^{3} – modulární řešení s QNC modulem (Quantum Node Controller), jenž umožňuje i složitější topologie jako hvězda a kruh; využívá COW protokol
- **Šifrátory**[2]
  - **Centauris CV1000** – virtuální šifrátor běžící na Linuxové distribuci Debian; podporuje šifrování na několika vrstvách a je kompatibilní s ostatními IDQ šifrátory
  - **Centauris CN4000/6000/8000/9000** – série klasických šifrátorů s QRNG modulem pracující na spojové vrstvě (L2 – MACSec); lze je ovšem používat i v kombinaci s QKD servery; využívá AES šifrování

Obr. 16.1: Loga firem IDQ a Thales [137, 138].

[2]Šifrátory IDQ jsou vyvíjeny ve spolupráci s firmou THALES.

16.3.2 Toshiba

Japonská korporace, jejíž pobočka v britském Cambridge se zabývá výzkumem QKD. Momentálně nabízí QKD servery ve dvou variantách. Oba využívají verzi návnadového protokolu BB84 známou jako T12 [139].

- **QKD servery**
  - **Multiplexovaný QKD systém** – využívá O-pásmo (1260-1360 nm) pro kvantový kanál a C-pásmo (1530-1565 nm) pro klasický přenos; používá 1 nebo 2 optická vlákna
  - **Dálkový QKD systém** – pouze pro temné vlákno; využívá C-pásmo (1530-1565 nm) pro kvantový kanál; jsou nutná 2 optická vlákna

Obr. 16.2: Logo firmy Toshiba [139].

16.3.3 Qubitekk

Americká firma vyvíjející QKD server pro použití v průmyslových řídících systémech. Pro výukové účely vyvinula i QKD demonstrátor, který interpretuje a znázorňuje procesy mezi dvěma běžícími QKD servery [140].

- **QKD servery**
  - **Quantum DataLoc Key Server** – použití v průmyslových oblastech; pro komunikaci mezi QKD serverem a šifrátorem používá rozhraní Modbus; využívá protokol BBM92

Obr. 16.3: Logo firmy Qubitekk [140].

16.3.4 MagiQ

Americká bezpečnostní společnost, nabízející jako první QKD komerčně. Kromě QKD se zabývá i seizmickým průzkumem a vojenstvím. Nabízí jednotný systém zvaný QPN. Poslední známou verzí je QPN Security gateway 8505 [141, 142].

- **Kompletní QVPN**
  - **QPN Security gateway 8505** – kompletní QVPN systém; QKD server využívá protokol BB84; podpora důvěryhodných opakovačů; šifrátor pracuje na síťové vrstvě (L3 – IPSec); šifrování pomocí AES-256 a 3DES

Obr. 16.4: Logo firmy MagiQ [141].

16.3.5 Quintessence Labs

Australská bezpečností společnost zabývající se kvantovými technologiemi. Nabízí komplexní řešení pomocí řady svých „qProduktů“ [143].

- **QKD servery**
  - **qOptica** – využívá jeden z CV-QKD protokolů, jedná se o tzv. free-space protokol, tzn. „bezdrátovou“ verzi QKD protokolů
- **Správa klíčů**
  - **qClient** – software pro správu klíčů využívající protokolu KMIP; rozhraní je integrováno jak u QKD serveru, tak u šifrátoru; může být dodáváno i zvlášť a upravováno
- **Šifrátory**
  - **qCrypt** – řada šifrátorů; možno pořídit v softwarové i hardwarové formě

Obr. 16.5: Logo firmy Quintessence Labs [143].

16.3.6 Quasky

Jedna ze dvou největších čínských firem podnikajících v kvantové kryptografii. Qasky vyrábí jak dva komerční typy QKD serverů, tak jejich akademickou verzi. Kromě toho nabízí též L3 šifrátory a speciální „kvantový router“ založený na WDM. Jedná se tedy o způsob, jak dosáhnout komplexnější výměny klíčů již na kvantové vrstvě [144].

- **QKD servery**
  - **QKD experimentální systém WT-QKDS** – akademická verze využívající protokol BB84
  - **QKD terminál WT-QKD-200** – samostatné zařízení, využívá návnadový protokol BB84
  - **GHz QKD terminál WT-QKD-400** – výkonnější verze QKD terminálu; kromě vyšší rychlosti generování klíče je schopna i složitějších topologií
- **Správa klíčů a multiplexory**
  - **Kvantový router WT-QRT** – zařízení pracující na kvantové vrstvě; k rozlišení zařízení využívá WDM, tzn. zařízení je přiřazena vlnová délka
  - **Kvantové konverzní zařízení WT-QOS** – zařízení pracující na kvantové vrstvě; jeho účelem je agregace kvantového a servisního kanálu do jedné linky; využívá TDM
- **Šifrátory**
  - **Kvantová bezpečnostní brána WT-QVPN** – aplikační brána pracující na síťové vrstvě (L3); využívá IPSec protokol

Obr. 16.6: Logo firmy Qasky [144].

16.3.7 QuantumCTek

Druhá hlavní čínská společnost, zabývající se kvantovou informatikou. QuantumCTek nabízí kvantové technologie především pro metropolitní a meziměstské páteřní sítě. V nabídce má několik variant QKD serverů běžících na návnadovém BB84 protokolu, stejně jako metropolitní ústředny pracující na složitějších topologiích typu hvězda [145].

- **QKD servery**
  - **QKD experimentální systém** – akademická verze; v plné verzi umí pracovat s protokolem SARG04 a s návnadovými protokoly BB84 a B92
  - **QKD terminály pro MAN QKDM-POL40-S** – QKD servery určené k nasazení v metropolitních sítích; lze pořídit variantu se správou klíčů nebo bez ní; využíván je návnadový BB84 protokol
  - **QKD terminály pro BN QKD-POL1250-S a QKD-PHA1250-S** – QKD servery určené k nasazení v páteřních sítích; rozdílem obou systémů je odlišná implementace (polarizační a fázová) návnadového BB84
- **Správa klíčů a multiplexory**
  - **Zařízení pro správu klíčů** – samostatné zařízení pracující mezi šifrátorem a QKD serverem; umožňuje použití důvěryhodného opakovače
  - **Optický přepínač** – samostatné zařízení využívají časového multiplexu; umožňuje efektivnější stavbu metropolitních sítí
  - **WDM pro kvantové kanály** – samostatné WDM multiplexory umožňující buď agregaci více kvantových kanálů, nebo agregaci klasického a kvantového kanálu do jedné fyzické linky
  - **MAN QKD kontrolní stanice** – stanice obsahující QKD servery spolu s výše zmíněnými prvky; využívá se v metropolitních sítích pro složitější topologie

Obr. 16.7: Logo firmy QuantumCTek [145].

- **Šifrátory**
  - **VPN brána SJJ1529** – samostatné zařízení, pracuje na síťové vrstvě (L3); používá protokol IPSec
  - **Šifrovací router EQR 2000/3000** – dvě série šifrovacích směrovačů (L3); pracují s protokolem IPSec
- **Kompletní QVPN**
  - **QKD síťový šifrátor SJJ1411** – kompletní QVPN systém; QKD server využívá návnadový protokol BB84; šifrování pomocí AES-256

16.3.8 |KETS>

Britský startup při Bristolské univerzitě, věnující se především kompaktnímu řešení QKD a kvantovému generování. V |KETS> vyvinuli jeden z prvních integrovaných kvantových šifrovacích čipů. V budoucnu by jejich technologie mohli být prodávány ve formátu rozšiřujících karet [146].

Obr. 16.8: Logo firmy |KETS> [146].

16.3.9 QRate

QRate je komerční značkou pro kvantové technologie Ruského kvantového centra (RQC), které se věnuje jak QKD, tak vývoji kvantových počítačů apod. Kromě QKD systému nyní komerčně nabízí QRNG moduly a jednofotonové detektory. Momentálně RQC nabízí akademickou a průmyslovou verzi QKD systémů. Obě využívají protokol BB84 [147, 148].

Obr. 16.9: Logo Ruského kvantového centra a značky QRate [147, 148].

16.3.10 Quantum Xchange

Americká firma, která se v současnosti nezabývá výrobou QKD systémů samotných, nýbrž sofistikovanější správou klíčů. Tento systém je označován jako PhioTX a sestává ze sítě speciálních zařízení, pracujících mezi QKD serverem a šifrátorem. Klíče je tak možno distribuovat po složitějších topologiích a dokonce i do míst, která nejsou přímo napojena QKDN. PhioTX používá ETSI API, tím pádem je schopno pracovat se zařízeními různých výrobců [149].

Obr. 16.10: Logo firmy Quantum Xchange [149].

16.3.11 ADVA Optical Networking

Německý výrobce v oblasti optických komunikací. Jeho vlajkovou lodí je multiplexovací systém FSP 3000 umožňující šifrování na úrovni fyzické vrstvy (L1 – WDM šifrování). Šifrovací subsystém je označován jako ConnectGuard a je možné propojit jej pomocí ETSI API s QKD servery. Pro symetrické šifrování je používán AES [150].

Obr. 16.11: Logo firmy ADVA [150].

16.3.12 Fortinet

Americká firma podnikající v IT bezpečnosti. S QKD serverem lze pomocí ETSI API propojit VPN brány Fortigate pracující na síťové (L3 – IPSec) a transportní vrstvě (L4 – SSL/TLS). Funkcionalita pro QKD je však dostupná pouze na L3. Zařízení Fortigate existuje v mnoha různých verzích, z tohoto důvodu nejsou jednotlivé varianty zahrnuty v tabulkách [151].

Obr. 16.12: Logo firmy Fortinet [151].

16.4 Srovnání dostupných komponent

Nyní budou formou tabulek postupně srovnány jednotlivé druhy výše zmíněných dostupných komponent. Zvláště pak QKD servery a šifrátory. Následně budou navržena možná řešení pro výstavbu komplexní QVPN sítě. Hodnoty v tabulkách 16.1 a 16.2 předpokládají použití optického kabelu s měrným útlumem 0,24 dB/km. Rychlostí generování klíče (Key rate) je zde myšlen počet qubitů, který dorazí v pořádku do cíle vzdáleného cca 50 km (10-12 dB). Výjimkou je zařízení od formy Qubitekk, u kterého je z důvodu nižšího dosahu uvedena maximální rychlost. Zkratky topologií jsou vysvětleny v poznámce níže[3].

QKD servery firmy IDQ existují i v tzv. prémiových verzích, s větším dosahem. Z tohoto důvodu je uvedeno více hodnot pro maximální útlum a dosah. První hodnota představuje základní variantu výrobku. QRNG generátory jsou již integrovány v QKD serverech. Pod každou tabulkou jsou umístěny fotografie daných zařízení.

Za šifrátory kompatibilní s QKD jsou považovány ty, jenž obsahují ETSI Key Delivery API. V QKD okrajově používaná rozhraní jako KMIP a Modbus nejsou v tomto srovnání uvažována.

[3] **BB** – Bod-Bod (Point-to-point), **DO** – Důvěryhodný opakovač (Trusted repeater), **H** – Hvězda (Hub-and-Spoke), **K** – Kruh (Ring)

Tab. 16.1: Přehled dostupných QKD serverů od firmy IDQ [137].

QKD Servery			
Model	**Clavis^3**	**Clavis^{300}**	**Cerberis^3**
Výrobce	IDQ	IDQ	IDQ
QKD protokol	COW	BB84	COW
Řešení	Samostatně	Modulární	Modulární
Velikost (19"ATCA šasi)	4U	6U	6U
Integrovaný šifrátor	NE	Volitelně	NE
ETSI API	ANO	ANO	ANO
Rychlost generování klíče	1,4 kb/s	6 kb/s	1,4 kb/s
Maximální útlum	12/14/16/18 dB	18/24 dB	12/14/16/18 dB
Dosah kvantového kanálu	50/58/66/75 km	75/100 km	50/58/66/75 km
Topologie	BB	BB, DO	BB, DO, H, K
Podpora WDM	Ano	Ano	Ano

Obr. 16.13: Zleva Clavis^3, Clavis^{300} a Cerberis^3 [137].

Tab. 16.2: Přehled dostupných QKD serverů od firem Toshiba a Qubitekk [139, 140].

QKD Servery			
Model	**MUX QKD**	**Dálkové QKD**	**DataLoc**
Výrobce	Toshiba	Toshiba	Qubitekk
QKD protokol	T12	T12	BBM92
Řešení	Samostatně	Samostatně	Samostatně
Velikost (19"ATCA šasi)	3U	3U	———————
Integrovaný šifrátor	NE	NE	NE
ETSI API	ANO	ANO	NE
Rychlost generování klíče	40 kb/s	300 kb/s	64 kb/s
Maximální útlum	17 dB	29 dB	6 dB
Dosah kvantového kanálu	70 km	120 km	25 km
Topologie	BB	BB	BB, DO
Podpora WDM	ANO	NE	Není známo

Obr. 16.14: Zleva Toshiba multiplexovaný a dálkový QKD systém a DataLoc Key Server od Qubitekku [139, 140].

Tab. 16.3: Přehled dostupných šifrátorů od IDQ / Thales a ADVA [137, 150].

Šifrátory kompatibilní s QKD			
Model	**ConnectGuard**	**CN 4000**	**CN 6000**
Výrobce	ADVA	IDQ / Thales	IDQ / Thales
Řešení	Samostatně	Samostatně	Samostatně
Velikost (19"ATCA šasi)	———————	———————	1U
Vrstva	L1	L2	L2
VPN protokol	Šifrovaná optika	MACSec	MACSec
Šifra	AES-256	AES-128/256	AES-128/256
Max. propustnost	600 Gb/s	1 Gb/s	1/10 Gb/s

Obr. 16.15: Zleva ADVA FSP 3000 s modulem ConnectGuard, IDQ / Thales Centauris CN4000 a CN6000 [137, 150].

Tab. 16.4: Přehled dostupných šifrátorů od IDQ / Thales [137].

Šifrátory kompatibilní s QKD			
Model	**CN 8000**	**CN 9000**	**CV 1000**
Výrobce	IDQ /Thales	IDQ / Thales	IDQ / Thales
Řešení	Samostatně	Samostatně	Virtuální
Velikost (19"ATCA šasi)	4U	1U	———————
Vrstva	L2	L2	L2/L3/L4
VPN protokol	MACSec	MACSec	MACSec/IPSec/ SSL/TLS
Šifra	AES-128/256	AES-128/256	AES-128/256
Max. propustnost	100 Gb/s	100 Gb/s	———————

Obr. 16.16: Zleva IDQ Centauris CN8000 a CN9000, vpravo potom logo virtuálního šifrátoru CV1000 [137].

17 Modelování a simulace QKD protokolů

V následující části práce lze nalézt výsledky provedených simulací polygonů pro protokoly BB84 a T12. Veškeré simulace byly prováděny pomocí nástroje *VPI Photonics*. Byly využity moduly a šablony obsažené v knihovně *VPI Toolkit QKD*.

Nejvýznamnějším parametrem, na kterém přímo závisí bezpečnost zmíněných QKD protokolů je tzv. QBER (Quantum-Bit Error Rate), neboli kvantová bitová chybovost. Obdobně jako běžnou bitovou chybovost ji lze v ideálním případě jednoduše spočítat jako:

$$QBER = \frac{v_{chyby}}{v_{cíl}} \tag{17.1}$$

$QBER$ – Kvantová bitová chybovost [–]
v_{chyby} – Počet přijatých chyb za sekundu [Hz] ≈ [bit/s]
$v_{cíl}$ – Přenosová (bitová) rychlost u cíle [Hz] ≈ [bit/s]

Tedy jako poměr za sekundu chybně přenesených bitů a přenosové rychlosti. Tato hodnota bývá také často vyjadřována v procentech. QBER je vypočítávána v průběhu prosévání klíče. Započítávají se tedy pouze správně a špatně přijaté fotony. Pulzy ztracené na optické trase započítávány nejsou. Rychlost $v_{cíl}$ je tedy rozdílem přenosové rychlosti u zdroje a počtem ztracených bitů za sekundu [152].

Hodnota QBER bývá u většiny QKD protokolů zásadní pro detekci odposlechu. Jak již bylo řečeno v teoretické části, díky větě o zákazu klonování, je odposlouchávající Eva nucena dělat při pokusu o replikování signálu chyby. To znamená, že bude vytvářet chybovost okolo 25 %. Za bezpečnou chybovost, kdy Eva ví méně než Bob, je u BB84 protokolů považována hranice 11 % (na bezztrátovém kanále) [65].

Na QBER však nemá vliv pouze Eva. Dalším faktorem působící na QBER je útlum na kvantovém kanále (optické vlákno). Útlum roste automaticky s prodlužujícím se kanálem a je zodpovědný za vyšší chybovost. Lze jej spočítat pomocí vzorce 17.2 níže [153].

$$a = \alpha l \tag{17.2}$$

a – Útlum kanálu [dB]
α – Měrný útlum [dB/km]
l – Délka (kvantového) kanálu [km]

Druhým velmi významným parametrem je rychlost generování klíče (Key Rate). V ideálním případě se jedná o rozdíl mezi $v_{cíl}$ a v_{chyby}. S prodlužujícím se kanálem dochází nejen ke ztrátám ale i k nárůstu chyb. Tato hodnota se již udává v bit/s.

V následujících simulacích budou uvažována pouze jednovidová optická vlákna s měrným útlumem 0,24 dB/km. Na QBER mají ovšem vliv i další faktory jako např. chyby detektorů[1], zdrojů[2] a apod. Tyto vedlejší parametry jsou v následujících simulacích rovněž uvažovány. Ztráty na optických spojích (zejména konektory) a disperze jsou naopak zanedbány.

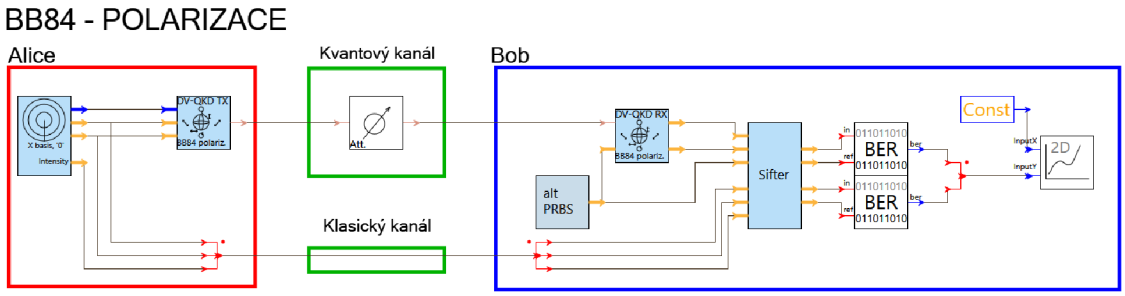
Níže popsané simulace jsou zaměřeny na závislost QBER na délce kvantového kanálu. Pro každý z protokolů jsou vybrány 3 vzdálenosti. QBER v těchto bodech je následně srovnána níže v tabulce 17.1.

[1] Nedetekování fotonu, nebo naopak falešná detekce tzv. *dark count*.

[2] Vyslán závadný nebo žádný signál.

17.1 BB84 s polarizačním kódováním

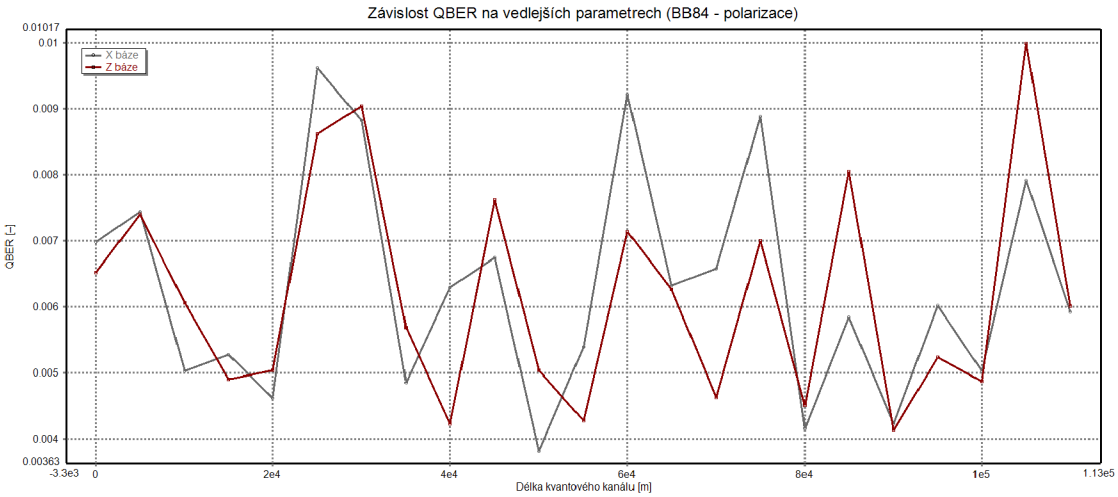
Nyní budou prezentovány výsledky simulací na modelu klasického návnadového protokolu BB84. Samotný návrh modelu je možné najít na níže na obrázku 17.1. Zobrazené grafy popisují závislost QBER na délce kvantového kanálu a zobrazují výsledky pro obě použité báze[3] zvlášť. Délka kvantového kanálu s každou iterací simulace roste o 5 km. Celkem je tak měření provedeno 23krát pro vzdálenosti od 0 do 110 km.



Obr. 17.1: Model návnadového protokolu BB84 využívajícího polarizace fotonů.

17.1.1 Závislost QBER na vedlejších parametrech

Nejdříve byla provedena simulace QKD přenosu na ideálním kvantovém kanále, tj. kanále s nulovým měrným útlumem. Hodnoty QBER jsou tak nyní závislé pouze na vedlejších parametrech. Jak lze vidět z grafu 17.2, QBER nepřekračuje hranici 1 %.

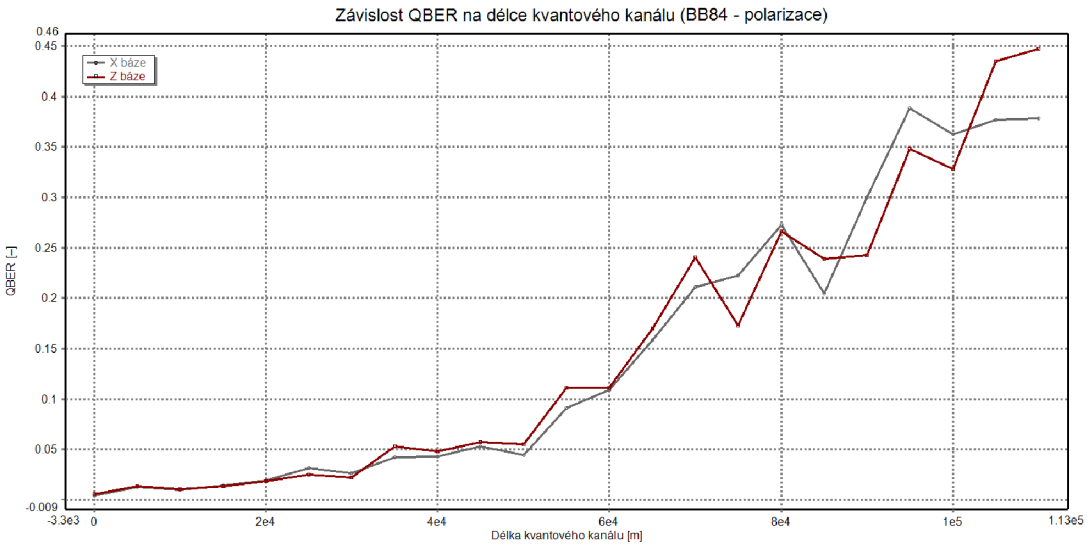


Obr. 17.2: Graf závislosti QBER na vedlejších parametrech (BB84 – polarizace).

[3]Báze Z odpovídá bázi $\{|\uparrow\rangle, |\rightarrow\rangle\}$, zatímco báze X bázi $\{|\nearrow\rangle, |\searrow\rangle\}$.

17.1.2 Závislost QBER na délce kvantového kanálu

Pokud bude nyní nastaven měrný útlum na nenulovou hodnotu (0,24 dB/km), začne se zvětšující se vzdáleností[4] docházet k nárůstu QBER. Z grafu 17.3 tak vyplývá, že pro hodnotu QBER 11 % by délka kvantového kanálu daného QKD systému neměla překročit cca 60 km.

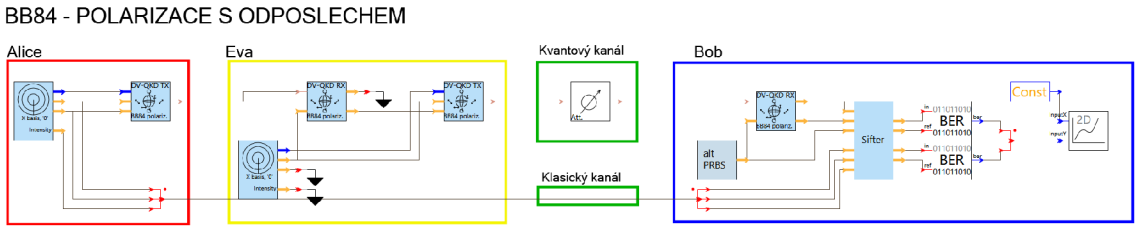


Obr. 17.3: Graf závislosti QBER na délce kvantového kanálu (BB84 – polarizace).

[4]Čím vyšší útlum (ztráty), tím vyšší pravděpodobnost falešné detekce fotonu (dark count).

17.1.3 Odhalení odposlechu pomocí QBER

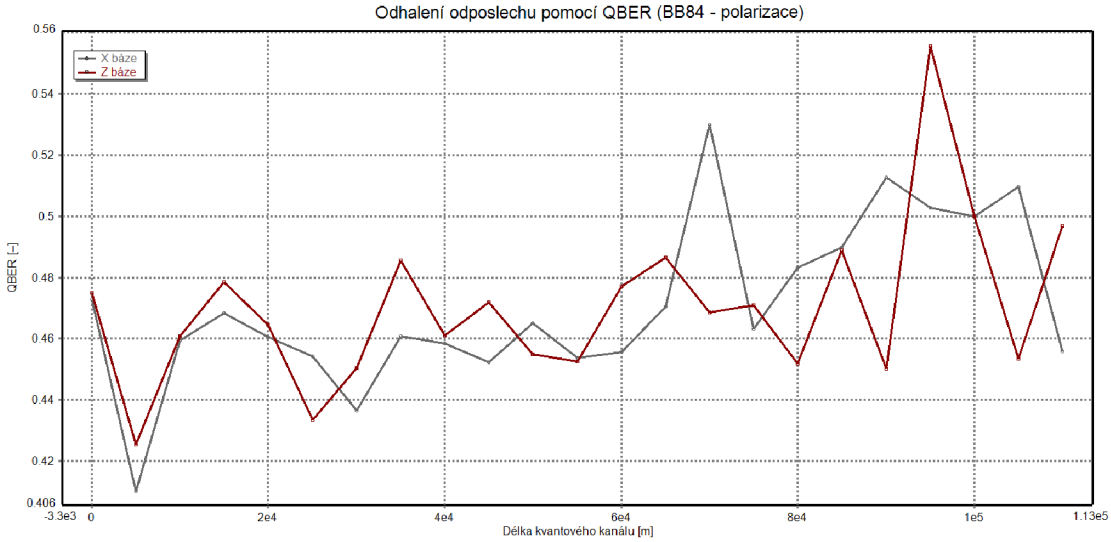
V následující simulaci už bude kromě Boba a Alice vystupovat také odposlouchávající Eva. Eva změří od Alice pocházející fotony v náhodné bázi. Jejich hodnoty následně namoduluje na nové fotony pomocí stejné báze, kterou měřila. Dojde-li při detekci k chybě, je hodnota nového bitu automaticky určena jako 0.



Obr. 17.4: Model návnadového protokolu BB84 využívajícího polarizace fotonů s odposlechem.

Oproti předchozímu měření lze z grafu 17.5 vyčíst prudký nárůst QBER. Ten je způsoben jak špatnou volbou bází Evy, tak nedokonalostmi Eviných zařízení. Podobným způsobem tedy dochází k detekci odposlechu. V ideální případě by chybovost zapříčiněná Evou by měla tvořit cca 25 %.

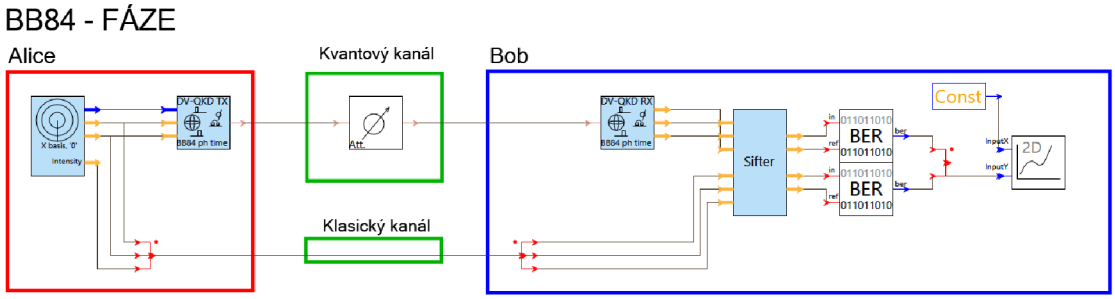
Kvůli nedokonalostem je ale QBER vyšší a osciluje kolem 48 %. To značí velmi nízkou míru korelace mezi Alicí a Bobem (nulová korelace odpovídá 50% QBER). Drtivá většina kvantových signálů tak k Bobovi dorazí poškozená.



Obr. 17.5: Graf zobrazující vliv Evy na nárůst QBER (BB84 – polarizace).

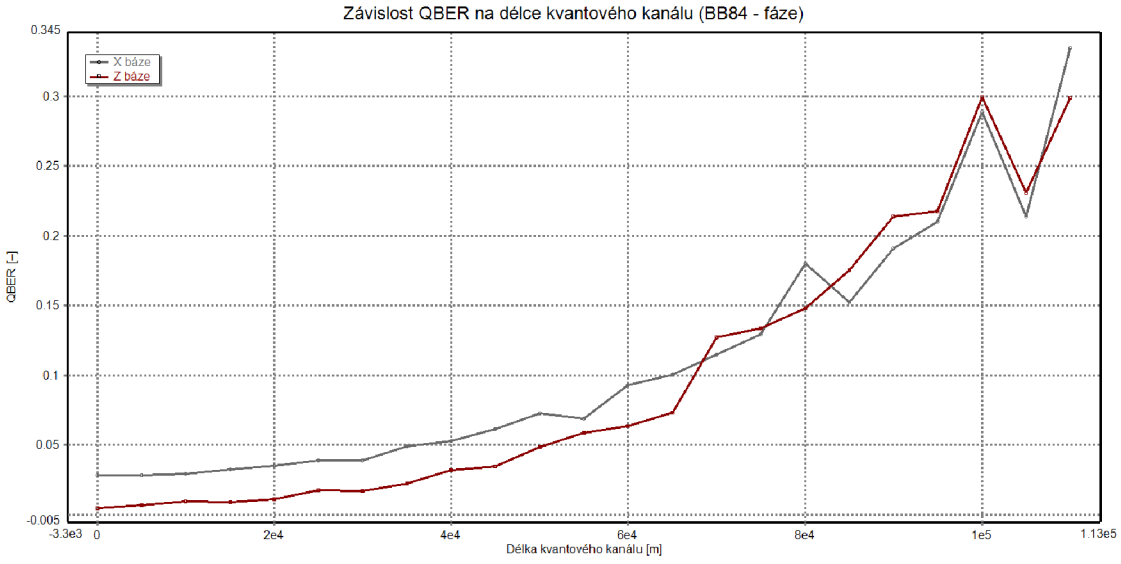
17.2 BB84 s fázovým kódováním

Většina moderních implementací BB84 již nepoužívá polarizační, ale fázové kódování. Výhodou je delší dosah. Jinak řečeno, s narůstající délkou kvantového kanálu roste QBER pomaleji, než u klasického BB84 využívajícího polarizace. Toto tvrzení bylo ověřeno na schématu 17.6 pomocí měření.



Obr. 17.6: Model protokolu BB84 využívajícího fázového kódování.

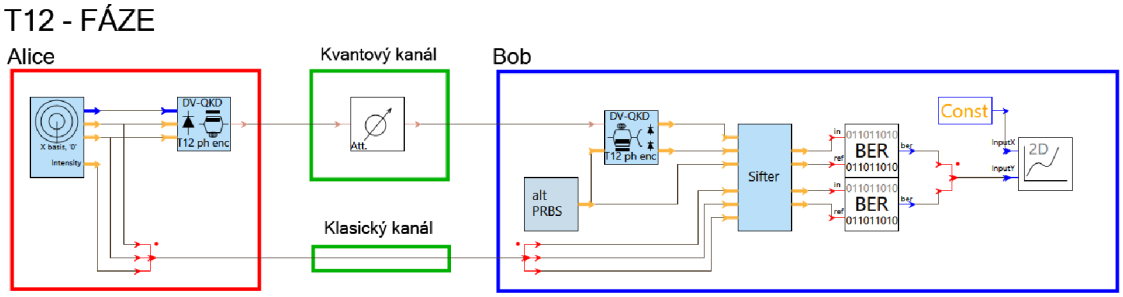
Výsledné hodnoty jsou zobrazeny v grafu 17.7. Z něj je patrná nižší chybovost fázového kódování oproti kódování polarizačnímu. Chybovost obou protokolů lze porovnat pomocí tabulky 17.1.



Obr. 17.7: Graf závislosti QBER na délce kvantového kanálu (BB84 – fáze).

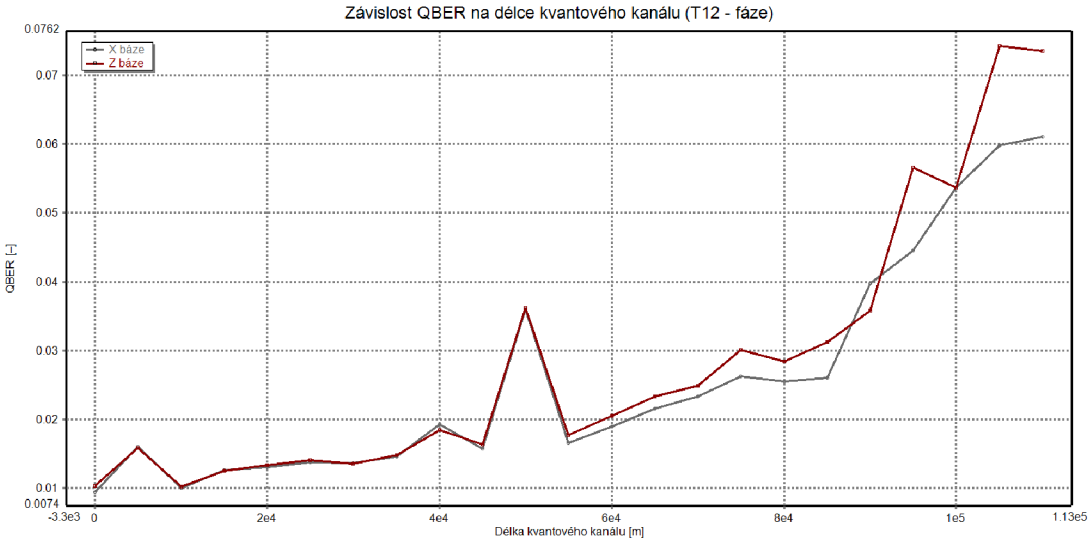
17.3 T12 s fázovým kódováním

Protokol T12 je efektivní variantou protokolu BB84, jenž většinou implementuje fázové kódování. Hlavním rozdílem je asymetrické používání bází X a Z. Minoritní báze X tak bývá vybrána např. pouze ve 20 % případů. Naproti tomu majoritní báze Z v 80 % případů. Tento poměr byl využit i v případě měření na obrázku 17.8.



Obr. 17.8: Model efektivního protokolu T12 využívajícího fázového kódování.

Z grafu 17.9 je zřejmá výhoda asymetrické pravděpodobnosti používání bází. QBER je zde mnohem nižší než u obou předchozích protokolů. Srovnání lze opět najít níže v tabulce 17.1.



Obr. 17.9: Graf závislosti QBER na délce kvantového kanálu (T12 – fáze).

17.4 Výsledky měření

V průběhu měření byly postupně srovnány tři protokoly rodiny BB84. Současně tak byly nastíněny a ověřeny výhody technik jako je fázové kódování nebo použití minoritní a majoritní báze nad standardní implementací. Vybrané hodnoty QBER pro měřené protokoly lze najít níže v tabulce 17.1.

Tab. 17.1: Výsledky měření simulací protokolů rodiny BB84.

Srovnání protokolů podle QBER			
Model	**20 km**	**60 km**	**110 km**
BB84 – polarizace	4 %	12 %	42 %
BB84 – fáze	3 %	6 %	32 %
T12 – fáze	1 %	2 %	7 %

U protokolu BB84 s polarizačním kódováním pak byla dále předvedena demonstrace odposlechu na kvantovém kanále. Zde je možné povšimnout si výrazného zvýšení chybovosti oproti stavu bez odposlechu. Vlivem nedokonalých zařízení se však hodnota QBER pohybuje kolem 48 %, což se blíží nulové korelaci, tedy zcela náhodným výsledkům.

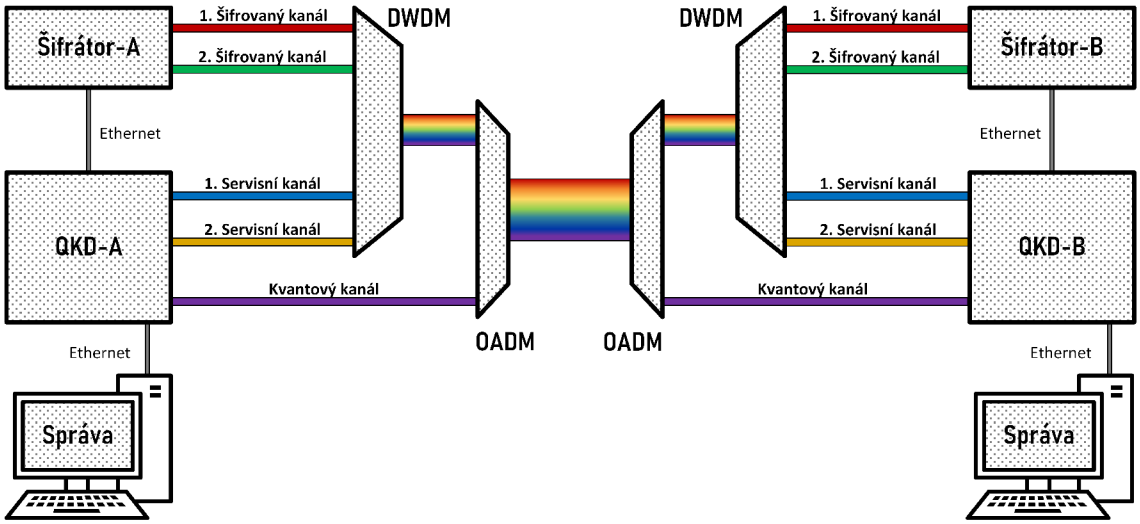
U stejného protokolu bylo dále provedeno měření zacílené na určení chybovosti zdrojů a detektorů (vedlejší parametry). Zde chybovost nepřekročila 1 %.

18 Návrh QKD polygonu

V souladu s obecnou topologií QKDN sítí a praktickou nutností začlenit QKD systémy do běžných optických sítí, byla navržena následující topologie testovacího polygonu. V praxi není temné vlákno vždy k dispozici a jednotlivé optické kanály jsou agregovány do jediného optického vlákna pomocí vlnového multiplexu (WDM).

Na rozdíl od klasických signálů má však kvantový kanál svá specifika. Jednofotonové pulzy totiž není možné jednoduše zesílit nebo zopakovat jako klasický signál. Navíc je výkon na kvantovém kanále mnohonásobně nižší a hrozí tak, že bude zcela ztracen v šumu produkovaným ostatními multiplexovanými kanály.

V následující části budou popsány jednotlivé části polygonu a představena konkrétní vybraná zařízení a optické prvky. Následovat bude simulace daného polygonu pomocí dříve uvedeného simulačního programu.



Obr. 18.1: Návrh polygonu pro kvantovou distribuci klíčů.

Cílem simulace je odhadnout parametry optických komponent nutných pro provoz QKD přes linky využívající vlnového multiplexu. Jedná se zejména o výběr vhodných optických filtrů. Ty musejí být nastaveny tak, aby se kvantový kanál neztrácel ve výkonnějších WDM kanálech. Ostatní kanály ovšem musejí rovněž zůstat funkční. Nelze je tedy ořezat příliš.

Oproti původní konfiguraci jsou jednotlivé kanály posunuty blíže k sobě takovým způsobem, aby šlo testovat vliv klasických kanálů na kanál kvantový. Všechny signály běží na DWDM kanálech dle specifikace ITU-T. Čísla kanálů jsou dále uváděna v závorce v příslušných tabulkách a grafech [154].

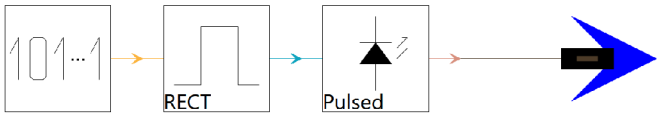
18.1 QKD servery

Z výše popsaných QKD serverů bylo pro sestavení zkušebního polygonu vybráno zařízení Clavis[3] firmy IDQ. Důvodem je jak to, že je systém postaven na částečně modifikovatelné otevřené platformě, tak samotná cena zařízení. K základním dvěma modulům (Alice a Bob) je rovněž poskytnut simulátor útoku odposlechem (Eva).

Některé parametry zařízení byly oproti standardní sestavě upraveny tak, jak je naznačeno v tabulkách 18.1 a 18.3. Parametry servisních kanálů současně nejsou řešeny na úrovni samotného QKD serveru, nýbrž připojeného SFP modulu. Zde byly zvoleny dva samostatné servisní kanály, z nichž každý zajišťuje provoz v jednom směru a operuje na jiné vlnové délce.

18.2 Modelování kvantového kanálu

K vymodelování zdroje kvantového kanálu byl použit modul pro generování náhodných čísel, zdroj obdélníkových pulzů a pulzní laser. Tuto sestavu lze najít níže na obrázku 18.2. Detailnější nastavení jednotlivých modulů lze dohledat v přiložených souborech simulace.



Obr. 18.2: Vymodelovaný zdroj kvantových signálů.

Parametry kanálu zjištěné u výrobce jsou zadány v tabulce 18.1. Pro vymodelování příslušných signálů ovšem bylo potřeba některé parametry dopočítat. Celý postup výpočtu je detailně popsán v kapitolách 18.2.1 a 18.2.2.

Tab. 18.1: Parametry kvantového kanálu zařízení Clavis[3].

Kvantový kanál	
Protokol	COW
Generování pulzů (v_p)	1,25 GHz
Generování klíče (v_k)	1,4 kb/s
Fotonové číslo (μ)	0,0075
Maximální útlum (a_{max})	14 dB
Maximální dosah (l_{max})	58 km
Vlnová délka (λ)	1551,72 nm (CH32)

Je nutné si ovšem uvědomit, že standardní (použité) moduly ve *VPI Photonics* nejsou určeny k simulaci takového typu optických pulzů. Jedná se proto pouze o odhad sloužící k návrhu vhodných komponent, zejména pak optických filtrů a vláken.

18.2.1 Výpočet tvaru pulzu

Na základě vlnové délky λ je nejdříve dopočítána energie jednoho fotonu. Protože pulz obsahuje pouze jeden foton, je energie v pulzu shodná s energií fotonu a označena E_{pulz}. Pro lepší orientaci je energie převedena na elektronvolty.

$$E_{pulz} = \frac{hc}{\lambda} = 1,28 \cdot 10^{-19}\ J = 0,8\ eV \tag{18.1}$$

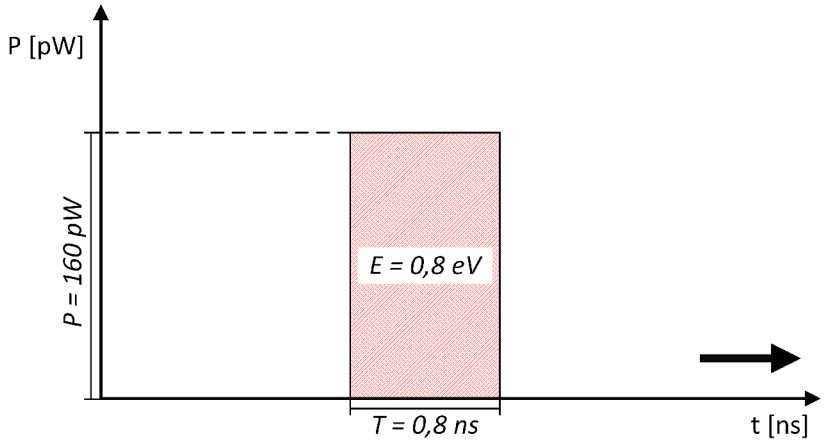
Dále lze z rychlosti generování pulzů určit dobu trvání pulzu neboli periodu T_{pulz}. Ta se vypočítá jako převrácená hodnota frekvence (rychlosti).

$$T_{pulz} = \frac{1}{v_p} = 8 \cdot 10^{-10}\ s = 0,8\ ns \tag{18.2}$$

Z obrázku 18.3 je zřejmé, že zatímco energie tvoří v časové oblasti obsah obdélníkového pulzu, perioda určuje jeho šířku. Nyní lze snadno spočítat výkon pulzu P_{pulz} jako výšku obdélníku.

$$P_{pulz} = \frac{E_{pulz}}{T_{pulz}} = 1,6 \cdot 10^{-10}\ W = 160\ pW \tag{18.3}$$

Výslednou podobu pulzu je možné najít na obrázku 18.3. Dále lze srovnat s výsledkem simulace na obrázku 18.4 níže.



Obr. 18.3: Tvar jednofotonového pulzu. Veličiny jsou zobrazeny bez indexů.

18.2.2 Výpočet celkového výkonu ve spektru

Protože jsou vysílány pouze samostatné fotony, které mají v daném momentu pouze jednu vlnovou délku (resp. frekvenci) je šířka spektrální čáry daného laseru nastavena na nulu. Pokud tedy bude nyní nastaven výkon kvantového kanálu, bude ve spektru přímo roven velikosti výkonu emitovaného při dané vlnové délce.

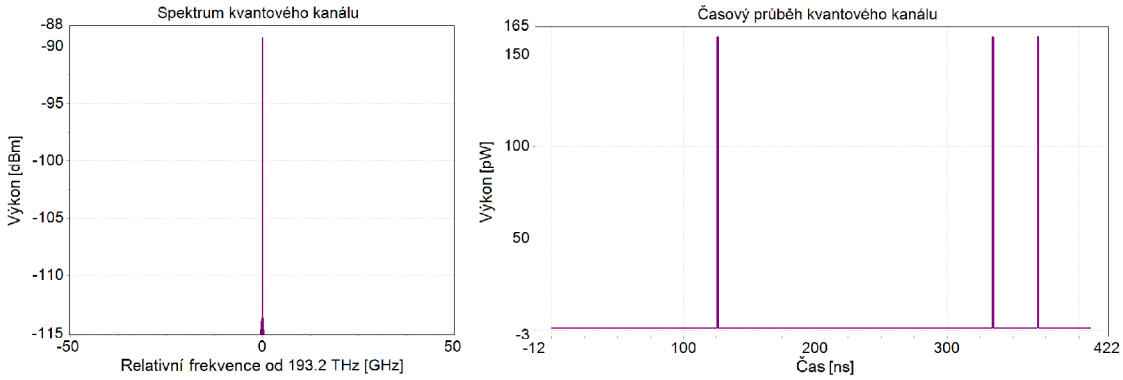
Pro výpočet celkového výkonu je opět nutné znát energii fotonu E_{pulz}. Ta se dále vynásobí rychlostí v_p (počtem pulzů za čas). Dalším důležitým faktorem je, že zdaleka ne každý pulz obsahuje foton. Poměr prázdných pulzů stanovuje fotonové číslo μ. Celkový výkon kvantového kanálu $P_{celkový}$ lze tedy spočítat následovně:

$$P_{celkový} = E_{pulz} v_p \mu = 1,2001475 \cdot 10^{-12}\ W = -89,2\ dBm \tag{18.4}$$

Z výsledku je zřejmé, že kvantový signál je velmi slabý. Vzhledem k tomu, že není možné jej cestou zesílit, je nutné přizpůsobit mu optickou trasu.

18.2.3 Výsledky simulace

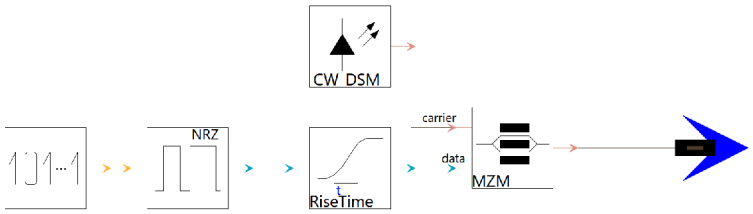
Z grafů 18.4 níže je zřejmé, že výsledky simulace odpovídají vypočteným hodnotám. Ve spektrální oblasti byla naměřena hodnota výkonu -89,22 dBm. Drobná odchylka od vypočtené hodnoty je důsledkem zaokrouhlování hodnot při výpočtech. Druhou příčinou je, že použité moduly nejsou určeny k modelování podobných signálů. Odchylka je tedy důsledkem ne zcela nulové šířky spektrální čáry v simulaci, jak je možné vidět na levém grafu.



Obr. 18.4: Kvantový kanál v časové a spektrální oblasti.

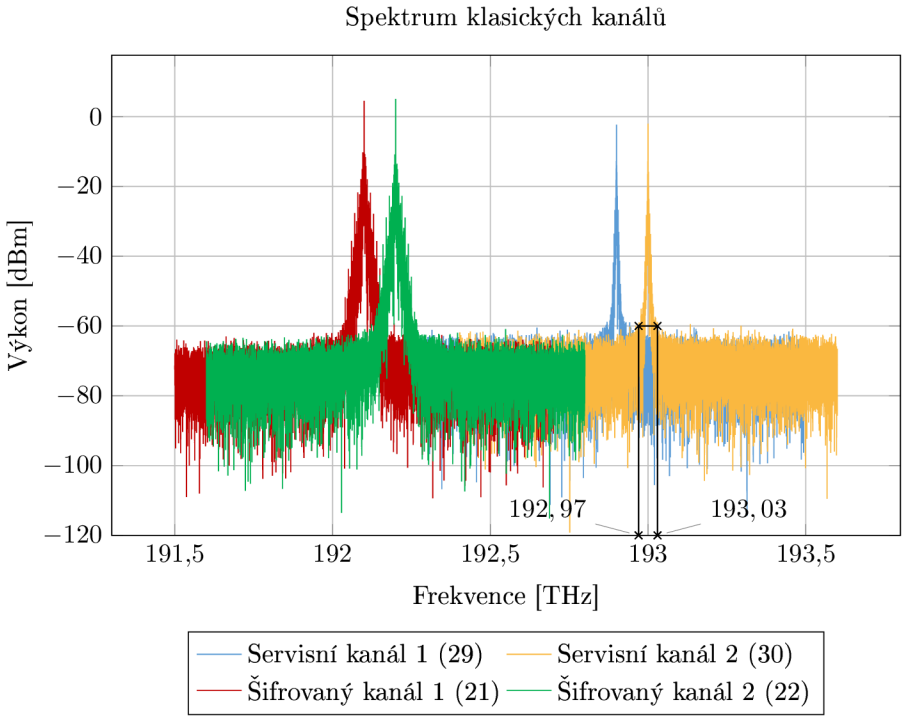
18.3 Modelování klasických a šifrovaných kanálů

V rámci simulace je rovněž nutné vymodelovat zdroje klasických signálů. Tedy servisní kanály, jejichž zdrojem je SFP modul zapojený do QKD serveru a šifrované kanály, vysílané ze šifrátorů. Protože zde již ale nejsou konkrétní zařízení specifikována, byly tyto signály vymodelovány s laserovou diodou a NRZ kódováním. Jako předloha částečně posloužila reálná zařízení. Nejdůležitější parametry je možné najít v tabulkách 18.2 a 18.3. Podrobnější nastavení je opět obsaženo v příloze [155, 156].



Obr. 18.5: Vymodelovaný zdroj šifrovaných a servisních kanálů.

První modul zleva, tedy PRNG je stejný jako u zdroje kvantového signálu. Následuje zdroj obdélníkových pulzů s NRZ (Non-Return To Zero) kódováním. Protože ale není možné vytvořit dokonale obdélníkové pulzy, jsou tyto „zešikmeny“ a „uhlazeny“ pomocí třetího modulu.



Obr. 18.6: Spektra všech čtyř zdrojů klasických signálů.

Zdrojem světla je laserová dioda. Jedná se o reálnější modul obsahující šum. Pomocí posledního modulu je upravený obdélníkový signál namodulován na světlo vystupující z diody.

Na grafu 18.6 jsou zobrazena spektra všech čtyř klasických signálů. Důležitou hodnotou je dosažený výkon ve špičce servisního kanálu 2, který je roven -2 dBm. Tato hodnota bude později využita při modelování optických filtrů. Dalším významným parametrem tohoto kanálu je šířka propuštěného spektra na úrovni -60 dBm (oblast šumu). Po odečtení ($P = |192,97 - 193,03| = 0,06\ THz$) byl zjištěn rozsah 60 GHz. Význam této hodnoty bude rovněž vysvětlen v kapitole 18.4.1.

18.3.1 Šifrátory

Ačkoliv parametry šifrovacích zařízení nejsou zatím specifikovány, očekává se, že se bude jednat o vysokorychlostní přenos dat. V simulaci je přenosová rychlost nastavena na 10 Gb/s.

Tab. 18.2: Parametry šifrovaných kanálů (zdroj šifrátor).

Servisní kanály	
Přenosová rychlost	10 Gb/s
Výkon	10 mW (10 dBm)
FWHM	10 kHz
Šifrovaný kanál 1	1560,61 nm (CH21)
Šifrovaný kanál 2	1559,79 nm (CH22)

18.3.2 Servisní kanály

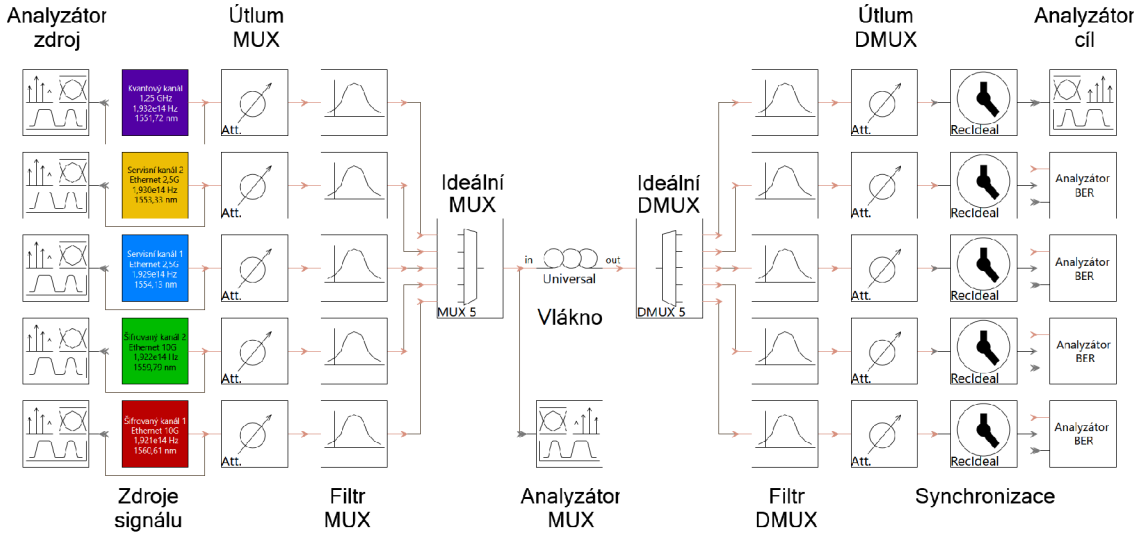
Podobně jako u šifrátorů není zatím rozhodnuto o konkrétním typu SFP modulu, který bude vložen do QKD serveru. Pro simulaci je momentálně uvažována přenosová rychlost 2,5 Gb/s.

Tab. 18.3: Parametry servisních kanálů (zdroj SFP modul).

Servisní kanály	
Přenosová rychlost	2,5 Gb/s
Výkon	2,5 mW (4 dBm)
FWHM	10 kHz
Servisní kanál 1	1554,13 nm (CH29)
Servisní kanál 2	1553,33 nm (CH30)

18.4 Optický spoj

Zatímco jednotlivé zdroje signálů již byly popsány v předchozích kapitolách, samotná optická trasa bude diskutována až nyní. Zásadní je tak obrázek 18.7, tedy vymodelovaná verze polygonu z obrázku 18.1. V barevných modulech se skrývají výše popsané zdroje. Následují útlumové články, které představují ztráty, ke kterým dochází při přenosu a optické filtry sloužící k ořezu signálu ve spektru tak, aby jej bylo pomocí WDM možné sloučit ostatními signály do jednoho vlákna. K tomu slouží modul ideálního multiplexoru a optického vlákna.



Obr. 18.7: Zapojení polygonu v simulačním software *VPI Photonics*.

Obdobná situace nastává i po výstupu z vlákna. Zde dochází k nakopírování signálu na pět výstupních portů. Dále je opět aplikován příslušný filtr a útlumový článek. Ostatní moduly slouží k časové synchronizaci a analýze signálu. Vše bude detailněji popsáno v následujících podkapitolách.

18.4.1 WDM filtry a multiplex

Vzhledem k malému výkonu kvantového kanálu může být přenos takového signálu přes složitější infrastrukturu problematický. Největší potíž může nastat ve chvíli, kdy dochází ke sloučení klasických signálů se signálem kvantovým do jediného vlákna pomocí WDM. Kvůli nízkému výkonu totiž hrozí, že by byl vlivem nedostatečné filtrace ztracen v šumu sousedních kanálů.

Z tohoto důvodu je při simulaci nutné uvažovat reálnou charakteristiku optických filtrů. Na rozdíl od ideálních modelů filtrů, které simulační software nabízí, a které zcela ořízno u daný kanál, u reálných filtrů dochází pouze k potlačení odfiltrované části spektra. To znamená, že v případě nízkého potlačení by jediný filtr použitý při multiplexování nebyl dostatečný.

Zapojení multiplexorů

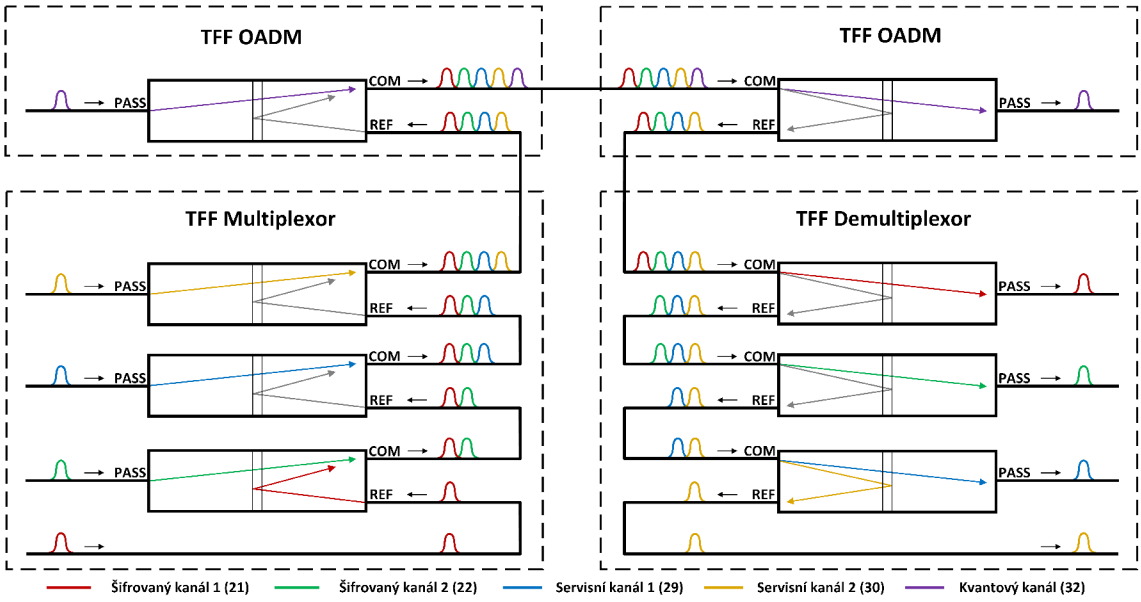
Pro sloučení více optických signálů do jediného vlákna se používá tzv. vlnový multiplex. V základu se jedná o sestavu multiplexoru (slučuje) a demultiplexoru (odděluje). Je-li nutné přidat nebo naopak vyčlenit pouze jednu vlnovou délku, používá se tzv. OADM, tedy Add-Drop Multiplexor. V obou případech jsou zařízení tvořena optickými filtry. V rámci této simulace budou použity tzv. TFF filtry (Thin Film Filter). TFF je založeno na principu Fabryho-Perotova interferometru se 3 různými porty [157].

Tab. 18.4: Značení a význam portů na TFF filtru [157].

Porty TFF filtru	
Port	**Účel**
COM (common)	Vstup / výstup všech λ.
PASS (passed)	Vstup / výstup vybrané (prošlé) λ.
REF (reflected)	Vstup / výstup odfiltrovaných (odražených) λ.

Multiplexory založené na technologii TFF jsou sestavou zmíněných filtrů zapojených do kaskády tak, jak je naznačeno na obrázku 18.8. Jednotlivé vlnové délky jsou tak přidávány postupně. Nevýhodou takového přístupu je, že vložný útlum roste s počtem kanálů [157].

Mimo kaskádu je zapojen další filtr, který tvoří OADM. Tím, že tento filtr není součástí kaskády, je útlum na kvantovém kanále konstantní a s počtem kanálů se nemění. U demultiplexorů je pak zapojení opačné.



Obr. 18.8: Průběh multiplexování klasických kanálů (MUX) s kanálem kvantovým (OADM) pomocí DWDM filtrů (zjednodušený nákres filtrů) [157].

Měření WDM filtrů

Aby bylo možné rozhodnout, zda je před multiplex nutné zařadit ještě dodatečné optické filtry, které by více potlačily přesahy klasických kanálů, je nejdříve nutné zjistit k jakému potlačení na reálném TFF skutečně dochází. Z tohoto důvodu bylo provedeno měření tří reálných filtrů pomocí spektrálního analyzátoru *Yenista OSA20*.

Pro srovnání byly měřeny dva DWDM filtry a jeden CWDM filtr. Jako zdroj optického signálu byl použit zdroj ASE (Amplified Spontaneous Emission) šumu, jehož výkon byl rovnoměrně rozložen ve spektru a pohyboval se kolem -20 dBm (v následujících grafech značeno žlutě). Charakteristika daných filtrů byla měřena celkem v šesti směrech tak, jak je naznačeno v tabulce 18.5.

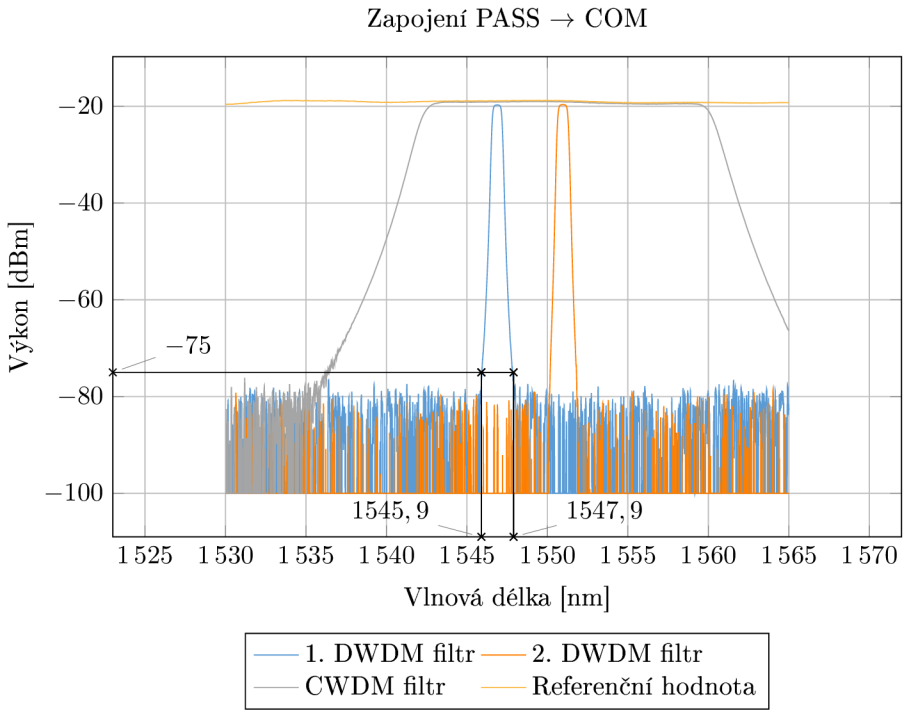
Tab. 18.5: Měření charakteristiky TFF filtrů.

Směr	**Opačný směr**	**Tvar**	**Graf**
PASS → COM	COM → PASS	$\wedge$	18.9
COM → REF	COM → REF	$\vee$	18.10
REF → PASS	PASS → REF	—	18.11

Pro následující výpočty bude uvažován pouze první DWDM filtr (modře). Druhý DWDM filtr (oranžově) je ještě „užší“, a proto lze následující postup aplikovat i na něj. CWDM filtr (šedě) naopak není pro vybrané rozvržení kanálů vhodný.

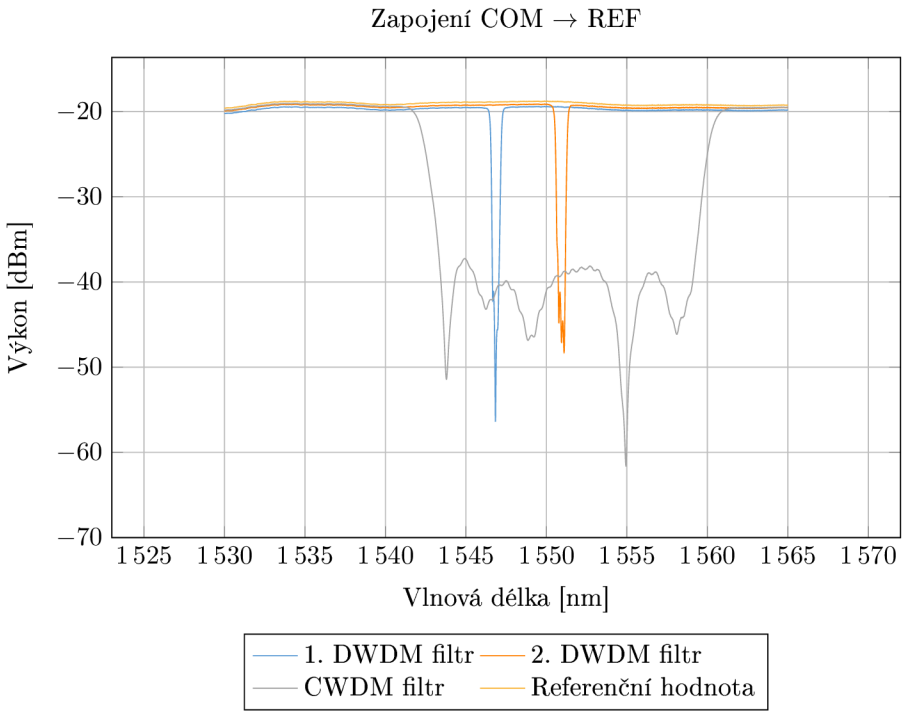
Charakteristiky jsou shodné pro oba směry zapojení, proto je do práce zařazen vždy jen jeden z grafů (celkem tedy 3).

Nejzásadnější je graf 18.9. Z něj je možné určit, jaký vliv bude filtr mít na propuštěný signál. Důležité je ovšem poznamenat, že citlivost měřícího zařízení byla pouze -75 dBm. Z tohoto důvodu není možné určit tvar charakteristiky filtru „ve větší hloubce“. Pro potřebu dané simulace je však i tento poznatek dostačující. Toto bude dále rozebráno v následující podkapitole.

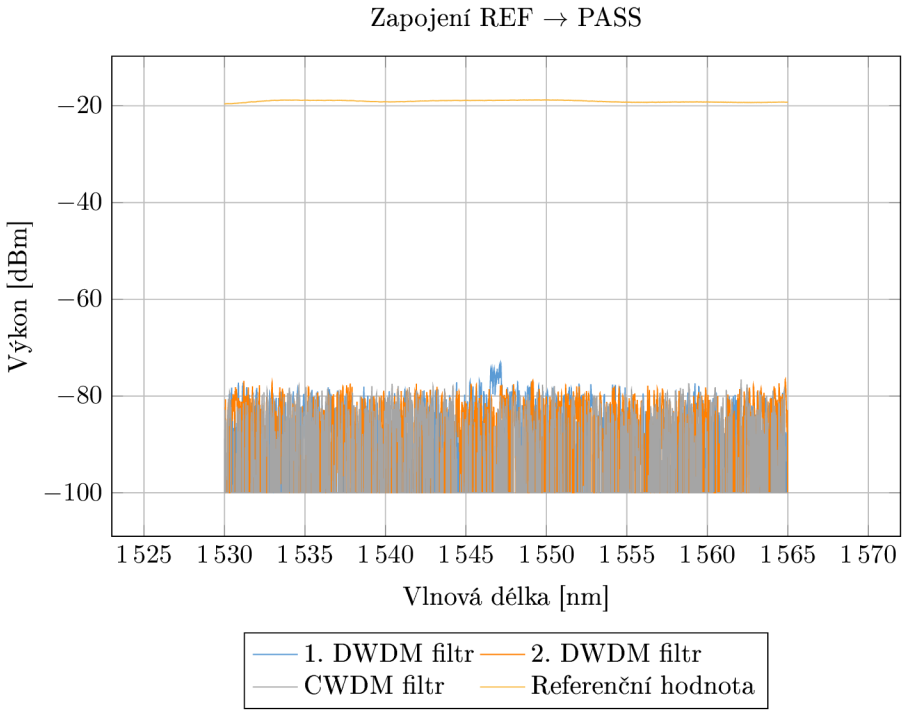


Obr. 18.9: Charakteristika měřených WDM filtrů ve směru PASS → COM.

Níže uvedené grafy 18.10 a 18.11 dokazují následující. Při přenosu mezi porty COM a REF dochází k vydělení určité části spektra. Tato část pak dále prochází portem PASS. Naopak mezi porty REF a PASS k žádnému přenosu nedochází. Nenulová hodnota přenosu na grafu je opět dána citlivostí spektrometru.



Obr. 18.10: Charakteristika měřených WDM filtrů ve směru COM → REF.



Obr. 18.11: Charakteristika měřených WDM filtrů ve směru REF → PASS.

Gaussův filtr

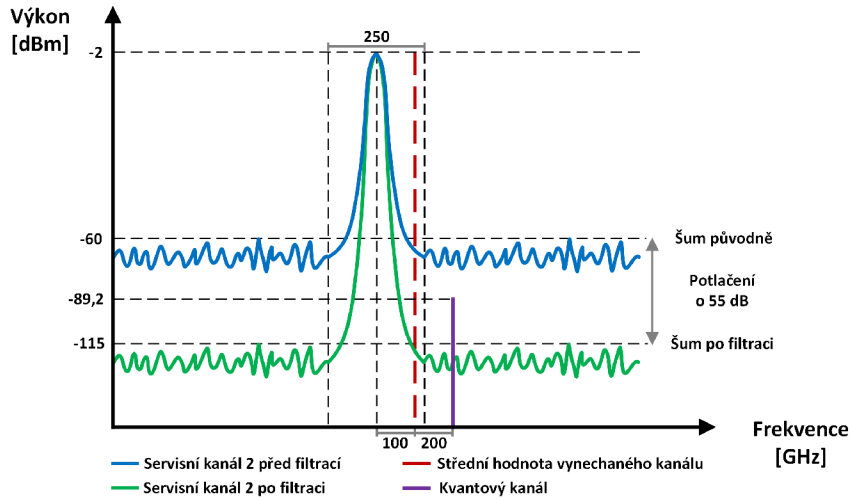
Jak již bylo řečeno, z výsledků měření není možné určit přesnou charakteristiku filtru. Z grafu 18.9 ovšem plyne, že dochází k potlačení vedlejších kanálů minimálně o 55 dB (bude-li uvažována původní hodnota -20 dBm a hodnota po filtraci -75 dBm). Největší hrozbu pro kvantový signál momentálně představuje jemu nejbližší druhý servisní kanál. Z předchozích kapitol je dále zřejmé, že šířka jeho spektrální čáry v oblasti kolem -60 dBm (oblast šumu) je 60 GHz (graf 18.6).

S tímto vědomím lze aplikovat následující úvahu. Z grafu 18.9 lze snadno dopočítat šířku filtrem propuštěné části spektra v oblasti poklesu o 55 dB. Vlnové délky ($\Delta\lambda$) jsou pro lepší orientaci převedeny na kmitočty ($\Delta\nu$).

Tab. 18.6: Šířka propuštěné části spektra při potlačení o 55 dB.

Vlnová délka	**Kmitočet**
$\lambda_1 = 1545,9\ nm$	$\nu_1 = 193,9275\ THz$
$\lambda_2 = 1547,9\ nm$	$\nu_2 = 193,677\ THz$
$\Delta\lambda = \lvert\lambda_2 - \lambda_1\rvert = 2\ nm$	$\Delta\nu = \lvert\nu_2 - \nu_1\rvert = 250,5\ GHz$

V tuto chvíli se využije obrázek 18.12. Modrá křivka představuje nejširší možnou šířku spektrální čáry druhého servisního kanálu, tedy 250,5 GHz (dále uvažováno 250 GHz). Protože má daný kanál v tomto místě šířku pouze 60 GHz, je zřejmé, že se do tohoto rozmezí „vejde“. Pokud bude na tento kanál aplikován změřený DWDM filtr, dojde k potlačení ostatních frekvenčních (mimo maximální rozsah) pásem o 55 dB. Tedy na hodnotu -115 dBm.



Obr. 18.12: Úvaha ospravedlňující použití ideálního Gaussova filtru.

Tomuto stavu odpovídá zelená křivka. Z obrázku je tak zřejmé, že kvantový kanál (fialově) nebude v druhém servisním kanálu ztracen. Izolace kvantového kanálu je tak minimálně 25,8 dB ($\Delta P = -115 - (-89,2) = 25,8\ dB$). Rozdíly v útlumech na jednotlivých kanálech jsou zanedbány. Protože ale na klasických kanálech dochází k vyšším ztrátám, byla by minimální izolace po jejich započtení ještě vyšší.

Na základě výsledků této úvahy je možné v simulaci použít ideální Gaussův filtr[1]. Postup jeho modelování je popsán v další kapitole.

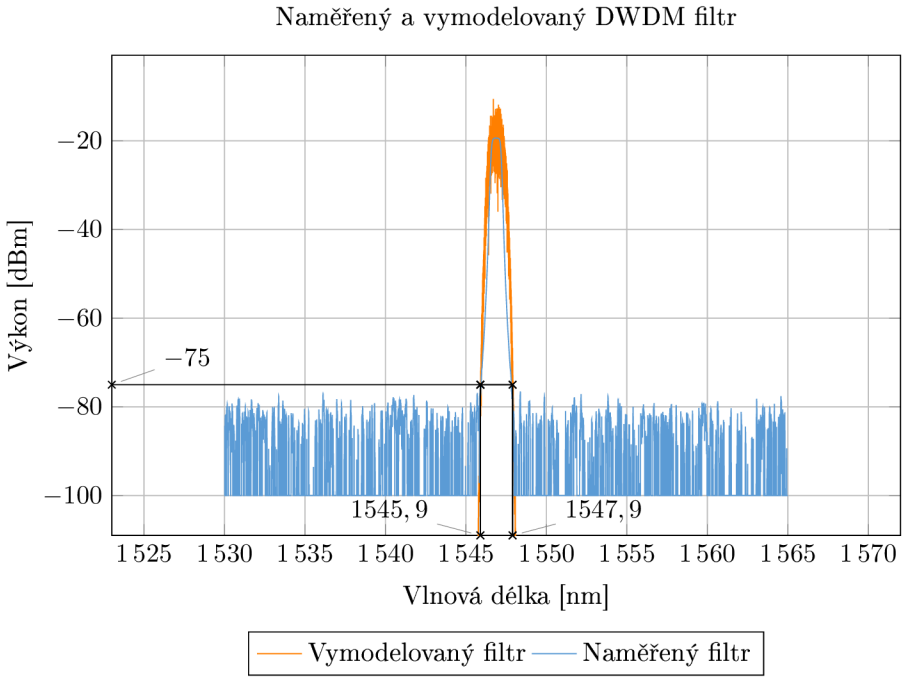
[1]Následující úvaha by ovšem neplatila, pokud by se kvantový kanál vyskytoval na kanále 31 (červeně). V takovém případě by se stále vyskytoval v rozsahu 250 GHz a bylo by potřeba provést detailnější měření.

Modelování DWDM filtru

Nyní je tedy možné přistoupit k vymodelování daného filtru ve *VPI Photonics*. Obdobně jako při reálném měření byl použit zdroj šumu (bílý šum), který se držel na -20 dBm. Následně byl nastaven řád Gaussova filtru na 1,6. Výslednou charakteristiku vymodelovaného filtru (oranžově) je možné najít v grafu 18.14, kde je porovnán s naměřeným DWDM filtrem 1 (modře).

Obr. 18.13: Vymodelovaný DWDM Filtr.

Tento vymodelovaný filtr (prostřední modul na obrázku 18.13) je dále použit v simulacích tak, jak bylo popsáno výše v kapitole 18.4.1.



Obr. 18.14: Charakteristika naměřeného a vymodelovaného filtru.

18.4.2 Konstantní útlum na trase

Do této chvíle nebyl zmíněn jeden z nejdůležitějších parametrů celé optické sítě. Jedná se samozřejmě o útlum na optické trase. Ačkoliv se jednotlivé ztráty na optických filtrech a konektorech mohou zdát zanedbatelné, obzvláště u kvantového kanálu je s nimi potřeba počítat.

U optických filtrů záleží na kombinaci portů, kterou světlo prochází. Jak již bylo řečeno, přenos je možný pouze mezi porty PASS → COM a REF → COM. Z tohoto důvodu stačí k označení zdroje útlumu jen první z portů[2].

Tab. 18.7: Hodnoty útlumu na trase [158].

Útlumy na trase	
Filtr PASS (a_{PASS})	0,63 dB
Filtr REF (a_{REF})	0,43 dB
Konektor (a_K)	0,25 dB

K útlumu samozřejmě dochází rovněž na konektorech. V simulaci se počítá se čtyřmi konektory (zdroj, vstup do multiplexoru, výstup z demultiplexoru a cíl). V ostatních případech se předpokládají sváry, úbytky na nich jsou zanedbány. Hodnoty ztrát na jednotlivých komponentách jsou zapsány v tabulce 18.7.

Do simulace je útlum vkládán pomocí dvou zmíněných útlumových článků na každé straně. Výsledné hodnoty útlumu nastavené na jednotlivých modulech jsou vyjádřeny v tabulce 18.8. Podstata výpočtu vychází z obrázku 18.8.

Tab. 18.8: Výsledné útlumy na trase.

Kanály	**U zdroje (MUX)**	**U cíle (DMUX)**
Kvantový kanál	$a_{PASS} + 2a_K$	$a_{PASS} + 2a_K$
Servisní kanál 2	$a_{PASS} + a_{REF} + 2a_K$	$4a_{REF} + 2a_K$
Servisní kanál 1	$a_{PASS} + 2a_{REF} + 2a_K$	$a_{PASS} + 3a_{REF} + 2a_K$
Šifrovaný kanál 2	$a_{PASS} + 3a_{REF} + 2a_K$	$a_{PASS} + 2a_{REF} + 2a_K$
Šifrovaný kanál 1	$4a_{REF} + 2a_K$	$a_{PASS} + a_{REF} + 2a_K$

[2]Hodnoty útlumu na optickém filtru byly převzaty z dokumentace přiložené k výrobku.

18.4.3 Optické vlákno

Kvantový kanál je omezen zejména útlumem. Maximální hodnota ztrát na celém kanále je 14 dB. Tato hodnota sestává jak z útlumu na vlákně, tak ze ztrát na optických filtrech a konektorech vyjádřených v předchozí kapitole. Útlum na vlákně se určí následovně:

$$a_{vlákno} = a_{max} - (2a_{PASS} + 4a_K) = 14 - 2,26 = 11,74\ dB \tag{18.5}$$

Ze vzorce 17.2 je pak vypočtena maximální délka vlákna tak, aby byl kvantový kanál stále funkční. Hodnoty měrného útlumu α jsou spolu s vypočtenou délkou uvedeny v tabulce 18.9.

$$a_{vlákno} = \alpha l \Longrightarrow l = \frac{a_{vlákno}}{\alpha}$$

Samotný výrobce QKD systému doporučuje používat optické vlákno SMF-28 firmy Corning vyhovující doporučení ITU-T G.657.A1. Toto konkrétní vlákno ale nemusí být vždy dostupné. Z tohoto důvodu je vypočtena maximální délka i pro samotný standard G.657.A1[3]. Tento standard má však mnohem větší toleranci a určuje tak nejnižší možnou maximální vzdálenost [159, 160, 161].

Tab. 18.9: Měrný útlum pro optická vlákna

Vlákno	**Měrný útlum** (α)	**Délka vlákna** (l)
G.657.A1	0,3 dB/km	39,13 km
SMF-28	0,18 dB/km	65,2 km

V závislosti na vybraném vlákně se tedy může maximální vzdálenost QKD serverů lišit až o 26,07 km. Z hlediska QKD se tak jedná o výrazný rozdíl. V simulaci je počítáno s nejhorší možnou variantou, tedy s 0,3 dB/km.

Disperze

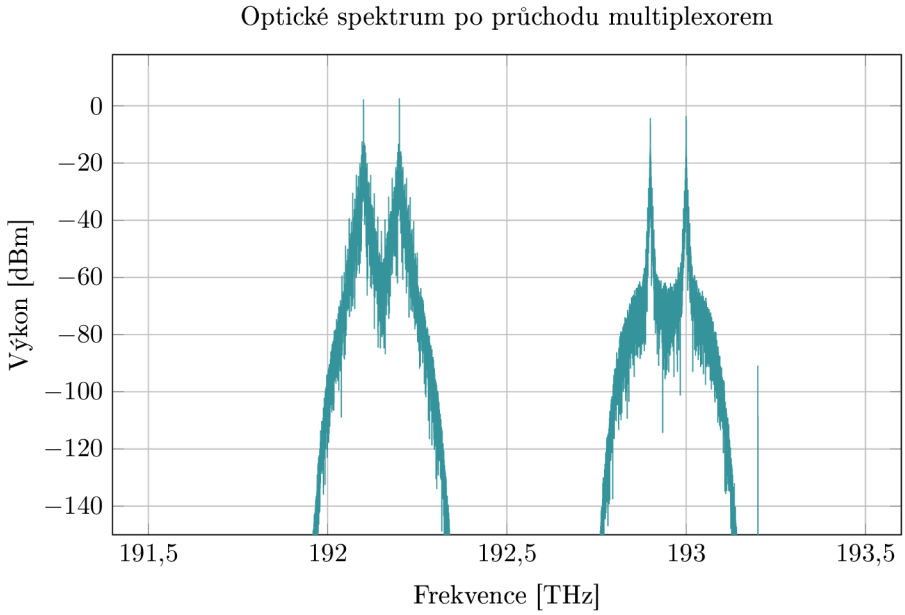
Protože je u kvantového kanálu uvažována nulová šířka spektrální čáry, k disperzi zde nedochází. Ostatní kanály dále nejsou hlavním zájmem této simulace. Z tohoto důvodu tak byly v simulaci ponechány výchozí přednastavené hodnoty.

[3]Dalším často používaným ITU-T standardem je vlákno G.652.D. Měrný útlum pro dané vlnové délky je zde ale srovnatelný s vláknem G.657.A1. Z tohoto důvodu s ním nebude dále počítáno.

Zmultiplexovaný signál

V simulaci vstupuje do společného vlákna již sloučený optický signál, který je zaznamenán v grafu 18.15. Zleva lze rozpoznat oba výkonnější šifrované kanály. Vpravo od nich jsou pak umístěny kanály servisní, sousedící se samotným kvantovým kanálem.

Je zřejmé, že pokud by klasické signály nebyly řádně odfiltrovány, kvantový kanál by v šumu (kolem -60 dBm) zanikl. Současně však vlivem ideální filtrace přesahuje nyní izolace kvantového kanálu vypočtenou minimální hodnotu 25,8 dB.



Obr. 18.15: Charakteristika naměřeného a vymodelovaného filtru.

18.4.4 Bitová chybovost na klasických kanálech

V průběhu simulace byla změřena bitová chybovost (BER) na klasických kanálech. Na základě výsledků v tabulce 18.10 je možné usoudit, že zdroje klasických signálů byly nastaveny správně. V případě šifrovaných kanálů je chybovost při použití FEC (Forward Error Correction) stále v přijatelných mezích. U servisních kanálů je ovšem zcela zanedbatelná. Důvodem je jak menší šířka pásma, tak použití ideálního Gaussova filtru, který razantně sníží možnosti přeslechů [162].

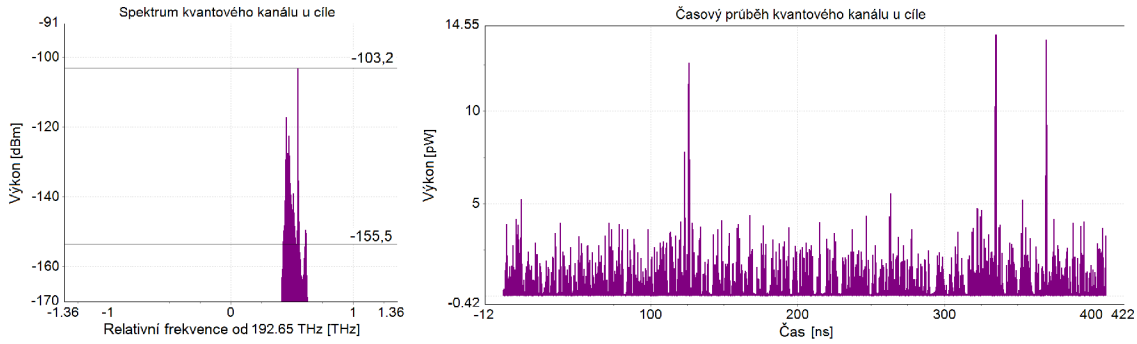
Tab. 18.10: Bitová chybovost klasických kanálů.

Bitová chybovost klasických kanálů	
Servisní kanál 2	$3,31 \cdot 10^{-110}$
Servisní kanál 1	$9,21 \cdot 10^{-96}$
Šifrovaný kanál 2	$1,947 \cdot 10^{-4}$
Šifrovaný kanál 1	$2,879 \cdot 10^{-4}$

18.4.5 Výsledný kvantový signál

Jako poslední lze porovnat původní hodnoty kvantového signálu s hodnotami naměřenými u cíle. Z grafu spektra je zřejmé, že skutečně došlo k poklesu o vypočtených 14 dB. Současně je vidět, že je kvantový signál obklopen zbytky druhého servisního kanálu, které nebyly dostatečně potlačeny. Je ovšem zřejmé, že izolace mezi těmito kanály jasně překračuje vypočtenou minimální hodnotu izolace ($25,8\ dB$). Tato hodnota izolace by měla být pro přenos dostatečná, minimální izolace 25 dB je garantována i u některých komerčních výrobků [163].

Při pohledu na průběh vlny je vidět, že všechny tři pulzy dorazily do cíle. Reálné fotony by se takto ovšem nechovaly. Foton může existovat pouze vcelku, nebo vůbec. Detekce zeslabeného pulzu, tedy části fotonu, neodpovídá skutečnosti.



Obr. 18.16: Výsledný kvantový kanál v časové a spektrální oblasti.

18.5 Shrnutí výsledků

V průběhu této části práce byl navržen polygon pro kvantovou distribuci klíčů, který byl následně vymodelován v simulačním software *VPI Photonics*. Aby byla simulace úspěšná, byly provedeny nezbytné výpočty, zaměřené zejména na parametry kvantového kanálu.

Dále byla provedena měření optických TFF filtrů. Ty byly následně použity pro sestavení multiplexoru a OADM. Protože polygon obsahuje pouze čtyři klasické kanály, je použití TFF výhodnější než AWG multiplexor (Arrayed Waveguide Grating). V případě TFF sice ztráty rostou s počtem kanálů, v tomto případě se ovšem hodnoty útlumu pohybují mezi 2,71 dB a 3,41 dB (vychází z tabulky 18.8). V případě více kanálů by ovšem druhá varianta mohla být díky konstantnímu vložnému útlumu (cca 3 dB až 3,5 dB) výhodnější. Charakteristika tohoto filtru však nebyla měřena, a proto není v simulaci použit.

Pomocí daných měření, výpočtů a úvah bylo dokázáno, že k úspěšnému přenosu kvantových signálů postačuje při daném rozložení kanálů jediný TFF filtr. Přidání dalších filtrů tak není nutné.

Na základě měřeného DWDM filtru byly vypočteny ztráty, ke kterým na jednotlivých kanálech dochází na optických spojích (zejména konektory, ztráty na svárech byly zanedbány) a filtrech. Vypočtena byla dále maximální délka optického vlákna, a to jak pro doporučené vlákno SMF-28, tak pro „tolerantnější“ ITU-T standard G.657.A1. Rozdíl mezi nejvyšší a nejnižší maximální délkou vlákna tak může tvořit až 26,07 km.

Rovněž byly prezentovány výsledky simulace, zejména pak spektrum zmultiplexovaných signálů a bitová chybovost klasických signálů. V neposlední řadě lze porovnat stav kvantového kanálu před a po průchodu optickou sítí. Získaná spektra odpovídají výpočtům, časový průběh na konci kvantového kanálu ovšem neodpovídá reálnému chování fotonu.

Závěr

V průběhu práce byly vysvětleny důvody vzniku kvantové kryptografie a nastíněny pojmy kvantové mechaniky potřebné k pochopení základních principů QKD protokolů. Postupně byly rozebírány mechanizmy nutné k bezpečnému utajení informací v postkvantové době, tedy zejména QRNG, QKD a PQC.

Pozornost byla věnována hlavně principům funkčnosti QKD protokolů. Po představení obecného postupu byly jednotlivé protokoly rozřazeny do skupin a popsány. Vysvětleny byly rovněž některé pojmy vztahující se k reálným implementacím QKD protokolů, jako jsou slabé koherentní pulzy, PNS útok a návnadové stavy.

Dále se práce věnovala možnostem budování QKD sítí a možným budoucím i současným standardům, jako je ETSI Key Delivery API nebo návrh referenčního modelu od ITU-T. Spolu s tím byla provedena rešerše dostupných QKD systémů obsahující stručný popis výrobce a nabízených zařízení. Vybraná zařízení byla poté detailněji srovnána níže, pomocí tabulek.

Praktická část práce byla realizována pomocí programu *VPI Photonics* a byla věnována modelovaní a simulaci QKD polygonů. K simulaci byly vybrány tři protokoly rodiny BB84. V závislosti na délce kvantového kanálu (optického vlákna) byla postupně měřena kvantová bitová chybovost (QBER). Výsledky simulací potvrzují nižší QBER pro verze protokolu implementující fázové kódování a pro protokol T12. Dále byla měřena závislost QBER na nedokonalostech daných zařízení a byl předveden pokus o odposlech vyvolávající velmi vysokou chybovost. Ta následně vedla k odhalení Evy.

Nakonec byl představen návrh QKD polygonu, který byl následně v daném software vymodelován a otestován. Některé vlastnosti byly rovněž ověřeny výpočty. Praktická část bakalářské práce byla dále prezentována na studentské konferenci EEICT 2021.

Literatura

[1] Alice a Bob. *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2001- [cit. 2021-5-28]. Dostupné z: https://cs.wikipedia.org/wiki/Alice_a_Bob

[2] BARTL, Eduard. Moderní šifry I. *Matematika — fyzika — informatika* [online]. Přírodovědecká fakulta UPOL, 2018 [cit. 2020-11-22]. Dostupné z: http://mfi.upol.cz/files/27/2701/mfi_2701_055_067.pdf

[3] Block Cipher. *TutorialsPoint* [online]. Madhapur: Tutorials Point, 2020 [cit. 2020-11-22]. Dostupné z: https://www.tutorialspoint.com/cryptography/block_cipher.htm

[4] Diffieho—Hellmanova výměna klíčů. In: *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2019 [cit. 2020-11-22]. Dostupné z: https://cs.wikipedia.org/wiki/Diffieho—Hellmanova_výměna_klíčů

[5] OPÁLENÝ, Filip. *P vs. NP — reálne dopady na webovú bezpečnosť* [online]. Devel.cz, 2019, 4. 11. 2017 [cit. 2020-11-22]. Dostupné z: https://www.zdrojak.cz/clanky/p-vs-np-realne-dopady-webovu-bezpecnost/

[6] BURGET, Radim. *Teoretická informatika: Vyčíslitelnost a složitost.* VUT v Brně, 2020.

[7] Kvantový Turingův stroj. *Matematická sekce* [online]. Univerzita Karlova, Matematicko-fyzikální fakulta, 2001-01-23 [cit. 2020-11-08]. Dostupné z: https://www2.karlin.mff.cuni.cz/h̃olub/soubory/qc/node15.html

[8] Kvantový seriál — díl 3. — Kvantové počítače — Jak si jej představit?. *Qubits.cz* [online]. 2020, 3. 01. 2020 [cit. 2020-11-08]. Dostupné z: https://qubits.cz/serialy/kvantovy-serial-dil-3-kvantove-pocitace-jak-si-jej-predstavit/

[9] Kvantový seriál — díl 4. — Kvantové počítače — Aplikace a použití. *Qubits.cz* [online]. 2020, 10. 01. 2020 [cit. 2020-11-08]. Dostupné z: https://qubits.cz/serialy/kvantovy-serial-dil-4-kvantove-pocitace-aplikace-a-pouziti/

[10] BEATTIE, Craig. *Shor-s Algorithm* [online]. Wells Media Group, 2020, May 6, 2020 [cit. 2020-11-08]. Dostupné z: https://www.carriermanagement.com/features/2020/05/06/206352.htm

[11] How a quantum computer could break 2048-bit RSA encryption in 8 hours. *MIT Technology review* [online]. May 30, 2019 [cit. 2020-11-08]. Dostupné z: https://www.technologyreview.com/2019/05/30/65724/how-a-quantum-computer-could-break-2048-bit-rsa-encryption-in-8-hours/

[12] HOVANOVÁ, Tatiana. *KVANTOVĚ BEZPEČNÁ KRYPTOGRAFIE* [online]. Brno, 2019 [cit. 2020-11-08]. Dostupné z: https://www.vutbr.cz/www_base/zav_prace_soubor_verejne.php?file_id=192221. Bakalářská práce. Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav telekomunikací. Vedoucí práce Doc. Ing. Václav Zeman, Ph.D.

[13] BAUMHOF, Andreas. *Breaking RSA Encryption: an Update on the State-of-the-Art* [online]. Quintessence Labs, 2019 [cit. 2021-5-28]. Dostupné z: https://www.quintessencelabs.com/blog/breaking-rsa-encryption-update-state-art/

[14] WAGNER, Lane. Is AES-256 Quantum Resistant? *Medium.com* [online]. Jul 9, 2019 [cit. 2020-11-08]. Dostupné z: https://medium.com/@wagslane/is-aes-256-quantum-resistant-d3f776163672

[15] Post-Quantum Cryptography: FAQs. *Nist.gov* [online]. NIST [cit. 2020-11-08]. Dostupné z: https://csrc.nist.gov/projects/post-quantum-cryptography/faqs

[16] GIRY, Damien. NIST Recommendations 2020. *BlueKrypt* [online]. [cit. 2020-11-08]. Dostupné z: https://www.keylength.com/en/4/

[17] SYSOJEV, Sergej Sergejevič. PETROHRADSKÁ STÁTNÍ UNIVERZITA. *Quantum Computing. Less Formulas - More Understanding* [online]. Coursera.org [cit. 2020-11-25]. Dostupné z: https://www.coursera.org/learn/quantum-computing-lfmu

[18] Wave function. In: *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2020 [cit. 2020-11-25]. Dostupné z: https://en.wikipedia.org/wiki/Wave_function

[19] GARFINKEL, Simson. Kde se uplatní kvantová kryptografie. *ScienceWorld* [online]. [cit. 2020-11-08]. Dostupné z: https://www.scienceworld.cz/neziva-priroda/kde-se-dnes-uplatni-kvantova-kryptografie-877/?switch_theme=mobile

[20] FEYNMAN, Richard Phillips. *Neobyčejná teorie světla a látky: kvantová elektrodynamika*. Praha: Aurora, 2001. ISBN 80-7299-045-4.

[21] ZEMAN, Václav. *Aplikovaná kryptografie: Náhodná čísla.* VUT v Brně, 2019.

[22] DUBEY, Rashmi, Sugandha AGARWAL a Rajesh SINGH. A Survey:The Next Generation Of High Quantum: Performance Of Quantum Computing Devices. *International Journal of Scientific & Engineering Research* [online]. 2010, February-2014, (Volume 5, 2) [cit. 2020-11-08]. ISSN 2229-5518. Dostupné z: https://www.ijser.org/paper/A-Survey-The-Next-Generation-Of-High-Quantum-Performance.htm

[23] KALVODA, Tomáš. Bit a qubit. *Marast* [online]. Praha: ČVUT FIT, 29. 10. 2017 [cit. 2020-11-08]. Dostupné z: https://marast.fit.cvut.cz/cs/blog_posts/26

[24] Lineární kombinace vektorů. *Matematika.cz* [online]. Nová média, 2006 [cit. 2020-11-08]. Dostupné z: https://matematika.cz/linearni-kombinace-vektoru

[25] Infrared. *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2021 [cit. 2021-5-28]. Dostupné z: https://en.wikipedia.org/wiki/Infrared

[26] POLARIZATION: LINEAR & CIRCULAR POLARIZERS. *Japanistry* [online]. Japanistry [cit. 2020-11-26]. Dostupné z: https://www.japanistry.com/polarization/

[27] REICHL, Jaroslav a Martin VŠETIČKA. Vlnové destičky. *Encyklopedie fyziky* [online]. 2006, 2018-04-01 [cit. 2020-11-08]. Dostupné z: http://fyzika.jreichl.com/main.article/view/1673-vlnove-desticky

[28] REICHL, Jaroslav a Martin VŠETIČKA. Kruhově polarizované světlo. *Encyklopedie fyziky* [online]. 2006 [cit. 2020-11-08]. Dostupné z: http://fyzika.jreichl.com/main.article/view/1672-kruhove-polarizovane-svetlo

[29] REICHL, Jaroslav a Martin VŠETIČKA. Polarizace polaroidem. *Encyklopedie fyziky* [online]. 2006 [cit. 2020-11-26]. Dostupné z: http://fyzika.jreichl.com/main.article/view/465-polarizace-polaroidem

[30] Polarizační mikroskopie. In: *WikiSkripta* [online]. Praha: 1. lékařská fakulta Univerzity Karlovy, 22. 11. 2018 [cit. 2020-11-08]. Dostupné z: https://www.wikiskripta.eu/w/Polarizační_mikroskopie

[31] Polarizace světla. In: *WikiSkripta* [online]. Praha: 1. lékařská fakulta Univerzity Karlovy, 9. 6. 2020 [cit. 2020-11-08]. Dostupné z: https://www.wikiskripta.eu/w/Polarizace_světla

[32] Polarizace světla a Brewsterův úhel. In: *YouTube* [online]. elmag.org, 1. 3. 2014 [cit. 2020-11-08]. Dostupné z: https://www.youtube.com/watch?v=PUiZz1afRJs&ab_channel=elmag.org

[33] PROTOCOLE BB84. *ALICE TO BOB: Cryptographie Quantique* [online]. Université de Nice, 2015 [cit. 2020-11-06]. Dostupné z: http://physique.unice.fr/sem6/2014-2015/PagesWeb/PT/Tomographie/?page=bb84

[34] Introduction to quantum computing: Bloch sphere. *Tasos´ Posts* [online]. [cit. 2020-11-08]. Dostupné z: http://akyrillidis.github.io/notes/quant_post_7

[35] GLENDINNING, Ian. *Rotations on the Bloch Sphere* [online]. In: . May 20, 2010 [cit. 2020-11-08]. Dostupné z: doi:10.13140/RG.2.2.27566.25922

[36] Kvantová Fourierova transformace. *Matematická sekce* [online]. Univerzita Karlova, Matematicko-fyzikální fakulta, 2001-01-23 [cit. 2020-11-26]. Dostupné z: https://www2.karlin.mff.cuni.cz/ holub/soubory/qc/node21.html

[37] Kvantové brány. *Matematická sekce* [online]. Univerzita Karlova, Matematicko-fyzikální fakulta, 2001-01-23 [cit. 2020-11-08]. Dostupné z: https://www2.karlin.mff.cuni.cz/ holub/soubory/qc/node18.html

[38] ASFAW, Abraham, Luciano BELLO, Yael BEN-HAIM, et al. Multiple Qubits and Entangled States. *Learn Quantum Computation Using Qiskit* [online]. **2020** [cit. 2020-11-08]. Dostupné z: http://community.qiskit.org/textbook

[39] HALENKOVÁ, Eva, Antonín ČERNOCH a Jan SOUBUSTA. *Spontánní sestupná frekvenční parametrická konverze a zdroj fotonových párů podle návrhu P. G. Kwiata* [online]. Olomouc: Univerzita Palackého v Olomouci Přírodovědecká fakulta, 2012 [cit. 2020-11-08]. ISBN 978-80-244-3111-6. Dostupné z: https://docplayer.cz/8701466-Spontanni-sestupna-frekvencni-parametricka-konverze-a-zdroj-fotonovych-paru-podle-navrhu-p-g-kwiata.html

[40] MALIK, Mehul a Robert BOYD. *Quantum Imaging Technologies* [online]. June 2014 [cit. 2020-11-08]. Dostupné z: doi:10.1393/ncr/i2014-10100-0

[41] LEE, Seung-Woo a Hyunseok JEONG. Bell-state measurement and quantum teleportation using linear optics: two-photon pairs, entangled coherent states, and hybrid entanglement. *ArXiv* [online]. [cit. 2020-11-08]. Dostupné z: https://arxiv.org/pdf/1304.1214.pdf

[42] KIM, Yong-Su, Tanumoy PRAMANIK, Young-Wook CHO, Ming YANG, Sang-Wook HAN, Sang-Yun LEE, Min-Sung KANG a Sung MOON. Informationally symmetrical Bell state preparation and measurement. *Optics Express* [online]. 2018, **26**(22) [cit. 2020-11-08]. ISSN 1094-4087. Dostupné z: doi:10.1364/OE.26.029539

[43] Bell measurement. *Quantiki: Quantum Information Portal and Wiki* [online]. October 26, 2015 [cit. 2020-11-08]. Dostupné z: https://www.quantiki.org/wiki/bell-measurement

[44] CAMPBELL, Luke. Bell Measurements and Teleportation: Overview Entanglement Bell states and Bell measurements Limitations on Bell measurements using linear devices Teleportation. In: *SlidePlayer.com* [online]. [cit. 2020-11-08]. Dostupné z: https://slideplayer.com/slide/8459670/

[45] ZEILINGER, Anton. Light for the quantum. Entangled photons and their applications: a very personal perspective. *Physica Scripta* [online]. 2017, **92**(7) [cit. 2020-11-08]. ISSN 0031-8949. Dostupné z: doi:10.1088/1402-4896/aa736d

[46] NORDÉN, Bengt. Quantum entanglement: facts and fiction — how wrong was Einstein after all? *Quarterly Reviews of Biophysics* [online]. 2016, **49** [cit. 2020-11-08]. ISSN 0033-5835. Dostupné z: doi:10.1017/S0033583516000111

[47] Kvantová mechanika: animace vysvětlující kvantovou fyziku. In: *YouTube* [online]. Physics Videos by Eugene Khutoryansky, 23. 3. 2013 [cit. 2020-11-08]. Dostupné z: https://www.youtube.com/watch?v=iVpXrbZ4bnU&ab_channel=PhysicsVideosbyEugeneKhutoryansky

[48] *Lab Course: Bell-s Inequality and Quantum Tomography* [online]. München: Ludwig-Maximilians Universität München, April 2020 [cit. 2020-11-08]. Dostupné z: https://xqp.physik.uni-muenchen.de/download/labcourse/bell_manual.pdf

[49] The EPR Paradox & Bell's inequality explained simply. In: *YouTube* [online]. Arvin Ash, 14. 2. 2020 [cit. 2020-11-08]. Dostupné z: https://www.youtube.com/watch?v=f72whGQ31Wg&t=822s&ab_channel=ArvinAsh

[50] Bell's theorem. In: *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2020 [cit. 2020-11-26]. Dostupné z: https://en.wikipedia.org/wiki/Bell's_theorem

[51] BROŽ, Pavel. Lokální realismus zemřel. Ať žijí kvantové nelokální korelace! *Osel* [online]. 01.11.2015 [cit. 2020-11-08]. ISSN 1214-6307. Dostupné z: https://www.osel.cz/8513-lokalni-realismus-zemrel-at-ziji-kvantove-nelokalni-korelace.html

[52] TU Delft — A loophole-free Bell test. In: *YouTube* [online]. TU Delft, 21. 10. 2015 [cit. 2020-11-08]. Dostupné z: https://www.youtube.com/watch?v=AE8MaQJkRcg&ab_channel=TUDelft

[53] Quantum Random Numbers Generator. *Quantum Flagship* [online]. Düsseldorf: The QFlag — Quantum Flagship Coordination and Support Action [cit. 2020-10-08]. Dostupné z: https://qt.eu/discover-quantum/underlying-principles/qrng/

[54] STORY OF THE MONTH: CHIP-BASED TECHNOLOGIES FOR QUANTUM COMMUNICATIONS. *QCALL* [online]. QCALL, 2016 [cit. 2020-11-06]. Dostupné z: http://www.qcall-itn.eu/2019/09/03/chip-based-technologies-for-quantum-communications/

[55] PIRANDOLA, Stefano, Ulrik ANDERSEN, Leonardo BANCHI, et al. Advances in Quantum Cryptography. *Advances in Optics and Photonics* [online]. [cit. 2020-11-07]. ISSN 1943-8206. Dostupné z: doi:10.1364/AOP.361502

[56] Quantum Communication FAQ — QKD Steps. *QuReP* [online]. QuReP, 2010 [cit. 2020-11-07]. Dostupné z: http://www.quantumrepeaters.eu/quantumrepeaters.eu/index.php/qcomm/component/content/article/71-qkd-protocols/

[57] BRÁDLER, Kamil. Kvantová kryptografie — zprávy z přední linie. *Osel* [online]. 12. 01. 2007 [cit. 2020-11-06]. ISSN 1214-6307. Dostupné z: https://www.osel.cz/2369-kvantova-kryptografie-zpravy-z-predni-linie.html

[58] LANCE, Andrew, John LEISEBOER a Thomas SYMUL. *Quantum Key Distribution Systems Compared* [online]. [cit. 2020-11-06]. Dostupné z: https://info.quintessencelabs.com/hubfs/PDFs/Whitepaper_QKD_Systems-Compared.pdf

[59] KUPKO, Timm, Martin VON HELVERSEN, Lucas RICKERT, et al. Tools for the performance optimization of single-photon quantum key distribution. *Npj Quantum Information* [online]. 2020, **6**(1) [cit. 2020-11-06]. ISSN 2056-6387. Dostupné z: doi:10.1038/s41534-020-0262-8

[60] 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. 2020-11-06]. ISSN 1548-5129. Dostupné z: doi:10.1177/1548512917698053

[61] HIROKI TAKESUE, TOSHIMORI HONJO, KIYOSHI TAMAKI a YASUHIRO TOKURA. Differential phase shift quantum key distribution. In: *2008 First ITU-T Kaleidoscope Academic Conference - Innovations in NGN: Future Network and Services* [online]. IEEE, 2008, 2008, s. 229-236 [cit. 2020-11-07]. ISBN 978-92-61-12441-0. Dostupné z: doi:10.1109/KINGN.2008.4542270

[62] DIAMANTI, Eleni a Anthony LEVERRIER. Distributing Secret Keys with Quantum Continuous Variables: Principle, Security and Implementations. *Entropy* [online]. 2015, **17**(12), 6072-6092 [cit. 2020-11-06]. ISSN 1099-4300. Dostupné z: doi:10.3390/e17096072

[63] NURHADI, Ali Ibnun a Nana Rachmana SYAMBAS. Quantum Key Distribution (QKD) Protocols: A Survey. In: *2018 4th International Conference on Wireless and Telematics (ICWT)* [online]. IEEE, 2018, 2018, s. 1-5 [cit. 2020-11-06]. ISBN 978-1-5386-6161-1. Dostupné z: doi:10.1109/ICWT.2018.8527822

[64] HAITJEMA, Mart. A Survey of the Prominent Quantum Key Distribution Protocols. *CSE571S: Network Security* [online]. Washington University in St. Louis, December 2, 2007, **Fall 2007** [cit. 2020-11-07]. Dostupné z: https://www.cse.wustl.edu/ jain/cse571-07/ftp/quantum/

[65] BB84 and Ekert91 protocols: BB84 protocol. *Quantiki* [online]. October 26, 2015 [cit. 2020-11-07]. Dostupné z: https://www.quantiki.org/wiki/bb84-and-ekert91-protocols

[66] STRÁSKÝ, Josef. *Kvantová kryptografie* [online]. Praha, 2008 [cit. 2020-11-07]. Dostupné z: http://quantum.karlov.mff.cuni.cz/archiv_praci/strasky/BPTX_2007_1_11320_NSZZ027_228462_0_49010.pdf. Bakalářská práce. Univerzita Karlova v Praze, Matematicko-fyzikální fakulta, Katedra chemické fyziky a optiky. Vedoucí práce Prof. RNDr. Lubomír Skála, DrSc.

[67] Quantum Communication FAQ — Key Sifting. *QuReP* [online]. QuReP, 2010 [cit. 2020-11-07]. Dostupné z: http://www.quantumrepeaters.eu/quantumrepeaters.eu/index.php/qcomm/component/content/article/74-sifting/

[68] Quantum Communication FAQ — Key Distillation. *QuReP* [online]. QuReP, 2010 [cit. 2020-11-07]. Dostupné z: http://www.quantumrepeaters.eu/quantumrepeaters.eu/index.php/qcomm/component/content/article/75-distillation/

[69] LI, Hong-Wei, Zhen-Qiang YIN, Shuang WANG, Yong-Jun QIAN, Wei CHEN, Guang-Can GUO a Zheng-Fu HAN. Randomness determines practical security of BB84 quantum key distribution. *Scientific Reports* [online]. 2015, **5**(1) [cit. 2020-11-07]. ISSN 2045-2322. Dostupné z: doi:10.1038/srep16200

[70] Quantum Hacking - Evan Meyer-Scott - QCSYS 2011. In: *YouTube* [online]. Institute for Quantum Computing, 11. 11. 2011 [cit. 2020-11-07]. Dostupné z: https://www.youtube.com/watch?v=C1wOIXMV14k&abq_channel=InstituteforQuantumComputing

[71] LO, Hoi-Kwong, Xiongfeng MA a Kai CHEN. Decoy State Quantum Key Distribution. *Physical Review Letters* [online]. 2005, **94**(23) [cit. 2020-11-07]. ISSN 0031-9007. Dostupné z: doi:10.1103/PhysRevLett.94.230504

[72] *Toshiba QKD system* [online]. Uxbridge: Toshiba Europe, 2020 [cit. 2020-11-07]. Dostupné z: https://www.toshiba.eu/pages/eu/Cambridge-Research-Laboratory/toshiba-qkd-system

[73] PAJTINOVÁ, MÁRIA. *METODY KVANTOVÉ KRYPTOGRAFIE* [online]. Brno, 2009 [cit. 2020-11-07]. Dostupné z: https://dspace.vutbr.cz/bitstream/handle/11012/11505/final-thesis.pdf?sequence=8&isAllowed=y. Bakalářská práce. Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav telekomunikací. Vedoucí práce Doc. Ing. Václav Zeman, Ph.D.

[74] SINGH, Hitesh, D.L. GUPTA a A.K SINGH. Quantum Key Distribution Protocols: A Review. *IOSR Journal of Computer Engineering* [online]. 2014, **16**(2), 01-09 [cit. 2020-11-07]. ISSN 22788727. Dostupné z: doi:10.9790/0661-162110109

[75] Cryptography: Boolean functions and related problems. In: *Coursera.org* [online]. Novosibirsk State University [cit. 2020-11-07]. Dostupné z: https://www.coursera.org/lecture/cryptography-boolean-functions/description-of-qkd-protocols-b92-and-e91-lbmGw

[76] QuEST: Activities: B92 Protocol. *Quantum Communication* [online]. Raman Research Institute, 2019 [cit. 2020-11-07]. Dostupné z: http://www.rri.res.in/quic/qkdactivities.php

[77] 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. 2020-11-07]. ISSN 1094-4087. Dostupné z: doi:10.1364/OE.21.024550

[78] INOUE, K. Quantum key distribution technologies. *IEEE Journal of Selected Topics in Quantum Electronics* [online]. 2006, **12**(4), 888-896 [cit. 2020-11-15]. ISSN 1077-260X. Dostupné z: doi:10.1109/JSTQE.2006.876606

[79] ALI, Sellami a Omer MAHMOUD. Implementation of SARG04 decoy state quantum key distribution. In: *2011 6th International Conference on Telecommunication Systems, Services, and Applications (TSSA)* [online]. IEEE, 2011, 2011, s. 86-90 [cit. 2020-11-07]. ISBN 978-1-4577-1442-9. Dostupné z: doi:10.1109/TSSA.2011.6095412

[80] AHMAD GHAZALI, Lizal Iswady, Ahmad Fauzi ABAS, Wan Azizun WAN ADNAN, Makhfudzah MOKHTAR, Mohd Adzir MAHDI a M. Iqbal SARIPAN. Security proof of Improved-SARG04 protocol using the same four qubit states. In: *International Conference On Photonics 2010* [online]. IEEE, 2010, 2010, s. 1-4 [cit. 2020-11-07]. ISBN 978-1-4244-7186-7. Dostupné z: doi:10.1109/ICP.2010.5604403

[81] SOFY, Ahmed Mahmoud, Mohamed SHALABY, Hisham Mohamed DAHSHAN a Alaa ROHIEM. Modeling One-way and Two-way quantum key distribution protocols. In: *2019 Ninth International Conference on Intelligent Computing and Information Systems (ICICIS)* [online]. IEEE, 2019, 2019, s. 239-244 [cit. 2020-11-07]. ISBN 978-1-7281-3995-1. Dostupné z: doi:10.1109/ICICIS46948.2019.9014729

[82] LOPES, Minal a Nisha SARWADE. Cryptography from Quantum Mechanical Viewpoint. *International Journal on Cryptography and Information Security* [online]. 2014, **4**(2), 13-25 [cit. 2020-11-07]. ISSN 18398626. Dostupné z: doi:10.5121/ijcis.2014.4202

[83] Quantum Computing. Less Formulas - More Understanding: E91. In: *Coursera.org* [online]. Saint Petersburg State University [cit. 2020-11-07]. Dostupné z: https://www.coursera.org/lecture/quantum-computing-lfmu/e91-MmIiW

[84] ELBOUKHARI, Mohamed, Mostafa AZIZI a Abdelmalek AZIZI. *Quantum Key Distribution Protocols: A Survey* [online]. HyperSciences, 2010 [cit. 2020-11-07]. Dostupné z: https://www.cs.nmsu.edu/ istrnad/cs478/presentations/QuantumCryptography.pdf

[85] LI, Leilei, Hengji LI, Chaoyang LI, Xiubo CHEN, Yan CHANG, Yuguang YANG a Jian LI. The security analysis of E91 protocol in collective-rotation noise channel. *International Journal of Distributed Sensor Networks* [online]. 2018, **14**(5) [cit. 2020-11-07]. ISSN 1550-1477. Dostupné z: doi:10.1177/1550147718778192

[86] ERVEN, Chris. *On Free Space Quantum Key Distribution and its Implementation with a Polarization-Entangled Parametric Down Conversion Source* [online]. Waterloo, Ontario, Canada, 2007 [cit. 2020-11-07]. Dostupné z: https://uwspace.uwaterloo.ca/bitstream/handle/10012/3021/Thesis_Chris Erven_SubmittedToGSO.pdf?sequence=1&isAllowed=y. Diplomová práce. University of Waterloo.

[87] KUMAR DATTA, Asit a Soumika MUNSHI. *Information Photonics: Fundamentals, Technologies, and Applications* [online]. Verze 20160523. Boca Raton: CRC Press, 2017 [cit. 2020-11-07]. ISBN 978-1-4822-3641-5. Dostupné z: https://books.google.cz/books?id=BRkNDgAAQBAJ&printsec=copyright&hl=cs&source=gbs_pub_info_r#v=onepage&q&f=false

[88] ZAWADZKI, Piotr a Jarosław Adam MISZCZAK. A General Scheme for Information Interception in the Ping-Pong Protocol. *Advances in Mathematical Physics* [online]. 2016, **2016**, 1-7 [cit. 2020-11-07]. ISSN 1687-9120. Dostupné z: doi:10.1155/2016/3162012

[89] CHEN ZUNING a QIN ZHENG. A “Ping-pong” Protocol with Authentication. In: *2010 5th IEEE Conference on Industrial Electronics and Applications* [online]. IEEE, 2010, 2010, s. 1805-1810 [cit. 2020-11-07]. ISBN 978-1-4244-5045-9. Dostupné z: doi:10.1109/ICIEA.2010.5515357

[90] BOSTRÖM, Kim a Timo FELBINGER. On the security of the ping-pong protocol. *Physics Letters A* [online]. 2008, **372**(22), 3953-3956 [cit. 2020-11-07]. ISSN 03759601. Dostupné z: doi:10.1016/j.physleta.2008.03.048

[91] PAVIČIĆ, Mladen. RETRACTED ARTICLE: Can Two-Way Direct Communication Protocols Be Considered Secure? *Nanoscale Research Letters* [online]. 2017, **12**(1) [cit. 2020-11-07]. ISSN 1931-7573. Dostupné z: doi:10.1186/s11671-017-2314-3

[92] LUCAMARINI, Marco a Stefano MANCINI. Quantum key distribution using a two-way quantum channel. *Theoretical Computer Science* [online]. 2014, **560**, 46-61 [cit. 2020-11-07]. ISSN 03043975. Dostupné z: doi:10.1016/j.tcs.2014.09.017

[93] ZEMAN, Václav. *Aplikovaná kryptografie: Quantum Key Distribution*. VUT v Brně, 2019.

[94] Wave interference. In: *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2020 [cit. 2020-11-26]. Dostupné z: https://en.wikipedia.org/wiki/Wave_interference

[95] TOKURA, Yasuhiro a Toshimori HONJO. Differential Phase Shift Quantum Key Distribution (DPS-QKD) Experiments. *NTT Technical Review* [online]. NTT Technical Review, 2020, Sep. 2011 [cit. 2020-11-07]. Dostupné z: https://www.ntt-review.jp/archive/ntttechnical.php?contents=ntr201109fa8.html

[96] INOUE, Kyo a Toshimori HONJO. Robustness of differential-phase-shift quantum key distribution against photon-number-splitting attack. *Physical Review A* [online]. 2005, **71**(4) [cit. 2020-11-07]. ISSN 1050-2947. Dostupné z: doi:10.1103/PhysRevA.71.042305

[97] LIU, Chang, Shanchao ZHANG, Luwei ZHAO, Peng CHEN, C. -H. F. FUNG, H. F. CHAU, M. M. T. LOY a Shengwang DU. Differential-phase-shift quantum key distribution using heralded narrow-band single photons. *Optics Express* [online]. 2013, **21**(8) [cit. 2020-11-07]. ISSN 1094-4087. Dostupné z: doi:10.1364/OE.21.009505

[98] TAKESUE, Hiroki, Toshimori HONJO, Kiyoshi TAMAKI a Yasuhiro TOKURA. Differential phase shift-quantum key distribution. *IEEE Communications Magazine* [online]. 2009, **47**(5), 102-106 [cit. 2020-11-07]. ISSN 0163-6804. Dostupné z: doi:10.1109/MCOM.2009.4939284

[99] INOUE, Kyo, Edo WAKS a Yoshihisa YAMAMOTO. Differential Phase Shift Quantum Key Distribution. *Physical Review Letters* [online]. 2002, **89**(3) [cit. 2020-11-07]. ISSN 0031-9007. Dostupné z: doi:10.1103/PhysRevLett.89.037902

[100] WAKS, Edo, Hiroki TAKESUE a Yoshihisa YAMAMOTO. Security of differential-phase-shift quantum key distribution against individual attacks. *Physical Review A* [online]. 2006, **73**(1) [cit. 2020-11-19]. ISSN 1050-2947. Dostupné z: doi:10.1103/PhysRevA.73.012344

[101] ETSI GR QKD 003. *Quantum Key Distribution (QKD); Components and Internal Interfaces*. V2.1.1 (2018-03). Sophia Antipolis Cedex: ETSI, 2018.

[102] STUCKI, D, N WALENTA, F VANNEL, et al. High rate, long-distance quantum key distribution over 250-km of ultra low loss fibres. *New Journal*

of Physics [online]. 2009, **11**(7) [cit. 2020-11-07]. ISSN 1367-2630. Dostupné z: doi:10.1088/1367-2630/11/7/075003

[103] PEEV, M, C PACHER, R ALLÉAUME, et al. The SECOQC quantum key distribution network in Vienna. *New Journal of Physics* [online]. 2009, **11**(7) [cit. 2020-11-07]. ISSN 1367-2630. Dostupné z: doi:10.1088/1367-2630/11/7/075001

[104] STUCKI, Damien, Sylvain FASEL, Nicolas GISIN, Yann THOMA a Hugo ZBINDEN. *Coherent one-way quantum key distribution* [online]. Ženeva: Université de Genève [cit. 2020-11-07]. Dostupné z: http://www.yannthoma.com/research/publications/stucki07coherent.pdf

[105] TUTORIAL: CONTINUOUS-VARIABLE QUANTUM COMMUNICATION. *Http://infiniquant.com* [online]. Max Planck Institute for the Science of Light [cit. 2020-11-07]. Dostupné z: http://infiniquant.com/tutorial-continuous-variable-quantum-communication/

[106] PASCHOTTA, Rüdiger. Squeezed States. *RP Photonics Encyclopedia* [online]. 2020-11-07 [cit. 2020-11-07]. Dostupné z: https://www.rp-photonics.com/squeezed_states_of_light.html

[107] PASCHOTTA, Rüdiger. Squeezed States. *RP Photonics Encyclopedia* [online]. 2020-11-07 [cit. 2020-11-07]. Dostupné z: https://www.rp-photonics.com/squeezed_states_of_light.html

[108] MIHULKA, Stanislav. Stlačené kvantové kočky. *Osel* [online]. 09. 06. 2015 [cit. 2020-11-07]. ISSN 1214-6307. Dostupné z: https://www.osel.cz/8285-stlacene-kvantove-kocky.html

[109] CHEKHOVA, Maria. *Lecture 12: Quantum key distribution.* [online]. Max Planck Institute for the Science of Light [cit. 2020-11-07]. Dostupné z: https://mpl.mpg.de/fileadmin/user_upload/Chekhova_Research_Group/Lecture_4_12.pdf

[110] LEVERRIER, Anthony a Philippe GRANGIER. Simple proof that Gaussian attacks are optimal among collective attacks against continuous-variable quantum key distribution with a Gaussian modulation. *Physical Review A* [online]. 2010, **81**(6) [cit. 2020-11-07]. ISSN 1050-2947. Dostupné z: doi:10.1103/PhysRevA.81.062314

[111] GROSSHANS, Frédéric a Philippe GRANGIER. Continuous Variable Quantum Cryptography Using Coherent States. *Physical Review Letters* [online]. 2002, **88**(5) [cit. 2020-11-07]. ISSN 0031-9007. Dostupné z: doi:10.1103/PhysRevLett.88.057902

[112] FEIHU XU, Marcos CURTY, BING QI a HOI-KWONG LO. Measurement-Device-Independent Quantum Cryptography. *IEEE Journal of Selected Topics in Quantum Electronics* [online]. 2015, **21**(3), 148-158 [cit. 2020-11-07]. ISSN 1077-260X. Dostupné z: doi:10.1109/JSTQE.2014.2381460

[113] QCrypt 2020: Experimental Measurement-Device-Independent QKD with Uncharacterized Sources. In: *YouTube* [online]. QCrypt conference, 3. 8. 2020 [cit. 2020-11-07]. Dostupné z: https://www.youtube.com/watch?v=Gif4eh5lenA&ab_channel=QCryptconference

[114] SESHADREESAN, Kaushik P., Masahiro TAKEOKA a Masahide SASAKI. Progress towards practical device-independent quantum key distribution with spontaneous parametric down-conversion sources, on-off photodetectors, and entanglement swapping. *Physical Review A* [online]. 2016, **93**(4) [cit. 2020-11-07]. ISSN 2469-9926. Dostupné z: doi:10.1103/PhysRevA.93.042328

[115] ZAPATERO, Víctor a Marcos CURTY. Long-distance device-independent quantum key distribution. *Scientific Reports* [online]. 2019, **9**(1) [cit. 2020-11-07]. ISSN 2045-2322. Dostupné z: doi:10.1038/s41598-019-53803-0

[116] KOŁODYŃSKI, Jan, Alejandro MÁTTAR, Paul SKRZYPCZYK, Erik WOODHEAD, Daniel CAVALCANTI, Konrad BANASZEK a Antonio ACÍN. Device-independent quantum key distribution with single-photon sources. *Quantum* [online]. 2020, **4** [cit. 2020-11-07]. ISSN 2521-327X. Dostupné z: doi:10.22331/q-2020-04-30-260

[117] MDI QKD. *Contact Quantum Communications Hub* [online]. University of York [cit. 2020-11-07]. Dostupné z: https://www.quantumcommshub.net/wider-community-and-schools/quantum-in-schools/talks-and-demos/demos/mdiqkd/

[118] TANG, Zhiyuan. *Measurement-Device-Independent Quantum Cryptography* [online]. Toronto, 2016 [cit. 2020-11-07]. Dostupné z: http://www.ecf.utoronto.ca/ qianli/publications/Zhiyuan-Tang_PhD_thesis.pdf. Disertační práce. University of Toronto, Department of Physics.

[119] 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. 2020-11-07]. ISSN 2079-9292. Dostupné z: doi:10.3390/electronics7040049

[120] YIN, Hua-Lei a Yao FU. Measurement-Device-Independent Twin-Field Quantum Key Distribution. *Scientific Reports* [online]. 2019, **9**(1) [cit. 2020-11-08]. ISSN 2045-2322. Dostupné z: doi:10.1038/s41598-019-39454-1

[121] GRASSELLI, Federico a Marcos CURTY. Practical decoy-state method for twin-field quantum key distribution. *New Journal of Physics* [online]. 2019, **21**(7) [cit. 2020-11-08]. ISSN 1367-2630. Dostupné z: doi:10.1088/1367-2630/ab2b00

[122] BOARON, Alberto, Boris KORZH, Raphael HOULMANN, Gianluca BOSO, Charles Ci Wen LIM, Anthony MARTIN a Hugo ZBINDEN. Detector-device-independent quantum key distribution: Security analysis and fast implementation. *Journal of Applied Physics* [online]. 2016, **120**(6) [cit. 2020-11-08]. ISSN 0021-8979. Dostupné z: doi:10.1063/1.4960093

[123] ITU-T Y.3800 (10/2019). *Overview on networks supporting quantum key distribution.* 2019-11-20. Ženeva: ITU-T, 2019. Dostupné také z: https://www.itu.int/rec/T-REC-Y.3800-201910-I

[124] ETSI GS QKD 014. *Quantum Key Distribution (QKD); Protocol and data format of REST-based key delivery API.* V1.1.1 (2019-02). Sophia Antipolis Cedex: ETSI, 2019.

[125] ETSI GS QKD 004. *Quantum Key Distribution (QKD); Application Interface.* V1.1.1 (2010-12). Sophia Antipolis Cedex: ETSI, 2010.

[126] BERNSTEIN, Daniel a Tanja LANGE. Post-quantum cryptography: Dealing with the fallout of physics success. *Cryptology ePrint Archive* [online]. 2017.04.09. [cit. 2020-11-08]. Dostupné z: https://eprint.iacr.org/2017/314.pdf

[127] ALAGIC, Gorjan, Jacob ALPERIN-SHERIFF, Daniel APON, et al. Status Report on the Second Round of the NIST Post-Quantum Cryptography Standardization Process: NISTIR 8309. *NIST* [online]. July 2020 [cit. 2020-11-08]. Dostupné z: doi:10.6028/NIST.IR.8309

[128] BERNSTEIN, Daniel J. Introduction to post-quantum cryptography. BERNSTEIN, Daniel J., Johannes BUCHMANN a Erik DAHMEN, ed. *Post-Quantum Cryptography* [online]. Berlin, Heidelberg: Springer Berlin Heidelberg, 2009, s. 1-14 [cit. 2020-11-08]. ISBN 978-3-540-88701-0. Dostupné z: doi:10.1007/978-3-540-88702-7_1

[129] JANG, Kyoungbae, Seungju CHOI, Hyeokdong KWON, Hyunji KIM, Jaehoon PARK a Hwajeong SEO. Grover on Korean Block Ciphers. *Applied*

Sciences [online]. 2020, **10**(18) [cit. 2020-11-08]. ISSN 2076-3417. Dostupné z: doi:10.3390/app10186407

[130] QUANTUM CRYPTOGRAPHY. *Qubitekk.com* [online]. Vista: Qubitekk, 2016 [cit. 2020-11-08]. Dostupné z: http://qubitekk.com/security/

[131] One-time pad. In: *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2020 [cit. 2020-11-26]. Dostupné z: https://en.wikipedia.org/wiki/One-time_pad

[132] *Difference Between IPsec and SSL* [online]. SolarWinds MSP, 2020, 15 April, 2019 [cit. 2020-11-27]. Dostupné z: https://www.solarwindsmsp.com/blog/ipsec-vs-ssl

[133] ETSI GS QKD 002. *Quantum Key Distribution; Use Cases*. V1.1.1 (2010-06). Sophia Antipolis Cedex: ETSI, 2010.

[134] Integrating Quantum-Safe Security with existing encryption solutions. *ID Quantique* [online]. Genève: ID Quantique, 2020 [cit. 2020-11-08]. Dostupné z: https://www.idquantique.com/quantum-safe-security/integrated-solutions/

[135] Cryptography: Boolean functions and related problems. In: *Coursera.org* [online]. Novosibirsk State University [cit. 2020-11-20]. Dostupné z: https://www.coursera.org/lecture/cryptography-boolean-functions/examples-of-using-cqn00

[136] GNATYUK, Sergiy, Myroslav RIABYI a Tetiana ZHMURKO. *Contemporary Commercial Quantum Information Security Systems* [online]. Lviv: Lviv Polytechnic National University, 2013, NOVEMBER 2013 [cit. 2020-11-20]. Dostupné z: http://ena.lp.edu.ua:8080/bitstream/ntb/23756/1/27-74-77.pdf

[137] *IDQ* [online]. Genève: IDQ, 2020 [cit. 2020-11-19]. Dostupné z: https://www.idquantique.com

[138] Thales. *Thales Group* [online]. 2021, 2021 [cit. 2021-5-29]. Dostupné z: https://www.thalesgroup.com/en

[139] *TOSHIBA QKD* [online]. Cambridge Science Park: TOSHIBA CORPORATION, 2020 [cit. 2020-11-19]. Dostupné z: https://www.toshiba.co.jp/qkd/en/index.htm

[140] *Qubitekk* [online]. Vista: Qubitekk, 2016 [cit. 2020-11-19]. Dostupné z: http://qubitekk.com

[141] *MagiQ* [online]. Somerville: MagiQ [cit. 2020-11-19]. Dostupné z: https://www.magiqtech.com

[142] KERMIT, Lilly. Information Security: Methods and Practices in Classical and Quantum Regimes. In: *SlideServe* [online]. SlideServe, 2020 [cit. 2020-11-20]. Dostupné z: https://www.slideserve.com/kermit/information-security-powerpoint-ppt-presentation

[143] *QuintessenceLabs* [online]. Canberra: QuintessenceLabs, 2020 [cit. 2020-11-19]. Dostupné z: https://www.quintessencelabs.com

[144] *Qasky* [online]. Wuhu: Qasky [cit. 2020-11-19]. Dostupné z: http://www.qasky.com/en/

[145] *QuntumCTek* [online]. Hefei: QuntumCTek, 2017 [cit. 2020-11-19]. Dostupné z: http://www.quantum-info.com/English/#hero

[146] */KETS>* [online]. Bristol: |KETS>, 2019 [cit. 2020-11-19]. Dostupné z: https://kets-quantum.com/our-technology/

[147] *Russian Quantum Center* [online]. Moscow: Russian Quantum Center, 2020 [cit. 2020-11-19]. Dostupné z: https://rqc.ru

[148] *Qrate* [online]. Moscow: Russian Quantum Center [cit. 2020-11-19]. Dostupné z: https://goqrate.com

[149] *Quantum Xchange* [online]. Bethesda: Quantum Xchange, 2020 [cit. 2020-11-19]. Dostupné z: https://quantumxc.com

[150] *ADVA* [online]. Munich: ADVA, 2020 [cit. 2020-11-19]. Dostupné z: https://www.adva.com/en

[151] *Fortinet* [online]. Sunnyvale: Fortinet, 2020 [cit. 2020-11-19]. Dostupné z: https://www.fortinet.com

[152] MUGA, Nelson J., Mário F. S. FERREIRA a Armando N. PINTO. QBER Estimation in QKD Systems With Polarization Encoding. *Journal of Lightwave Technology* [online]. 2011, **29**(3), 355-361 [cit. 2020-12-10]. ISSN 0733-8724. Dostupné z: doi:10.1109/JLT.2010.2099643

[153] FILKA, Miloslav. *Přenosová média* [online]. Brno, 2011 [cit. 2020-12-09]. Dostupné z: https://optolab.utko.feec.vutbr.cz/wp-content/uploads/BPRM.pdf. Skripta. Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav telekomunikací.

[154] CWDM / DWDM CHANNELS. *Flextopix.net* [online]. [cit. 2021-5-27]. Dostupné z: https://www.flexoptix.net/en/dwdm-channels

[155] LDX-1550-1L: 1550nm, Turn-Key Ultra-Narrow < 10 kHz Linewidth Laser Diode Source Module. *Laser Diode Source* [online]. [cit. 2021-5-27]. Dostupné z: https://www.laserdiodesource.com/shop/1550nm-10mW-narrow-linewidth-module-denselight

[156] FWLF1632xx Datasheet by Finisar Corporation. *Digikey.com* [online]. [cit. 2021-5-28]. Dostupné z: https://www.digikey.com/htmldatasheets/production/2035728/0/0/1/fwlf1632xx-.html

[157] BHATIA, Vikram. Thin Film Filter. *Guided Wave Optical Components and Devices* [online]. ScienceDirect, 2006 [cit. 2021-5-28]. Dostupné z: https://www.sciencedirect.com/topics/engineering/thin-film-filter/pdf

[158] FC/APC Fiber Connectors: Single Mode. *Thorlabs.com* [online]. [cit. 2021-5-28]. Dostupné z: https://www.thorlabs.com/newgrouppage9.cfm?objectgroup_id=6246

[159] *G.657 (11/16)*. 2016-11-13. Geneva, Switzerland: ITU-T, 2016. Dostupné také z: https://www.itu.int/rec/T-REC-G.657-201611-I/en

[160] *G.652 (11/16)*. 2016-11-13. Geneva, Switzerland: ITU-T, 2016. Dostupné také z: https://www.itu.int/rec/T-REC-G.652-201611-I/en

[161] *Corning SMF-28 Ultra Optical Fiber*. NY, USA: Corning, 2014. Dostupné také z: https://www.corning.com/media/worldwide/coc/documents/Fiber/SMF-28%20Ultra.pdf

[162] Juniper Networks. *TechLibrary* [online]. 2021 [cit. 2021-5-29]. Dostupné z: https://www.juniper.net/documentation/us/en/software/junos/interfaces-ethernet/topics/topic-map/fec-ber-otn-interfaces.html#id-understanding-pre-fec-ber-monitoring-and-ber-thresholds

[163] AFL GLOBAL. *DWDM Single-channel OADM*. 8. 31. 2020. AFL Global, 2015. Dostupné také z: https://www.aflglobal.com/productlist/Product-Lines/Optical-Connectivity-Apparatus/DWDM-Single-Channel-OADM/doc/DWDM-Single-Channel-OADM.aspx

Seznam symbolů a zkratek

AES	Advanced Encryption Standard
API	Application Programming Interface
ASE	Amplified Spontaneous Emission
AWG	Arrayed Waveguide Grating
B92	Bennett roku 1992 (protokol)
BB	Topologie Bod-Bod
BB84	Bennett a Brassard roku 1984 (protokol)
BBM92	Bennett, Brassard a Mermin roku 1992 (protokol)
BER	Bit Error Rate
BSM	Bell-State Measurement
CHSH	Clauserova-Horneova-Shimonyho-Holtova nerovnost
CH00	DWDM kanál dle ITU-T
CM	Control Mode
CNOT	Controlled NOT
COM	TFF port Common
COW	Coherent One Way (protokol)
CV-B92	Continuous-Variable B92 (protokol)
CV-QKD	Continuous-Variable QKD
CWDM	Coarse Wavelength-Division Multiplexing
dB	Decibel
dBm	Decibel-miliwatt
DDI-QKD	Detector-Device-Independent QKD
DH	Diffieho-Hellmanův protokol
DI-QKD	Device-Independent QKD

(D)MUX	(De)multiplexor
DOS	Denial of Service
DPR	Distributed Phase-Reference
DPS	Differential Phase-Shift (protokol)
DTM	Deterministic Turing Machine
DV-QKD	Discrete-Variable QKD
DWDM	Dense Wavelength-Division Multiplexing
E91	Ekert roku 1991 (protokol)
EB	Entanglement-Based
ECPP	Encryption Control Protocol
eV	Elektronvolt
EM	Encryption Mode
EPR	Einstein, Podolsky a Rosen (paradox)
ETSI	European Telecommunications Standards Institute
FEC	Forward Error Correction
FWHM	Full Width At Half Maximum
GG02	Grosshans a Grangier roku 2002 (protokol)
G.657.A1	Kategorie optického vlákna dle ITU-T
G.652.D	Kategorie optického vlákna dle ITU-T
GA	Groverův algoritmus
Gbit, Gb	Gigabit
GHz	Gigahertz
H	Topologie Hvězda
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure

ID	Identifikátor
IKE	Internet Key Exchange
IPSec	Internet Protocol Security
ISO-OSI	International Organization for Standardization – Open Systems Interconnection (model)
ITU-T	Telecommunication Standardization Sector – Telecommunication Standardization Sector
J	Joule
K	Topologie Kruh
kbit, kb	Kilobit
kHz	Kilohertz
km	Kilometr
KM	Key Management
KMB09	Khan, Murphy a Beige roku 2009 (protokol)
KME	Key Management Entity
KMIP	Key Management Interoperability Protocol
L1-L7	Layer 1-7
LEA	Lightweight Encryption Algorithm
LM05	Lucamarini a Mancini roku 2005 (protokol)
MACSec	Medium Access Control Security
MDI-QKD	Measurement-Device-Independent QKD
MITM	Man-In-The-Middle (útok)
mW	Miliwatt
NIST	National Institute of Standards and Technology
nm	Nanometr
NRZ	Non Return To Zero (kódování)

ns	Nanosekunda
NTM	Nondeterministic Turing Machine
OADM	Optical Add-Drop Multiplexer
OTP	One-Time Pad
P, X	Kvadratury; P – hybnost, X - poloha
PASS	TFF port Passed
PC	Osobní počítač
PKI	Public Key Infrastructure
PM	Prepare-and-Measure
PNS	Photon-Number-Splitting
PP	Ping-Pong (protokol)
PPP	Point to Point Protocol
PQC	Post-Quantum Cryptography
PRNG	Pseudorandom Number Generator
pW	Pikowatt
QBER	Quantum-Bit Error Rate
QKD	Quantum Key Distribution
QKDE	Quantum Key Distribution Entity
QKDN	Quantum key distribution Network
QPN	Quantum Private Network
QRNG	Quantum Random Number Generator
QSC	Quantum-Safe Cryptography
QTM	Quantum Turing Machine
QVPN	Quantum Virtual Private Network
REF	TFF port Reflected

REST	Representational State Transfer
RQC	Russian Quantum Center
RSA	Rivestova-Shamirova-Adlemanova šifra
s	Sekunda
S13	Serna roku 2013 (protokol)
SAE	Secure Application Entity
SARG04	Scarani, Acin, Ribordy a Gisin roku 2004 (protokol)
SFP	Small Form-Factor Pluggable (Transceiver)
SK	Soukromý klíč
SMF-28	Single-Mode Fiber (vlákno, výrobce Corning)
SPDC	Spontaneous Parametric Down-Conversion
SPS	Single-Photon Source
SSH	Secure Shell
SSP	Six State protocol
T12	Toshiba roku 2012 (protokol)
TCP/IP	Transmission Control Protocol / Internet Protocol (model)
TDM	Time-Division Multiplexing
TFF	Thin Film Filter
TF-QKD	Twin-Field QKD
THz	Terahertz
TLS/SSL	Transport Layer Security / Secure Sockets Layer
TN	Trusted Node
TR/DO	Trusted Repeater / Důvěryhodný opakovač
TRNG	True Random Number Generator
U	Unit

VK	Veřejný klíč
VPN	Virtual Private Network
WCP	Weak Coherent Pulse
WDM	Wavelength-Division Multiplexing

Matematické veličiny

α	Koeficient α, nebo měrný útlum
β	Koeficient β
γ	Koeficient γ
δ	Koeficient δ
θ	Úhel θ definující Blochovu kouli
λ	Vlnová délka
μ	Průměrné množství fotonů na pulz
ν	Frekvence
$\sigma_I, \hat{I}$	Operace Identita
$\sigma_H, \hat{H}$	Hadamardova brána / operace
$\sigma_X, \hat{X}$	Pauliho X-brána / operace
$\sigma_Y, \hat{Y}$	Pauliho Y-brána / operace
$\sigma_Z, \hat{Z}$	Pauliho Z-brána / operace
φ	Úhel φ definující Blochovu kouli
a	Útlum kanálu
$\vec{B}$	Vektor magnetického pole
e	Eulerovo číslo
E	Energie
$\vec{E}$	Vektor elektrického pole
$f(x)$	Libovolná funkce
$g(x)$	Funkce inverzní k libovolné funkci $f(x)$
K_{AB}	Klíč sdílený mezi uzly A a B
l	Délka kanálu
P	Výkon

$p(x), P(X)$	Pravděpodobnost
T	Perioda
$\vec{v}$	Poyntingův vektor
v	Přenosová rychlost
x	Neznámá x, např. diskrétní množství fotonů na pulz
$\|\Psi\rangle$	Libovolný stav zapsaný pomocí KET vektoru
$\|\Phi^{\pm}\rangle, \|\Psi^{\pm}\rangle$	Bellovy stavy
$\oplus \otimes \odot$	Horizontálně-vertikální, diagonální a rotační báze

Seznam příloh

A Moduly simulace BB84 – polarizace

První příloha obsahuje parametry vybraných modulů protokolu BB84 s polarizačním kódováním. Detaily o nastavení je možné najít v přiloženém archivu.

Name	Value	Unit	Type
T12 DV QKD			
NumberOfSymbols	NumberOfSymbols		S
Signal	0.5		S
Decoy	0.044		S
Vacuum	0.001		S
p_S	0.9		S
p_D	0.07		S
p_V	0.03		S
p_Z	0.5		S
RandomNumberSeed	1		S

Obr. A.1: Parametry modulu *Generator_1* (u Alice).

Name	Value	Unit	Type
Coding			
PulseShape	sin4		S
BasisSet	XZ		S
Enhanced			
RandomNumberSeed	0		S
Physical			
SampleRate	SampleRateDefault	Hz	S
Laser_EmissionFrequency	193.1e12	Hz	S
Laser_Linewidth	3e4	Hz	S

Obr. A.2: Parametry modulu *Vysilac* (u Alice).

Name	Value	Unit	Type
General			
MarkProbability	0.5		S
NumberOfSymbols	NumberOfSymbols		S
RandomNumberSeed	1		S

Obr. A.3: Parametry modulu *Generator_2* (u Boba).

Name	Value	Unit	Type
General			
SampleRate	SampleRateDefault	Hz	S
SymbolRate	BitRateDefault	Hz	S
TCSPC_GateOpeningTime	0.1	sym...	S
TCSPC_GateClosingTime	0.4	sym...	S
Enhanced			
SPCM0_RandomNumber...	0		S
SPCM1_RandomNumber...	0		S
Physical			
SPCM_DeadTime	1e-7	s	S
SPCM_DarkCountRate	2000	Hz	S
SPCM_TimingJitterStdev	1e-10	s	S
SPCM_TimingJitterExpo...	0.01		S
SPCM_TimingJitterExpo...	50e-12	s	S
SPCM_AfterPulsingProb...	0.02		S
SPCM_AfterPulsingTime...	1e-7	s	S
Coding			
BasisSet	XZ		S

Obr. A.4: Parametry modulu *Prijimac* (u Boba).

B Moduly simulace BB84 – fáze

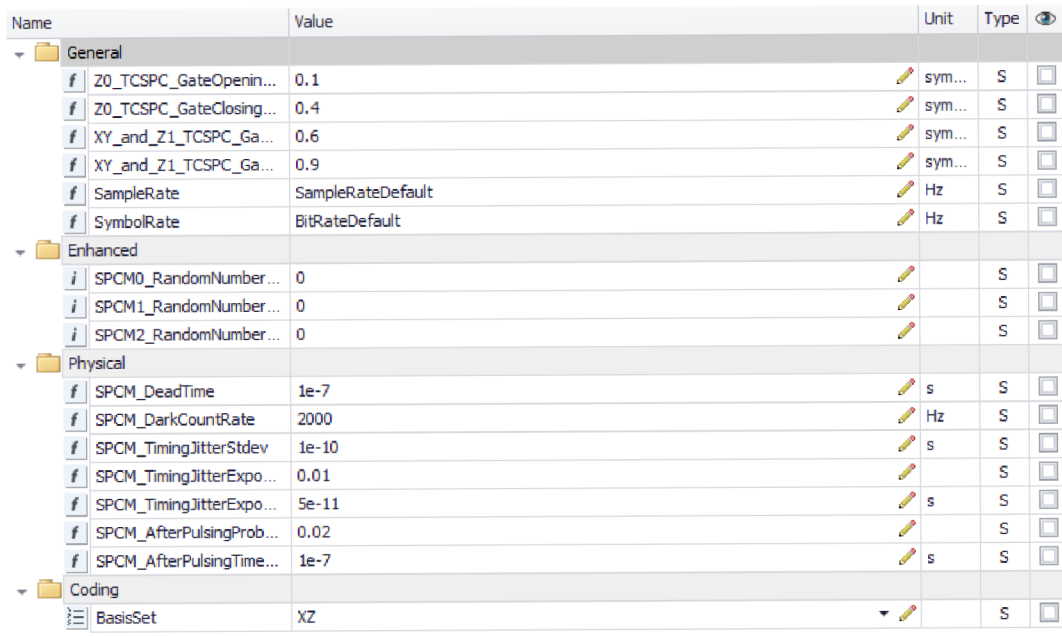
Druhá příloha obsahuje parametry vybraných modulů protokolu BB84 s fázovým kódováním. Detaily o nastavení je možné najít v přiloženém archivu.

Name	Value	Unit	Type
T12 DV QKD			
NumberOfSymbols	NumberOfSymbols		S
Signal	0.5		S
Decoy	0.044		S
Vacuum	0.001		S
p_S	0.9		S
p_D	0.07		S
p_V	0.03		S
p_Z	0.5		S
RandomNumberSeed	1		S

Obr. B.1: Parametry modulu *Generator_1* (u Alice).

Name	Value	Unit	Type
Coding			
PulseShape	sin4		S
BasisSet	XZ		S
Enhanced			
RandomNumberSeed	0		S
Physical			
SampleRate	SampleRateDefault	Hz	S
Laser_EmissionFrequency	193.1e12	Hz	S
Laser_Linewidth	3e4	Hz	S

Obr. B.2: Parametry modulu *Vysilac* (u Alice).



Name	Value	Unit	Type
General			
Z0_TCSPC_GateOpenin...	0.1	sym...	S
Z0_TCSPC_GateClosing...	0.4	sym...	S
XY_and_Z1_TCSPC_Ga...	0.6	sym...	S
XY_and_Z1_TCSPC_Ga...	0.9	sym...	S
SampleRate	SampleRateDefault	Hz	S
SymbolRate	BitRateDefault	Hz	S
Enhanced			
SPCM0_RandomNumber...	0		S
SPCM1_RandomNumber...	0		S
SPCM2_RandomNumber...	0		S
Physical			
SPCM_DeadTime	1e-7	s	S
SPCM_DarkCountRate	2000	Hz	S
SPCM_TimingJitterStdev	1e-10	s	S
SPCM_TimingJitterExpo...	0.01		S
SPCM_TimingJitterExpo...	5e-11	s	S
SPCM_AfterPulsingProb...	0.02		S
SPCM_AfterPulsingTime...	1e-7	s	S
Coding			
BasisSet	XZ		S

Obr. B.3: Parametry modulu *Prijimac* (u Boba).

C Moduly simulace T12 – fáze

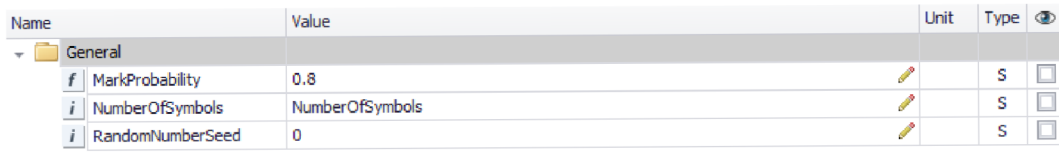
Třetí příloha obsahuje parametry vybraných modulů protokolu T12 s fázovým kódováním. Detaily o nastavení je možné najít v přiloženém archivu.

Name	Value	Unit	Type
T12 DV QKD			
NumberOfSymbols	NumberOfSymbols		S
Signal	0.425		S
Decoy	0.044		S
Vacuum	0.001		S
p_S	1 - p_D - p_V		S
p_D	1/128		S
p_V	1/256		S
p_Z	0.8		S
RandomNumberSeed	1		S

Obr. C.1: Parametry modulu *Generator_1* (u Alice).

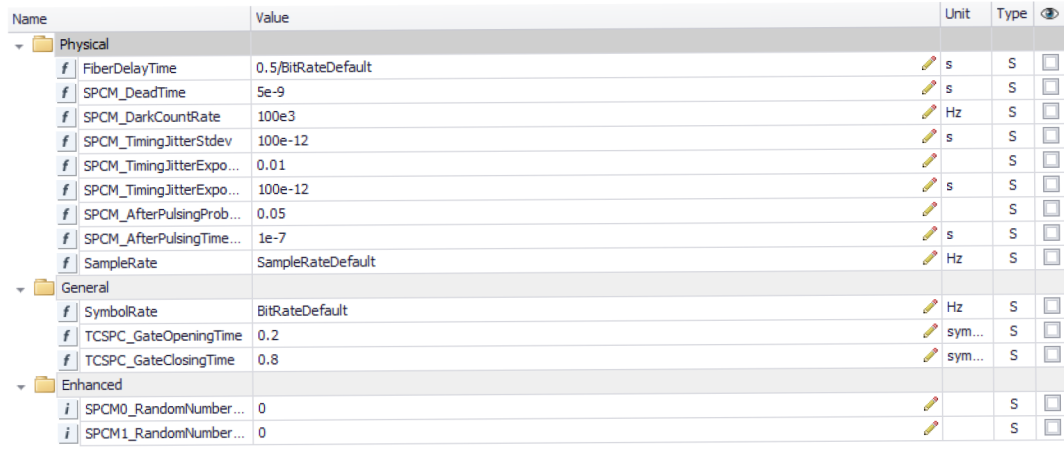
Name	Value	Unit	Type
Coding			
PulseShape	sin4		S
Enhanced			
RandomNumberSeed	0		S
Physical			
SampleRate	SampleRateDefault	Hz	S
Laser_EmissionFrequency	193.1e12	Hz	S
Laser_Linewidth	3e4	Hz	S
FiberDelayTime	0.5/BitRateDefault	s	S

Obr. C.2: Parametry modulu *Vysilac* (u Alice).



Name	Value	Unit	Type
General			
MarkProbability	0.8		S
NumberOfSymbols	NumberOfSymbols		S
RandomNumberSeed	0		S

Obr. C.3: Parametry modulu *Generator_2* (u Boba).



Name	Value	Unit	Type
Physical			
FiberDelayTime	0.5/BitRateDefault	s	S
SPCM_DeadTime	5e-9	s	S
SPCM_DarkCountRate	100e3	Hz	S
SPCM_TimingJitterStdev	100e-12	s	S
SPCM_TimingJitterExpo...	0.01		S
SPCM_TimingJitterExpo...	100e-12	s	S
SPCM_AfterPulsingProb...	0.05		S
SPCM_AfterPulsingTime...	1e-7	s	S
SampleRate	SampleRateDefault	Hz	S
General			
SymbolRate	BitRateDefault	Hz	S
TCSPC_GateOpeningTime	0.2	sym...	S
TCSPC_GateClosingTime	0.8	sym...	S
Enhanced			
SPCM0_RandomNumber...	0		S
SPCM1_RandomNumber...	0		S

Obr. C.4: Parametry modulu *Prijimac* (u Boba).

D Obsah přiloženého archivu

Přiložený archiv obsahuje modely využité v simulacích popsaných výše. Kořenová složka obsahuje tři adresáře s porovnávanými protokoly a složku s testovacím polygonem. V případě protokolů, se v každé složce vyskytují následující tři typy souborů.

- **Protokol_kódování.vtmu** – obsahuje základní model s nastaveními.
- **Protokol_kódování.vsw** – obsahuje nastavení simulace (délku kanálu).
- **Protokol_kódování.vpa** – obsahuje nastavený graf, tedy výsledek simulace.

Struktura odevzdaných souborů

- `VPI_modely` – Kořenový adresář přiloženého archivu
  - `BB84_faze` – **Protokol BB84 – fáze**
    - `BB84_faze.vtmu_pack`
      - `Outputs`
        - `BB84_faze.vpa` – Soubor s grafem
      - `Resources`
        - `Spustit.vsw` – Spustitelný soubor
    - `BB84_faze.vtmu` – Model BB84 – fáze
  - `BB84_polarizace` – **Protokol BB84 – polarizace**
    - `BB84_polarizace.vtmu_pack`
      - `Outputs`
        - `BB84_polarizace.vpa` – Soubor s grafem
      - `Resources`
        - `Spustit.vsw` – Spustitelný soubor
    - `BB84_polarizace_alfa=0.vtmu_pack`
      - `Outputs`
        - `BB84_polarizace.vpa` – Soubor s grafem
      - `Resources`
        - `Spustit.vsw` – Spustitelný soubor
    - `BB84_polarizace_eva.vtmu_pack`
      - `Outputs`
        - `BB84_polarizace.vpa` – Soubor s grafem
      - `Resources`
        - `Spustit.vsw` – Spustitelný soubor
    - `BB84_polarizace.vtmu` – Model BB84 – polarizace
    - `BB84_polarizace_alfa=0.vtmu` – Model vedlejší parametry
    - `BB84_polarizace_eva.vtmu` – Model odposlech
  - `T12_faze` – **Protokol T12 – fáze**
    - `T12_faze.vtmu_pack`
      - `Outputs`
        - `T12_faze.vpa` – Soubor s grafem
      - `Resources`
        - `Spustit.vsw` – Spustitelný soubor
    - `T12_faze.vtmu` – Model T12 – fáze

Ve složce **Testovaci_QKD_Polygon** se nacházejí dvě vymodelované topologie. Obsah jim příslušných složek nebude z důvodu velkého množství souborů v příloze dále rozepisován.

- **QKD_Polygon.vtmu** – obsahuje topologii vymodelovaného polygonu.
- **Gaussuv_Filtr.vtmu** – obsahuje vymodelovaný Gaussův filtr.

```
VPI_modely ..... Kořenový adresář přiloženého archivu
└── Testovaci_QKD_Polygon ..... QKD Polygon
    ├── QKD_Polygon.vtmu ..... Polygon
    ├── QKD_Polygon.vtmu_pack ..... Adresář s dalšími soubory
    ├── Gaussuv_filtr.vtmu ..... Gaussův filtr
    └── Gaussuv_Filtr.vtmu_pack ..... Adresář s dalšími soubory
```

Simulace byly provedeny v programu *VPI Photonics* verze 11.0 x64 (Build 736). Konkrétně byly využity nástroje *VPI Transmission Maker Optical Systems 11.0* a *VPI Toolkit QKD 1.6*.