VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA INFORMAČNÍCH TECHNOLOGIÍ
FACULTY OF INFORMATION TECHNOLOGY

ÚSTAV POČÍTAČOVÉ GRAFIKY A MULTIMÉDIÍ
DEPARTMENT OF COMPUTER GRAPHICS AND MULTIMEDIA

KVANTOVÁ KRYPTOGRAFIE A LASEROVÉ PŘENOSY DAT

QUANTUM CRYPTOGRAPHY AND LASER DATA TRANSFERS

DIPLOMOVÁ PRÁCE
MASTER'S THESIS

AUTOR PRÁCE **Bc. MARTIN LITWORA**
AUTHOR

VEDOUCÍ PRÁCE **prof. Dr. Ing. PAVEL ZEMČÍK, dr. h. c.**
SUPERVISOR

BRNO 2023

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA INFORMAČNÍCH TECHNOLOGIÍ

Zadání diplomové práce

147256

Ústav:	Ústav počítačové grafiky a multimédií (UPGM)
Student:	**Litwora Martin, Bc.**
Program:	Informační technologie a umělá inteligence
Specializace:	Kybernetická bezpečnost
Název:	**Kvantová kryptografie a laserové přenosy dat**
Kategorie:	Bezpečnost
Akademický rok:	2022/23

Zadání:

1. Nastudujte dostupnou literaturu a existující řešení na téma kvantová kryptografie a kvantově zabezpečené přenosy dat jak po vláknových optických spojích, tak i "bezvláknových" laserových spojích.
2. Změřte přenosové rychlosti kvanotvě zabezpečené informace i standardních dat za různých atmosférických podmínek (a počasí) na vhodném laserovém "bezvláknovém" spoji, případně přenosové rychlosti změřte na vhodném vláknovém spoji (například mezi FEKT a FIT) a změnu atmosférických podmínek simulujte vhodným útlumovýcm článkem.
3. Na základě zjištěných vlastnosti spojů navrhněte vhodné šifrování pro různé aplikace a platformy (včetně embedded systémů) tak, aby bylo šifrování jak odolné proti "prolomení", tak i efektivní z pohledu spotřeby výpočetního výkonu a energie.
4. Popište dosažitelné vlastnosti navrženého šifrování a možné zlepšení oproti "state of the art".
5. Diskutuje dosažené výsledky a možnsoti pokračování práce.

Literatura:
Dle pokynu vedoucího a konzultantů.

Při obhajobě semestrální části projektu je požadováno:
Bod 1 zadání

Podrobné závazné pokyny pro vypracování práce viz https://www.fit.vut.cz/study/theses/

Vedoucí práce:	**Zemčík Pavel, prof. Dr. Ing., dr. h. c.**
Vedoucí ústavu:	Černocký Jan, prof. Dr. Ing.
Datum zadání:	1.11.2022
Termín pro odevzdání:	17.5.2023
Datum schválení:	3.11.2022

Abstrakt

Záměrem této práce bylo prozkoumat a popsat možnosti kvantové distribuce klíčů. Popsat jednotlivé protokoly založené na kvantové mechanice, různé varianty kvantových kanálů bezdrátových laserových spojení. Současně provést analýzu jednotlivých šifrovacích algoritmů z pohledu jejich bezpečnosti, spotřeby energie a rychlosti šifrování. Dále bylo součástí práce změření přenosových vlastností reálného systému pro kvantovou distribuci klíčů, včetně měření útlumu daného spoje pomocí útlumového článku. Cílem následně bylo aplikovat tyto výsledky měření na laserové přenosy dat. Laserové spojení ovlivňují atmosférické podmínky, zejména oblačnost. Pro tyto účely byl vytvořen simulační nástroj, který slouží pro simulaci laserových kvantových kanálů v atmosféře.

Abstract

The purpose of this work was to explore and describe the possibilities of quantum key distribution. Describe individual protocols based on quantum mechanics, and different variants of quantum channels of wireless laser connections. At the same time, analyze individual encryption algorithms from the point of view of their security, energy consumption and encryption speed. Furthermore, part of the work included measuring the transfer properties of a real system for the quantum key distribution, including measuring the attenuation of a given connection using an attenuation cell. The goal then was to apply the measurement results to laser data transfers. Laser connections are affected by atmospheric conditions, especially cloud cover. For these purposes, a simulation tool was created that serves to simulate laser quantum channels in the atmosphere.

Klíčová slova

kvantová distribuce klíčů. QKD systémy, laserové přenosy dat, šifrovací algoritmy, parametry přenosu kvantových kanálů, simulace laserových spojení, atmosférické podmínky

Keywords

quantum key distribution. QKD systems, laser data transfers, encryption algorithms, transmission parameters of quantum channel, simulation of laser data transfers, atmospheric conditions

Citace

LITWORA, Martin. *KVANTOVÁ KRYPTOGRAFIE A LASEROVÉ PŘENOSY DAT.* Brno, 2023. Diplomová práce. Vysoké učení technické v Brně, Fakulta informačních technologií. Vedoucí práce prof. Dr. Ing. Pavel Zemčík, dr. h. c.

KVANTOVÁ KRYPTOGRAFIE A LASEROVÉ PŘENOSY DAT

Prohlášení

Prohlašuji, že jsem tuto diplomovou práci vypracoval samostatně pod vedením pana prof. Dr. Ing. Pavla Zemčíka. Další informace mi poskytl doc. Ing. Jan Hajný, Ph.D. Uvedl jsem všechny literární prameny, publikace a další zdroje, ze kterých jsem čerpal.

.....
Martin Litwora
16. května 2023

Poděkování

Chtěl bych poděkovat své rodině, přátelům a všem, kteří mě během vypracování této práce a studia podporovali. Dále prof. Dr. Ing. Pavlu Zemčíkovi za dohled a pomoc při vypracování. V neposlední řadě kamarádce Anežce Pelantové za odbornou korekturu a finální doladění práce.

Obsah

Kapitola 1

Úvod

Kvantová kryptografie je způsob, kterým lze generovat kryptografické klíče a přenášet je kanálem, u něhož je bezpečnost založena na principech kvantové mechaniky, jako je například Heisenbergův princip neurčitosti nebo nemožnost kvantového klonování. Tyto kvantové kanály mohou být realizovány buď optickým kabelem, nebo bezdrátovým laserovým spojem. První varianta trpí na vysoce rostoucí útlum kanálu se zvyšující se délkou spoje. Bezdrátové přenosy pomocí laserů jsou alternativa, která umožňuje komunikaci na dlouhé vzdálenosti. Laserové paprsky jsou ovšem snadno ovlivnitelné aktuálními atmosférickými podmínkami, jež mohou kvalitu daného kvantového kanálu výrazně měnit. Záměrem této práce je simulovat laserové přenosy kvantově zabezpečených dat v prostředí ovlivněném počasím.

V současnosti je šifrování založeno na utajeném kryptografickém klíči, který speciální algoritmy používají pro šifrování zpráv na internetu. Asymetrická kryptografie je založena na složitých matematických výpočtech, je ale neefektivní a zranitelná vůči kvantovým počítačům v budoucnu. Naproti tomu symetrická kryptografie je rychlejší a méně složitá. Její nedostatek tkví v problémové distribuci stejného klíče mezi komunikujícími stranami. Řešením této situace může být kvantová distribuce klíčů, která zajistí spolehlivou a bezpečnou výměnu kryptografických klíčů. Bezpečnost je dána fyzikálními vlastnostmi kvantové mechaniky. Tyto QKD systémy mohou mít vícero podob. Zajímavé jsou bezdrátové přenosy pomocí laserů, které jsou však velice ovlivněny aktuálním stavem počasí, zejména oblačností.

Cílem této práce je zdokumentovat jednotlivé protokoly, které se mohou použít pro kvantovou distribuci klíčů. Dále popsat různé topologie kvantových systémů. Především se tato práce zaměřuje na využití laserových přenosů u kvantově zabezpečených dat. Pro zjištění přenosových vlastností je součástí práce také provedení měření nad kabelovým kvantovým kanálem. Do kanálu je dále připojen útlumový článek. Výsledky měření jsou poté využity k simulování laserových přenosů v proměnných atmosférických podmínkách.

V následující kapitole 2 jsou v úvodu popsány základy kvantové fyziky, které jsou nutné pro pochopení fungování jednotlivých protokolů kvantové distribuce klíčů zmíněné dále. Kapitola 3 shrnuje topologie QKD systémů, různé přenosové kvantové kanály, včetně popisu QKD systému na univerzitě VUT v Brně. Kapitola 4 se věnuje šifrovacím algoritmům s důrazem na symetrickou kryptografii, kterou kvantově generované klíče mohou použít pro šifrování. Následuje kapitola 5 se zhodnocením aktuálního stavu a návrhu řešení. Další kapitola 6 se věnuje analýze vybraných symetrických algoritmů z hlediska bezpečnosti, spotřeby elektrické energie a rychlosti šifrování. Kapitola 7 popisuje měření vlastností daného kvantového kanálu. Závěrečná kapitola 8 shrnuje implementaci simulačního nástroje a výsledky simulace pro laserové přenosy ovlivněné během dne různou oblačností.

Kapitola 2

Teorie Kvantové kryptografie

Tato kapitola se zabývá úvodem do kvantové kryptografie. Na začátku je zmíněna teorie kvantové fyziky a mechaniky nutná pro pochopení problematiky protokolů používaných pro kvantovou distribuci klíčů. Dále jsou zmíněny klasické protokoly založené na polarizaci fotonů či na kvantovém provázání částic a protokoly distribuované fázové reference. Tyto protokoly popisují způsob distribuce zabezpečených klíčů po kvantových kanálech. Velký důraz je kladen na protokol COW, který je i jedním z důležitých prvků této práce. U tohoto protokolu jsou také zmíněné různé typy útoků, které se mohou v kvantové kryptografii objevit, a to, jaká proti nim existují opatření. Seznam protokolů zmíněných v této kapitole není výčtem všech existujících. Jedná se pouze o ty nejvíce známé a používané pro kvantovou distribuci klíčů.

2.1 Základy kvantové fyziky a kryptografie

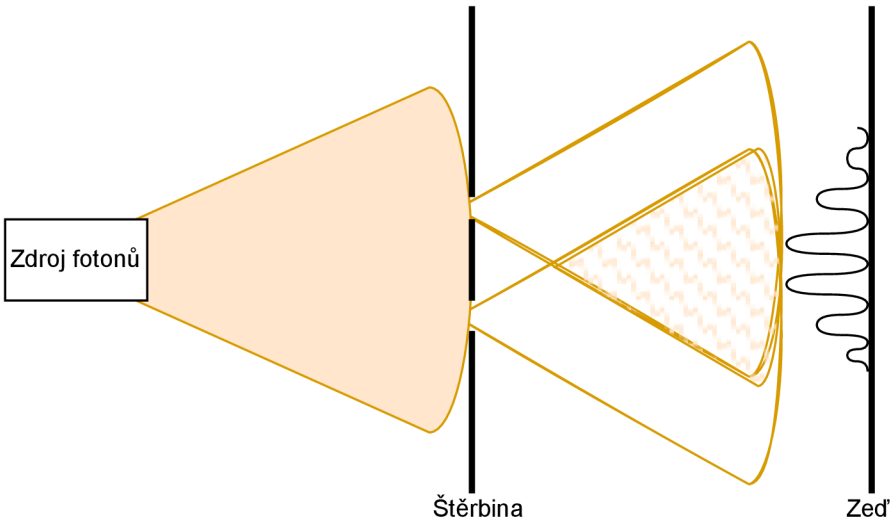
Tato sekce obsahuje základní teorii kvantové fyziky nutnou k pochopení protokolů, jež se používají pro distribuci klíčů po kvantově zabezpečeném kanále. Teorie zmíněná v této práci vychází z Kodaňské interpretace kvantové mechaniky. Jedná se o nejznámější a nejpoužívanější interpretaci kvantové mechaniky. Podle Kodaňské interpretace se kvantový systém vyvíjí v čase v závislosti na Schrödingerově rovnici. Kodaňská interpretace není deterministická a nelze se stoprocentní jistotou říct, že je pravdivá. Existují i jiné interpretace či nesouhlasné názory (vč. Alberta Einsteina) [53]. Ostatní interpretace jsou nad rámec této práce.

2.1.1 Heisenbergův princip neurčitosti

Světlo jakožto částice je možné popsat dvěma způsoby. Buď jako vlnu, nebo jako částici. V kvantové mechanice to lze obecně aplikovat na jakoukoliv elementární částici. Tomu se říká dualita částice a vlnění [86].

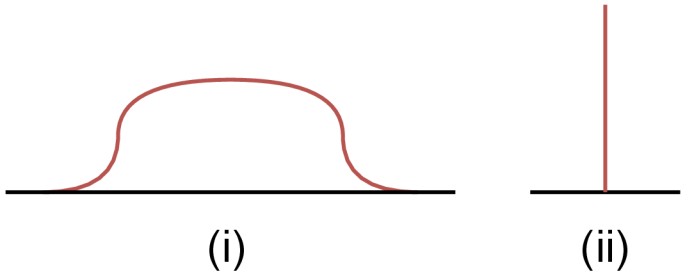
Youngův experiment je fyzikální pokus, při němž bylo v roce 1801 dokázáno, že světlo je vlnění. Zobrazení experimentu je na obrázku 2.1. Světlo prochází dvěma malými štěrbinami a vytváří interferenční obrazec. Pokud bychom posílali fotony na štěrbinu jeden za druhým, vznikal by interferenční obrazec, jako by foton procházel oběma štěrbinami zároveň (vlnění). Pokud se během experimentu pokusíme zjistit, kterou z obou štěrbin foton prošel, začne se chovat jako částice a k interferenci nedojde [86].

Elementární částice lze popsat kanonicky konjugovanými veličinami, a to polohou a hybností. Heisenbergův princip neurčitosti byl představen v roce 1927 německým fyzikem Wer-



Obrázek 2.1: Youngův experiment

nerem Heisenbergem. Ten tvrdí, že čím přesněji změříme polohu dané částice, tím méně přesné bude změření její hybnosti (informace o hybnosti je více neurčitá) a naopak [129]. Jinými slovy, čím více se pokusíme změřit polohu vlny, tím více narušíme informace o její hybnosti (vlnové délce). Tento přechod se označuje jako kolaps vlnové funkce. To se využívá u protokolu BB84 2.2.1. Kolaps vlnové funkce je zobrazen na obrázku 2.2. Ve chvíli, kdy



Obrázek 2.2: Tvar vlnové funkce u částice před měřením polohy (i) a po změření (ii)[1]

se částice pohybuje (i), nejsme schopni přesně určit její polohu. Známe pouze její vlnovou funkci. Můžeme určit jen to, že se daná částice nachází v určité oblasti. Pokud se pokusíme elementární částici změřit (ii), dojde ke kolapsu a vlnová funkce se změní. Je vidět, že z (ii) jsme schopni určit polohu daleko přesněji, ale ztratili jsme informace o její hybnosti [129, 57]. Obecně lze říci, že samotným měřením zanášíme do systému chybu.

2.1.2 Nemožnost klonování

Teorém o nemožnosti klonování kvantového stavu nepřímo vychází z Heisenbergova principu neurčitosti. V podstatě se jedná o rozvinutí myšlenky, jež tvrdí, že sestrojit měřicí zařízení, které by nenarušilo kvantový systém, není možné. Bez změření daného stavu nelze

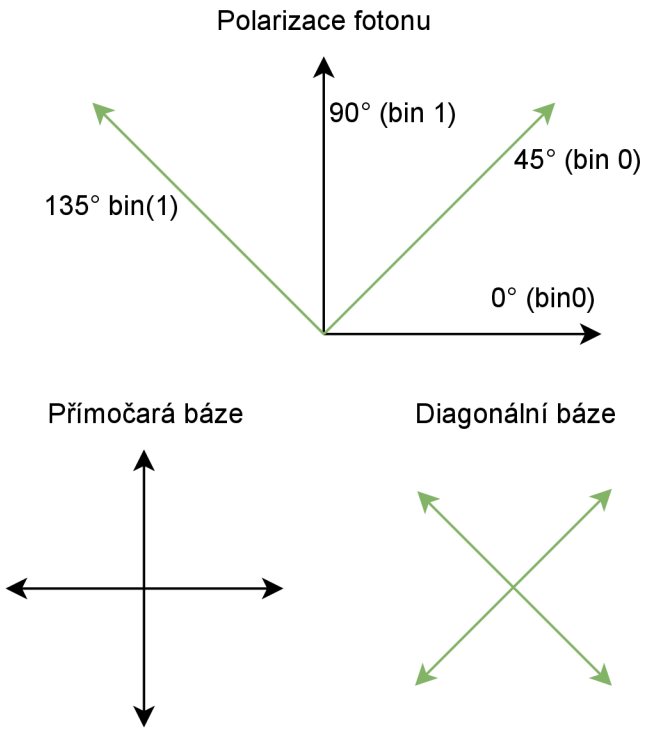
[1] Obrázek je inspirován podobným obrázkem v bakalářské práci [57].

vytvořit jeho kopii. Tento teorém nám tedy říká, že je nemožné vytvořit identickou kopii kvantového stavu (např. qubitu) [130]. Na tomto faktu je založena myšlenka kvantové bezpečnosti, podle které jsme při odposlechnu schopni odhalit přítomnost útočníka. S tím souvisí teorém o nemožnosti teleportace, který tvrdí, že je nemožné převést kvantový stav na hodnoty klasických bitů, přenést tyto bity na jiné místo nebo vytvořit na novém místě kopii originálního kvantového stavu.

2.1.3 Qubity a polarizace

V kvantovém systému se nejčastěji používá polarizace fotonu pro uchování informace. Fotonem se obecně rozumí libovolná částice popisující kvantum elektromagnetického záření (vlnění). Nejčastěji se používá infračervené světlo, které má vlnovou délku 700 nm – 1 mm a frekvenci 300 GHz – 430 THz. Elektromagnetické vlnění se skládá z vektoru elektrického pole a z vektoru magnetického pole. Tyto vektory jsou na sebe navzájem kolmé. Směr šíření je dán Poyntingovým vektorem. Polarizovaný foton osciluje pouze v jedné složce vlnění (v jedné rovině) [19, 45].

Polarizovat foton můžeme buď lineárně, nebo elipticky. U QKD systémů se používá lineární polarizace. Ta může být dvojího druhu, a to přímočará nebo diagonální. Těmto typům se říká polarizační báze. Obě opět mohou nabývat dvou stavů. Přímočará báze může být buď horizontální (značeno →), nebo svislá (značeno ↑). Horizontální (vodorovná) představuje hodnotu 0, zatímco svislá hodnotu 1. Diagonální báze může být buď pozitivně diagonální (značeno ↗) reprezentující hodnotu 0, nebo negativně diagonální (značeno ↘) reprezentující hodnotu 1 [19, 45]. Tyto báze jsou znázorněny na obrázku 2.3.



Obrázek 2.3: Lineární polarizace fotonů

2.1.4 Kvantové provázání

Kvantové provázání (angl. Quantum Entanglement) je jev, u něhož se při vzniku dvou fotonů tyto fotony navzájem provážou do tzv. Bellova stavu [15, 125]. V tomto stavu není možné jednotlivé fotony od sebe odlišit, a to ani v případě, že jsou od sebe fotony odděleny velkou vzdáleností. Měření jedné částice ovlivní měření druhé částice. Kompletním změřením dojde ke kolapsu vlnové funkce a oba fotony přestanou být provázané .

Pro následující nastínění situace či uvedení do problematiky se používá dvojice Alice a Bob, v níž je Alice odesílatelem a Bob příjemcem. V případě, že obě strany komunikace (Alice i Bob) obdrží jeden foton, jsou tyto fotony navzájem provázané. V momentě, kdy je Alice fotonu blíž, změří jeho stav jako první. Pokud by měl tento qubit hodnotu 1 při změření, pak druhý qubit automaticky zkolabuje do opačného stavu, tedy do hodnoty 0. Jedná se o tzv. maximální antikorelaci. Tento jev je součástí kvantové fyziky a nemá obdobu v klasické fyzice [15, 125].

Zajímavá situace nastává v momentě, kdy jsou oba detektory (tedy Alice a Bob) stejně vzdálené od zdroje provázaných částic. Podle teorie relativity neexistuje větší rychlost než rychlost světla. Pokud by došlo k měření ve stejnou chvíli, musel by existovat nějaký nadsvětelný (okamžitý) způsob komunikace mezi fotony. Jinak by totiž nevěděly, do jakých stavů mají zkolabovat. Einstein se to snažil vysvětlit pomocí tzv. EPR (Einstein–Podolsky–Rosen) paradoxu [15, 125]. V podstatě se jev snažil objasnit tím, že provázané fotony by se musely předem domluvit na tom, do jakých stavů zkolabují. Tuto informaci si uchovávají částice v nějakých „skrytých proměnných“. Einstein se tak snažil přijít s vysvětlením kvantové fyziky, která tvrdí, že propletené částice se nachází v obou stavech zároveň [15, 125].

Odpověď přinesl roku 1964 severoirský fyzik J. S. Bell, který představil matematickou nerovnost, jež dala za pravdě kvantové fyzice. Pomocí tzv. Bellových testů se povedlo vyvrátit existenci „skrytých proměnných“ uvnitř částic [57]. Jak se fotony navzájem ovlivní, závisí na úhlu měření na detektorech. Když budou oba detektory fotonů v úhlu 0°, dojde vždy k antikorelaci, tzn. že jeden foton bude změřen jako 0 a druhý 1. Pokud jsou oba pootočeny o 180°, dojde k maximální korelaci a výsledky obou měření budou shodné. Pokud jsou pootočeny o 90°, korelace bude nulová a měření na jednom z detektorů neovlivní zbytek (je 50% šance na daný stav). U Bellových testů se provádí měření v neklasických úhlech (např. 45°, 135° atd.). Podle kvantové fyziky se ale pravděpodobnost nebude měnit lineárně, ale podle sinusové vlny. Pro 45° tak bude např. pravděpodobnost opačných výsledků asi 84,4 % namísto 75 %. Dosud všechny provedené Bellovy testy naznačují, že kvantové provázaní nelze popsat „skrytými proměnnými“. V současnosti je kvantové provázání stále otevřené a neprobádané zákoutí kvantové fyziky [15, 125, 57]. Na kvantovém provázání je postaven protokol E91 pro kvantovou distribuci klíčů.

2.2 Protokoly diskrétní proměnné

Protokoly diskrétní proměnné (angl. Discrete Variable – DV) jsou první protokoly, které byly navrženy pro kvantovou distribuci klíčů. Informaci kódují do polarizace jednoho fotonu. Jejich bezpečnost je založena na Heisenbergově principu neurčitosti. Řada těchto protokolů je založena na nějaké variaci prvního BB84 protokolu [57]. Původní návrhy protokolů jsou náročné na praktickou implementaci z důvodu obtížné realizace jednofotonových generátorů. Proto některé protokoly mohou podporovat variantu posílání pulsů o malém počtů fotonů [57]. Seznam protokolů není kompletní, jsou zde zmíněné jen ty nejznámější. Dále existuje řada dalších, např. třístavový kvantový protokol nebo KMB09.

Alternativou jsou CV protokoly (se spojitou proměnnou), které používají pulsy o větším množství fotonů. Informace je kódována do amplitudy a fáze daného pulsu. K přenosu se používají lasery generující koherentní pulsy spolu s homodynními detektory. Tyto protokoly nejsou v současnosti tolik rozšířené, ale jeví se jako lepší volba v případě kvantových kanálů vedených k satelitům ve vesmíru. Příkladem těchto protokolů je např. CV varianta B92 nebo GG02 [59].

2.2.1 BB84

Jedná se o první protokol pro kvantovou distribuci klíčů. Vytvořili ho v roce 1984 Charles Bennett a Gilles Brassard. Protokol využívá polarizaci fotonů, jak bylo nastíněno v předešlé části 2.1.3. Patří do rodiny tzv. příprav a změř (angl. Prepare-And-Measure) protokolů [57]. Nachází se zde dva uzly, Alice a Bob, které mezi sebou chtějí vytvořit kvantově zabezpečený klíč. Alice je odesílatelem. Náhodně generuje sekvenci bitů 0 a 1. Ty zakóduje pomocí náhodně zvolené buď přímočaré, nebo diagonální báze. Jednotlivé fotony následně posílá Bobovi [19, 81].

Bob pro každý z přijímaných fotonů náhodně volí bázi, ve které se pokusí daný foton změřit. Pokud Bob zvolí stejnou bázi pro daný foton jako zvolila Alice, dostane vždy správnou hodnotu bitu. Pokud zvolí opačnou bázi, dostane správnou hodnou pouze s 50% úspěšností [19]. Reálně se používají 4 analyzátory ($\rightarrow$, $\uparrow$, $\nearrow$ a $\searrow$), v nichž foton pro náhodně zvolenou bázi projde děličem svazků do dvou analyzátorů. Například Alice zašle bit 0 v přímočaré bázi ($\rightarrow$). Pokud Bob náhodně zvolí stejnou bázi, foton se dostane k jednomu z analyzátorů (má 100% šanci, že projde skrz ($\rightarrow$) a 0%, že projde skrz ($\uparrow$). Pokud zvolí opačnou bázi (diagonální v tomto případě), pak je 50% šance, že foton projde skrz jeden z analyzátorů ($\nearrow$, $\searrow$) [19, 81].

Bob ale netuší, které bity naměřil správně. Proto po veřejném kanálu zašle Alici pořadí jednotlivých bází [19]. Ta si poznačí, jak Bob měřil, a zašle mu zpětně pořadí měření, v nichž použil správnou bázi. Špatně změřené bity si oba odstraní. Příklad této komunikace je vidět v následující tabulce 2.1, znak $\oplus$ představuje přímočarou bázi, $\otimes$ pak diagonální bázi.

Eva, neboli útočník snažící se odposlouchávat, nezná báze, v nichž Alice posílá fotony. Díky teorému o nemožnosti klonování si nemůže vytvořit kopii qubitu [19, 57]. Zároveň podle Heisenbergova principu neurčitosti nemůže daný qubit změřit, aniž by zanesla chybu do původního fotonu. Musí tedy nutně náhodně volit báze podobně jako Bob a pokusit se je měřit [81]. Netuší ovšem, zda je její měření úspěšné. Bobovi proto následně zašle fotony, u kterých musí náhodně volit polarizaci fotonu. Tím nevyhnutelně zanese do systému chyby a dojde k jejímu odhalení. Čistě na základě pravděpodobnosti, pokud Eva změří n fotonů

Náhodný řetězec bitů	1	0	1	1	0	0	1
Báze zvolená Alicí	$\oplus$	$\oplus$	$\otimes$	$\oplus$	$\otimes$	$\otimes$	$\otimes$
Polarizace zvolená Alicí	$\uparrow$	$\rightarrow$	$\searrow$	$\uparrow$	$\nearrow$	$\nearrow$	$\searrow$
Bobem náhodně zvolená báze	$\oplus$	$\otimes$	$\otimes$	$\oplus$	$\oplus$	$\otimes$	$\oplus$
Bobem změřené bity	1	1	1	1	1	0	0
Schválené bity	1	-	1	1	-	0	-
Náhodně zvolené bity pro kontrolu	-	-	-	1 (✓)	-	-	-
Finální řetězec	1	-	1	-	-	0	-

Tabulka 2.1: Tabulka s ukázkovými hodnotami během přenosu kvantově zabezpečeného klíče protokolem BB84

a zašle vlastní vygenerované, neodhalena zůstane v jednom ze $(3/4)^n$ případů. Pro $n = 10$ je tato pravděpodobnost 0,0563 % [81]. Bob s Alicí v rámci amplifikace bezpečnosti odhalí několik konkrétních bitů a porovnají je mezi sebou. Tyto bity se později zahodí a nejsou použity v ustanoveném klíči. Pokud by tyto bity byly odlišné, je pravděpodobné, že kanál byl odposloucháván Evou.

Kvantová komunikace mezi Alicí a Bobem je náchylná na tzv. man-in-the-middle útok, u něhož se Eva může vydávat za jednoho z účastníků. Je proto nutné, aby se prvně mezi sebou Alice a Bob autentizovali na jiném kanále. Protokol BB84 je ze své podstaty bezpečný [109]. V praxi je ovšem obtížné mít kvalitní zdroj jednotlivých fotonů a jednofotonové detektory. Proto se často používají lasery produkující světelné pulsy, které obsahují malé množství fotonů. To ovšem umožňuje tzv. PNS útok (popsaný níže 2.4.5), ve kterém Eva daný puls zachytí, vezme si z něho jeden foton a zbytek nechá být. Z tohoto důvodu se do protokolu zavádí tzv. návnadové pulsy, které pomáhají Evu detekovat. Návnadové pulsy obsahují větší množství fotonů na jeden puls, což však Eva nedokáže určit. Při měření chybovosti (QBER) Bob odhalí větší míru ztrátovosti obyčejných pulsů oproti návnadovým, čímž se zjistí přítomnost Evy.

2.2.2 B92

Krátce poté, co byl představen BB82, zjistil Charles Bennet, jeden z tvůrců BB82, že je zbytečné používat čtyři možnosti pro zakódování hodnoty do qubitu. Stačí použít dvě k sobě neortogonální báze. Bezpečnost protokolu zůstane zachována. Alice tedy používá pouze dvě báze pro generování bitů, přímočarou ($\rightarrow$) pro qubit 0 a diagonální ($\nearrow$) pro qubit 1 [112]. Bob zde volí svoji bázi náhodně. Pokud zvolí přímočarou bázi $\oplus$ a Alice poslala ($\rightarrow$) qubit, pak Bob dostane vždy správnou odpověď a naměří qubit 0. Pokud by ovšem použil diagonální bázi $\otimes$, tak pravděpodobnost, že foton zkolabuje do jednoho z diagonálních stavů, je 50 %. Bob ovšem netuší, zda použil správnou bázi. Musí proto měřit přesně opačné báze, než jaké se používají k zakódování hodnoty do qubitu. Bob tedy používá k měření polarizátor nastavený v úhlu 90° ($\uparrow$) a -45° ($\searrow$) [112]. Pokud Bob naměří foton s ($\uparrow$) polarizací, pak ví, že Alice musela poslat qubit 1 ($\nearrow$), ten zkolaboval s 50% šancí. Bitovou 0 Alice poslat nemohla, jelikož tento qubit by nikdy neprošel. Obdobně situace funguje při měření s ($\searrow$). Detekuje-li Bob foton, musela Alice zaslat qubit 0. Je zřejmé, že Alice musí vždy Bobovi sdělit, že posílá nový foton, aby věděl, že jej může očekávat. Výhodou je, že Bob nemusí sdílet báze, které použil k naměření. Pouze prozradí, kdy detekoval fotony. Nevýhodou je poměrně nízká rychlost generování klíče. Využito je pouze 25 % všech zaslaných qubitů Alicí, zbytek se nedá použít [112].

2.2.3 SARG04

SARG04 je protokol, který je založen na BB84, jenž je implementován pomocí pulsů obsahujících malé množství fotonů. Tento způsob je sice lehčí na praktickou implementaci, ale BB84 je zranitelnější na útok dělením počtu fotonů (PNS útok). Hlavní výhodou SARG04 oproti BB84 je tedy větší odolnost vůči tomuto útoku. SARG04 generuje pulsy stejně jako BB84, tedy kóduje informace do daného způsobu polarizace fotonu. Liší se následně způsobem, kterým komunikují po klasickém kanálu. Alice nesděluje Bobovi použité báze. Namísto toho zašle ke každému fotonu informaci, která se skládá z dvojice bází, jež k sobě nejsou ortogonální a zároveň je jedna z dvojice ta, kterou Alice použila pro polarizaci [112]. Například když Alice zašle foton s přímočarou polarizací ($\rightarrow$), Bob si vybere, že bude volit v diagonální bázi $\otimes$. V tomto případě foton zkolabuje do ($\nearrow$ nebo $\searrow$) se stejnou pravdě-

podobností. Nastane-li situace, že foton zkolabuje do (↗) a Alice pošle dvojici (→, ↘), pak je jasné, že Bob zvolil špatnou bázi, a tedy první z dvojice je Alicina polarizace. Bob tak zná hodnotu bitu [57]. Pokud by Alice zaslala informaci (→, ↗), pak Bob netuší, jestli použil správnou bázi nebo měl štěstí a foton zkolaboval do odpovídajícího stavu. Bob proto nedokáže určit hodnotu bitu a daný foton zahodí. To samé by platilo, kdyby Bob použil přímočarou bázi ⊕ pro měření. V takovém případě by foton vždy zkolaboval do (→), nicméně Bob by se nikdy nedozvěděl, zda měřil správně, a musel by tedy daný bit zahodit. Pouze ty bity, u nichž má Bob jistotu, že ví, kterou bázi Alice použila, se nakonec použijí pro ustanovení klíče [57]. Tento způsob je odolnější proti PNS útoku, ale pouze čtvrtina všech bitů je použita pro klíč a QBER je dvakrát tak větší jako u BB84 [112].

2.2.4 SSP

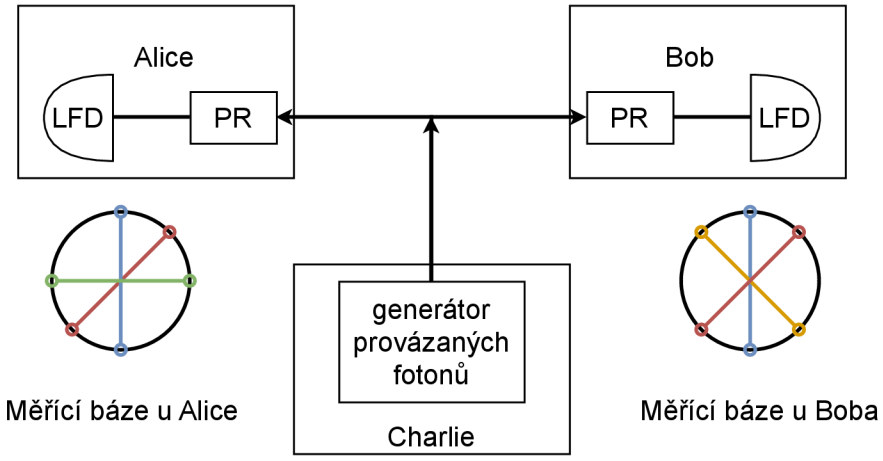
Šestistavový protokol (angl. Six-State Protocol) je obdoba BB84, pouze pracuje se šesti různými polarizacemi neboli stavy pro kódování dat do qubitu. Polarizace u klasického BB84 jsou zavedeny na ose x a y. SSP přidává třetí osu prostoru – z. Třetí typ báze bývá označován jako rotační – po směru hodinových ručiček (↻) a proti směru hodinových ručiček (↺) [112]. Bob musí přidat další bázi, ve níž se pokusí měřit hodnotu qubitu. To znamená, že statisticky pouze 1/3 všech fotonů zaslaných Alicí bude použita pro sestavení klíče. Výhodou tohoto protokolu je větší symetrie. To ve výsledku znamená, že protokol se hodí více do prostředí, v němž je větší šum, takže i vyšší kvantová bitová chybovost QBER. Zároveň je snazší odhalit útočníka odposlouchávajícího kanál [112].

2.3 Protokoly kvantového provázání

Protokoly kvantového provázání nabízí několik výhod oproti klasickým jednofotonovým protokolům. Generování provázaných fotonů je v současnosti jednodušší než generovat jednotlivé fotony. Také jsou obecně méně náchylné na ztrátovost kanálu, a systém tak může být veden i na delší vzdálenosti [113].

2.3.1 E91

Protkol E91 je založen na kvantovém provázaní částic. Generování fotonů může provádět kterákoliv strana, tedy Alice, Bob nebo i třetí strana (Charlie). Charlie generuje fotony, které jsou vzájemně provázané, jsou tedy v Bellově stavu, přičemž měření jedné částice ovlivní výsledek měření druhé částice. Charlie zašle Alici i Bobovi každému jeden z páru provázaných fotonů. Alice měří přicházející fotony pod úhlem z množiny $\{0°, 45°, 90°\}$ a Bob z množiny $\{45°, 90°, 135°\}$. Pokud náhodně oba zvolí stejnou bázi, dostanou přesně antikorelované výsledky [48]. Jednomu tak stačí pouze invertovat bity, aby dostal stejnou hodnotu. Pokud použijí odlišné báze, výsledek jejich měření není jasný. Např. Alice změří pod úhlem 45° hodnotu 1 a Bob má poté pod úhlem 90° přesně poloviční šanci, že změří 1 nebo 0. Alice ani Bob ovšem netuší, které báze použili, proto si musí sdělit informace o použitých bázích po klasickém kanále. Nyní když navzájem znají měřicí báze, rozdělí výsledky do dvou skupin [48]. Skupina G_1, v níž jsou výsledky měření, u kterých nepoužili stejné báze, a skupina G_2, v níž použili stejnou bázi. Skupina G_1 slouží pro odhalení útočníka, který by se snažil kanál odposlouchávat. Obě strany spočítají statistickou hodnotu S, podobně jako se tomu děje u Bellových testů [112]. Pokud se hodnota S nebude rovnat $|2\sqrt{2}|$, značí to nějaký problém a Alice i Bob přeruší komunikaci. Pokud se rozhodnou, že kanál je bezpečný,



Obrázek 2.4: Lineární polarizace fotonů

použijí skupinu G_2 k ustanovení klíče. Výsledky skupiny G_1 jsou zahozeny. Schéma zapojení protokolu E91 je znázorněno na obrázku 2.4, u něhož je PR polarizační rotátor, který určuje úhly, pod kterými se měří, a LFD jsou velmi citlivé lavinové fotodiody [48, 112].

Pokud by byl Charlie pod kontrolou útočníka (Evy), nikterak si nepomůže, jelikož nezná samotné hodnoty provázaných fotonů, ty jsou známy až po změření. Pokud by se Eva pokusila nahradit provázané částice klasickými, kontrola Bellovy nerovnosti by tento fakt odhalila (výsledek nerovnosti by byl příliš malý). Eva by tak působila jako „skrytá proměnná“ v Bellových testech [48].

2.3.2 BBM92

Tento protokol je opět založen na kvantovém provázání částic. Ve svém fungování je velice podobný E91. Znovu se zde vyskytuje Charlie, který vytváří jednotlivé provázané fotony, jež následně zašle Alici a Bobovi. Bob i Alice náhodně měří v přímočaré $\oplus$ nebo diagonální bázi $\otimes$ [35]. Po klasickém kanále si mezi sebou vymění báze, ve kterých jednotlivé fotony naměřili. Kdykoliv, kdy měří ve stejné bázi, si daný výsledek ponechají. Výsledky jsou antikorelované, tudíž jedna strana (většinou Bob) musí výsledek invertovat, aby dostala stejné hodnoty klíče [35]. Vytvoří se tak hrubý klíč. Obě strany následně spočítají kvantovou bitovou chybovost (QBER), tím že obětují několik bitů hrubého klíče. Pokud by hodnota přesáhla zhruba 14,6 %, bude to naznačovat přítomnost Evy [35]. Vzhledem k tomu, že v reálném nasazení se vyskytují nedokonalosti kanálů a snímačů, není možné dosáhnout nulové chybovosti přenosu.

2.4 Protokoly distribuované fázové reference

Protokoly distribuované fázové reference (angl. Distributed Phase Reference) jsou novějším typem protokolů pro kvantovou distribuci klíčů. Vyznačují se tím, že kvantové signály jsou provázány slabě koherentními pulsy. Důvodem ke vzniku těchto protokolů je především jejich praktické využití. Klasické QKD protokoly jsou založeny na vysílaní jednotlivých fotonů. Nicméně vysílače schopny generovat fotony po jednom nejsou dostupné, maximálně pouze v laboratorních a experimentálních podmínkách [74]. Většina komerčních systémů je schopna vysílat fotony pouze po pulsech, což způsobuje, že některé signály obsahují více než

jeden foton. Tento přístup ovšem umožňuje útok skrze dělení počtu fotonů, více zde 2.4.5. Vzdálenost, na kterou mohou systémy takto komunikovat, je značně limitována. Protokoly distribuované fázové reference naproti tomu dokázaly, že jsou snadno implementovatelné do současných optických sítí [68]. Zástupci těchto protokolů jsou DPS a COW. Protoklu COW bude věnována větší pozornost, jelikož je využit u QKD systému, u něhož se budou provádět praktické experimenty. Bezpečnost těchto protokolů však není matematicky dokázána. Je to dáno tím, že neidentifikujeme jednotlivé qubity, ale sekvence koherentních signálů. Klasické techniky jako u BB84 tedy nelze přímo použít [12]. Pouze na určitých typech útoků byla teoreticky ověřena jejich odolnost.

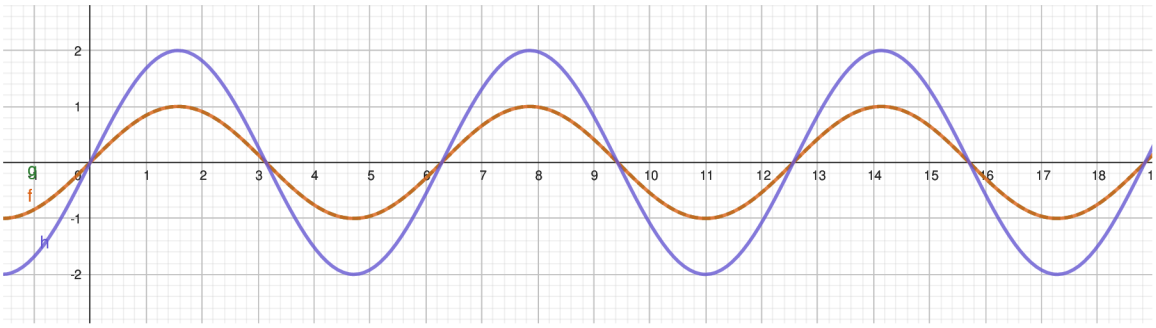
2.4.1 Koherence a interference vln

Koherencí se obecně rozumí souvislost. Zde se jedná o souvislost mezi vlnami světla. Dvě vlny jsou koherentní, pokud jejich frekvence a průběh signálu (angl. waveform) jsou identické. Jedná se o důležitý koncept v kvantové fyzice a zároveň důležitý blok pro pochopení fyzikálních vln. Koherence úzce souvisí s interferencí vln. Z matematického hlediska je interference součet vlnových funkcí. Jedna vlna může interferovat i sama se sebou, neboť se stále jedná o součet dvou vln (např. Youngův experiment) [127]. Plně konstruktivní nebo destruktivní interference jsou hraniční případy, vlny interferují vždy. Při interferenci dvou vln se tyto vlny buď sečtou, nebo odečtou. Pokud se sečtou, dojde k vytvoření jedné vlny s větší amplitudou – tzv. konstruktivní interference, znázorněno na obrázku 2.5. Opačný případ, při němž se vlny navzájem odečtou a výsledná vlna má menší amplitudu, se nazývá destruktivní interference, na obrázku 2.6. Záleží na jejich vzájemném relativním fázovém posunu [127]. Míra koherence, tedy podobnost signálů, se označuje jako viditelnost. Pokud vlnění vychází ze stejného místa, ale s určitým časovým odstupem, mluvíme o časové koherenci. Pokud sčítáme vlny z různých míst plošného zdroje, mluvíme o prostorové koherenci [127].

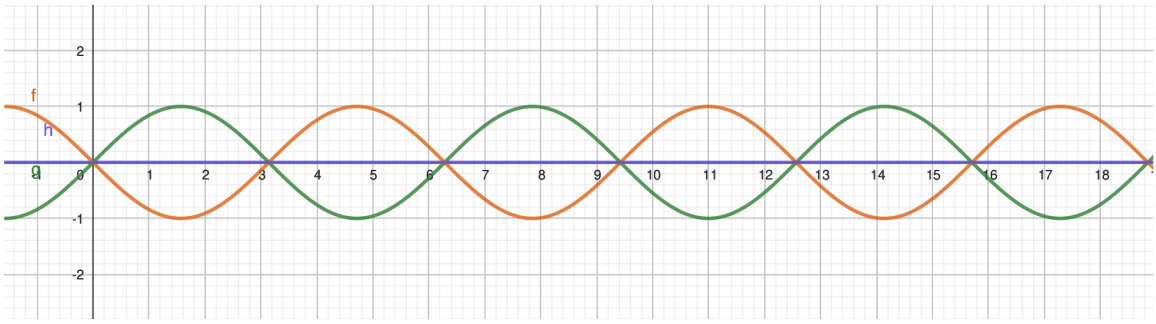
2.4.2 Interferometr

Interferometr je přístroj, jehož princip je založen na interferenci světla. Je určen pro velmi přesná měření. Existuje mnoho typů a interferometrů [69]:

- Interferenční komparátory – používají se k měření vlnových délek, např. Michelsonův interferometr.



Obrázek 2.5: Konstruktivní interference. Funkce f a g mají stejnou fázi. Výsledkem je funkce h (fialová), která je jejich součtem.



Obrázek 2.6: Destruktivní interference. Funkce f a g mají přesně opačnou fázi. Při jejich sečtení je výsledná funkce h (fialová) nulová.

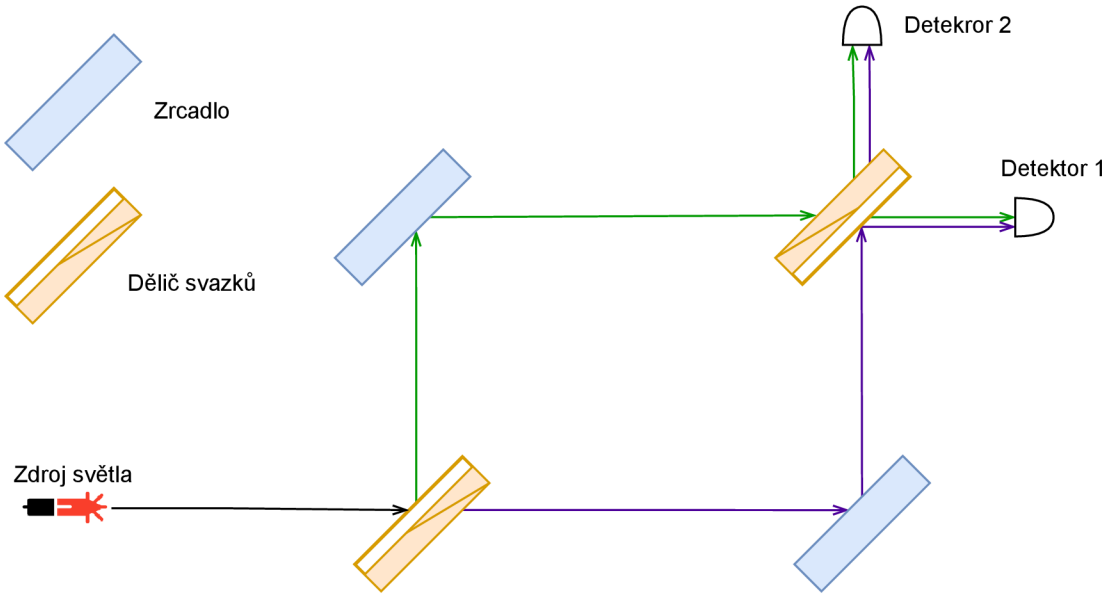
- Intereferční refraktometry – používají se k měření indexů lomu, např Jaminův interferometr.
- Interferenční spektroskopy – používají se k určení jemné struktury spektrálních čar, např. Fabryův-Perotův interferometr.

U protokolů distribuované fázové reference se používá Mach-Zehnderův interferometr. Princip jeho fungování je znázorněn na obrázku níže 2.7. K jeho pochopení je potřeba si ujasnit pár pojmů z optiky.

- Dělič svazků je součástka, která reflektuje polovinu dopadajícího světla a druhou polovinu propustí. Někdy se taky označuje pojmem jednocestné zrcadlo (angl. beam splitter nebo half-silvered mirror).
- Rychlost světla ve vakuu c je skoro stejná jako ve vzduchu. Index lomu při průchodu paprsku zrcadlem je většinou 1,5.
- Když se světelný paprsek odrazí do prostředí, které má vyšší index lomu, než ve kterém se aktuálně nachází (tedy rychlost světla je v novém prostředí menší), fáze světla se posune přesně o jednu polovinu vlnové délky.
- Když se světelný paprsek odrazí do prostředí, které má nižší index lomu, než ve kterém se aktuálně nachází, fáze světla se nijak nezmění.

Interferometr funguje následovně. Všechna zrcadla a děliče svazků jsou natočeny o 45 stupňů. Ze zdroje světla (např. laser) vychází paprsek světla o vlnové délce. Uvažujme vlnovou délku např. 2π. Paprsek dopadne na dělič svazků, na obrázku vlevo dole. Polovina se zlomí a odrazí do zelené větve, nastane fázový posun o polovinu vlnové délky, tedy π. Světlo dále pokračuje do zrcadla vlevo nahoře, od něhož se odrazí a opět bude zpožděno o polovinu vlnové délky. Poté narazí na druhý dělič svazků (vpravo nahoře) a světlo se znovu rozdělí. Polovina se odrazí do detektoru 2, zde se paprsek však odrazí od zadní strany jednosměrného zrcadla, a nedojde tak k fázovému posunu (dohromady je posun 2π), druhá polovina projde skrz dělič svazků do detektoru 1, paprsek bude fázově posunut o konstantní hodnotu c (zde posun o $2\pi + c$) [43, 132].

Fialový paprsek (tedy druhá polovina z děliče svazků dole vlevo) projde skrz s fázovým posunem c. Dále se odrazí od zrcadla vpravo dole. Fáze se posune o π. Poté dorazí do děliče svazků vpravo nahoře. Polovina fialového paprsku projde skrz s konstantním fázovým posunem $-c$. Druhá polovina se odrazí do detektoru 1 s fázovým posunem π. Obě vlny



Obrázek 2.7: Mach-Zehnderův interferometr

před detektorem 1 mají stejný fázový posun, nastane tedy konstruktivní interference a detektor bude detekovat přicházející vlny. Naopak na druhém detektoru nastane destruktivní interference, vlny se vyruší a detektor 2 nic nezachytí [43, 132].

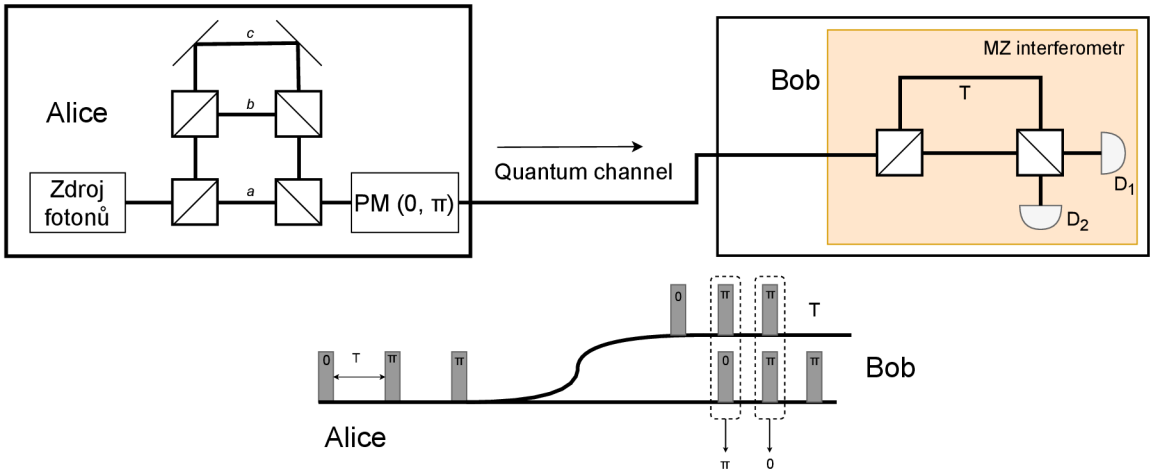
Toho se využívá u COW a DPS protokolu k ověření přicházejících koherentních pulsů. Kdyby se útočník snažil odposlouchávat, naruší koherenci a detektor 2 bude detekovat signál.

2.4.3 Protokol DPS

Protokol je založen na diferenciálním fázovém posunu (angl. Differential Phase Shift). Alice posílá sekvence o třech koherentních pulsech Bobovi. Každý puls je fázově posunut náhodně o hodnotu 0 nebo π [50]. Na obrázku 2.8 je zobrazeno schéma fungování protokolu. Alice vytváří pulsy, které jdou do jedné ze tří větví *a, b* nebo *c*. Mezi jednotlivými větvemi je zpoždění T. Jednotlivé děliče svazků jsou nastaveny tak, aby pravděpodobnost, kudy se puls vydá, byla všude stejná [50, 49]. Fotony se tak rozloží mezi tři jednotlivé pulsy, přičemž pulsy jsou od sebe odděleny časem T [50]. Následně Alice náhodně nastaví fázi na 0 nebo $\pm\pi$ (PM na obrázku) .

Bob rozděluje příchozí pulsy do dvou větví za pomoci děliče svazků 50:50. Zpoždění druhého ramene je nastaveno na T. Podle schématu může Bob počítat fotony ve čtyřech časových instancích:

1. Puls projde větví *a* u Alice a kratší větví u Boba.
2. Puls projde větví *a* u Alice a delší větví u Boba, nebo větví *b* u Alice a kratší větví u Boba.
3. Puls projde větví *b* u Alice a dlouhou větví u Boba, nebo větví *c* u Alice a kratší větví u Boba.
4. Puls projde větví *c* u Alice a dlouhou větví u Boba.



Obrázek 2.8: Schéma fungování DPS protokolu

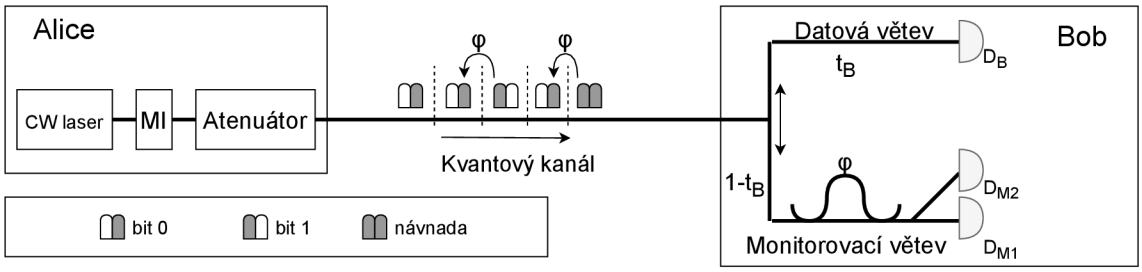
Fázové posuny se měří pouze u možnosti 2 nebo 3, jak je znázorněno v dolní části obrázku. Fázové rozdíly mezi jednotlivými pulsy jsou buď 0 (bit 0), nebo $\pm\pi$ (bit 1). Detektor 1 u Boba bude svítit pro nulový fázový posun a detektor 2 pro $\pm\pi$ posun.

Klíč se následně ustanoví tak, že Bob si zaznamená časy, v nichž došlo k detekci na detektorech pro 2. a 3. časové instance. Poté zašle Alici tyto časy. Jelikož Alice zná fázové posuny, které poslala, a časy detekcí u Boba, je schopna si odvodit stejný klíč, jaký má Bob.

DPS protokol je odolný vůči *beam splitting*, *intercept-resend* a *PNS* typu útoku. Naopak zranitelný může být proti *USD* útoku. Princip jednotlivých útoků je více rozveden u COW protokolu zde 2.4.5. DPS protokol poskytuje vyšší rychlosti přenosu kvantových klíčů než klasický BB84 [50, 49].

2.4.4 Protokol COW

Coherent One Way (COW) protokol je v dnešní době velice populární především díky jednoduché implementaci a schopnosti tolerovat sníženou viditelnost způsobenou chybovostí optických zařízení. Implementace je založena na slabých koherentních pulsech. Klíč získá Bob jednoduše měřením času příchodu jednotlivých pulsů [117, 41].



Obrázek 2.9: COW

Generování pulsů - Alice

Alice jako zdroj používá CW (angl. Continous Wave) laser a modulátor intenzity. Fotonové číslo μ specifikuje průměrný počet fotonů ve vyprodukovaném pulsu (většinou je u COW hodnota $\mu = 0,5$). Pokud Alice blokuje paprsek, dojde k vygenerování vakuovaného (prázdného) pulsu. Pulsy jsou odděleny časovým úsekem daným hodnotou τ. Bity jsou reprezentovány dvojicí po sobě jdoucích pulsů, tzv. time-bin kódováním.

$$|0_k\rangle = |\sqrt{\mu}\rangle_{2k-1}|0\rangle_{2k} \tag{2.1}$$
$$|1_k\rangle = |0\rangle_{2k-1}|\sqrt{\mu}\rangle_{2k} \tag{2.2}$$

Hodnota bitu „0“ je reprezentována dvojicí plného a následně prázdného pulsu – $|0_k\rangle$. Bit „1“ je reprezentován naopak, tedy prvně prázdný a poté plný puls – $|1_k\rangle$. Nutno podotknout, že tyto dva stavy nejsou navzájem ortogonální kvůli přítomnosti prázdných pulsů [117]. Pro malé hodnoty μ se oba stavy mohou překrývat. Alice také generuje s pravděpodobností f návnadové (angl. decoy) bity, které slouží ke zvýšení bezpečnosti protokolu. Jinak by útočník (Eva) mohl odposlechnout počet fotonů, jež se nachází mezi dvěma po sobě jdoucími pulsy. Tento odposlech by nenarušil koherenci pulsů [41]. Povaha vysílacího laseru umožňuje vysílat neprázdné pulsy o přesně dané fázi φ. Vakuované pulsy jsou tedy navzájem koherentní.

$$Decoy = |\sqrt{\mu}\rangle_{2k-1}|\sqrt{\mu}\rangle_{2k} \tag{2.3}$$

Návnadový bit je tvořen dvěma plnými pulsy. Alice generuje bity „1“ a „0“ se stejnou pravděpodobností $\frac{1-f}{2}$. Posílá sekvence bitů opakovaně a Bob je opakovaně vyhodnocuje (statisticky).

Příjem pulsů - Bob

Pulsy od Alice putují k Bobovi po kvantovém kanálu, který je charakterizován přenosem t (předpokládají se jisté nedokonalosti kanálu). Pulsy se poté dělí do dvou větví pomocí děliče svazků (je možné použít i optický switch) [40]. Charakteristika přenosu se označuje $t_B \lesssim 1$. Do datové větve putují pulsy, ze kterých se měřením času příchodu pulsů ustanoví zabezpečený klíč. Bob musí úspěšně rozlišit mezi dvěma stavy (0 a 1). Pravděpodobnost R, že se mu to podaří, udává:

$$R = 1 - e^{-\mu t t_B \eta} \approx \mu t t_B \eta \tag{2.4}$$

přičemž η je kvantová účinnost detektoru fotonů. Kvůli nedokonalostem Bobových detektorů je nutné vzít toto v potaz, typicky se udává $\eta = 10$ %. Bob poté Alici oznámí, co naměřil. Pokud se detekují návnadové pulsy na datové větvi, jsou během diskuze zahozeny [41]. Bity se interpretují stylem zleva doprava podle času příchodu. Tedy první příchozí bit (dvojice pulsů) je nejvýznamnější bit.

Pro ověření, že komunikační kanál nikdo neodposlouchává, se používá druhá větev – monitorovací. Bob zde posílá $(1 - t_B) \ll 1$ ze všech pulsů (většinou okolo 10 % pulsů jde do monitorovací větve). Testuje se koherence mezi dvěma pulsy pomocí Mach-Zehnderova interferometru, v němž jedno rameno interferometru má zpoždění φ, a je tak možné detekovat dva po sobě jdoucí pulsy [40]. Koherenci lze testovat mezi dvěma plnými k a $k + 1$

pulsy. Tedy buď mezi dvojicí bitů „1-0“, nebo testovat návnadový bit. Pokud není koherence porušena, bude detekovat pulsy pouze detektor DM1 v čase $k+1$, na detektoru DM2 nastane destruktivní interference. Pokud se útočník pokusí změřit pulsy, naruší jejich koherenci a detektor DM2 se rozsvítí. Pokud by jeden z pulsů byl vakuový, je pravděpodobné, že by se kterýkoliv z detektorů rozsvítil 0,5 [41]. Koherence pulsů na kvantovém kanálu mezi Alicí a Bobem se počítá jako viditelnost V:

$$V = \frac{p(D_{M1}) - p(D_{M2})}{p(D_{M1}) + p(D_{M2})} \tag{2.5}$$

u čehož je $p(D_{Mj})$ pravděpodobnost, že detektor D_{Mj} něco detekuje v čase, v němž má svítit pouze $p(D_{M1})$. Tyto pravděpodobnosti jsou malé, průměrná míra detekce na monitorovací větvi se rovná $\frac{1}{2}\mu t(1-t_B)\eta$ za puls. Pokud je rychlost generování bitů dostatečně velká, lze odhadnout míru detekce v relativně rozumném čase.

Účinnost neboli to, jak je daný protokol dobrý, se často určuje na základě rychlosti generování zabezpečených klíčů R_{sk} (angl. key rate). Pro vypočítání této hodnoty je nutné uvést další parametry:

$$R_s(\mu) = [R + 2p_d(1-R)]p_s \tag{2.6}$$

u kterých je R_s počet bitů po prosetí klíče, R je pravděpodobnost, že Bob správně určí stav, viz rovnice 2.4, p_d pravděpodobnost počtů tzv. dark pulsů[2], typicky $p_d = 10^{-5}$ a $p_s = 1-f$ [41]. Další důležitý parametr je kvantová bitová chybovost (angl. Quantum Bit Error Rate), označovaná jako Q nebo $QBER$. Předpokládá se, že Eva (útočník) zná zlomek klíče I_{Eve}. Je proto nutné ještě pomocí různých metod, jako je oprava chyb a amplifikace bezpečnosti, zvýšit úroveň bezpečnosti klíče. Z klíče se odebere určitá část $h(Q) + I_{Eve}$, přičemž h je funkce binární entropie [117].

$$R_{sk} = R_s(\mu)(1 - h(Q) - I_{Eve}) \tag{2.7}$$

Nejvíce R_{sk} závisí na μ. Alice a Bob musí tuto hodnotu zvolit tak, aby co nejvíc maximalizovali rychlost generování klíče. Robustnost protokolu proti PNS (útok dělením počtem fotonů) umožňuje nastavit tuto hodnotu relativně vysoko (obvykle 0,5) [117].

Shrnutí protokolu

Shrnutí COW protokolu a jeho fungování:

1. Alice posílá několikrát sekvenci pulsů reprezentujících hodnoty bitů 0 a 1, obě s pravděpodobností $\frac{1-f}{2}$. Návnadové pulsy s pravděpodobností f.

2. Bob na konci výměny odhalí pozice bitů, které zachytil na datové lince, a ustanoví z nich hrubý klíč. Zároveň sdělí časy, ve kterých zachytil pulsy na detektoru DM2.

3. Alice řekne, které pulsy byly návnadové a které si má odstranit z hrubého klíče (prosetí klíče).

[2]Dark puls (angl. dark count) – když detektor detekuje příchozí puls bez jakéhokoliv zdroje světla. Často tepelného původu [85].

4. Alice zanalyzuje detekce na DM2 a odhadne narušení koherence pomocí viditelnosti V_{1-0} a V_d, které souvisí s bitovou sekvencí „1-0“ a sekvencí návnad. Na základě viditelnosti odhadne míru informací, které Eva mohla získat.

5. Pokud Eva nemá dostatek informací o klíči, Alice i Bob nad prosetým klíčem provedou nápravu chyb a amplifikaci bezpečnosti. Ustanoví tak bezpečný klíč mezi sebou.

2.4.5 Útoky a zranitelnosti COW protokolu

Bezpečnost protokolu je velice důležitá. Jak již bylo uvedeno v úvodu této sekce 2.4, obecný důkaz pro COW protokol neexistuje [116]. Současné důkazy potvrzující bezpečnost QKD protokolů v kvantové kryptografii fungují pouze v případě, že máme protokol, který je založen na posílání fotonů po jednom. U COW protokolu se používají pulsy s určitým obsahem fotonů. Bezpečnost se tedy dokazuje/předpokládá pouze vůči určitým typům útoků [116].

V části níže je představeno několik známých útoků na COW protokol. U těchto útoků předpokládáme, že Eva má dokonalé vybavení, které nemusí být z technologických důvodů v současné době k dispozici (ale mohlo by být za několik let). Nutno také dodat, že řada těchto útoků je pouze v teoretické a experimentální fázi.

I-R útok

Anglicky *Intercept-Resend* je typ útoku, který je nejzřejmější a pro COW protokol neproveditelný. Eva detekuje puls letící k Bobovi s pravděpodobností μt. V takovém případě puls změří a připraví nový, který zašle Bobovi v souladu s time-bin kódováním. Koherence pulsů je ovšem narušena, a Eva tak bude odhalena na monitorovacím kanálu Boba. Množství informací, které by Eva mohla získat, se rovná [41, 116]:

$$I_{Eve}(\mu) = (1 - V)\frac{1 + e^{-\mu t}}{2e^{-\mu t}} \tag{2.8}$$

PNS útok

Útok dělením počtu fotonů (angl. Photon Number Splitting Attack) je typ útoku, který využívá nedokonalosti fotonových laserů [38]. Důvod vzniku COW protokolu je fakt, že Alice není schopna vysílat fotony po jednom, nebo pouze velice obtížně a na krátkou vzdálenost. Proto se informace kódují do slabě koherentních pulsů. Ty ovšem mohou obsahovat více jak jeden foton [38].

Princip je zobrazen na obrázku 2.10. Eva neboli útočník zde odposlouchává na obou kanálech. Na kvantovém kanálu Eva měří počet fotonů v kvantovém pulsu (pro každý puls). Pokud je počet fotonů vyšší nebo roven 2, Eva si uloží jeden foton do kvantové paměti[3]. Zbytek Eva přeposílá dále Bobovi [128, 38]. Pokud je v daném pulsu pouze jeden foton, Eva ho zahodí a Bob jej nikdy nedostane. Tady se využívá fakt, že daný kvantový kanál je ztrátový, a tudíž se může stát, že některé pulsy nedorazí. Eva tak zůstane nedetekována. Jakmile si poté mezi sebou budou Alice s Bobem předávat informace o klíči na klasickém kanálu, Eva bude odposlouchávat a klíč si odvodí na základě měření fotonů v kvantové paměti [57, 128, 38].

Takovému typu útoku jde však velice snadno zabránit. K tomuto účelu slouží návnadové stavy, které Alice vysílá. Pulsy se posílají s větším fotonovým číslem μ než klasické datové

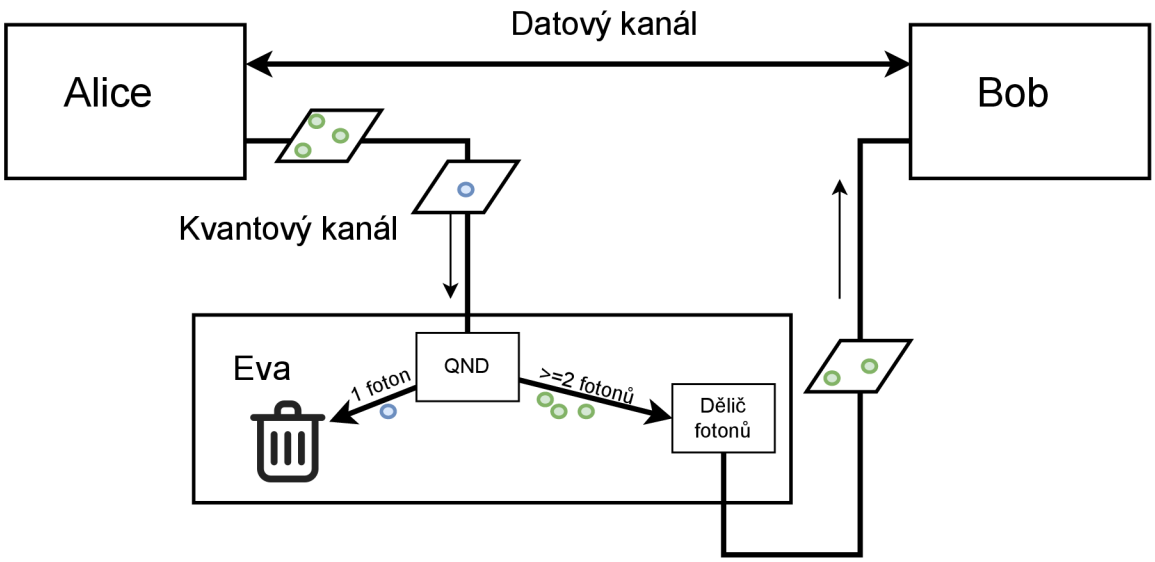
[3] V současnosti jsme schopni vytvořit kvantovou paměť, která udrží informaci pouze 20 milisekund [83].

pulsy. Eva není schopna rozeznat, jestli se jedná o návnadový puls nebo datový, a tudíž kontroluje všechny. Pokud by kanál Eva neodposlouchávala, potom ztráta datových i návnadových pulsů bude zhruba stejná. Při odposlechu bude ale ztráta datových bitů daleko větší, neboť bude Eva zahazovat pulsy s jedním fotonem [57, 128]. Cílem je tedy mít fotonové číslo μ co nejmenší pro datové pulsy. Ovšem malá hodnota také znamená větší ztrátu pulsů na kanálu, a tudíž Bob nedostane žádnou informaci. Rychlost generování klíčů tedy značně klesá [38].

Návnadové pulsy jsou častým způsobem ochrany proti PNS útoku i u ostatních protokolů kvantové distribuce klíčů.

BS útok

Beam splitting útok je velice podobný PNS útoku. Eva má na kvantovém kanálu nastaven dělič svazků (beam splitter). Opět se využívá ztrátovosti kvantového kanálu mezi Alicí a Bobem, která je charakterizována parametrem t. Eva simuluje ztrátovou linku tím, že odebere $(1-t)$ signálu pomocí děliče svazků a zbylou očekávanou část t zašle po bezztrátové lince směrem k Bobovi (Eva má k dispozici bezztrátový kanál). Svoji část si opět ponechá buď v kvantové paměti, nebo se ji rozhodne hned změřit [41, 116]. Vzhledem k tomu, že dělič svazků je ekvivalentní ke ztrátě kanálu, je tento typ útoku vždy proveditelný. Je nemožné ho detekovat na monitorovací lince u Boba. I přesto, že se tomuto útoku nedá zabránit, množství informací, které Eva takto získá, není příliš velké a během fáze amplifikace bezpečnosti klíče se eliminuje množství informací, které má Eva k dispozici[116]. Tento útok se nepovažuje za příliš silný, ale nastavuje horní hranici, s jakou je možné generovat bezpečné klíče (secret key rate). Množství informací, které Eva získá, se rovná $I_{Eve} = \mu(1-t)$. Tento typ útoku se řadí do třídy tzv. útoků nulové chyby (angl. Zero-Error Attack), u nichž se předpokládá, že útok neovlivní $QBER$ ani viditelnost V [41, 116, 13, 14].



Obrázek 2.10: Útok dělením počtů fotonů

USD útok

Pro pochopení tohoto útoku je nutné si uvědomit několik věcí ohledně COW protokolu. První fakt je, že koherence mezi pulsy se kontroluje pouze mezi neprázdnými sousedními pulsy. Tedy mezi prázdnými (vakuovými) pulsy se koherence nekontroluje. Pokud Eva pozná, který puls je prázdný, dokáže provést útok v místě tohoto prázdného pulsu, čímž sice naruší koherenci, ale nebude odhalena [17]. Obecněji řečeno, Eva se může pokusit rozeznat sekvenci n pulsů, které začínají a končí prázdným pulsem. Pokud se jí to povede, může přeposlat tuto n sekvenci tak, aby nedošlo k narušení koherence. Druhým faktem je, že jednotlivé stavy, které Alice posílá, jsou vzájemně lineárně nezávislé [17, 13, 120].

Útok je založen na tzv. jednoznačném rozlišení stavů (angl. Unambiguous State Discrimination), u nichž chceme zjistit stav, v jakém byl systém připraven, aniž bychom zanesli chybu. Předpokládáme, že množina všech možných stavů je známá a nachází se v Hilbertově prostoru[4] $\mathcal{H}$. Jednoznačné rozlišení jakéhokoliv stavu $|\psi\rangle$ je možné pouze, pokud je tento stav lineárně nezávislý na dalších stavech v množině stavů [17]. Obvykle se mluví o rozpoznání všech stavů, nicméně nám stačí identifikovat pouze jeden stav $|\psi\rangle$ z množiny. Mohou nastat dva výsledky, buď se nám povede stav úspěšně identifikovat, nebo je výsledek nejasný. Zvolíme jeden stav $|\phi\rangle$, který je ortogonální ke všem ostatním kromě stavu $|\psi\rangle$. Provedeme von Neumanovo měření nad množinou $\{P_c = |\phi\rangle\langle\phi|, P_\perp = \mathbb{1} - P_c\}$. Výsledkem je $\perp$, pokud stav nebyl $|\psi\rangle$. Pokud je výsledkem c, potom byl stav určitě $|\psi\rangle$. Tento výsledek nastane s pravděpodobností $p_c = |\langle\psi|\phi\rangle|^2$ [17, 13, 120].

Eva v tomto případě chce rozeznat konečnou sekvenci pulsů od ostatních. Vybraná sekvence musí být taková, že první a poslední puls je vakuový. Pokud je výsledek rozpoznání jednoznačný (úspěšný), Eva dokáže připravit stejnou sekvenci a poslat ji Bobovi. Pokud je výsledek nejasný, může Eva celou sekvenci zahodit (jsou možné i jiné strategie, ty ale zanedbáme). Takový útok zanechá $QBER = 0$ a $V = 1$, jelikož Bob obdrží pouze pulsy, které se Evě podařilo identifikovat a u kterých se jí povedlo vytvořit stejnou sekvenci pulsů [17]. Díky prázdným pulsům nedojde k narušení koherence, a Bob tedy neodhalí přítomnost Evy. Nicméně i tímto způsobem Eva zavede určitou chybu, jelikož je výsledek měření pouze pravděpodobnostní, statistické měření u Boba se také pozmění.

Útok se skládá ze tří částí:
Eva zaútočí na sekvenci tří pulsů (útok označme jako USD3) $|0\mu0\rangle$ a pokusí se ji jednoznačně rozlišit od všech ostatních sekvencí o třech pulsech:

$$|00\mu\rangle,\ |0\mu\mu\rangle,\ |\mu00\rangle,\ |\mu0\mu0\rangle,\ |\mu\mu0\rangle,\ |\mu\mu\mu\rangle \tag{2.9}$$

Všimněme si, že sekvence $|000\rangle$ Alice neprodukuje. Navíc $|\mu00\rangle$ a $|00\mu\rangle$ znamenají, že separace bitů je mezi dvěma prázdnými pulsy. Pokud Eva zná dvojice pulsů, které spolu souvisí, stačí jí je pouze jednoznačně rozpoznat mezi $|0\mu0\rangle$ a 5 dalšími stavy. Když se rozeznání povede, Eva zašle sekvenci Bobovi, pokud ne, nepošle nic [17, 120]. Nevýhodou útoku je, že Eva nic neposílá, pokud Alice poslala dva neprázdné pulsy. V případě, že Eva takto útočí pravidelně, Alice i Bob si všimnou, že žádné návnadové pulsy nebyly zjištěny a že nemají ani dostatek dat k výpočtu viditelnosti.

Eva zaútočí na sekvenci čtyř pulsů (útok označme jako USD4a) $|0\mu : \mu0\rangle$ a pokusí se ji jednoznačně rozlišit od všech ostatních sekvencí o čtyřech pulsech. Dvojtečka v zápisu znázorňuje separaci bitů v sekvenci. Útok je stejný jako v případě USD3 a nezanáší žádnou

[4] Hilbertův prostor je vektorový prostor, ve kterém je možné měřit úhly a velikosti vektorů a konstruovat ortogonální projekce vektorů na podprostory [42].

chybu. Na rozdíl od USD3, jsou tentokrát Bob s Alicí schopni vypočítat viditelnost. Ale pouze z bitových sekvencí „1 - 0“, návnadové bity opět chybí.

Eva zaútočí na sekvenci čtyř pulsů (útok označme jako USD4b) $|0 : \mu\mu : 0\rangle$ a pokusí se ji jednoznačně rozlišit od všech ostatních sekvencí o čtyřech pulsech [17, 120]. Způsob provedení útoku je stejný jako v předchozích případech. Tímto útokem Eva nezjistí žádnou část klíče, ale dojde k přeposílání návnadových sekvencí bitů.

Eva poté kombinuje jednotlivé možnosti mezi sebou tak, aby detekce na jednotlivých detektorech a statistické měření nevyvolávalo neočekávané chování a Eva zůstala v utajení. Provádí útok USD3 s pravděpodobností q_1, USD4a s pravděpodobností q_2 a USD4b s pravděpodobností q_3:

$$q_0 + q_1 + q_2 + q_3 = 1 \tag{2.10}$$

přičemž q_0 je pravděpodobnost, že Eva pouze přepošle pulsy po bezztrátovém kanálu. Eva může střídat tyto útoky dle libosti, ale nesmí tak činit příliš často, jinak by zanesla chybu. Ačkoliv se zdá, že tento útok je kritický pro COW protokol, realita není tak vážná. Je úspěšnější než BS útok, pokud je vzdálenost mezi Bobem a Alicí více jak 100 km, což je v současnosti limit pro COW protokol [40]. I přesto, že by Eva dokázala správně simulovat míru detekcí jednotlivých detektorů, se stále dá statisticky zjistit, že veškeré návnadové pulsy přišly ve formě $|0 : \mu\mu : 0\rangle$ [17, 13, 120]. Dále je možné potlačit tento útok zavedením další návnadové sekvence skládající se ze dvou prázdných pulsů. USD útok se řadí také do třídy tzv. útoků nulové chyby [17].

Pro tento typ USD útoku vznikají i různé modifikace a vylepšení, více o nich je možné nalézt zde [120, 58].

Shrnutí útoků na COW protokol

Některé útoky jako například I-R a PNS nejsou příliš velkou hrozbou pro COW protokol, ale naopak BS a USD útoky sice nemusí nutně znamenat, že protokol není bezpečný, ale dokazují, že protokol obsahuje jisté chyby a zranitelnosti, kterých lze potenciálně zneužít. Krom výše jmenovaných existuje i řada dalších, které v této práci nejsou blíže popsány. Jmenovitě například útok na dva pulsy (angl. Two-Pulse Attack) [14] nebo útok překrytím s náhodnou sekvencí [115].

Zajímavým poznatkem je fakt, že třída útoků způsobující nulovou chybu (BS a USD útoky) ukázala, že bezpečnost protokolu nemůže být závislá pouze na testování koherence mezi plnými pulsy. Musí zahrnout buď další návnadové stavy, nebo u Boba umožnit testování koherence i mezi pulsy, které spolu nutně nesousedí. Další variantou je testovat více statistických údajů a hledat v nich odchylky a nesrovnatelnosti.

Problém bezpečnosti COW protokolu je stále součástí mnoha výzkumů, u nichž vznikají různá vylepšení a modifikace, která zajišťují větší míru bezpečnosti protokolu. Jedním z nich je např. článek [60], ve kterém se používají dva vakuované pulsy a jeden plný puls pro zakódování bitové informace.

Kapitola 3

Topologie kvantových sítí

Úvod kapitoly se zaměřuje na podrobnější popis typického zapojení sítí, ve kterých je umístěn kvantový systém (QKD) pro distribuci kvantově zabezpečených klíčů. Jaké jsou různé varianty topologií a jejich využití, včetně bezdrátového kvantového kanálu, který používá laserové přenosy se satelitem. Jsou zde zmíněné různé druhy zařízení, které se pro distribuci kvantově zabezpečených klíčů používají. Příkladem skutečné topologie sloužilo pracoviště na univerzitě VUT v Brně, které je v této kapitole také popsáno. Výčet topologií není seznam všech možných řešení, které mají bezprostřední vztah k této práci.

3.1 Popis topologie

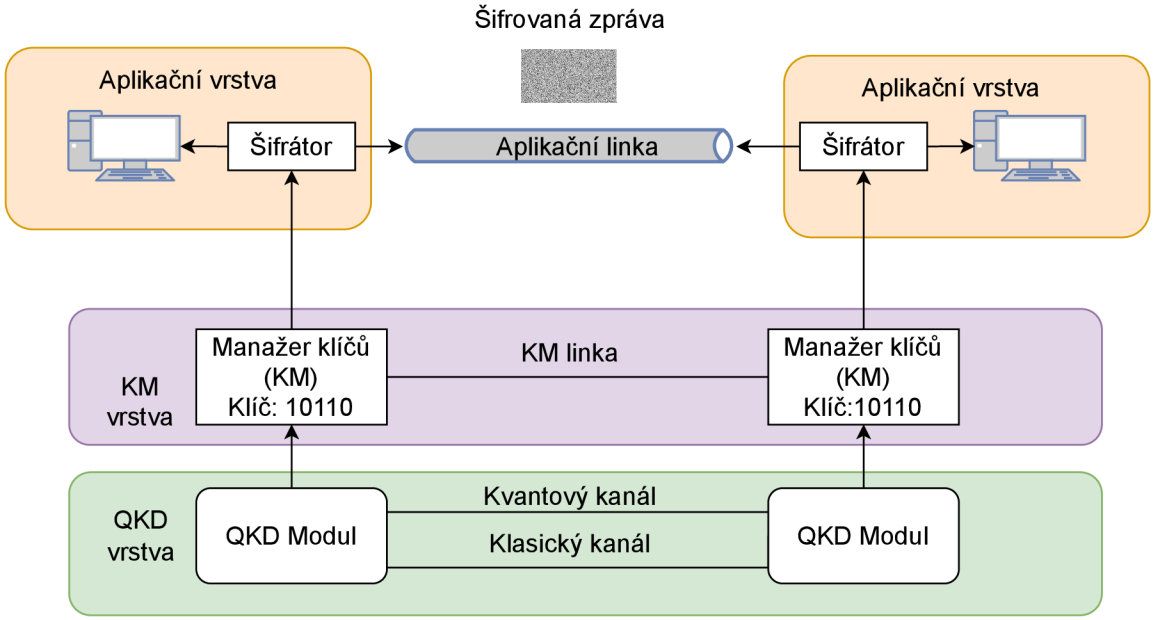
Tato sekce se soustředí na různé druhy topologií, které můžeme v současné době vytvořit, přestože některé jsou velice náročné nebo je doposud nikdo nezrealizoval. Prvně je nastíněné obecné schéma, které QKD systémy používají, na nich se poté staví složitější sítě. Většina z nich je realizována pomocí optického kabelového propojení. Existuje i řada bezdrátových spojení a především komunikace za použití satelitů přináší do kvantové distribuce klíčů globální pokrytí.

3.1.1 Obecné schéma

QKD systémy umožňují distribuci a vytváření náhodných bitových řetězců, které lze považovat z pohledu teoretické informatiky za bezpečné. Takto vygenerované řetězce lze poté použít jako klíče pro klasickou symetrickou kryptografii využívající např. AES, OPT (One Time Pad) nebo HMAC [84]. Bezpečnost je založena na zákonech kvantové fyziky, proto je správné zapojení QKD systému důležité. Standard, jak by síť měla vypadat, ovšem není k dispozici. Nicméně existuje již řada referenčních modelů. Na obrázku níže 3.1 je možné vidět příklad základního schématu, reprezentujícího jednoduché Point-to-Point (P2P) zapojení mezi dvěma QKD uzly.

QKD vrstva

Základními elementy jsou dva QKD moduly. Ty se starají o generování kvantových dat. Způsob, jakým to provádějí, je dán zvoleným protokolem. Jsou navzájem propojeny kvantovým kanálem. Oba moduly musí být také spojeny klasickou (nekvantovou) linkou. Ta slouží především pro komunikaci, synchronizaci, zahajování spojení a vzájemnou výměnu informací mezi těmito QKD moduly (včetně výměny informací o bezpečnosti klíče) [84].



Obrázek 3.1: Základní schéma zapojení QKD

Bylo dokázáno, že je možné klasický i kvantový kanál spojit do sdíleného optického spojení a přenášet kvantové a klasické informace po jednom vláknovém spoji [20], je ovšem nutné zavést speciální techniky na odstranění interference. Dohromady tvoří jednu společnou vrstvu nazvanou QKD vrstva (na obrázku úplně dole). Kvantový kanál je většinou realizován pomocí optických vláken. Instalování dedikovaných kabelů pro kvantové spojení však není vždy možné nebo praktické. Existuje proto i možnost přenášet kvantovou informaci ve volném prostoru pomocí světla. Více je tento způsob popsán v sekci o bezdrátových spojeních 3.2. Při zavádění nových QKD spojení je důležité vzít v potaz vzdálenost, která je mezi dvěma body. S rostoucí vzdáleností prudce klesá rychlost generování klíčů. Až bude vzdálenost příliš velká, bude detektor zachytávat příliš mnoho dark fotonů a nebude možné ustanovit klíč [121, 72]. Absence kvantových opakovačů značně omezuje možnosti toho, na jakou vzdálenost je možné v současné době komunikovat pomocí kabelového spojení. Vzdálenost bodů současných komerčních řešení se pohybuje okolo 100 kilometrů pro optické kabely. Objevují se i experimentální řešení na dlouhé vzdálenosti čítající několik stovek kilometrů [121, 72]. V těchto případech je ale rychlost generování klíčů tak malá, že se nedá reálně použít.

KM a aplikační vrstva

QKD moduly generují náhodné řetězce bitů, které posílají o vrstvu výše, do tzv. manažera klíčů (angl. Key Management). Tato část je zodpovědná za formátování řetězců bitů do podoby klíčů a jejich následné uchovávaní v databázi platných klíčů. Ty jsou identifikovány podle určitého ID [121, 72]. Aplikační vrstva (na obrázku úplně nahoře) se poté dotazuje KM modulu, zda jí poskytne klíč. Pokud je k dispozici volný klíč, obě komunikační strany se dohodnou skrz KM vrstvu, který z nich chtějí použít. Ten následně bude předán aplikační vrstvě. Uvnitř aplikační vrstvy se nachází šifrátor, který šifruje zprávy pomocí daného klíče a vybraného šifrovacího algoritmu. Zprávy se následně začnou posílat mezi oběma body klasickým způsobem po aplikační lince. Ta je oddělena od kvantové linky, která slouží pouze

pro tvorbu klíčů. Jakmile je klíč předán aplikační vrstvě, je z KM odstraněn. Obvykle se neponechává v databázi, ale záleží na politice správce klíčů [121]. Míra, s jakou se konzumují klíče, závisí na množství dat nutných zašifrovat a na typu šifrovacího algoritmu. KM vrstva také umožňuje provádět specifické operace nad vygenerovanými klíči. Pokud by aplikace požadovala menší klíč než ten, který má KM v databázi, může klíč rozdělit. Naopak kdyby aplikace požadovala větší délku klíče, může KM některé klíče spojit dohromady, pokud jsou k dispozici [84, 121, 72]. Nutno podotknout, že nikde není specifikován způsob, s jakým mohou aplikace ke klíčům přistupovat. Je proto nutné zabezpečit a povolit dotazování se na klíč pouze autorizovaným aplikacím a uživatelům.

Podle obrázku 3.1 je patrné, že QKD systém může být pouze přidanou technologií do už existující infrastruktury. Obrázek pouze zobrazuje spojení mezi dvěma body. To není povinností. Rozdílné topologie jsou také podporovány, jmenovitě např. kruhové nebo hvězdicové topologie [121, 72]. Pokud chceme mít vícero uzlů v síti, musíme zavést další vrstvu, tzv. QKDN (angl. QKD Network). Ta se nachází mezi aplikační a KM vrstvou.

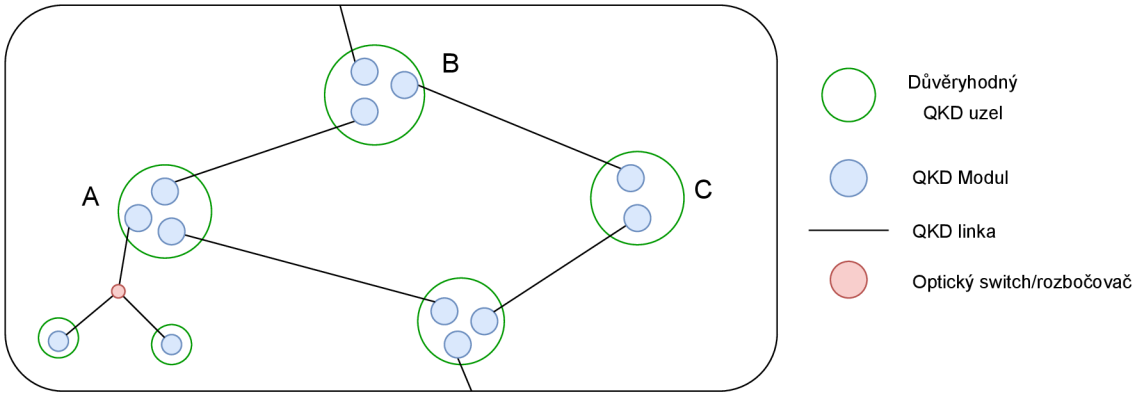
3.1.2 Síť o vícero uzlech – QKDN

Hlavním důvodem, proč zavádíme novou vrstvu – QKDN, je to, aby se zvýšila bezpečnost a aby bylo možné komunikovat mezi dvěma uzly, které spolu nejsou přímo fyzicky propojeny. Tím se vzdálenost, na kterou mohou dva body komunikovat, zvětší. QKDN vrstva a její kontroléry zajišťují bezpečné doručení klíčů skrz důvěryhodné uzly a směrování mezi nimi. Vrstva může také zajišťovat QoS služby [121].

V souvislosti s QKDN se používá další termín – důvěryhodný QKD uzel. To znamená, že uzel je zabezpečen proti proniknutí a napadení od jakékoliv neautorizované třetí strany (a to i zvenčí) [84, 121]. Pokud chce bod A komunikovat s bodem C, aniž by byli přímo spojeni, musí QKDN vrstva prvně najít vhodný důvěryhodný uzel B. Poté se ustanoví rozdílné klíče K_{AB} a K_{BC}, pomocí kterých komunikuje uzel B s uzly A a C. Uzel A následně vytvoří klíč K_{AC}, který zašifruje pomocí K_{AB} a odešle uzlu B. Pro šifrování se používá OTP. Uzel B klíč dešifruje a zašifruje klíčem K_{BC} a pošle uzlu C. Takto vznikne zabezpečený klíč mezi body A a C. Protože B zná klíč komunikace K_{AC} musí být důvěryhodný. Nevýhodou tohoto typu komunikace je také to, že ji lze považovat za sériovou. Pokud by jeden z uzlů byl více zatížen, obecně řečeno by generoval klíče menší rychlostí, čímž by ovlivnil celé spojení. Tento hop-by-hop přístup, jak se často nazývá, je hojně využíván napříč organizacemi v Evropě, Japonsku, Číně, Švýcarsku a v dalších zemích [72]. V Číně existuje spojení z Pekingu do Šanghaje čítající okolo 2 000 km, které je rozděleno do několika krátkých segmentů (každý méně jak 100 km) a které používá 32 důvěryhodných uzlů pro přenos kvantové informace [18].

QKDN vrstva je často zodpovědná za ovládání správce klíčů (KM) a zároveň tvoří pomyslnou demarkační linii mezi uživatelskou (aplikační) a QKD vrstvou [84]. Obě vrstvy mohou mezi sebou sdílet pouze minimum informací. QKD vrstvy nepotřebují vědět, k čemu jsou klíče využívané. Aplikační vrstva může pouze pokládat podmínky na velikost klíče. QKDN může být v topologii centralizovaný, přičemž stačí, aby pouze jeden tento uzel poskytoval QKDN vrstvu. V distribuované topologii naopak musí mít každý uzel svoji QKDN vrstvu.

Příklad složitější topologie je znázorněn na obrázku 3.2. Optický rozbočovač představuje alternativu k důvěryhodnému uzlu, u kterého je možné stanovit spojení mezi vícero body bez nutnosti přítomnosti spojovacího uzlu. Použití optického rozbočovače má ale dvě nevýhody [121]. Vzdálenost, na kterou jsou schopny uzly komunikovat, se nikterak nezvýší,



Obrázek 3.2: Schéma QKDN sítě propojující vícero bodů

což je hlavní důvod současného zapojení sítí s vícero uzly. Praktické nedokonalosti zapojení této součástky často spíše zhorší kvalitu kanálu, a tedy i komunikační vzdálenost. Druhá nevýhoda spočívá v nutnosti použití stejného komunikačního protokolu mezi všemi zúčastněnými stranami .

3.2 Přenos ve volném prostoru

Přenos kvantových dat bezdrátovým způsobem (angl. označení Free-Space Link) se dá rozdělit na dvě kategorie. Na přenos optikou pozemním způsobem a za pomoci satelitů. Obě možnosti mají své pro i proti, největším rozdílem je nicméně vzdálenost, na jakou spolu dokážou komunikovat. Zatímco satelitní spojení se podařilo sestrojit až na vzdálenost 1 000 kilometrů, pozemní bezdrátový způsob dosahuje zhruba 10 kilometrů [124]. Zařízení používaná pro vysílání kvantové informace jsou často lasery vysílající paprsky infračerveného světla. Obě varianty jsou nicméně omezené atmosférickými podmínkami, které mohou do značné míry ovlivnit rychlost přenosu [124, 80].

3.2.1 Laserové přenosy dat

Přenosy dat za pomoci laseru jsou v experimentálních fázích vývoje. Nicméně využití laserů pro kvantové kanály se jeví jako nadějná budoucnost, jelikož umožňují komunikaci na dlouhé vzdálenosti. Obecně přenos dat laserem představuje razantní zlepšení oproti stávající bezdrátové Wi-Fi technologii. Ta využívá k přenosu dat rádiové frekvence, lasery naproti tomu používají k přenosu dat modulaci světelné intenzity. Světelné vlny mají daleko vyšší frekvenci, mohou tedy přenášet větší objem dat vyšší rychlostí [122]. V květnu roku 2022 byl vypuštěn satelit, který vynesl malou krabičku TBIRD (TeraByte InfraRed Delivery) na oběžnou dráhu. Tento laser byl schopen přenášet data rychlostí 100 gigabitů za sekundu, což je více než 1 000 násobek oproti radiofrekvenčním spojením. NASA cílí na dvojnásobek této rychlosti [101]. Z pohledu bezpečnosti je laserový přenos také krokem vpřed. Data přenášená laserem nelze zachytit tak snadno jako v případě rádiových vln. Jedná se totiž o úzký paprsek světla.

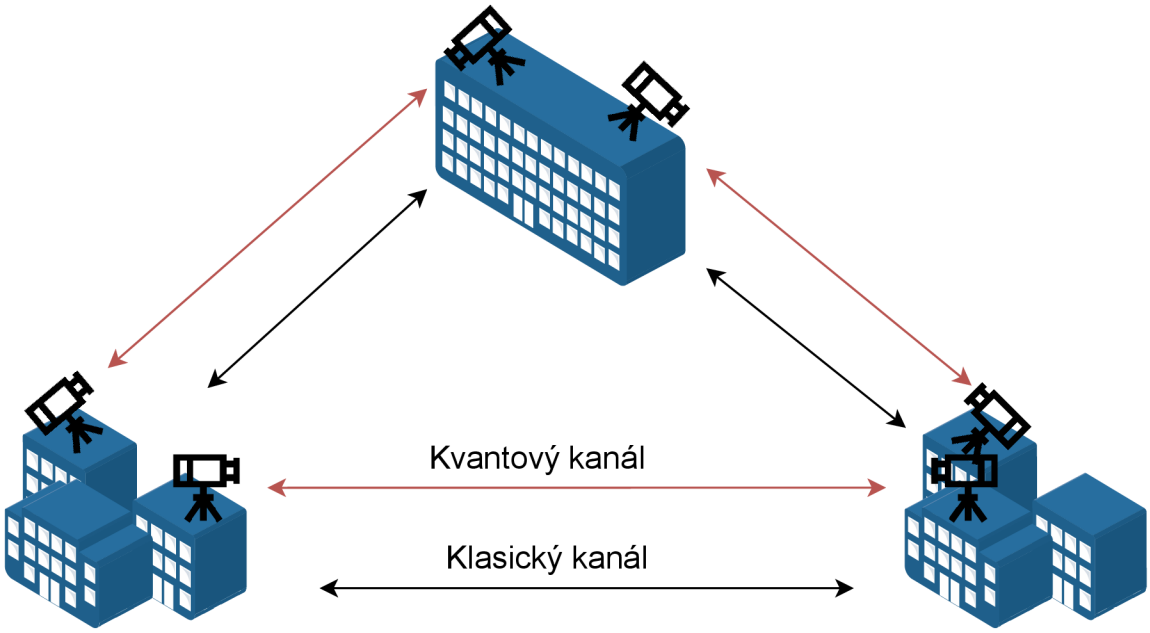
Velký problém pro laserové spojení ovšem představují situace, kdy je světelný paprsek narušen oblačností, mlhou nebo jinými vlivy atmosféry. Oblaka dokážou svou hustotou laserový paprsek narušit a zničit přenášenou informaci. S jedním z možných řešení přišli vědci z Ženevské univerzity [103]. Spočívá ve vytvoření díry do mraku pomocí paprsku, který

zahřeje okolní vzduch o 1 500 stupňů Celsia a vyprodukuje rázovou vlnu, která odstrčí kapky vody tvořící mrak do strany. Vzniklá díra o velikosti několika centimetrů stačí k tomu, aby se skrz ni přenesla data.

Je nutné také podotknout, že záleží i na vlnové délce laseru. Například krátké vlnové délky (fialová, modrá barva) budou oproti infračervenému záření daleko častěji narušeny atmosférou, zvlášť při delší trase.

3.2.2 Přenos po zemi

Přenos po zemi je znázorněn na obrázku 3.3. Na rozdíl od kabelového spojení jsou zde kvantové optické vysílače a přijímače umístěné na střechách budov. U klasického kanálu v tomto případě nezáleží na tom, jestli bude taky bezdrátový nebo klasický kabelový. Tento přístup má několik nevýhod. Optické laserové spojení zde závisí na přímé viditelnosti (angl. line of sight), tzn. oba body na sebe musí „vidět“ [124]. I přesto, že atmosféra má menší útlum signálu, pouze 0,07 dB/km ve výšce asi 2 500 m. n. m., než optický kabel, spojení je značně závislé na atmosférických podmínkách, jako je např. tlak, oblačnost, déšť, mlha, různé vibrace, poměr signálu k šumu[1], zakřivení Země atp [124]. To omezuje efektivní vzdálenost na necelých 10 km a používá se spíše na komunikaci v malých lokálních topologiích. Výhoda bezdrátových optických zařízení je, že jsou jednoduší na instalaci, jelikož nevyžadují kabelovou infrastrukturu [124, 121].



Obrázek 3.3: Pozemní bezdrátové optické spojení

[1] Signal-to-noise – poměr mezi přijatým světelným signálem a šumem spojeným se získáním tohoto signálu.

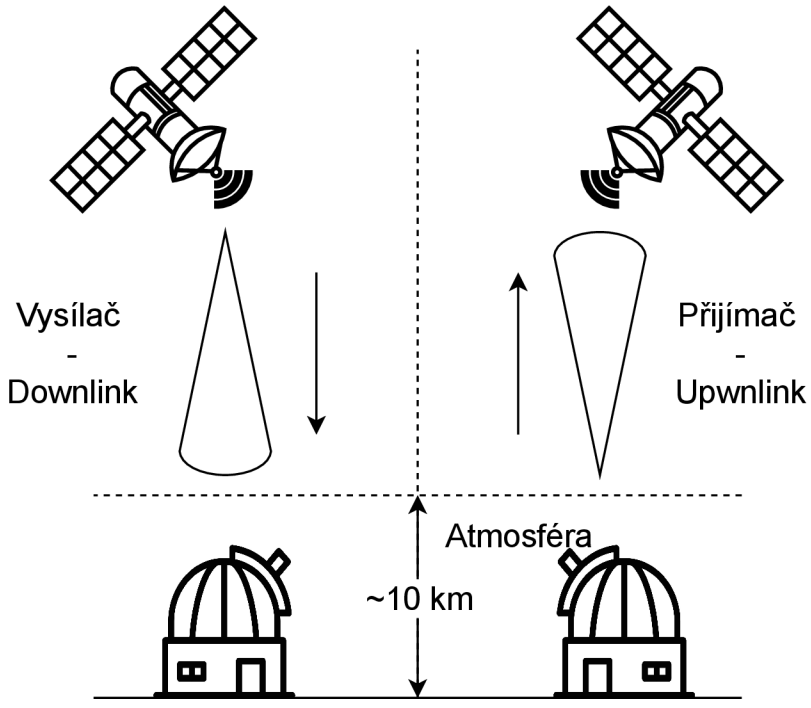
3.2.3 Přenos pomocí satelitu

V současné době je jediný způsob, jak zavést kvantovou komunikaci v globálním měřítku, za pomoci využití satelitů. Vzhledem k tomu, že většina signálu putuje vakuem, je ztráta signálu převážně v místech atmosféry. Nedávné úspěchy to potvrzují, když se povedlo čínskému satelitu *Micius* navázat kvantové spojení mezi Rakouskem a Čínou, vzdálenost čítající zhruba 7 600 kilometrů [63]. Satelity létají ve třech úrovních oběžných drah kolem Země:

- Nízká oběžná dráha – nachází se ve výšce 200–2 000 km nad Zemí. Díky nízkým efektům kosmického záření se jedná o nejčastěji využívané místo pro umístění satelitů, angl. název LEO (Low Earth Orbit).
- Střední oběžná dráha – nachází se ve výšce 2 000–35 786 km, angl. název MEO (Medium Earth Orbit).
- Vysoká oběžná dráha – ve výšce 35 786 km a více. Výška 35 786 km se nazývá geosynchronní dráha Země, satelity zde mají dobu oběhu stejnou, jako je rotace Země kolem své osy, angl. název GSO (Geosynchronous Orbit).

Současné QKD satelity se pohybují v nízké oběžné dráze [62]. Výhodou je nižší ztrátovost kvantového kanálu za cenu nutné vyšší rychlosti, kterou se musí satelit pohybovat po oběžné dráze, a tedy i větší náročnost pro přesnou koordinaci míření satelitu a stanice. Ve vysoké oběžné dráze se nemusí satelit pohybovat tak rychle a spokojení se stanicí může trvat delší dobu, na druhou stranu je zde daleko větší ztrátovost způsobená vzdáleností [8].

Existují dvě varianty, jak využít satelit. Buď jako vysílač kvantového signálu, nebo jako přijímač [62, 8]. Na obrázku 3.4 jsou znázorněné tyto možnosti.



Obrázek 3.4: Dvě možnosti, jak se bude satelit chovat. Buď jako vysílač, nebo jako přijímač kvantového signálu.

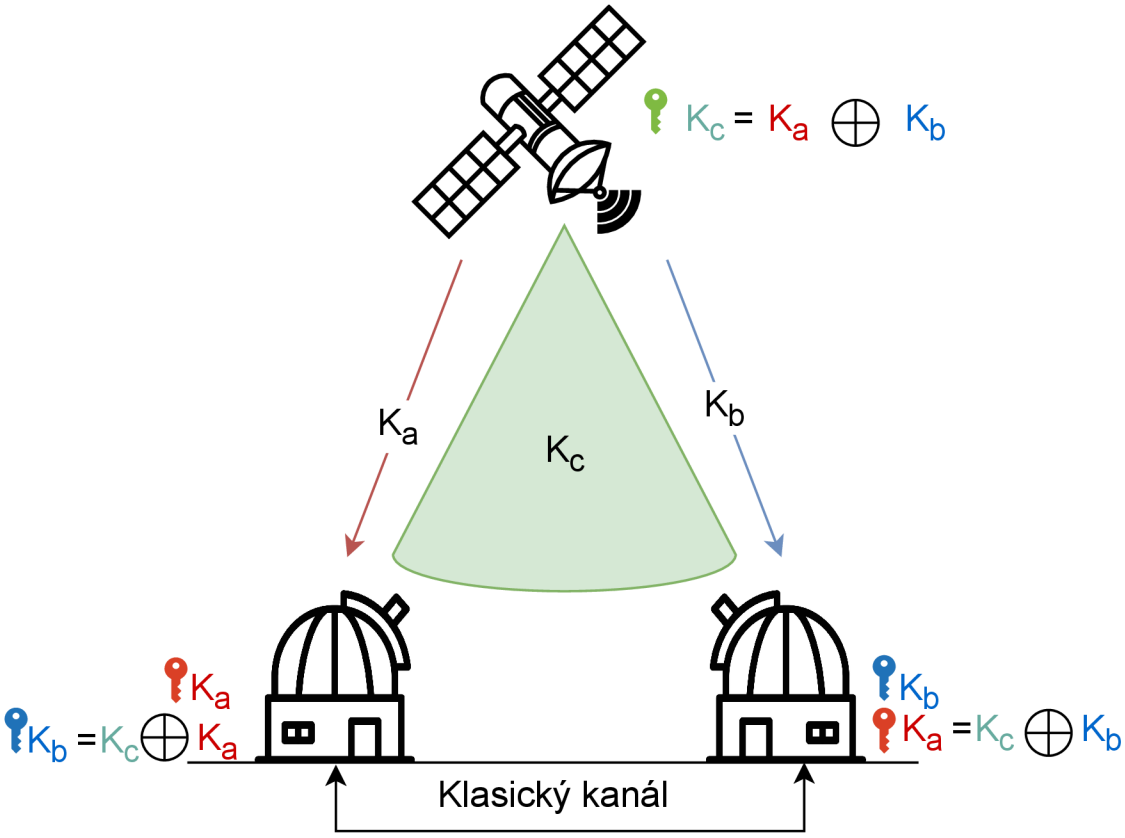
Satelit jako vysílač (anglické označení downlink) je preferovaná varianta. Satelit vysílá paprsky pozemní stanici. Signál prvně prochází vakuem. Ztrátovost v této oblasti je nejvíce zapříčiněna difrakcí paprsku. Atmosférou (cca 12 km) prochází paprsek v závěru své cesty, přičemž směrem z vesmíru nedojde tolik k jeho útlumu [62, 8]. Navíc je snazší vybudovat kvalitnější a větší přijímač na pozemní stanici.

Druhá varianta (angl. uplink) je satelit přijímač. Výhodou je to, že je u něj lehčí nasměrování paprsku směrem k satelitu ve vesmíru než naopak. Zároveň lze obecně říci, že potenciální útok, který cílí na vysílače, je náročnější [8, 62]. Nicméně nevýhodou je daleko větší ztrátovost kanálu. Paprsky nejdříve musí projít atmosférou, což klade velké nároky na samotný pozemní vysílač. Šířka paprsků se ve výšce 500 km může roztáhnout až do 50 metrů. To je daleko více než v případě downlinku, u něhož je šířka cca 12 m po uražení dvojnásobné dráhy. Velký přijímač (schopný detekovat jednotlivé fotony) na straně satelitu je příliš těžký a drahý. Navíc se musí potýkat s dalšími jevy ve vesmíru. Vibrace, extrémní rozdíly teplot během oběžné doby a velký výskyt nesprávných měření díky radiaci . Proto se obecně preferuje varianta, ve které satelit obsahuje vysílač, zatímco drahé a citlivé detektory jsou ponechány na Zemi [124, 8, 62]. Oproti uplink satelitu je snazší provést potenciální DoS útok, u něhož stačí mířit dostatečně velkým paprskem na optický přijímač satelitu a tím mu znemožnit validní měření.

Na obrázku 3.5 je zobrazen princip generovaní klíčů mezi dvěma body. Satelit, který se nachází v nízké oběžné dráze (LEO), slouží jako důvěryhodný uzel. Vygeneruje klíč K_a, který si předá se stanicí A po kvantovém kanálu. Stejným způsobem vytvoří jiný klíč K_b, který zašle stanici B [62]. K tomu, aby mohl komunikovat s danou stanicí, na sebe musí stanice a satelit vzájemně vidět. Koordinace a synchronizace mezi satelitem a pozemní stanicí může probíhat po klasickém kanálu. Není přímo nutné, aby satelit viděl na obě stanice zároveň, klíče může předat později, až satelit bude nad stanicí přelétat. Také se může realizovat varianta, při níž bude k dispozici více satelitů, ty pak mohou mezi sebou vzájemně komunikovat (důvěryhodné informace si ovšem musí předávat na kvantové lince), a pokrýt tak větší oblast. Jakmile spolu budou chtít stanice A a B zahájit komunikaci, satelit vygeneruje $K_c = K_a \oplus K_b$, který vytvoří jako bitovou paritu nad K_a xor K_b [62]. Vzhledem k tomu, že původní klíče jsou nezávislé bezpečné řetězce bitů, broadcast K_c neprozradí žádnou užitečnou informaci potenciálnímu útočníkovi. Stanice A a B jsou pak schopny samy vypočítat klíč druhé strany. Značné bezpečnostní riziko zde představuje fakt, že satelit zná veškerá tajemství, a musí být tedy zabezpečen proti jakémukoliv útoku [124, 8, 62].

Alternativně jde použít techniku, při které satelit posílá navzájem provázané fotony oběma stanicím současně. Ty poté provedou náhodné nezávislé měření stavů fotonů a obě získají identický klíč. Satelit nemá žádnou informaci o tom, jaké měření stanice provedly či do jakých stavů fotony zkolabovaly, a tudíž jakýkoliv útok na satelit neposkytne útočníkovi žádnou informaci. Toto funguje ale pouze za předpokladu, že satelit „vidí“ obě stanice současně. Anglicky se tento způsob nazývá MDI-QKD (measurement-device-independent), jedná se prakticky o ekvivalent protokolu E91 zmíněného dříve 2.3.1. Tato metoda je však poměrně prakticky náročná na zprovoznění [16, 124, 8].

Zařízení operující ve vesmíru představují řadu výzev, se kterými je třeba se vypořádat. Velikost, váha, zdroje elektrické energie, resp. spotřeba samotného zařízení, radiace a vesmírné záření kladou nároky na samotný satelit. Dále přesná koordinace satelitu s pozemní stanicí a trasování kladou velké nároky na výrobce těchto systémů [124]. Nicméně pro globální kvantové spojení představují satelity zářnou a nadějnou budoucnost.



Obrázek 3.5: Proces generování klíčů mezi dvěma místy za pomoci satelitu

3.2.4 Klasifikace oblak

Základní klasifikace mraků je založena na jejich tvarech, tzv. morfologické klasifikaci. Ta vychází z Mezinárodního atlasu oblaků, který vydává Světová meteorologická organizace (WMO) [51]. Pro potřeby simulace jsem vycházel z klasifikace na základě výšky, ve které se typy mraků vyskytují:

- Nízká oblaka – vyskytují se ve výšce do 2 000 metrů nad povrchem Země. Mraky, které se tvoří v této výšce, jsou obvykle větší než ve vyšších výškách a mají větší hustotu. Příkladem mraků v této výšce jsou *Stratocumulus, Stratus* a *Cumulus*. *Cumulus* má kadeřavý tvar a obvykle není zdrojem srážek, ale může se dále vyvinout v oblaka se srážkovým a bouřkovým potenciálem. *Stratus* je velice podobný mlze, ze které nejčastěji vzniká. Vyskytuje se v nejnižších výškách. *Stratocumulus* je schopen se rozpínat také vertikálně a někdy může zatahovat celou oblohu.

- Střední oblaka – vyskytují se ve výšce od 2 000 do 7 000 metrů. Příkladem oblak středního patra je *Altostratus* a *Altocumulus*. *Altostratus* je složen z vodních kapek a ledových krystalků. Má šedavou či namodralou barvu. Horizontálně pokrývá stovky až tisíce kilometrů. Vertikálně ovšem není příliš velký (několik stovek metrů, jsou skrz něj tedy místy vidět obrysy Slunce). *Altocumulus* je skupina menších oblak, které jsou navzájem oddělené bezoblačnými pásy. Tvoří je drobné kapky vody.

- Vysoká oblaka – tvoří se ve výšce 5 až 13 km nad povrchem Země. Zástupci této vrstvy jsou *Cirrus, Cirrocumulus* a *Cirrostratus*. *Cirrus* vzniká za nízkých teplot (-40 až -50°C), složen výhradně z ledových krystalků. Tato oblaka vypadají jako jasně bílá vlákna, Slunce i Měsíc skrz ně snadno prosvítá. Podobně jsou charakterizována zbylá oblaka v této výšce, tedy že jsou tenká, průsvitná a složená z ledových krystalů.

Výška je určena pro střední klimatické pásmo, pro oblasti rovníku jsou oblaka situována výše, zatímco v polárních oblastech níže. Krom jmenovaných oblak existují i tzv. vertikálně mohutná oblaka, která přesahují jednotlivé vrstvy. Např. *Nimbostratus* a *Cumulonimbus* [51]. Vertikální velikost těchto mraků je až několik kilometrů, a když se vytvoří, téměř vždy jsou zdrojem dešťů a bouřek. Vzhledem k jejich mohutnosti jimi slunce neprosvítá, a tedy ani laserové paprsky jimi neprojdou.

3.3 Popis existující topologie

V této sekci je blíže přiblížen kvantový systém, který se nachází na univerzitě VUT v Brně. Do detailu je zde znázorněno schéma včetně použité technologie. Pro systém kvantové kryptografie je použit *Clavis*^{3} od švýcarské firmy IDQ. Dále jsou zde krátce zmíněna další zařízení této firmy, která vyrábí různé platformy kvantové komunikace.

3.3.1 Zařízení firmy IDQ

Clavis^3 je navržen a určen převážně pro akademické a laboratorní prostředí [21]. Zařízení je postaveno tak, aby uživatel mohl konfigurovat různé parametry a snadno vyčíst různé statistiky. A to buď automatizovaně, nebo manuálně [21, 57]. Mimo toto konkrétní zařízení firma nabízí i další. Lze je rozdělit na QKD zařízení a na šifrátory, které za pomoci vygenerovaného klíče zajišťují zabezpečenou komunikaci po klasickém kanále.

QKD systémy

- *Clavis XG QKD* – zařízení určené pro podnikové, vládní sítě a rozsáhlejší topologie. Nabízí vysokou rychlost generování klíčů (až 100 kbit/s). Je zaměřeno na použití v kritické infrastruktuře a finančnictví.
- *Clavis*^{300} – modulární zařízení vhodné pro testování různých konfigurací sítě. Dosah kvantového spoje u tohoto stroje je 70 km. Volitelně do něj může být integrován korejský LEA šifrátor. Používá BB84 jako QKD protokol.
- *Cerberis XG QKD/Cerberis*^{3} – umožňuje zapojení složitějších topologií, jako je např. hvězdicové, kruhové a smíšené propojení. Používá se pro data centra a v systémech odolných proti výpadku některých uzlů. Obsahuje také QNC (Quantum Node Controller), který usnadňuje distribuci klíčů mezi QKD uzly a dobře funguje jako důvěryhodný uzel pro delší spojení.

Šifrátory

- *Centauris CV1000* – virtuální šifrátor běžící na Linuxu. Flexibilní, snadně integrovatelná varianta. Podporuje vícevrstvou komunikaci a rychlost šifrování je 5 Gbs.

- *Centauris CN9000* – Zvládá vytvářet klíče jak ve dvou uzlových sítích, tak pro vícebodové sítě a plně propojené sítě. Využívá 256bitový AES pro šifrování a FPGA karty pro real-time zpracování velkého množství dat (až 100 Gbs).

QKD Systém Clavis^3

Celý *Clavis*^{3} systém se skládá ze dvou modulů, jeden je znázorněn na obrázku 3.6. Vysílač (Alice) kvantových dat a přijímač (Bob). Protokol kvantové komunikace je založen na koherentním jednosměrném protokolu – COW, ten je blíže popsán ve druhé kapitole 2.4.4. Alice i Bob jsou propojeni kvantovým i servisním kanálem[2] pomocí optických kabelů, které jsou zakončené LC/UPC konektory. Bezpečná výměna klíčů je možná pouze, pokud je útlum na kvantovém kanále 12 až 18 dB [21]. *Clavis*^{3} také obsahuje integrovaného správce klíčů (KM), který vyřizuje požadavky na klíč od externích šifrátorů. Ten není součástí. Nutno podotknout, že generování klíčů je jednosměrné, tedy pouze Alice má zabudovaný vysílač a na straně Boba je přijímač.

Pro předání klíče mezi KM a šifrátorem slouží bezpečné rozhraní `ETSI API`, na kterém lze komunikovat [92]. Obě zařízení musí být v zabezpečené oblasti, aby nebyla narušena bezpečnost systému. Tento protokol standardizuje rozhraní na zařízeních pro QKD a šifrátory od jiných výrobců. Je založen na principu `REST API`, u kterého komunikace probíhá pomocí HTTPS [57, 92].

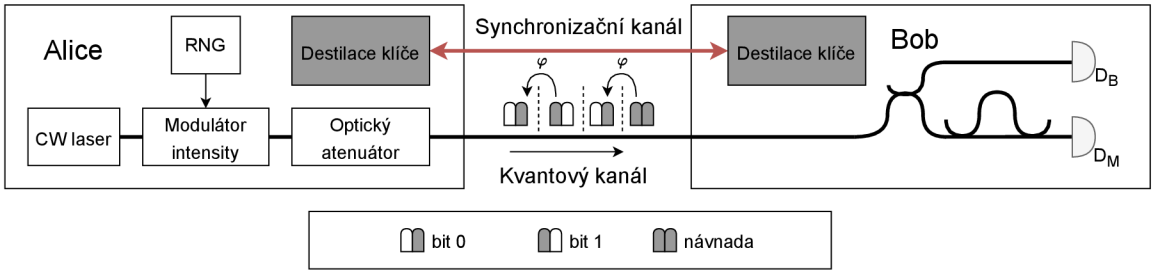
Na obrázku níže 3.7 je znázorněné fungování COW protokolu u *Clavis*^{3} QDK. Alice generuje spojité vlny o stejné amplitudě a frekvenci pomocí CW laseru (angl. Continuous Wave). Světelné paprsky jsou následně modulovány tak, aby tvořily koherentní optické pulsy reprezentující bit 0, bit 1 nebo návnadový bit (dva plné pulsy). Bit je reprezentován dvojicí pulsů, u nichž je optická energie fotonu obsažena buď v prvním, nebo ve druhém pulsu. Dále pulsy putují do optického atenuátoru, který slouží ke snižování útlumu [79].

Na straně příjemce (Boba) pak přijatá data jdou buď do větve D_B, ve které se z přijatých fotonů generuje klíč, nebo do větve D_M, v níž se nachází interferometr a monitoruje se, zda generování klíče neodposlouchává útočník (Eva).

Poté, co se vymění dostatečný počet bitů, musí dojít ještě k tzv. zpracování neboli destilaci klíče. Cílem této činnosti je opravit chyby, které se mohly objevit během přenášení klíče, a omezit počet informací (bitů), které by potenciální útočník mohl znát. U *Clavis*^{3} je tato činnost plně automaticky implementována. Destilace klíče probíhá po veřejném zabezpečeném kanále, na kterém se obě strany musí navzájem autentizovat. Destilace klíče se skládá z několika kroků [57, 21, 3]:

[2]Servisním kanálem se rozumí „nekvantový“ kanál, který slouží pouze k synchronizaci obou zařízení. Šifrovaná komunikace mezi oběma body probíhá na jiném kanále.

Obrázek 3.6: *Clavis*^{3}



Obrázek 3.7: Fungování COW protokolu uvnitř *Clavis*[3]

- Prosetí klíče – odstranění bitů, které nelze použít do klíče, např. návnadové bity. Jedná se o první filtraci hrubého klíče. V této fázi také dojde ke spočítaní chybovosti během přenosu – QBER. Ta může být způsobena ztrátovostí kvantového kanálu, nedokonalostmi detektorů apod. Chybovost může být způsobena také Evou, která kvantový kanál odposlouchává. Je tak nutno statisticky odvodit množství informací, které má Eva k dispozici I_{Eve}. Většinou se toleruje QBER do cca 11 %. Pokud by byla chybovost větší, Alice a Bob přeruší komunikaci a klíč zahodí.

- Schválení klíče – dochází k nápravě bitů neboli korekci chyb. K tomu se používá LDPC (nízkohustotní kód s kontrolou parity) algoritmus. Sice Eva nemůže narušit tento proces, teoreticky ale může odposlouchávat. Naroste tak množství informací, které zná o $|M|$, tedy o počet paritních bitů zveřejněných během kontroly – $I_{Eve} + |M|$.

- Amplifikace bezpečnosti – za použití Wegman-Carter univerzálního hašování se redukuje množství informací, které má Eva k dispozici. Nevýhodou této fáze je, že dojde k redukci velikosti klíče. Čím víc má Eva informací, tím je nutná větší komprese, a tedy menší velikost klíče. Celková velikost zabezpečeného klíče, který je možné použít, se rovná $I - I_{Eve} + |M|$. Cílem hašovací funkce je, aby každý bit výstupu závisel na co možná nejvíce vstupních bitech. Tedy aby v případě, že Eva zná bit x_1, nebyla nikterak schopna odvodit bit x_2.

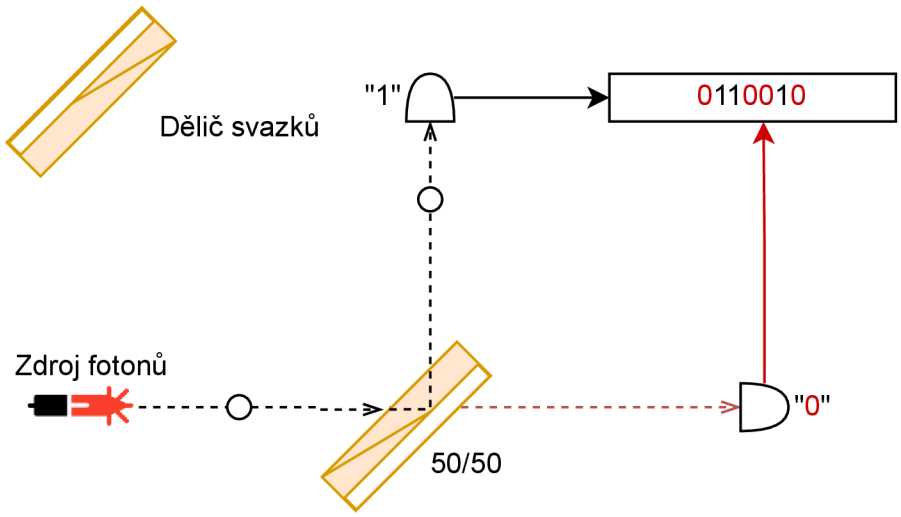
- Autentizace – Alice i Bob se navzájem autentizují za použití OTP. Cílem je zabránit Man-in-the-middle útoku. Autentizace probíhá za pomoci předsdíleného klíče na klasickém kanálu. Klíč se použije pouze pro prvotní data, poté se už používají části vyprodukovaného klíče.

Poté, co je klíč ustanoven a uložen, může být zpřístupněn skrz manažera klíčů (KM).

3.3.2 Generátor náhodných čísel

Pro správné generování náhodné posloupnosti, která bude využita jako základ pro budoucí klíč, je důležité, aby tato posloupnost byla náhodná. Je tedy nutné mít k dispozici opravdový (true) generátor náhodných čísel (RNG). Pseudonáhodné generátory jsou v kryptografii naprosto nepřijatelné. RNG použité v zařízeních QKD mohou být založené na principech kvantové fyziky, která zaručuje spolehlivou náhodnost. Jedna z možností je zobrazena na následujícím obrázku. Využívá dělič svazků, na který se střílí částice světla. Je postaven tak, že z 50 % se foton odrazí k detektoru 1 a z 50 % projde skrz k detektoru 2. Podle toho, který detektor zachytí foton, se generuje číslo 1 nebo 0 [91]. Tento princip je znázorněn na obrázku 3.8. Existuje také varianta, která používá obrazový snímač CMOS (založený

na unipolárních tranzistorech). Zdroj světla LED je ovlivněn kvantovým šumem a vysílá náhodný počet fotonů na snímač. Podle toho, kolik jich snímač zachytí, je ustanovena náhodná sekvence čísel. Tento generátor je patentován firmou IDQ a nachází se v jejich Quantis QRNG čipech [90]. Mohou být použity v různých zařízeních od mobilů, IoT až po náročná bezpečnostní zařízení. Podle použití mají také jinou rychlost generování entropie (náhodnosti). V současnosti se tyto hodnoty pohybují od 250 Kbps až po 20 Mbps. Zároveň generátor průběžně testuje, zda jsou všechny součástky funkční.

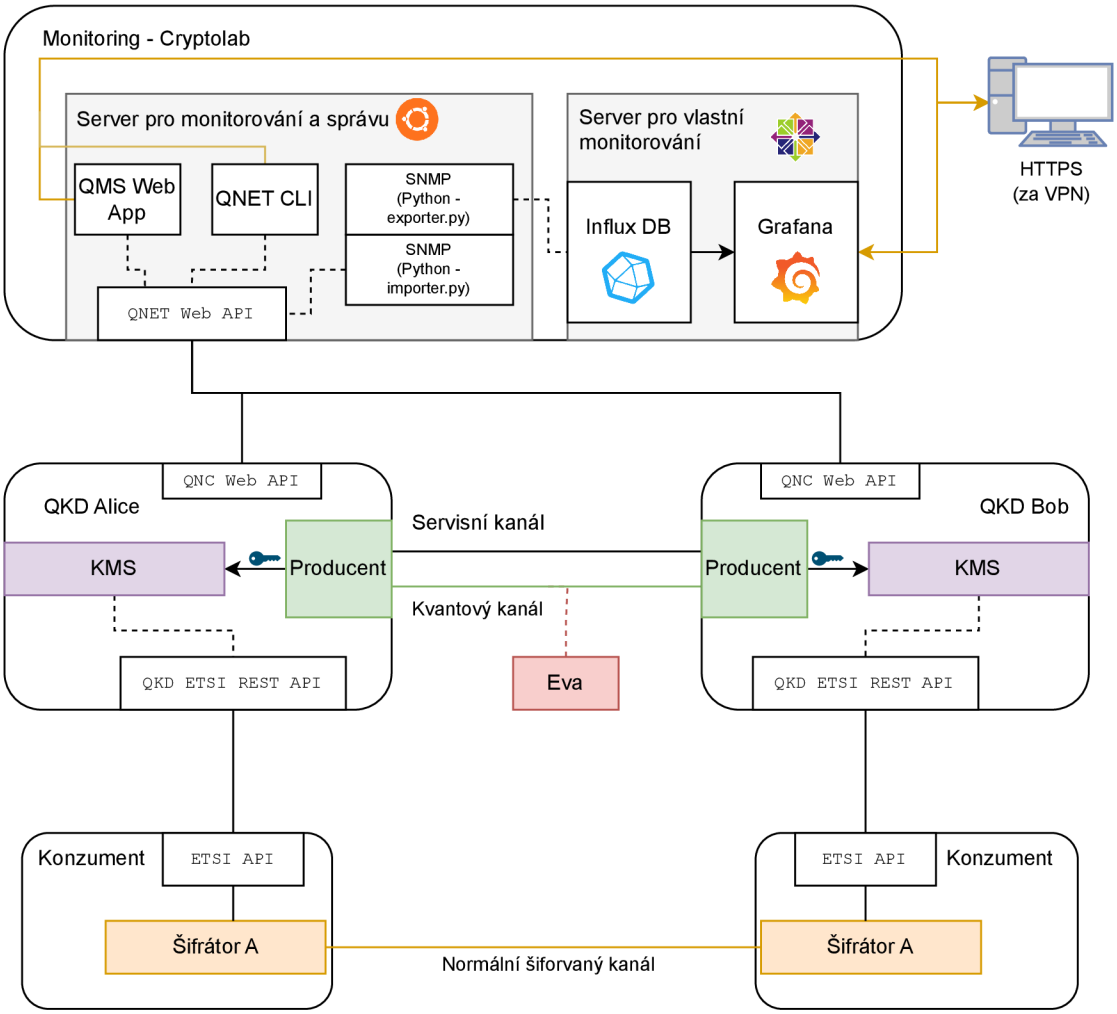


Obrázek 3.8: Kvantový generátor náhodných čísel (QRNG)

3.3.3 Schéma topologie

Schéma topologie, které se využívá mezi fakultami informačních technologií a elektrotechniky VUT v Brně, je znázorněno na následujícím obrázku 3.9. Aby bylo možné QKD modul konfigurovat a monitorovat, obsahuje rozhraní `QNC Web Api`. S tímto rozhraním komunikuje server s Linuxovou distribucí Ubuntu, který ke komunikaci využívá `QNET Web Api`. Nad tímto rozhraním se používá QMS (angl. Quantum Management System) [92, 99, 52, 93]. Jedná se o grafickou aplikaci, skrz kterou lze ovládat systém správy klíčů (KMS). QNET CLI slouží k ovládání modulů skrz příkazovou řádku. Tento software lze nainstalovat za použití Docker Enginu, jenž dokáže virtualizovat OS v podobě kontejnerů. Dále se na serveru používá dvojice skriptů, která se stará o alternativní monitorování skrz protokol SNMP[3]. Jeden pro import a druhý pro export statistik z QKD modulů. Pro zobrazení a zpracovávaní dat slouží druhý server s nainstalovaným systémem CentOS. Data si stahuje z prvního serveru a ukládá do InfluxDB databáze. InfluxDB je obecně open-source databáze a slouží k ukládání časových údajů. Je užitečná pro monitorování, sbírání dat ze senzorů a analýzu dat v reálném čase. Z InfluxDB se poté data načítají do Grafany, která umožňuje vytvářet z dat grafy a různé statistiky. Oba servery se nachází v síti Cryptolab, která je schovaná uvnitř sítě VUT. Pro přístup mimo VUT síť je nutné použít zabezpečené VPN spojení. Konzumenti klíčů komunikují za pomoci rozhraní `ETSI API` [92, 57, 99, 52, 93]. Schéma obsahuje také útočníka (Evu), více o ní bude zmíněno v pozdější sekci 7.3.

[3]SNMP protokol se hojně používá pro sběr dat pro potřeby sítě, jejího monitorování a správy. Pracuje nad UDP.



Obrázek 3.9: Schéma topologie na univerzitě VUT v Brně

Kapitola 4

Kryptografické algoritmy

Tato kapitola se zaměřuje na kryptografii, která se používá pro šifrování dat na internetu. Na začátku jsou zmíněny problémy a výzvy, jež jsou spjaty se současnou kryptografií. Dále jsou popsány dva typy kryptografických algoritmů: asymetrické a symetrické šifry. Větší prostor je věnován symetrické kryptografii z důvodu menší energetické spotřeby daných algoritmů a propojení s QKD systémy. Seznam popsaných algoritmů není výčtem všech existujících. Výběr je zvolen tak, aby obsáhl zástupce různých tříd. V práci jsou zmíněni zástupci blokových či proudových šifer, light-weight šifer pro energeticky náročná zařízení a post-kvantové šifry.

4.1 Problémy kryptografie

Algoritmů, které se používají pro zašifrování zpráv přenášených po síti, existuje velké množství. Každý z nich nabízí jiné vlastnosti a má rozdílné využití. Základní dělení, které se používá, je asymetrická a symetrická kryptografie [28]. Jak je více rozvedeno v části 4.4, s příchodem dostatečně výkonných kvantových počítačů nejvíce utrpí algoritmy asymetrické kryptografie. Další nevýhodou asymetrické kryptografie je její relativně velká výpočetní náročnost. Pro běžné domácí počítače to není problém. Existuje ale mnoho zařízení, u nichž výkon není velký a jsou často limitována zdrojem elektrické energie. Jsou to například bezdrátová síťová zařízení, různá IoT[1] zařízení a vestavěné (embedded) systémy [28]. S čím dál větším nasazením 5G sítí, které umožní větší kanály (větší rychlost přenosu dat), nižší latenci (lepší odezvu) a schopnost připojit mnohem více zařízení najednou, se očekává ještě větší množství IoT zařízení, senzorů a inteligentních zařízení. Jejich využití je takřka všude od průmyslu, zdravotnictví, automobilismu, až po systémy pro chytrá města a domácnosti Napájení různých bezdrátových a na dálku ovládaných systémů stále zůstává problém. Výměna baterií pro bezdrátový senzor může být náročný a drahý proces. Vzniká tak řada projektů a výzkumů, které se zaměřují na bezdrátové nabíjení (WPT – Wireless Power Transfer) [87]. Ta se snaží tato zařízení dobíjet pomocí harvestování energie z okolí, přičemž je zařízení schopno se dobíjet radiofrekvenčním signálem pomocí dedikované dobíjecí stanice. Symetrická kryptografie je z pohledu spotřeby energie i délky klíče pro tato zařízení efektivní a vhodná. Problém symetrické kryptografie spočívá v podobě bezpečné výměny klíčů, u níž obě zařízení musí mít ten stejný identický klíč [28]. Tento problém mohou pomoci vyřešit kvantové QKD systémy pro generování klíčů, u kterých je bezpečnost předání klíčů založena na fyzikálních zákonech.

[1] Někdy též označované jako WSN (Wireless Sensor Network) sítě.

4.2 Asymetrická kryptografie

Asymetrické šifry jsou založeny na matematických problémech, které lze snadno vyřešit v jednom směru, ale v druhém už nikoliv, resp. jedná se o výpočetně náročnou operaci a pro velká čísla je prakticky nemožné je spočítat v reálném čase [70]. Důvodem toho je existence velmi vysokého počtu možných řešení, přičemž je nutné ověřit všechny. Jedná se o tzv. jednosměrné funkce.

Asymetrická kryptografie používá dvojici klíčů: veřejný a soukromý [70]. Veřejný klíč je dostupný všem a jeho pravost lze ověřit pomocí digitálního certifikátu, který vydává certifikační autorita (CA). Soukromý klíč musí zůstat v tajnosti a neměl by opustit počítač. Většinou se veřejný klíč používá k zašifrování zprávy, kterou dokáže rozluštit pouze majitel soukromého klíče. Dvojice klíčů musí být matematicky svázaná. Odesílatel může zároveň zprávu zašifrovat i svým soukromým klíčem. Tím ho podepíše a prokáže druhé straně, že právě on je původcem zprávy a ne nikdo jiný. Příjemce si může podpis ověřit veřejným klíčem [70].

S příchodem výkonných kvantových počítačů utrpí asymetrická kryptografie nejvíce. V roce 1994 Peter Shor přišel s kvantovým algoritmem, který je založen na kvantové Fourierovské transformaci [110]. Algoritmus je schopen řešit problém faktorizace nebo problém diskrétního logaritmu v polynomiálním čase (klasické počítače řeší tento problém s exponenciální složitostí). Toto představuje obrovský problém, neboť algoritmus bude možné využít na prolomení běžně používaných asymetrických šifer, jako jsou např. RSA nebo Eliptické křivky [70].

Výhodou asymetrické kryptografie je, že není problém se sdílením klíčů, jako tomu bylo v případě symetrické kryptografie. Je ale nutné správně ověřit pravost veřejného klíče. Na druhou stranu je asymetrická kryptografie pomalejší a více výpočetně náročná [70].

4.3 Symetrická kryptografie

Symetrická kryptografie využívá k šifrování zpráv jeden společný klíč, který musí mít k dispozici pouze komunikující strany [123]. Klíč představuje sdílené tajemství, které následně šifrovací algoritmy použijí pro zašifrování zprávy. Příjemce zprávy je poté schopen stejným klíčem zprávu dešifrovat. Oproti asymetrické kryptografii jsou klíče daleko kratší (s výjimkou Vernamovy šifry 4.5.2) a jsou méně výpočetně a paměťově náročné. Jejich obrovskou nevýhodou je problém distribuce klíčů, tzn. to, aby bylo bezpečně zajištěno, že obě strany mají k dispozici identický klíč. Varianta, kdy člověk nahraje klíč na paměťové médium a přenese ho k druhé straně, je značně nepraktická. Existuje proto Diffieho-Hellmanova výměna klíčů. Jedná se o protokol, který umožňuje mezi komunikujícími stranami ustanovit klíč po nezabezpečeném kanále, aniž by byl kdykoliv přenesen v otevřené formě. Princip se opírá o složitost výpočtu diskrétního logaritmu. Tento protokol je ovšem zranitelný proti Man-in-the-middle útoku, protože neumožňuje autentizaci účastníků. Lze ho tedy použít pouze tam, kde útočník nemůže aktivně zasahovat do komunikace [31]. Často se proto používá hybridní forma šifrování, při které se zpráva prvně zašifruje symetrickou šifrou. Výstup včetně klíče se následně zašifruje asymetrickým šifrováním s veřejným klíčem. Symetrické šifrování nezajišťuje tzv. účtovatelnost, tedy nelze určit třetí stranou, který z dvojice mající klíč je původcem zprávy. Zbylé bezpečnostní funkce jako integrita, důvěrnost a autentizace jsou zajištěny [123, 28].

Pro bezpečnou výměnu klíčů lze využít QKD systémy, které bezpečným způsobem zajistí shodné klíče mezi oběma komunikujícími stranami. Tyto klíče pak mohou odebírat nejrůznější aplikace a zařízení.

4.4 Vliv kvantových počítačů na současnou kryptografii

Současná kryptografie spoléhá na robustnost v podobě velikosti šifrovacího klíče, přičemž nejlepší útok je hrubou silou[2]. U nejrozšířenější asymetrické šifry RSA je v současnosti doporučena velikost klíče 2048–4096 bitů. Nižší hodnoty jsou náchylné na prolomení jinou než hrubou silou [24]. Se zvyšujícím se výkonem kvantových počítačů však není udržitelné zvětšovat velikost klíče. Jako náhradu za asymetrickou kryptografii se začínají vyvíjet post-kvantové algoritmy. Americký Národní institut standardů a technologie (NIST) provádí výběrové řízení post-kvantových algoritmů, které by se měly standardizovat a začít v nejbližší době používat. Jeden z těchto algoritmů – *CRYSTALS-Kyber* už byl dokonce doporučen k používání [1]. Tento algoritmus se řadí do skupiny úloh na bodových mřížích (angl. Lattice Based Problem). Ty jsou založeny na problému nejkratšího vektoru na bodové mřížce [71, 97]. Algoritmy založené na tomto problému se jeví jako dostatečná náhrada za asymetrickou kryptografii, neboť se ukázalo, že jsou v současnosti odolné jak vůči klasickým, tak i kvantovým počítačům. Bohužel mřížkové algoritmy neškálují příliš dobře a do budoucna bude potřeba najít náhradu i za ně. Příkladem dalších mřížkových algoritmů je např. *NTRU* [24, 1].

Další typ „post-kvantových“ algoritmů je založen na hašování, sloužící především pro elektronické podepisování dokumentů [24]. Tyto haše jsou pouze na jedno použití – OTS (angl. One Time Signature). Fungují na principu toho, že pro podepisovanou hodnotu se vytvoří dlouhý řetězec náhodných znaků (soukromý klíč). Ten se poté dá na vstup hašovací funkce, která z něho vytvoří haš, který je následně zveřejněn (jako veřejný klíč) [24, 98]. NIST zvolil algoritmy $SPHINCS^+$, *Falcon* a *CRYSTALS-Dilithium* jako standardy pro hašovací a podpisové algoritmy odolné proti kvantovým počítačům [1].

Ani symetrická kryptografie nezůstane nepoškozena s příchodem kvantového počítače. Groverův kvantový prohledávací algoritmus oproti hledání klíče hrubou silou vykazuje výrazné kvadratické zrychlení [24]. Nepředstavuje to ovšem takovou hrozbu, jako tomu bylo v případě asymetrické kryptografie. Pro asymetrické algoritmy bude stačit zdvojnásobit délku klíče, čímž se zajistí jejich bezpečnost [24, 6]. Níže je tabulka 4.1, která porovnává míru zabezpečení u asymetrické a symetrické kryptografie.

Bity bezpečnosti si lze představit jako počet kroků na druhou mocninu, které musí počítač provést, aby rozluštil klíč při použití nejvíce efektivního algoritmu pro prolomení. Například 112 bitů bezpečnosti znamená, že k prolomení je potřeba provést 2^{112} kroků.

[2] Útok hrubou silou znamená systematicky vyzkoušet všechny možné kombinace klíčů, dokud se nenalezne ten správný. Jedná se o nejrychlejší způsob jak prolomit šifru.

Typ počítače	Symetrická kryptografie			Asymetrická kryptografie		
	algoritmus	délka klíče	bity bezpečnosti	algoritmus	délka klíče	bity bezpečnosti
Klasický počítač	AES-128 AES-256	128 256	128 256	RSA-2048 RSA-15,360	2048 15 360	112 256
Kvantový počítač	AES-128 AES-256	128 256	64 128	RSA-2048 RSA-15,360	2048 15 360	25 31

Tabulka 4.1: Porovnání bezpečnosti asymetrické a symetrické kryptografie s příchodem kvantových počítačů. Asymetrická kryptografie nebude ani s velkým klíčem dostatečně bezpečná[3].

4.5 Zástupci symetrických šifer

Algoritmy jsou často založeny na jednoduchých kryptografických operacích, které se opakují několikrát. Výsledkem je dostatečně silný zašifrovaný text. Symetrickou kryptografii lze rozdělit na dva typy [28] zmíněné níže. Nelze obecně říci, který druh je bezpečnější. Záleží především na kvalitě šifrovacího klíče [22].

- Proudové šifry – šifrují zprávu po jednotlivých znacích. Jsou užitečné v prostředích, v nichž dochází k velkým ztrátám při přenosu, neboť chyba jednoho znaku neovlivní zbytek (platí pro asynchronní šifry). Popřípadě tam, kde je nutné transformovat postupně symbol jeden po druhém, například v systémech s chybějícím paměťovým zařízením. Příkladem proudové šifry je např. RC4, Salsa20, SEAL, FISH.

- Blokové šifry – šifrují zprávu po blocích, většinou o velikosti 64 nebo 128 bitů. Pokud délka šifrované zprávy není násobkem 8, používá se zarovnání. Např. pro zašifrování 150 bitů textu se vytvoří dva bloky o 128 bitech. Druhý blok zašifruje 22 zbylých bitů zprávy a přidá redundanci v podobě zbylých 106 bitů. Jsou rozšířenějším typem. Příkladem blokových šifer je např. AES, 3DES, BLOWFISH.

Operační režimy šifer

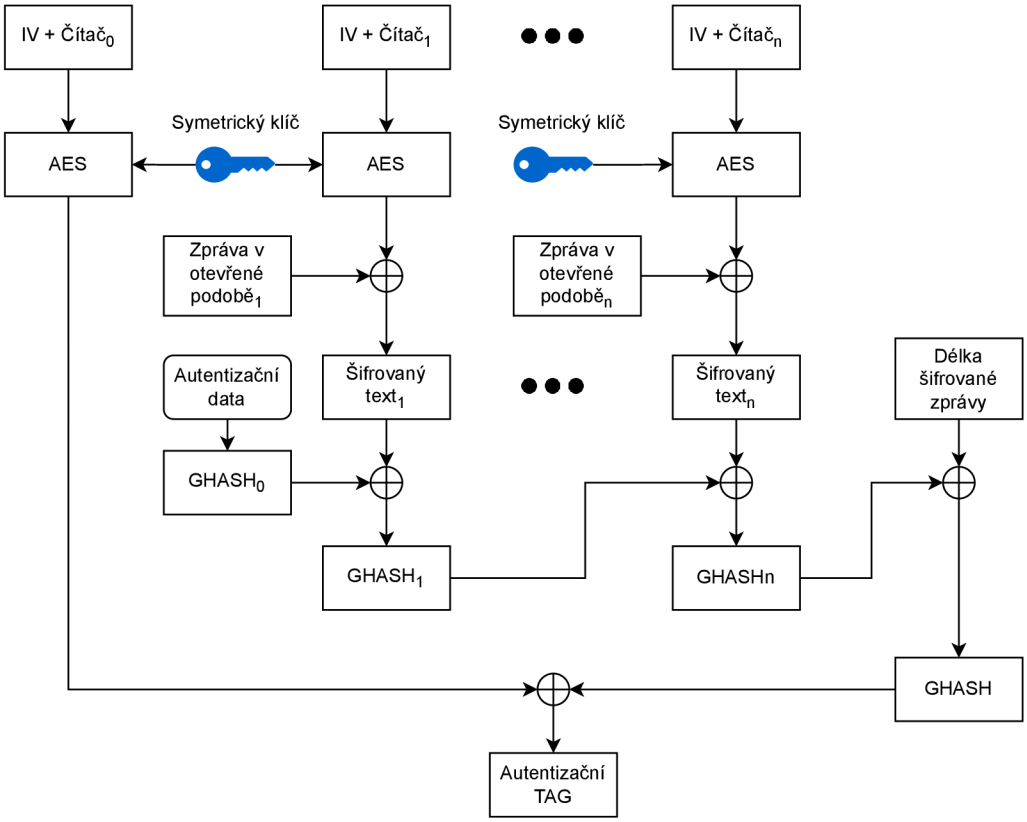
Pro blokové šifry existuje několik operačních módů, které ovlivňují jejich chování [119, 22]:

- ECB (Electronic Codebook) – nejjednodušší a nejméně bezpečný režim. V tomto režimu je zpráva rozdělena do bloků a každý blok je zašifrován zvlášť. Výhodou je možné paralelní zpracování. Tento režim ovšem poskytuje příliš mnoho informací o zašifrovaném textu. Lze tak snadno odvodit podobné vzory. Pokud pošleme jinou zprávu, která bude velice podobná další zprávě, budou mít tyto zprávy podobné kryptogramy, což může být využito na prolomení šifrovaného textu.

- CBC (Cipher block chaining) – v tomto režimu se kombinuje otevřený blok textu se zašifrovaným blokem textu z předchozího bloku. Kombinace se provádí operací XOR. Teprve poté se daný text zašifruje. Na první blok textu je použit inicializační vektor[4] (IV). Tento režim je bezpečnější než ECB, nicméně je pomalejší. Každý blok dat musí čekat na výsledek předchozího kroku, a není tedy možná paralelizace. Pokud by útočník byl schopen ovlivnit některý blok dat, ovlivní to všechny následující.

[3] Převzato z [55].

[4] Inicializační vektor je náhodná sekvence znaků, která se použije pro zašifrování prvního bloku dat.



Obrázek 4.1: Režim GCM, který využívá čítače a zároveň poskytuje autentizaci

- CFB/OFB (Cipher Feedback/Output Feedback) – CFB má na vstupu šifrovacího algoritmu výsledný zašifrovaný text z předchozího bloku. Výstup algoritmu je poté XORován se zprávou, kterou chceme šifrovat. Výsledek je šifrovaný text, který se zároveň vyskytuje i na vstupu dalšího bloku. Pro první blok se použije inicializační vektor. OFB pracuje podobně, pouze s tím rozdílem, že na vstupu šifrovacího algoritmu je výsledek předchozího bloku ještě před XORováním s šifrovanou zprávou.
- CTR (Counter Mode) – jeden z novějších režimů, je doporučen NISTem jako bezpečná varianta. Podobně jako v ECB je každý blok šifrován zvlášť. Nicméně na vstupu šifrovacího algoritmu je čítač, který funguje podobně jako inicializační vektor. Sekvence, kterou čítač generuje, se nesmí opakovat po dostatečně dlouhou dobu. Výstup algoritmu je poté XORován se šifrovanou zprávou. Poté se hodnota čítače zvýší (většinou o 1, ale není to pravidlem).
- GCM (Galois/Counter Mode) – režim kombinuje čítač s autentizací. Princip je znázorněn na obrázku 4.1. Blok zprávy, který chceme zašifrovat, je XORován s výstupem šifrovacího algoritmu, jenž má na vstupu čítač s inicializačním vektorem. Šifrovaný text je poté XORován s výstupem autentizační funkce, která má na začátku autentizační data, jež vzniknou násobením na Galoisově tělese. Posledním krokem je XORování hodnoty délky šifrované zprávy s výstupem prvního kroku algoritmu. Vznikne tag, který je poté použit pro autentizaci a kontrolu integrity.

Mimo výše jmenované existují i další režimy blokových šifer, např. SIV s autentizací, CCM nebo PCBC [119, 22].

4.5.1 AES (Rijndael)

AES (Advanced Encryption Standard) je bloková šifra založená na substitučně-permutační síti. Pracuje vždy s pevně danou velikostí bloku 128 bitů. Velikost klíče použitého pro šifrování může být 128, 192 nebo 256 bitů. V roce 2001 byla standardizována a schválena NISTem (původní název byl Rijndael) a její implementace je volně dostupná [26]. V dnešní době se jedná o nejvíce používanou a rozšířenou symetrickou šifru, která poskytuje vysokou úroveň zabezpečení. Je používána americkou vládou k šifrování tajných dokumentů, u SSL/TLS protokolu, pro bezdrátové Wi-Fi sítě v rámci zabezpečení WPA2 a u mnoha dalších aplikací. Podle velikosti klíče má buď 10, 12 nebo 14 kol. Na začátku se spočítají rozdílné klíče pro jednotlivá kola (Round Keys). Ta se odvodí z klíče na vstupu za pomoci tzv. Key Schedule algoritmu. Se vstupním blokem 128 bitů pracuje algoritmus jako s maticí 4x4 bajtů. Jednotlivá iterační kola se poté skládají z následujících akcí:

- Záměna bajtů – substituční část algoritmu. Každý bajt je nahrazen jiným bajtem za pomoci vyhledávací tabulky (angl. lookup table) neboli S-boxu.
- Prohození řádků – každý řádek matice je posunut o daný počet řádků.
- Kombinování sloupců – jedná se v podstatě o maticové násobení. Každý sloupec je roznásoben se specifikovanou maticí. Změní se tak pozice každého bajtu ve sloupci.
- Přidání klíče – za pomoci operace XOR se přidá klíč speciálně vytvořený pro dané kolo (Add Round Key).

Prohození řádků a kombinace sloupců tvoří permutační část algoritmu. V posledním kole je vynechán krok s kombinací sloupců. Po provedení všech kol je na výstup dán zašifrovaný 128bitový blok dat. Tento postup se aplikuje na celou délku šifrované zprávy. Pro dešifrování zprávy se použijí stejné operace v opačném pořadí [26, 28].

4.5.2 Vernamova šifra

Vernamova šifra neboli OTP (angl. One Time Pad) je jednoduchý způsob, jak zašifrovat zprávu. Zpráva se zašifruje pomocí náhodného klíče tak, že každý znak zprávy se posune abecedně o tolik písmen, kolik je určeno pozicí klíče [65]. Např. zpráva ABCD se při použití klíče 3825 změní na CIDH. Jedná se o šifru, která byla patentována v roce 1917 a za splnění daných podmínek je nerozluštitelná:

- Délka klíče je stejná jako délka přenášené zprávy.
- Klíč musí být zcela náhodný. Nesmí vzniknout z pseudonáhodného generátoru, ale musí se jednat o opravdový generátor náhodnosti, např. za využití šumivých diod, hardwarových prvků, radioaktivního rozpadu atd.
- Klíč nesmí být použit více než jednou. Pro zašifrování další zprávy je potřeba vytvořit nový klíč.
- Klíč znají pouze příjemce a odesílatel.

Za splnění těchto podmínek je šifra neprolomitelná. Toto tvrzení je podpořeno matematickým důkazem [108], který je založen na myšlence, že zašifrovaný text může být přeložen do jakékoliv jiné posloupnosti znaků se stejnou pravděpodobností. Šifrovaný text nedává

žádnou užitečnou informaci potřebnou k rozlousknutí zprávy. Statická kryptoanalýza není možná, neboť z každého písmene vznikne jakékoliv písmeno abecedy. Útok hrubou silou také není možný – jedná se o jedinou šifru odolnou i proti tomuto typu útoku. I kdyby měl útočník k dispozici neomezený výpočetní výkon a vyzkoušel by všechny možnosti, výsledkem budou opět jenom posloupnosti všech možných zpráv o dané velikosti. Nelze z toho určit, která je správná [121, 65].

Ačkoliv je tato šifra zcela bezpečná, z praktických důvodů se takřka nepoužívá. Omezení na zcela náhodný klíč o velikosti stejné jako přenášená zpráva je problematické. I samotné předání klíče mezi dvěma účastníky musí být zcela bezpečné. Pro předání klíčů mohou sloužit právě kvantové QKD systémy, u nichž je bezpečnost zaručena fyzikálními vlastnostmi přenosu. Musí být ale dostatečně výkonné, aby stíhaly vytvářet klíče požadované délky dostatečně rychle.

4.5.3 DES/3DES

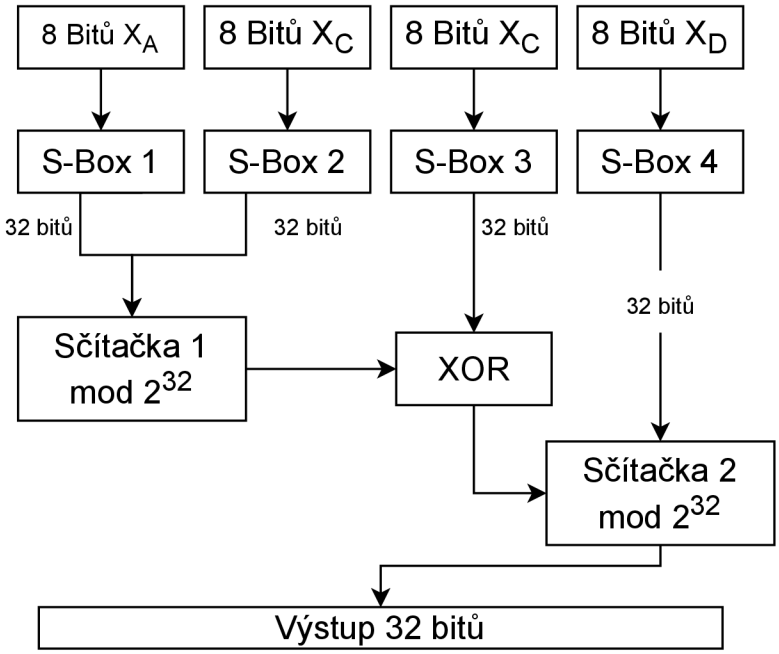
Jedna z prvních blokových šifer. Šifruje bloky o velikosti 64 bitů 56bitovým klíčem. Zbylých 8 bitů se používá na kontrolu parity. Blok šifrovaného textu se rozdělí na dva bloky o velikosti 32 bitů, které se střídají ve zpracování. Používá se tzv. Feistelova funkce, která zahrnuje 4 kroky [9]. Rozšíření 32bitového bloku na velikost 48 funguje tak, že se duplikuje polovina bitů. Ve druhém kroku se blok zkombinuje s podklíčem za pomoci XOR (podklíče jsou odvozeny od vstupního klíče). Dále se provede substituce za pomoci S-boxů, z nichž vyleze 32bitový blok, na který se finálně aplikuje permutace (P-box). Na konci se spojí dva původní 32bitové bloky a prohodí se. Tento postup se aplikuje celkem 16krát. Výstupem je 64bitový zašifrovaný blok dat. S-boxy jsou jedinou nelineární částí algoritmu, avšak jejich bezpečnost je zpochybňována. Kvůli velikosti klíče přestal být DES braný jako bezpečný. 3DES je snaha o zvýšení bezpečnosti, při níž se aplikuje algoritmus DES 3krát po sobě na stejný blok dat. Velikost klíče se sice 3krát zvětší, ale tím i výpočetní náročnost algoritmu. Algoritmus je zranitelný proti diferenciální a lineární kryptografii [28, 44, 9]. V roce 2016 bylo zveřejněno CVE [25], které odhaluje zranitelnost DES/3DES proti narozeninovému útoku. Následující rok NIST doporučil algoritmus přestat zcela používat, do roku 2023 by měly tento algoritmus všechny aplikace přestat podporovat [44].

4.5.4 Blowfish a Twofish

Blowfish je bloková šifra, kterou v roce 1993 vytvořil Bruce Schneier. Byla vytvořena jako náhrada za nedostatečně bezpečný DES. V době svého vzniku se jednalo o jednu z mála šifer, které nebyly patentovány a dodnes je volně dostupná komukoliv. Šifruje bloky o délce 64 bitů klíčem, který může nabývat velikosti od 32 do 448 bitů. Co se týče délky podporovaného klíče, je tato šifra jedna z nejbezpečnějších. Obdobně jako DES je založena na Feistelově schématu[5]. Šifrování probíhá následovně [104, 56]:

- Generování podklíčů – celkem je potřeba 18 podklíčů, které jsou uloženy do pole P. Každý podklíč má velikost 32 bitů. Jejich hodnoty se inicializují podle hexadecimálního zápisu Ludolfova čísla Pí. Hodnoty podklíče se poté postupně XORují s 32bitovými hodnotami tajného klíče na vstupu (ten se případně opakuje, pokud není dostatečně velký). Generovaní podklíčů je nejdražší operací algoritmu. Provede se pouze

[5] Feistelovo schéma znamená, že se blok šifrovaného textu rozdělí na levou a pravou část. Nad jednou se provedou šifrovací operace a poté se levá a pravá část spojí a prohodí. Takto se provede několik kol.



Obrázek 4.2: Funkce F u Blowfish šifry

jednou na začátku, hodnoty se poté uloží a lze je využít pro další zprávy šifrované stejným klíčem.

- Inicializace substitučních boxů (S-boxů). Celkem se použijí 4 S-boxy, které mají na vstupu 256 hodnot, přičemž každá hodnota je 32bitová. Počáteční hodnoty jsou opět založeny na čísle Pí.
- Šifrování – skládá se ze 16 kol. Vezme se levá část (32 bitů) šifrovaného bloku a provede se operace XOR s klíčem pro dané kolo. Výstup jde do funkce F. Funkce F je znázorněna na obrázku 4.2. Vstup se rozdělí do 4 bloků o velikosti 8 bitů. Ty jsou poté zpracovány S-boxy, u nichž každý vytvoří 32bitovou hodnotu. Hodnoty prvního a druhého S-boxu se sečtou. Následně se XORují s výstupem třetího S-boxu. Výsledek se sečte s výstupem posledního S-boxu. Výstupem funkce je 32bitová hodnota. Výstup funkce F se XORuje s pravou částí šifrovaného bloku. Nakonec se prohodí pravá část s levou a následuje další kolo.
- Po posledním 16. kole, se provede další prohození pravé a levé půlky a následně se nad levou polovinou použije 18. podklíč. Pro pravou polovinu se použije 17. podklíč.

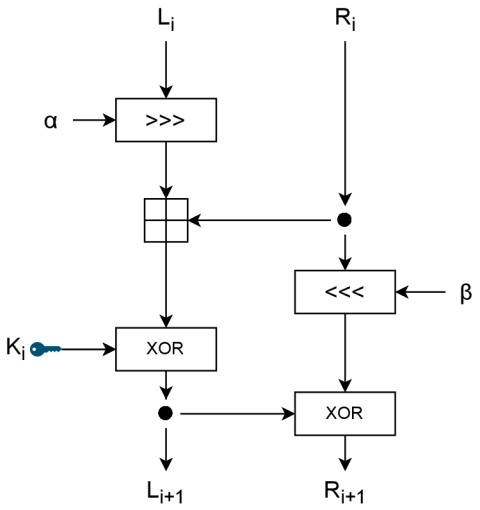
Dešifrování probíhá stejně jako šifrování, pouze pořadí, v němž se používají podklíče, je opačné [104]. Blowfish je rychlejší, efektivnější a kompaktnější algoritmus než DES. Jeho rychlost je ale ovlivněna měnícím se šifrovacím klíčem, jelikož jeho zpracování zabírá nejdelší dobu. Blowfish tedy není uzpůsobený na časté výměny klíčů. Samotné zpracování klíče je náročné na RAM paměť, je proto potřeba ekvivalent 4 KB textu, což zamezuje použití algoritmu na nejmenších vestavěných systémech a čipových kartách. Slabinou algoritmu je malá velikost šifrovaného bloku (64 bitů), je tedy zranitelný proti narozeninovému útoku. Nedoporučuje se Blowfish algoritmem šifrovat soubory o velikosti větší jak 4 GB. Jiné úspěšné útoky na šifru nebyly zaznamenány. Blowfish používá hodně aplikací, např. CryptoDisk, PasswordWallet nebo v minulosti i OpenVPN [104, 56].

Nástupcem Blowfish algoritmu je Twofish. Jedná se o jeden z pětice finalistů soutěže standardu AES. Twofish šifruje bloky dat o velikosti 128 bitů. Velikost klíče může být 128, 192 nebo 256 bitů, tedy stejně jako AES (Rijndael) [105]. Opět se používá Feistelovo schéma s 16 koly. Implementace algoritmu není nikterak patentována, může jej tedy použít kdokoliv. Šifra je navržena tak, aby byla dostatečně rychlá i na méně výkonných zařízeních, a to i v případě často měnících se klíčů, které byly problémem u Blowfish. Zároveň lze algoritmus použít na zařízeních s žádnou nebo jen silně omezenou RAM/ROM pamětí. Je tedy vhodný jak pro klasické počítače, tak vestavěné systémy a čipové karty [105, 131]. Algoritmus je možné upravit tak, aby vyhovoval dané aplikaci, hardwaru i použití. Je možné nastavit delší dobu inicializace klíče, což vyústí ve větší šifrovací rychlost. Toto je užitečné pro šifrování většího množství dat stejným klíčem. Nebo naopak inicializace klíče bude rychlá, ale samotné šifrování se zpomalí. To se hodí v momentě, kdy chceme šifrovat menší bloky dat různými klíči. Algoritmus je také flexibilní z hlediska paměti, protože při menší paměti běží šifrování delší dobu. Jedná se o velice bezpečný algoritmus (je považován za bezpečnější než AES). Twofish lze snadno optimalizovat pro různé použití a prostředí. Twofish se používá u PGP protokolu, GnuPG nebo TrueCrypt [105, 131].

4.5.5 Speck

Speck a Simon jsou algoritmy navržené pro systémy s omezenými zdroji, jako je nízká spotřeba, paměť a výkon. Speck je zaměřen na softwarovou implementaci, zatímco Simon na hardwarovou. Zde bude popsán pouze Speck. Byla snaha AES a mnohé další hojně užívané šifry optimalizovat a upravit tak, aby fungovaly i v omezených podmínkách. AES se podařilo optimalizovat na velikost ekvivalentu 2 400 hradel [73] na speciálních čipech. Tyto optimalizace jsou sice rychlé, ale poměrně komplexní. Navíc rozlohou to zdaleka není to, co by bylo možné provést na některých čipech (např. RFID čipy) [54]. Americká NSA proto vyvinula algoritmy Speck a Simon, které jsou flexibilní z hlediska síly šifrování (ne vždy je potřeba mít velikost bloku a klíče 128 bitů, když 96 může být dostačující), a zároveň jsou snadno použitelné a implementovatelné na různých 8bitových či 16bitových mikroprocesorech a na zařízeních s vysokými nároky na nízkou spotřebu. Speck používá tzv. add-rotate-xor schéma. Podporuje různé velikosti bloků, od 32 bitů po 128. Velikost klíče může být 64 až 256 bitů. Velikosti klíče přímo určují počet kol algoritmu, pro klíče 128, 192 a 256 má Speck 32, 33 a 34 kol. Princip jednoho kola algoritmu je na následujícím obrázku 4.3, na němž L_i a R_i jsou levou a pravou polovinou šifrovaného bloku. Operace $>>>$ je bitová rotace doprava, $<<<$ je bitová rotace doleva. Pro 128bitovou velikost bloku jsou hodnoty $\alpha = 8$ a $\beta = 3$. Operace $\boxplus$ představuje modulární sčítání. Jedná se o nelineární operaci algoritmu. K_i je část klíče odvozená z hlavního klíče pro dané kolo [96, 114].

Žádný úspěšný útok na algoritmus nebyl doteď zaznamenán. Bylo zveřejněno více než 70 prací zabývajících se kryptoanalýzou. Jediná nalezená slabina podle [64] je malá náhodnost šifrované zprávy v některých statistických testech NISTu. Bezpečnost algoritmu zůstává pro mnohé otázkou. Pomocí diferenciální kryptoanalýzy se povedlo dostat přes 70 % kol algoritmu [32]. V budoucnu tak může být tento algoritmus prolomen. Algoritmus je pro některé bezpečnostní experty kontroverzní z důvodu spojitosti s NSA. Existují podezření, zda neobsahuje nějaká tajná vrátka. Algoritmus byl standardizován ISO v říjnu 2018. Vzhledem k tomu, že algoritmus nepoužívá S-boxy, je imunní vůči časovému útoku (postranním kanálem). Stejně jako většina ostatních šifer je zranitelný vůči výkonové analýze [96, 114].

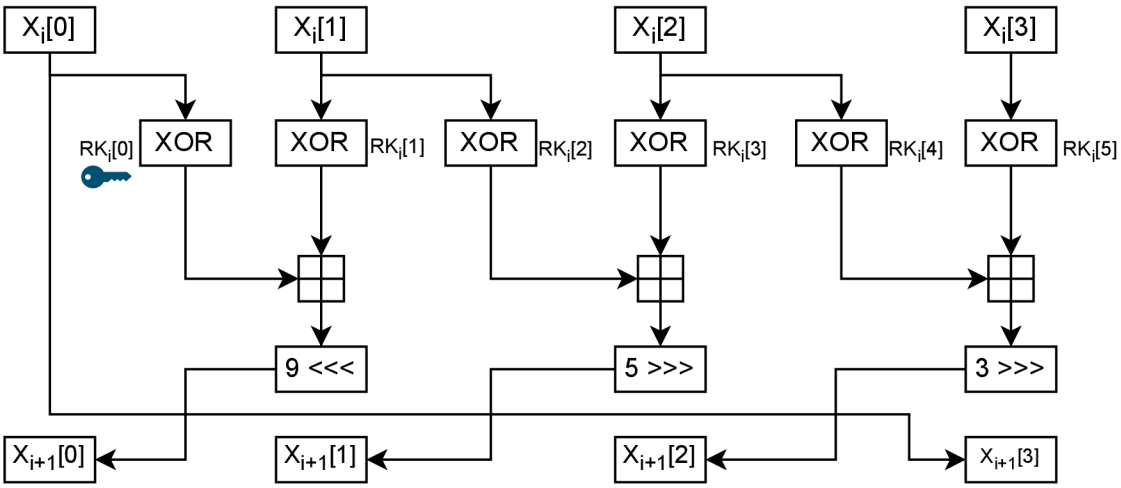


Obrázek 4.3: Průběh jednoho kola u algoritmu Speck

4.5.6 LEA

Anglicky Lightweight Encryption Algorithm je podobně jako Speck vyvinut primárně pro použití u IoT zařízení. Jedná se blokovou šifru, s velikostí bloku 128 bitů. Pochází z Jižní Koreje a je volně dostupný pro všechny. Nabízí tři velikosti klíčů, 128, 192 a 256 bitů. Počet kol je 24, 28 a 32 v závislosti na velikosti klíče [46]. Průběh šifrování je na obrázku 4.4. Vstupní blok je rozdělen na slova ve velikosti 32 bitů ($X_i[n]$). Ta se poté XORují s klíčem kola (angl. Round Key), který je odvozen od vstupního klíče algoritmu. Operace $\boxplus$ představuje modulární sčítání. Operace >>> je bitová rotace doprava, <<< je bitová rotace doleva, vždy o příslušný počet bitů.

Algoritmus je určen primárně pro 32 a 64bitové architektury. Lze ho implementovat jak softwarově, tak hardwarově [46]. Hodí se tak nejvíce na ARM architektury, které často používají 32bitové embedded procesory. Nejúspěšnější útok, tzv. boomerang attack, prolo-



Obrázek 4.4: Průběh jednoho kola u algoritmu LEA

mil maximálně 15 kol algoritmu. Mnohé operace lze snadno paralelizovat, a jedná se tak o poměrně rychlý algoritmus, který je zároveň úsporný z hlediska velikosti kódu [46, 27].

4.5.7 ChaCha20-Poly1305

Tento algoritmus kombinuje proudovou šifru ChaCha20 s hašovací funkcí Poly1305, což zajišťuje důvěrnost, integritu a autentizaci zprávy. Způsob je velmi podobný GCM režimu šifer (např u AES). Jedná se však o variantu autentizovaného šifrování s připojenými daty (angl. Authenticated Encryption with Associated Data – AEAD) [78]. Spolu se šifrovanou částí se volitelně přenáší i hlavička, která je nešifrovaná a obsahuje např. informace o adresátovi. U této hlavičky musí být rovněž zajištěna integrita a autentizace. Vstupem šifry je 96bitový inicializační vektor a 256bitový klíč. ChaCha20 generuje pomocí inkrementujícího čítače pseudo-náhodný řetězec bitů, které se poté XORují s šifrovanou zprávou. Poly1305 také používá klíč s inicializačním vektorem pro vytvoření haše zprávy. Na rozdíl od GHASH (použit u AES-GCM) se zde díky inicializačnímu vektoru, který je jiný pro každou zprávu, mění i celkový hašovací klíč [78]. Vygenerovaný haš slouží pro zachování integrity zprávy. Výstupem algoritmu je spolu se zašifrovaným textem tzv. autentizační tag (angl. Message Authentication Code – MAC). Vzhledem k tomu, že se jedná o proudovou šifru, není nutné znát celý šifrovaný text dopředu. To umožňuje velkou míru paralelizace výpočtu a jeho efektivitu [78, 106].

ChaCha20-Poly1305 je jedna z mála proudových šifer, které jsou považovány za bezpečné a vhodné k použití. Alternativa proudové šifry v podobě RC4 má predikovatelné části a není považována za bezpečnou [106]. Nejsou známé žádné účinné útoky na ChaCha20-Poly1305, pokud jsou tedy oba algoritmy implementovány správně a je zvolen vhodný inicializační vektor. Algoritmus se využívá v mnoha aplikacích a síťových protokolech, jako je např. IPsec, SSH nebo TLS 1.3 [78, 106].

4.5.8 Chaskey

Chaskey je velmi efektní algoritmus, který je primárně užíván pro 32bitové architektury. Řadí se mezi tzv. light-weight algoritmy a pro šifrování používá 128bitové bloky. Obdobně jako Speck využívá tzv. add-rotate-xor schéma [75]. Chaskey je používán k zajištění integrity zpráv (MAC), k autentizaci uživatelů pomocí challenge-response protokolů a pro generování náhodných čísel. Je standardizován ISO/IEC 29192-6, v němž má 12 kol algoritmu. Je volně dostupný, není chráněn žádným patentem. Byl podroben několika kryptoanalýzám, které neobjevily žádné závažné problémy. Standardizovaná ISO verze algoritmu je tedy bezpečná [75].

4.5.9 Fantomas

Fantomas je 128bitová šifra, která používá LS-design. Jedná se o způsob návrhu light-weight šifry za účelem potlačit nebo zcela znemožnit postranní útoky. Jde se o kombinaci bitově říznutých S-boxů a L-boxů, přičemž L-box slouží jako difúzní (rozptylová) vrstva. Tento způsob znemožňuje výkonovou analýzu na postranní kanály. Charakteristickou vlastností LS-designu je to, že postrádá tzv. key-schedule algoritmy. Master klíč je jednoduše přidán během každého kola. V současnosti není znám žádný úspěšný útok na Fantomas šifru s plným počtem kol [23, 27].

4.5.10 RC6

RC6 používá Feistelovo schéma[5]. Jedná se o jednoho z finalistů soutěže o standard AES. Používá tedy klasickou velikost klíče 128, 192, 256 a šifruje bloky o velikosti 256 bitů. Má celkem 20 kol. Může být ale snadno upraven tak, aby podporoval klíče o velikosti až 2 040 bitů. Používá rotace v závislosti na datech, modulární sčítání a XOR operace. Šifra je velice kompaktní. Její kód i data se snadno vlezou do cache paměti. RC6 je nejvíce zranitelný proti X2 kryptoanalýze (Terada & Ueda, 2009). Proto vznikla RC6T verze algoritmu, která přidává T funkci, jež přidává další operaci prohození u každého kola [44, 118].

4.5.11 CRYSTALS

Jedná se o první z „post-kvantových“ algoritmů, který byl schválen NISTem [1]. CRYSTALS (Cryptographic Suite for Algebraic Lattices) je dvojice kryptografických primitiv: *Kyber* a *Dilithium*. Oba algoritmy jsou založeny na výpočetně složitých problémech na bodové mřížce a na učení se s chybami (angl. Learning with errors), v nichž je schovaná tajná informace v několika rovnicích, které obsahují chybu [4, 5].

Kyber je algoritmus pro bezpečné zapouzdření klíčů (angl. Key Encapsulation Mechanism). Jedná se o mechanismus používaný pro hybridní šifrování, tedy když se algoritmy veřejného klíče používají k přenosu symetrického klíče, který se teprve použije na zašifrování zprávy. Kyber se dělí na tři úrovně: Kyber-512, Kyber-768 a Kyber-1024. Tyto úrovně by měly mít podobnou míru bezpečnosti jako AES-128, AES-192 a AES-256. *Dilithium* je algoritmus, který slouží pro digitální podepisování zpráv. Je založen na „Fiat-Shamir with Aborts“ technice [4, 5].

Kapitola 5

Zhodnocení aktuálního stavu a návrh řešení

V této kapitole jsou zhodnoceny protokoly zajišťující kvantovou distribuci klíčů. Dále jsou zhodnoceny jednotlivé topologie QKD sítí a různé varianty kvantových kanálů. Následuje krátké shrnutí šifrovacích algoritmů, které mohou dané kryptografické klíče odebírat. Na základě těchto analýz je vypracován návrh nástroje, který umožňuje simulaci kvantového kanálu pro laserové přenosy. V závěru je sepsán postup řešení daného problému včetně technických parametrů nástroje.

5.1 Shrnutí aktuálního stavu QKD systémů

V druhé kapitole 2 byly představeny různé protokoly, které se používají pro kvantovou distribuci klíčů. Protokoly, které vyžadují spolehlivý generátor jednotlivých fotonů, jako jsou např. BB84 nebo B92, jsou stále spíše teoretické a do praktického nasazení se zatím moc nedostávají. Díky jejich vysoké citlivosti na kvalitu kanálu ani nedosahují velkých přenosových vzdáleností. Protokoly, které jsou založeny na kvantovém provázání (E91, BBM92), se mohou v budoucnu začít více rozvíjet. Principy a fungování kvantového provázání jsou však stále nejasné. V současnosti jsou nejrozšířenější protokoly založené na slabě koherentních pulsech COW a DPS. Pulsy obsahují malé množství fotonů. To umožňuje snadnější realizaci a větší toleranci na útlum přenosového kanálu. Obecné porovnání jednotlivých protokolů je zobrazeno tabulkou 5.1.

Ve třetí kapitole 3 byly představeny různé topologie a schémata zapojení QKD systémů. Velikým problémem kvantových topologií je vzdálenost, na kterou je možné funkční kanál vytvořit. Existuje možnost vytvořit vícero uzlů za sebou, které si budou navzájem předávat kvantově zabezpečená data. Tato varianta je ovšem poměrně nepraktická a nákladná. Hrozí i riziko kompromitace jednoho uzlu v cestě. Alternativou jsou bezdrátové přenosy. Pro přenos kvantových dat musíme použít optické neboli laserové zdroje. Klasické radiofrekvenční spojení není možné. Laserové paprsky jsou lehce ovlivnitelné atmosférickými podmínkami. Zároveň je nutné, aby na sebe oba body současně „viděly“. Pro přenos dat pouze v atmosféře je jejich využití velmi limitující, jelikož dosah kvůli útlumu nemusí být příliš velký. Využití proto najdou spíše u menších lokálních a podnikových sítí. Naopak nadějná budoucnost tkví v použití satelitů pro přenos kvantově zabezpečených klíčů na delší vzdálenosti. Atmosférické podmínky jsou sice stále přítomny, ale jedná se pouze o část cesty (cca 10 km), kterou

musí paprsek v atmosféře překonat. Obecné porovnání jednotlivých typů řešení kvantových kanálů je zobrazeno tabulkou 5.2.

Čtvrtá kapitola 4 se zaměřuje na různé šifrovací algoritmy, které mohou následně použít kvantově zabezpečené klíče k šifrování. Symetrické šifry jsou daleko efektivnější z hlediska spotřeby a výkonu. Jsou i více odolné proti kvantovým počítačům v budoucnu. V současnosti vznikají mnohé tzv. light-weight šifry, které jsou určené především pro různá IoT, vestavěné systémy a baterií limitovaná zařízení. Ty mohou poskytovat dobrou alternativu k standardní AES šifře.

Protkol	Jednoduchost implemetace	útlumová tolerance
Protokoly diskrétní proměnné	velice náročná	nízká
Protokoly kvantového provázání	střední	střední
Protokoly distribuované fázové reference	snadná	střední

Tabulka 5.1: Porovnání obecných vlastností jednotlivých protokolů

Způsob přenosu	Komunikační vzdálenost	Cena implementace
Optické kabely	omezená (max 100 km)	střední
Lokální laserové spojení	nízká (kolem 10 km)	nízká
Satelitní laserové spojení	velká (globální pokrytí)	vysoká

Tabulka 5.2: Porovnání různých typů kvantových kanálů

5.2 Návrh zlepšení oproti aktuálnímu stavu

Na základě zhodnocení dosavadního stavu jsem se rozhodl simulovat přenos kvantově zabezpečených klíčů pomocí laserových přenosů a satelitních družic. Laserové spojení pomocí družic je ze své podstaty velmi nákladné řešení, proto je užitečné mít nějaký nástroj, který dokáže simulovat rychlost kvantově zabezpečených klíčů skrz atmosféru. Laserová spojení do vesmíru umožňují pokrytí kvantovým kanálem na globální úrovni. Zároveň se jeví užitečné určit vhodné šifrování, které by bylo efektivní z hlediska spotřeby i bezpečnosti. Kvalita laserového spojení velice závisí na aktuálních atmosférických podmínkách, zejména na oblačnosti. Daná simulace tedy bude brát v potaz oblačnost, která se však může měnit během dne.

5.3 Návrh postupu řešení

Vzhledem k přítomnosti QKD systému mezi fakultou FIT VUT a FEKT VUT lze přenosové vlastnosti změřit v rámci tohoto systému. QKD systém implementuje COW protokol, který je v komerční sféře jeden z nejrozšířenějších díky své relativně jednoduché implementaci a dobré toleranci na ztrátovost kanálu. Cíl této práce se dá rozdělit do několika problémů, které je třeba splnit:

- Změřit přenosové rychlosti kvantově zabezpečených klíčů. Kanál se nachází mezi fakultami FIT VUT a FEKT VUT. Mj. změřit i další parametry přenosu v klidovém stavu.
- Popsat fungování útlumového článku, který bude přidán do spoje. Tento článek simuluje útlum daného kvantového kanálu a měnící se rychlost generování klíčů v čase.
- Zapojit tento útlumový článek do spoje a změřit jednotlivé přenosové vlastnosti, které se mohou v čase razantně měnit.
- Porovnat jednotlivé symetrické algoritmy z hlediska jejich bezpečnosti, spotřeby elektrické energie, rychlosti šifrování a paměťové náročnosti.
- Sesbírat data o oblačnosti během několika dnů. Vybrané dny by měly pokrýt jak letní, tak zimní roční období.
- Vytvořit nástroj pro simulování rychlosti generování klíčů po kvantovém kanálu v závislosti na aktuálních atmosférických podmínkách během dne.

5.4 Technické parametry nástroje

Daný simulační nástroj by měl správně reflektovat aktuální stav oblačnosti, která mu bude zadána na vstupu. Podle dané oblačnosti bude simulovat kvalitu, a tedy rychlost kvantového kanálu. S jakou mírou se bude měnit daná rychlost, bude záležet na výstupech měření pro kvantový kanál, který je ovlivněn útlumovým článkem. Mimoto bude nástroj měřit energetickou spotřebu vybraných šifrovacích algoritmů pro přenos klasických dat. Nástroj bude výstupní hodnoty simulace zaznamenávat do výstupního souboru ve formátu CSV.

Kapitola 6

Porovnání algoritmů

Tato část je zaměřena na analytické porovnání jednotlivých symetrických šifer. Porovnány budou následující šifry: AES (Rijndael), Twofish, SPECK, LEA a ChaCha20-Poly1305. Tyto algoritmy jsou vybrány, protože se v současnosti jedná o nejlepší šifry z každé kategorie symetrických šifer [37, 102, 27, 39]. Zástupci pokrývají jak skupinu klasických šifer (AES, Twofish), tak tzv. light-weight šifry (LEA, Speck) a jeden zástupce patří mezi proudové šifry (ChaCha20-Poly1305). Jedná se o algoritmy, které se hodí do různých prostředí a to včetně IoT zařízení, které jsou velice omezené svým výkonem i spotřebou. OTP je příliš specifická šifra pro porovnání a z praktických důvodů se příliš nepoužívá.

Algoritmy budou postupně porovnávány na základě jejich bezpečnosti, rychlosti šifrování dat, energetické spotřeby a paměťové náročnosti. Tyto parametry byly zvoleny tak, aby bylo možné nejlépe určit vhodné šifrování v dané situaci a pro dané aplikační použití. Výsledky jsou zobrazeny v tabulce 6.1 na konci této kapitoly.

6.1 Porovnání na základě bezpečnosti

Bezpečnost algoritmu je ovlivněna mnoha faktory. U blokových šifer obecně platí, že větší velikost bloku znamená větší bezpečnost. Je to dáno narozeninovým paradoxem, který říká, že stačí druhá odmocnina všech možných bloků k tomu, abychom našli kolizi, resp. dvojici stejných dat, což by umožnilo útočníkovi zjistit informace o šifrované zprávě. Pro velikost bloku 64 bitů se nedoporučuje poslat více než 32 GB šifrovaného textu, aniž by se změnil šifrovací klíč. Tudíž čím větší velikost bloku, tím menší šance, že nastane kolize. Všechny porovnávané šifry podporují velikost bloku 128 bitů. S velikostí bloku úzce souvisí šifrovací režim šifry. ECB režim je považován za nejméně bezpečný a neměl by se používat, lepší je použít CBC nebo jednu z variant CFB/OFB. Nejvíce bezpečný je režim čítače (CTR), ideálně v kombinaci s autentizací – GCM. Režim má ovšem i negativní vliv na bezpečnost. Pro GCM je degradace bezpečnosti $\sigma^2/2^n$, u čehož je σ celkový počet provedených permutací a n je velikost bloku. Ve výsledku to znamená, že čím více dat zašifrujeme pomocí daného režimu, tím méně je daný režim bezpečný [111, 67].

Délka klíče představuje odolnost proti útoku hrubou silou. Všechny šifry podporují minimální velikost klíče 128 bitů, čímž jsou považovány za bezpečné z pohledu současnosti. Zároveň podporují i 256bitové klíče, tudíž je lze do budoucna považovat za rezistentní vůči kvantovým počítačům (Groverův algoritmus dokáže snížit efektivní délku klíče o polovinu). Bezpečnosti jednotlivých algoritmů jsem se rozhodl porovnat z hlediska poměru počtu prolomených kol k celkovému počtu kol algoritmu.

$$Security = \frac{n_{broken}}{n_{total}} \tag{6.1}$$

Čím je tato hodnota menší, tím je bezpečnost algoritmu větší. Prolomení jednotlivých kol je založeno na diferenciální kryptoanalýze. U šifer se používá na měření toho, jak moc změna vstupu ovlivní výstup šifry. Pokud je tato změna málo náhodná, může to vést k prolomení šifrovaného textu nebo k prolomení klíče [10].

AES (Rijndael) byl podroben mnoha různým studiím. Nejvíce se povedlo prolomit 7 kol pro 128bitový klíč. Pro 192bitové a pro 256bitové klíče se povedlo prolomit také 7 kol se stejnou časovou složitostí, tedy 2^{99}. Existuje i útok na plný počet kol pro 192- a 256bitové klíče zapříčiněné strukturálními chybami v key-schedule algortimu. Nicméně jejich časová a prostorová složitost je stále za možnostmi aktuálních počítačů [29, 11].

Blowfish má slabinu v podobě velkého množství slabých klíčů a je zranitelný vůči diferenciální kryptoanlýze druhého řádu [44]. Největší problém v současnosti je velikost šifrovacího bloku – pouze 64 bitů. I sám autor šifry doporučil z hlediska bezpečnosti použít jejího následovníka Twofish. Ten adresuje chyby svého předchůdce a je daleko více bezpečnější. U Twofish se podařilo prolomit 6 kol z celkových 14 s časovou složitostí 2^{128} pro 128bitový klíč, 2^{160} pro 192bitový klíč a 2^{192} pro 256bitový klíč [36].

Speck byl podroben více než 70 různým kryptoanalýzám a žádná neobjevila slabiny v algoritmu. Speck umožňuje malé velikosti klíče (64 bitů) i šifrovacích bloků (32), ty ale nejsou bezpečné. Autoři algoritmu jejich přítomnost zdůvodňují použitím v zařízeních, která nemají příliš energie či výpočetního výkonu a u kterých se nepředpokládá šifrování velkého množství textu. Jiná alternativa pro ně tedy neexistuje. Provedené porovnání uvažuje pouze o verzi šifrující blok o velikosti 128 bitů. Pro 128bitový klíč bylo prolomeno 23 z 32 kol, pro 192bitový klíč 24 z 33 a pro 256bitový klíč 25 z 34 kol [47].

LEA podobně jako Speck nebyl prolomen. Nejúspěšnější útok, tzv. Boomerang dokázal prolomit maximálně 15 kol pro 128bitový klíč. Předpokládá se, že pro 192bitový klíč to bude 16 a pro 256bitový klíč 17 kol [46].

Bezpečnost u ChaCha20-Poly1305 závisí podobně jako u AES-GCM na vhodně zvoleném inicializačním vektoru. Používá se hojně na mobilních zařízeních, která často používají architekturu založenou na ARMech [78]. Autoři šifry identifikovali slabiny pro 6. a 7. kolo algoritmu. Časová složitost těchto útoků je 2^{139} pro 6. kolo a 2^{248} pro prolomení 7. kola z 20 [30, 106].

Provedené porovnání bezpečnosti má ovšem několik slabin. Například trpí tím, že některým algoritmům nebylo věnováno tolik studií a kryptoanalýz, jako tomu bylo u jiných. Algoritmu AES, který je nejvíce rozšířený symetrický algoritmus, bylo věnováno nejvíce pozornosti a proběhlo u něj nejvíce pokusů ho prolomit či zjistit jakékoliv slabiny. Dalším faktem je, že porovnání se zaměřuje čistě na sílu jednotlivých kol algoritmu a nezohledňuje další části, jako je práce s klíčem a postprocessing. Nicméně tato analýza udává představu o tom, které algoritmy budou s příchodem výkonných kvantových počítačů potenciálně prolomeny nejdříve.

6.2 Porovnáni na základě rychlosti šifrování

Rychlost šifrování je ovlivněna jednak samotným algoritmem, jednak procesorem, na kterém běží. Záleží i na samotné implementaci. Tedy buď přímo hardwarové, nebo softwarové. U softwarové implementace závisí také na samotném programovacím jazyce. Při porovnání je potřeba mít co nejvíce podobné podmínky.

Čas šifrování udává, jak dlouho bude algoritmu trvat zašifrovat zprávu. Propustnost se poté počítá jako celková velikost zprávy M (popř. velikost jednoho bloku), kterou chceme zašifrovat v bajtech, vynásobenou o frekvenci procesoru a dělenou časem šifrování t. Obecně se dá propustnost vyjádřit [66]:

$$Throughput = \frac{|M| \times f_{cpu}}{t} \tag{6.2}$$

Rovnice nám udává rychlost šifrování. Z klasických šifer AES a Blowfish vychází Blowfish jako rychlejší algoritmus [82, 34], dokonce několikanásobně. Blowfish má ovšem dlouhou dobu přípravy klíče, samotná šifrovací kola jsou následně rychlá. Byl proto vhodný pro šifrování většího objemu dat, u kterých se nemění klíč příliš často. Twofish vykazuje většinou lepší nebo podobnou rychlost jako AES. Pokud máme podle analýzy od IEEE [100] k dispozici více RAM paměti, tak je Twofish schopen šifrovat text a audio soubory rychleji než AES (Rijndael). Porovnání rychlostí je ovšem velmi závislé na zvolené architektuře [100].

Pro AES vznikly i speciální hardwarové instrukce, které jsou často přítomny v řadě moderních procesorech, u nichž je na to prostor. Tato HW akcelerace dokáže zrychlit šifrování o několik řádů (až o 75 %–87 %) [2]. HW podpora pro AES je i u kryptografických knihoven, např *Crypto++, OpenSSL, LibgCrypt*.

Tzv. light-weight algoritmy jsou považovány za rychlejší a efektivnější než AES, nemáme-li k dispozici speciální HW instrukce pro AES, jak dokazuje studie [27]. Algoritmy LEA a Speck jsou na tom z hlediska rychlosti velice podobně.

Při porovnání šifer budu vycházet z informací primárně sepsaných v [102]. Algoritmy byly testovány na dvou mobilních zařízeních. Jedno z nich byl Samsung Galaxy Core Prime, 1 GB RAM a CPU ARMv7-a Cortex-A7, 4 cores, 1.2 GHz. Nejedná se tedy o nikterak výkonné zařízení. Rychlost dat v tabulce 6.1 pochází z měření na tomto zařízení. Zvolil jsem ho, jelikož více odpovídá typickému IoT zařízení. Bylo provedeno 100 různých testování, postupně pro velikosti paketů 1, 5 a 10 MB. Data v tabulce jsou průměrem hodnot ze všech tří velikostí paketů. Vždy byl použit nový klíč, ale fáze přípravy klíče nebyly měřeny. Šifry byly implementovány v režimu GCM, pro proudový algoritmus ChaCha20-Poly1305 bylo přidáno 16 bajtů autentizačních dat (AAD).

Ze studie [102] jde dále zjistit, že na druhém mobilu, který je výkonnější a má dostupné větší množství RAM paměti[1], byla rychlost šifrování daleko větší u všech algoritmů. Zajímavým zjištěním bylo, že pro větší velikost klíče u AES a LEA se algoritmy daleko více zpomalily. U ostatních nebyla změna velikosti klíče tolik rozdílná. Druhé zařízení podporuje také speciální instrukce pro HW akceleraci AES, tato varianta byla ve všech parametrech nejvíce efektivní. Speck z přidaného výkonu i paměti profitoval daleko více než LEA nebo ChaCha20-Poly1305.

Existuje celá řada studií, které porovnávají rozdílné algoritmy. Konkrétní hodnoty vždy záleží na dané implementaci a architektuře, která ovlivní rychlost šifrování jako takovou.

[1] Xiaomi Redmi Note 3 – CPU: ARMv8-a Cortex-A53, 4 cores, 1.4 GHz + ARMv8-a Cortex-A72, 2 cores, 1.8 GHz, RAM: 3GB

Provedená analýza nám tak poskytuje spíše hrubé porovnání pro představu, jak si algoritmy vedou mezi sebou.

6.3 Porovnání na základě energetické náročnosti

Podobně jako v případě rychlosti šifrování je i tento faktor ovlivněn konkrétní implementací algoritmu. Energetická spotřeba je jeden z nejdůležitějších faktorů výběru algoritmu v mnoha IoT zařízeních, a to zvlášť u těch, které jsou napájeny baterií. Obecně se dá energetická spotřeba vyjádřit pomocí vzorce [133]:

$$E = (P_{cpu} \times C_{enc}/f_{cpu}) \times N_{PL}/u \tag{6.3}$$

u něhož jsou P_{cpu} a f_{cpu} výkon a frekvence CPU, C_{enc} je počet cyklů procesoru nutných k zašifrování bloku zprávy o velikosti u. Pro proudové šifry je u velikost keystreamu k zašifrování části textu. N_{PL} je celkový počet bitů zprávy, která se šifruje. Na tuto problematiku vzniklo také několik studií, např. [95, 77]. Pro porovnání budu ale vycházet ze stejného výzkumu [102] jako v případě porovnání šifrovacích rychlostí. Energetická náročnost a šifrovací rychlost spolu souvisí. Dá se říci, že čím větší šifrovací rychlost, tím menší energetická spotřeba. V dané studii je energetická spotřeba uvedena v mAh. Jednotlivá měření probíhala po celou dobu běhu testovací sady, přičemž velikost zpráv byla postupně 1, 5 a 10 MB. Každá varianta měla 100 měření. Abychom tedy dostali výslednou hodnotu pro jeden běh (včetně fáze přípravy klíče), je nutné hodnoty vydělit 3∗100. Podle měření mají light-weight algoritmy menší spotřebu oproti klasickým algoritmům. Výjimkou je AES používající speciální optimalizované instrukce procesoru. Tato varianta byla testována na druhém zařízení[1] (není uvedeno v tabulce) a z porovnávaných šifer byla nejvíce šetrná k baterii. Nutno dodat, že hodnoty v tabulce 6.1 se vztahují ke spotřebě pro konkrétní zařízení a nelze očekávat přesně tyto hodnoty. Slouží tak spíše pro porovnání mezi jednotlivými algoritmy.

6.4 Porovnaní na základě paměťové náročnosti

U šifrovacích algoritmů lze rozdělit spotřebu paměti na dvě části: paměť potřebnou pro uchování podklíčů (Round Keys) a paměť nutnou pro samotné šifrování či dešifrování. V aplikacích, v nichž se klíč nemění často, jej lze uložit do EEPROM nebo ROM paměti, což vede k redukci spotřeby RAM paměti. Většina aplikací ale používá tzv. klíče relací, které se mohou měnit s každou transakcí, a bývají proto uloženy v RAM paměti. U HW implementací se měří paměťová náročnost pomocí počtu hradel, které jsou zapotřebí pro správný běh šifry. Tato práce se zaměřuje na softwarovou implementaci šifer, u kterých se měří spotřebovaná RAM paměť.

Twofish lze různě modifikovat a upravit, aby běžel i na zařízení s malou RAM pamětí. Zároveň pokud máme více dostupné paměti, je možné algoritmus zrychlit spočítáním určitých dat dopředu. Teoreticky by Twofish měl spotřebovat 60 bajtů pro 128bitový klíč, přičemž 24 bajtů je pro uložení jednotlivých podklíčů (Round Keys) a 36 pro samotné šifrování [126]. Nicméně pro porovnání spotřeby algoritmů AES a Twofish jsem vycházel ze studií [94], které porovnávají 256bitové verze algoritmů na třech různých mobilních zařízeních.

Data o paměťové náročnosti LEA a Speck pocházejí ze studií [107, 27] porovnávajících řadu algoritmů na 8bitové, 16bitové a 32bitové architektuře. K tomu slouží framework FELICS[2], který se snaží sjednotit porovnání jednotlivých algoritmů. Studie obsahuje porov-

[2]FELICS framework je dostupný zde: https://www.cryptolux.org/index.php/FELICS

nání s AES, jejíž výsledek byl podobný jako v případě předchozí zmíněné studie [94]. Měření probíhala pro šifrování i dešifrování 128 bajtů dat v režimu CBC, včetně fáze přípravy klíče (key schedule). Fáze přípravy klíče je náročnější na paměť (provádí se ale pouze pro šifrování první zprávy daným klíčem). Pro ChaCha20-Poly1305 pochází data ze stejné studie, hodnoty byly zveřejněny pouze online na webu[3]. Existují i další studie, které porovnávají paměťovou náročnost symetrických šifer, např. [66, 7].

6.5 Vyhodnocení

Tabulka s výsledky hodnot porovnání jednotlivých algoritmů na základě jejich míry bezpečnosti, rychlosti šifrování, spotřeby energie a paměti. Porovnat jednotlivé šifry mezi sebou je dosti náročné, jelikož každá šifra může být vhodná pro jiné situace a aplikace.

Šifra	Bezpečnost	Rychlost šifrování [MiB/s]	Energetická spotřeba [mAh]	Paměťová náročnost RAM [B]
AES-128	0,70	12,820	0,0346	-
AES-192	0,583	12,022	0,041	-
AES-256	0,5	11,224	0.0447	433,1
Twofish-128	0,429	17,263	0,0258	-
Twofish-192	0,429	17,141	0,0291	-
Twofish-256	0,429	17,053	0,0292	429,6
Speck-128	0,719	23,857	0,0186	256
Speck-192	0,728	23,635	0,0205	272
Speck-256	0,7206	23,380	0,0211	288
LEA-128	0,625	24,086	0,0173	592
LEA-192	0,571	23,102	0,0216	688
LEA-256	0,531	22,442	0,0222	784
ChaCha20-Poly1305	0,35	38,177	0,0113	328

Tabulka 6.1: Porovnání jednotlivých algoritmů na základě bezpečnosti, rychlosti šifrování, energetické a paměťové spotřeby. Číslo u algoritmu označuje bitovou velikost klíče. ChaCha20-Poly1305 používá pouze 256bitový klíč.

V současnosti jsou všechny porovnávané šifry dostatečně bezpečné. Proti žádné z nich neexistuje takový útok, který by ji v současnosti prolomil. Z hodnot lze pouze odvodit závěr, že AES-128 nebo Speck budou mít v budoucnu největší šanci na prolomení. Nelze to říci s jistotou, neboť na AES bylo provedeno nejvíce kryptoanalýz, které jeho bezpečnost neprolomily.

Rychlost šifrování je poměrně důležitý faktor, jelikož obecně platí, že čím rychleji zašifrujeme danou zprávu, tím kratší dobu algoritmus poběží, a bude tedy spotřebováno méně energie, což je velice důležité pro IoT zařízení. Lze vidět, že AES je na tom nejhůře, toto ovšem platí pro procesory, které nepodporují optimalizované HW instrukce pro zrychlení výpočtu. Pokud máme akcelerované instrukce k dispozici, jedná se jednoznačně o nejrychlejší algoritmus, který má zároveň nejmenší spotřebu, jak dokazuje studie [102]. Light-weight algoritmy LEA a Speck si vedly z pohledu rychlosti lépe jak „klasické“ algoritmy, rozdíly

[3] https://www.cryptolux.org/index.php/FELICS_Stream_Ciphers_Brief_Results

mezi LEA a Speck nejsou nikterak velké, a dá se proto říci, že jejich rychlost je stejná. Nejlépe dopadla proudová šifra ChaCha20-Poly1305, která šifruje téměř dvakrát rychleji než LEA a Speck. Blowfish je zajímavý, jelikož po fázi ustanovení klíče dokáže data šifrovat poměrně rychle. Je tedy vhodný tam, kde se šifrovací klíč nemění často. Podobně je na tom šifra ChaCha20-Poly1305 z pohledu energetické spotřeby, protože vykazuje nejmenší spotřebu baterie. Speck a LEA vykazují shodnou energetickou spotřebu. Samozřejmě spotřeba je i přímo úměrná velikosti klíče. Pokud chceme větší bezpečnost, bude spotřeba větší. Z pohledu náročnosti na RAM paměť je na tom nejlépe Speck, který nepotřebuje tolik místa pro běh. Naopak LEA zde vyžaduje daleko více paměti, a není proto vhodná pro zařízení s limitovaným prostorem pro paměť. Nutno připomenout, že algoritmus LEA byl navržen primárně pro 32- a 64bitové architektury, zatímco algoritmus Speck lze dobře implementovat i pro 8- a 16bitové architektury. Zároveň umožňuje šifrovat i po malých blocích dat (minimum je 32bitový blok). Hodí se tedy pro zařízení, u nichž se nepředpokládá velký objem přenášených dat.

Nejvíce používané a nejlépe hodnocené symetrické algoritmy byly mezi sebou porovnány podle parametrů, které pomohou určit, jaké algoritmy vybrat pro bezpečné šifrování. Nejlépe vyšel AES, který využívá speciální AES-NI instrukce procesoru, následován proudovou šifrou ChaCha20-Poly1305. Light-weight algoritmy dopadly lépe jak klasické varianty symetrických šifer. Mimo zmíněných Speck a LEA algoritmů existuje i celá řada dalších, např. E^3LCM [88] nebo EELVE [95]. Tyto algoritmy nejsou příliš prozkoumané, především z pohledu bezpečnosti. Nicméně vykazují větší výkon jak současný AES.

Kapitola 7

Měření statistik QKD systému

Tato kapitola se věnuje měření statistik QKD systému. Měření probíhalo na fakultě informatiky VUT v Brně, kde se nachází zařízení *Clavis*[3] od firmy IDQ, jehož fungování bylo nastíněno v kapitole o topologiích sítí 3. Ze zařízení je možné vyčíst řadu různých informací a statistik během generování klíčů po kvantově zabezpečeném kanále mezi dvěma body. Především to, s jakou rychlostí jsou klíče generovány a jaká chybovost se na kanále vyskytuje. Naměřená data jsou znázorněna pomocí grafů a shrnuta do tabulky 7.1. Následně bylo do topologie zapojeno zařízení simulující útočníka, který ovlivňuje jednotlivé parametry a bezpečnost klíče. Takto se dá simulovat vliv různých útlumových článků na daný spoj. Samotné hodnoty byly získány ze systému, jehož schéma a fungování je popsáno zde 3.3.3.

7.1 Nastavitelné parametry QKD modulu

Tyto parametry lze přímo nastavit na jednotlivých koncových uzlech zařízení, a tím konfigurovat vlastnosti kvantového kanálu. Popis parametrů vychází z dokumentace zařízení výrobce. Těmito parametry lze upravovat základní chování QKD modulu, a měnit tak celkovou funkčnost systému.

FPGA Distillation Compression Ratio

Určuje míru komprese, která se aplikuje během fáze amplifikace bezpečnosti 3.3.1. Čím je větší hodnota, tím menší vznikne klíč, nicméně množství informací, které má Eva k dispozici, bude menší. Hodnota se u přístroje nastavuje v rozmezí 0 % – 30 %. Pokud je nastavena hodnota `FPGA Model Filter` (popsáno níže 7.1) na `True`, pak musí být tato hodnota nastavena pevně na hodnotu 30 %.

FPGA Model Filter

Příznak, který lze nastavit buď na pravdivou (`True`), nebo nepravdivou (`False`) hodnotu. V případě, že je nastaveno `True`, počítá se míra komprese pro každý blok klíče na základě hodnot QBER, viditelnosti, fotonového čísla a dalších. Dynamicky se tak mění délka klíče podle bezpečnosti a spolehlivosti kvantového kanálu. Pokud je nastavena hodnota `False`, je míra komprese nastavena na hodnotu určenou `FPGA Distillation Compression Ratio` nezávisle na jiných hodnotách. Toto nastavení musí být stejné na obou vzájemně propojených QKD modulech.

QRNG\RNG

Přepínač, který ovlivňuje, zda bude použit integrovaný QRNG čip (popsán zde 3.3.2) pro generovaní náhodných čísel. RNG se používá pro určení hodnot bitů, které slouží jako základ budoucího klíče, ale také pro určení momentů, při kterých se návnadové stavy mají generovat. Pokud je přepínač nastaven na `False`, použijí se AES jádra pro generování matic u amplifikace bezpečnosti klíče, procentuální rozložení návnadových stavů či generování kvantových bitů a vakuové stavy pro čtyřstavový COW protokol.

Optics/Alignment Photon Number

Stanovuje hodnotu, která určuje průměrný počet fotonů na optický puls při generování qubitů. U zařízení je možné nastavit tuto hodnotu v rozmezí 0.01–0.1.

Optics Pulse Width

Nastavení šířky radiofrekvenčních pulsů, které se nacházejí v modulátoru intenzity na Alici. Hodnota přímo ovlivňuje tvar, šířku a míru extinkce (angl. Extinction Ratio). Tato hodnota by se za normálních situací neměla měnit.

Regulation Dark Counts

Během kalibrace zařízení, při němž se neposílají žádné fotony, se na detektorech měří počet dark pulsů. Jedná se o situace, ve kterých detektor něco zachytí, přestože by neměl. Hodnota se používá pro korekci hodnot výpočtu QBER, viditelnosti a amplifikace bezpečnosti. Lze ji nastavit zvlášť pro monitorovací D_M a pro datový detektor D_B (na obrázku 3.7).

Regulation Integration Time

Interval v sekundách, určující dobu mezi dvěma regulačními kroky. Tedy dobu, po které dojde k přepočtu nových hodnot QBER a viditelnosti. Lze specifikovat interval zvlášť pro QBER i pro viditelnost.

Optics Detectors deadtime

Doba, po kterou jsou detektory (D_M a D_B) neaktivní, a to od okamžiku, kdy detekují příchozí pulsy. Typicky se hodnota nastavuje v rozmezí 15 μs – 50 μs. Jakmile dojde k detekci na jednom z detektorů, synchronně se vypnou všechny ostatní. Čím nižší je tato hodnota (čas neaktivity), tím je naměřený QBER vyšší, ale viditelnost bude větší.

Zařízení umožňuje nastavit i další parametry, jako je například testování správné funkčnosti systému při startu, šířka radiofrekvenčních pulsů u detektorů pulsů na straně příjemce (Boba) a další.

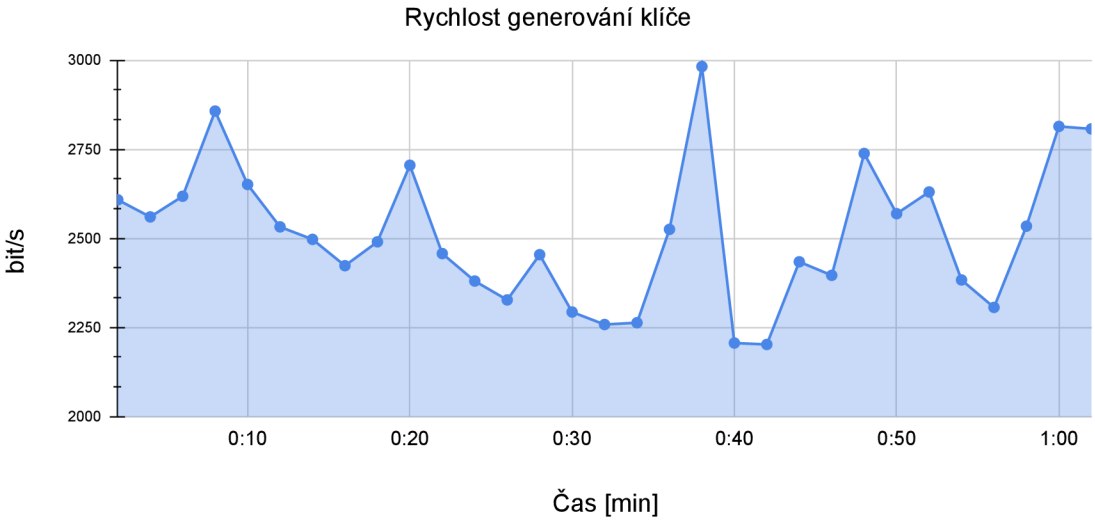
7.2 Měření přenosu kvantového kanálu

Pro vybrané charakteristiky, které popisují kvalitu kvantového kanálu během generování kvantově zabezpečeného klíče, proběhlo měření v klidovém provozním režimu. Tzn. do kvantového spoje nebylo zapojené žádné útlumové/odposlouchávací zařízení. Hodnoty nastavitelných parametrů, zmíněné dříve, byly ponechány ve výchozím nastavení. Měření probíhala jednu hodinu, během které se data sbírala po 2minutových intervalech. Výsledky jsou zobrazeny v grafu a výsledné tabulce na konci.

Rychlost generování klíčů

Patrně nejvíce důležitý parametr, který udává rychlost, s jakou dva navzájem propojené uzly generují velikost klíče. Udává se v bitech za sekundu. V grafu 7.1 je na ose y znázorněna rychlost. Čím větší je tato hodnota, tím více použitelných klíčů jsou zařízení schopna vyrobit a použít. Kdyby velikost vyrobeného klíče byla malá, můžeme jednoduše spojit dva menší klíče, a tím získat klíč větší velikosti. Obecně nám tento parametr říká, jak moc je použitý kvantový systém efektivní. Je ovlivněn parametry zmíněnými dále.

Interně uvnitř zařízení je možné vyčíst hodnotu z parametru: `QKDFpga_KeyRate`.



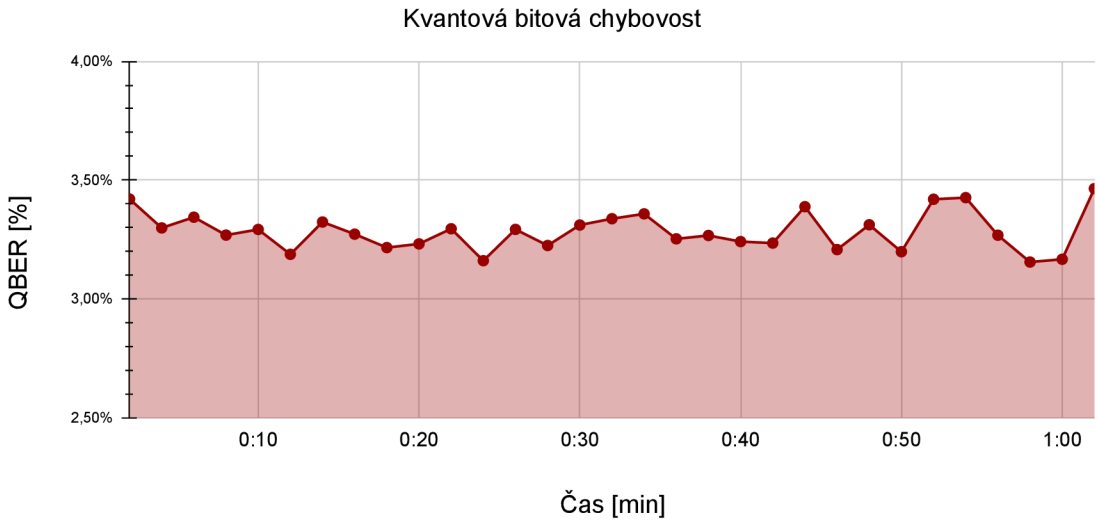
Obrázek 7.1: Rychlost generování klíčů (key rate)

QBER

Kvantová bitová chybovost (angl. Quantum Bit Error Rate). Je to důležitá hodnota, která určuje míru bezpečnosti klíče. Pokud by se tajný klíč snažil útočník odposlechnout, bude tato hodnota vykazovat vyšší hodnoty. V teoreticky perfektním prostředí by tato hodnota byla nula, nedokonalosti spoje a detektorů však způsobují určité chyby. Počítá se na základě špatně přijatých (detekovaných) bitů. V grafu 7.2 je zobrazen průběh chybovosti. Pohybuje se průměrně kolem hodnoty 3,25 %. Většinou se udává maximální povolená chybovost kolem 11 % pro COW protokol. Pokud by byla hodnota QBER vyšší, vygenerovaný klíč není považován za bezpečný a oba uzly ho zahodí. Prakticky také dojde k dočasnému přeru-

šení komunikace. Společně s rychlostí generování klíče tvoří nejzásadnější měřené hodnoty kvantového kanálu.

Interně uvnitř zařízení je možné vyčíst hodnotu z parametru: `QKDFpga_Qber`.

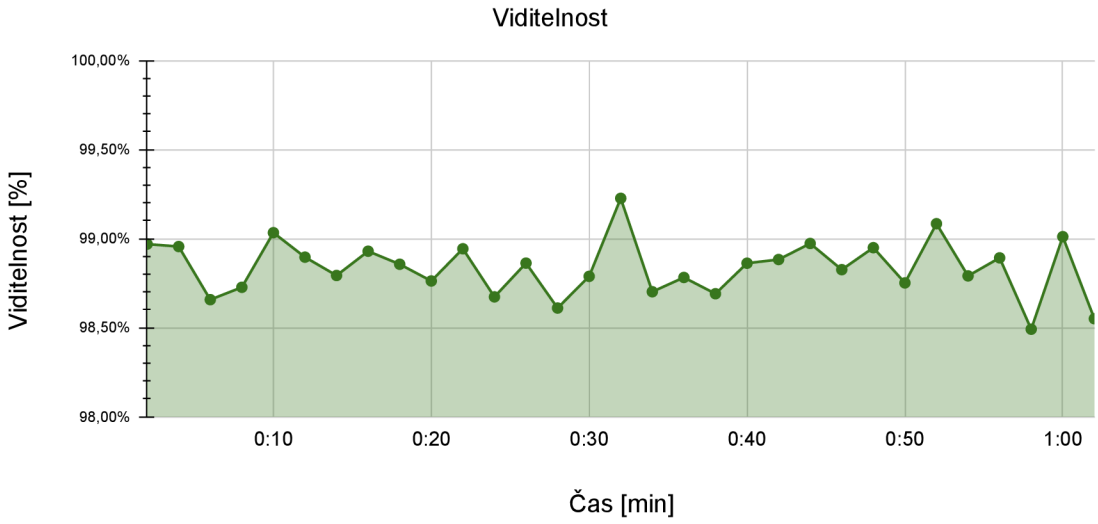


Obrázek 7.2: Kvantová bitová chybovost (QBER)

Viditelnost

Hodnota, která značí po sobě přicházející koherentní pulsy. Je udávána v procentech jako poměr konstruktivních a destruktivních detekovaných pulsů. Více je tato vlastnost vysvětlena v části o interferenci vln 2.4.1. Na grafu 7.3 je vidět průběh viditelnosti. Je patrné, že se pohybuje kolem hodnoty 98,75 %. Chyby jsou zde způsobeny nedokonalostí detektorů.

Interně uvnitř zařízení je možné vyčíst hodnotu z parametru: `QKDFpga_Visibility`.

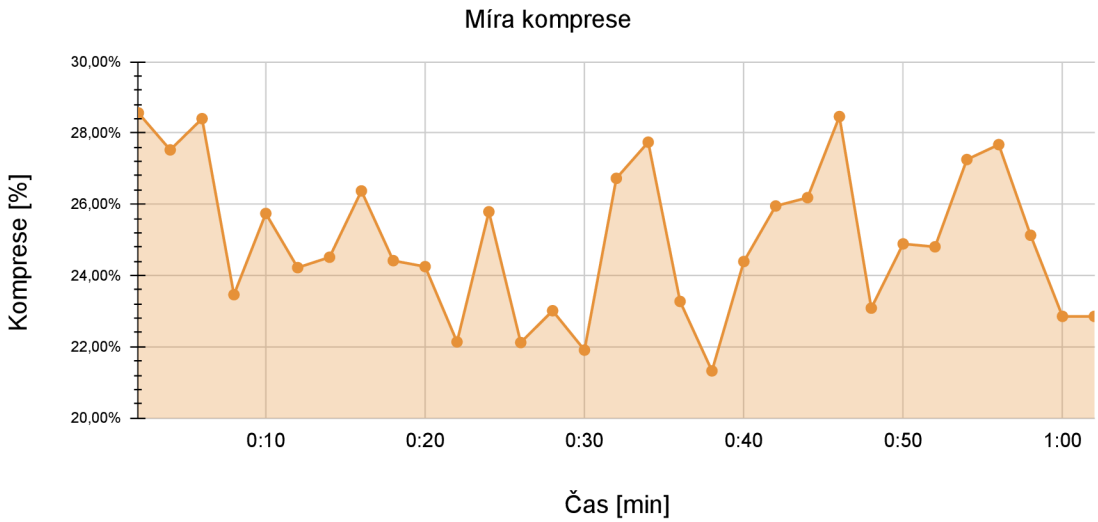


Obrázek 7.3: Viditelnost na detektorech

Míra komprese

Míra výsledné komprese během fáze opravy chyb. Hodnota modelového filtru byla nastavena na `True`, tudíž komprese závisela na vlastnostech přenosu, což je více popsáno v předchozí sekci 7.1. Jak se mění míra komprese je znázorněno na grafu 7.4. Hodnoty nemohou přesáhnout více jak 30 %. S větší mírou bitových chyb tato hodnota roste a přibližuje se ke 30 %.

Interně uvnitř zařízení je možné vyčíst hodnotu z parametru: `QKDFpga_CompressionRatio`.



Obrázek 7.4: Míra komprese (compress ratio)

Souhrn

V následující tabulce 7.1 je vyčíslen průměr naměřených hodnot, minimum a maximum.

Parametr	MAX	MIN	PRŮMĚR
Rychlost generování klíče	2,982 kbit/s	2,203 kbit/s	2,506 kbit/s
QBER	3,464 %	3,155 %	3.284 %
Viditelnost	99,226 %	98.491 %	98,832 %
Míra komprese	28,564 %	21,323 %	25,032 %

Tabulka 7.1: Tabulka naměřených hodnot pro kvantový spoj v běžném provozu

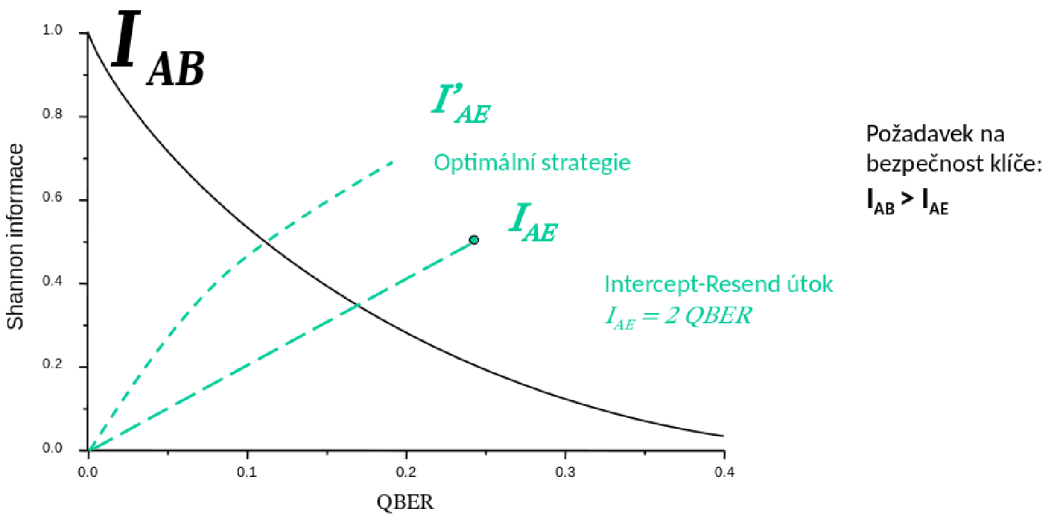
Mimo to lze sbírat i další statistiky, jmenovitě např. počet zachycených pulsů na datových a monitorovacích detektorech (D_M, D_B), dále teplotu, výkonost laserů vysílače či paměťovou a CPU zátěž zařízení.

7.3 Nasazení útočníka

Eva (angl. Eavesdropper) se snaží odposlouchávat na kvantovém kanále a zachytit co největší množství informací, které by jí napomohly k prolomení klíče. V kapitole 2.4.5 jsou více popsané jednotlivé typy útoků. Zajímavé jsou především ty, které nezanášejí žádnou chybu. Jejich praktická realizace je v současnosti buď nemožná, nebo velice náročná. Společnost IDQ k zařízení *Clavis*^{3} poskytuje také simulátor útočníka, na obrázku 7.5. Princip fungování je velice podobný útoku dělením počtu fotonů nebo I-R útoku.

Simulátor je zapojen do kvantového spoje, tzn. veškeré pulsy jdou skrze něj. Uvnitř se nachází optické děliče (angl. Optical Coupler). Jedná se o součástku, která rozdvojí optický signál do dvou různých výstupních portů. Počet vstupních a výstupních portů není daný, stejně tak jako poměr, v jakém se světlo do výstupu rozdělí [61]. V simulátoru se nachází dělič rozdělující jej do dvou výstupních kanálů, světelný signál je v jednom kanále zpožděn o fixní počet bitů (pulsů), které se přenesou na kvantovém kanále. Tím se simuluje měření, které by Eva mohla provést. Poté je signál z obou větví opět spojen do jednoho pomocí druhého děliče. To zanese ztrátu asi 3 dB do kanálu. Poměr, s jakým je signál rozdělen prvním děličem, je možné měnit otočným kolečkem na přední straně simulátoru. Tím, že Eva oddělí určité množství fotonů a pak je zase navrátí, zanáší chybu do komunikace. Čím větší bude poměr dělení a Eva odkloní větší množství signálu, tím bude QBER větší. Alice i Bob to zaznamenají a budou se to snažit kompenzovat silnější amplifikací bezpečnosti. Což vyústí v menší velikost zabezpečeného klíče, a tedy i menší rychlost generování klíčů (key rate). Pokud by se Eva pokusila odklonit příliš mnoho fotonů, Alice i Bob přeruší komunikaci. Tímto způsobem sice Eva nezíská žádné informace, ale přeruší komunikaci, a provede tak DoS útok.

Obrázek 7.5: Simulátor útočníka – Eva



Obrázek 7.6: Graf zobrazující, jak množství informace, kterou má Eva k dispozici, ovlivňuje chybovost[1].

Na grafu 7.6 je znázorněno množství informací, které mají jednotlivé body mezi sebou k dispozici. Pojem množství informace se vztahuje k Shannovu způsobu chápání informace. Entropie (neurčitost) je základním pojmem v teorii informace a představuje míru neurčitosti ve zprávě. Informace potom znamená odstranění této neurčitosti. Tedy s narůstající informací klesá entropie a naopak [89]. Čím méně informací mají Alice a Bob (I_{AB}), tím je chybovost větší. Cílem Evy je získat co nejvíce informací tak, aby způsobila co možná nejmenší chybu. Například pokud $I_{AB} = 0,7$, potom při optimální strategii $I'_{AE} = 0,28$ a $QBER = 0,05$. Alice a Bob stále mohou vytvořit společný klíč, který je bezpečný, ale musí projít procesem amplifikace bezpečnosti [33].

Měření vlivu útočníka bylo provedeno postupně pro následující poměry odkloněného světelného signálu, tedy 5, 30, 40 a 45 %. Všechna měření probíhala zhruba 20 minut.

Poměr 5 %

Parametr	MAX	MIN	PRŮMĚR
Rychlost generování klíče	1,44 kbit/s	929 bit/s	1,14 kbit/s
QBER	5,19 %	1,27 %	2,22 %
Viditelnost	100 %	91,7 %	97,5 %
Míra komprese	15,2 %	9,83 %	11,550 %

Tabulka 7.2: Parametry kvantového kanálu pro 5% odklon signálu

[1] Graf převzat z prezentace [33].

Poměr 30 %

Parametr	MAX	MIN	PRŮMĚR
Rychlost generování klíče	1,66 kbit/s	1,05 kbit/s	1,37 kbit/s
QBER	4,25 %	1,52 %	2,82 %
Viditelnost	100 %	94,1 %	97,8 %
Míra komprese	15,7 %	11,2 %	13,2652 %

Tabulka 7.3: Parametry kvantového kanálu pro 30% odklon signálu

Poměr 40 %

Parametr	MAX	MIN	PRŮMĚR
Rychlost generování klíče	1,17 kbit/s	406 bit/s	797 bit/s
QBER	10,9 %	2,62 %	4,77 %
Viditelnost	100 %	90 %	97 %
Míra komprese	30 %	30 %	30 %

Tabulka 7.4: Parametry kvantového kanálu pro 40% odklon signálu

Poměr 45 %

Parametr	MAX	MIN	PRŮMĚR
Rychlost generování klíče	436 bit/s	239 bit/s	399 bit/s
QBER	14,3 %	2,73 %	5,30 %
Viditelnost	100 %	91,2 %	96,7 %
Míra komprese	30 %	30 %	30 %

Tabulka 7.5: Parametry kvantového kanálu pro 45% odklon signálu

Můžeme vidět, že již při 5% poměru došlo k poklesu rychlosti generování klíče o zhruba polovinu oproti normálnímu stavu. Stavy s poměrem 5 a 30 % produkovaly podobné výsledky. Pravděpodobně díky nedokonalostem optického děliče. Když dále odkláníme množství fotonů (tedy zvyšujeme dělicí poměr), dochází k prudkému poklesu rychlosti generování klíčů, přičemž hranice 45 % už generuje minimální velikosti klíče. Při nastavení větší hodnoty došlo k přerušení generování klíče. QBER přesáhl povolenou hranici po delší časový úsek, obě strany tak označily kanál za nedostatečně bezpečný. Zajímavým poznatkem bylo, že míra komprese u 5%–30% poměru nebyla příliš velká. Hodnoty viditelnosti spíše detekovaly přicházející pulsy, tato hodnota tak příliš nereflektuje přítomnost útočníka. QBER se během odposlechu zvýšil. Přítomnost Evy nejvíce ovlivnilo generování klíčů, jelikož obě strany musely obětovat větší velikost klíče za cenu bezpečnosti. Eva tedy do jisté míry dokáže simulovat použití různých útlumových článků, které se mohou objevit na kvantovém kanále. Toto je především zajímavé u bezdrátových kvantových kanálů, jež mohou být ovlivněny různými atmosférickými podmínkami. Na obrázku 7.7 je zařízení Bob na VUT v Brně.

Obrázek 7.7: *Clavis*^{3} – příjemce (Bob) na VUT v Brně

7.4 Vyhodnocení

Bylo provedeno měření klidového stavu, přičemž se rychlost generování klíčů pohybovala v průměru okolo 2,5 kbit/s a kvantová bitová chybovost QBER byla 3,25 %. Dále byl zapojen simulátor útočníka, který může obecně představovat jakýkoliv útlumový článek (např. horší kvalitu kabelů, vnější atmosférické vlivy apod.). Bylo zjištěno, že i menší narušení koherence pulsů dokáže ovlivnit spoj natolik, že klesne key rate na polovinu. Pokud útočník odposlouchává větší množství dat, může rychlost klesnout až k 400 bit/s. Rychlost generování klíče není vždycky stabilní a může se rapidně měnit. Je tedy nutné s tímto faktem počítat při návrhu a realizaci kvantové sítě.

Kapitola 8

Simulace laserových přenosů

V této kapitole je popsána simulace přenosu dat pomocí laserů. Laserové přenosy směrem k satelitu jsou výrazně ovlivněny stavem počasí, nejvíce oblačností. Prvně se tedy zmiňuje sekce s popisem sběru dat o oblačnosti ve vybraných dnech. Tu následuje popis simulačního nástroje a modelu reprezentujícího kvantové spojení za pomoci laserů. Výsledky simulace jsou prezentovány formou grafu a vyhodnoceny v závěru kapitoly.

8.1 Sběr dat o oblačnosti

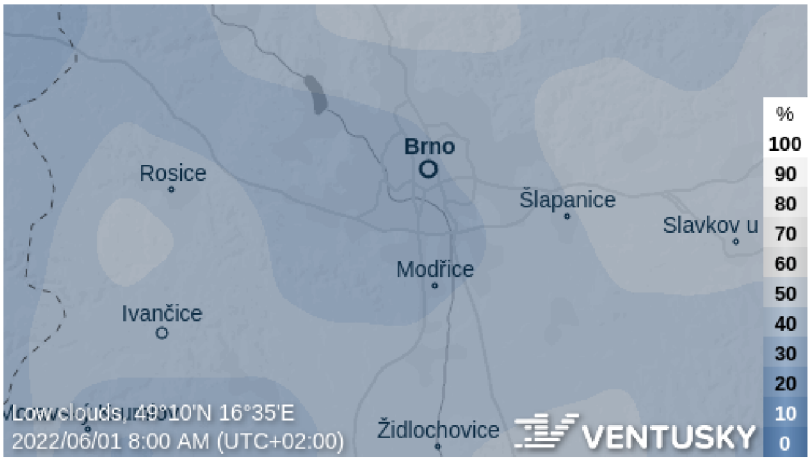
Pro potřeby simulace je nutné získat data o oblačnosti. Oblačnost i celkové pokrytí se může během dne razantně měnit. Záleží také na ročním období. V zimě se obecně vyskytuje více oblačnosti než v létě. Některá oblaka se mohou tvořit pouze v zimě, nebo v létě a v opačném ročním období je neuvidíme. To je dáno zejména různými procesy v atmosféře, které souvisí s daným obdobím. Tato oblaka však nebudou brána v potaz.

Pro sběr dat oblačnosti jsem využil aplikaci *Ventusky*[1]. Jedná se o českou aplikaci spuštěnou v roce 2016, která se zaměřuje na vizualizaci meteorologických dat a předpovědí počasí. Aplikace úzce spolupracuje s portálem in-pocasi.cz. Aplikace nabízí několik numerických modelů, které slouží k předpovědi počasí. Data pro simulaci vychází z modelu ICON EU, který je regionálním modelem vyvíjeným Německým meteorologickým institutem (DWD). ICON je počítán globálně pro celý svět. Na něj navazuje regionální ICON EU, který je počítán s vyšším rozlišením pro Evropu – jeho rozlišení je 7 km.

Data byla sesbírána během prvních dnů v letních měsících v červnu, červenci a srpnu. Obdobně data pro zimu v prosinci, lednu a únoru. Zde jsou data dostupná pouze po 3hodinových intervalech. Dále byla sbírána data také tři dny v dubnu, konkrétně 21., 25. a 26. dubna 2023. Tyto dny obsahují informace o oblačnosti po jednotlivých hodinách. Ve všech případech se jedná o data pro Brno v roce 2022/2023. *Ventusky* nabízí procentuální pokrytí jednotlivých výškových úrovní mraků včetně celkové oblačnosti.

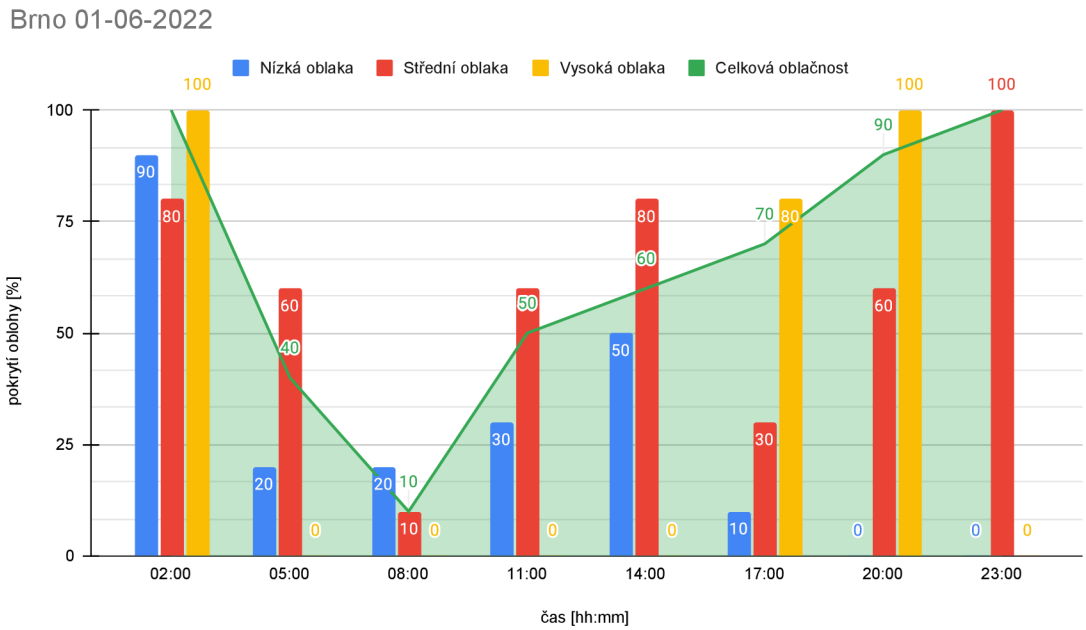
Na obrázku níže je příklad nízké oblačnosti zobrazené aplikací *Ventusky* 8.1.

[1] https://www.ventusky.com/abouthttps://www.ventusky.com/about



Obrázek 8.1: Mapa pokrytí oblohy nízkou oblačností v okolí Brna 1. června 2022

V grafu 8.2 je zobrazeno procentuální pokrytí všech typů oblačnosti 1. června 2022 v Brně na základě dat získaných z portálu *Ventusky*. Procentuální pokrytí se udává od 0 % do 100 %, přičemž 100 % znamená, že není vidět čistá obloha. Celkové pokrytí není součet procentuálních pokrytí jednotlivých výškových vrstev. Například 50 % oblohy každé vrstvy může dát celkové pokrytí 100 %, ne ale 150 %. Popřípadě 50% pokrytí nízkou a střední oblačností může dát celkové pokrytí pouze 60 %, neboť velká část oblohy stále nemusí být pokrytá oblačností. Celkové pokrytí záleží na konkrétních typech oblak. Veškerá posbíraná data jsou uložena do formátu CSV, odkud je později bude čerpat simulační nástroj.

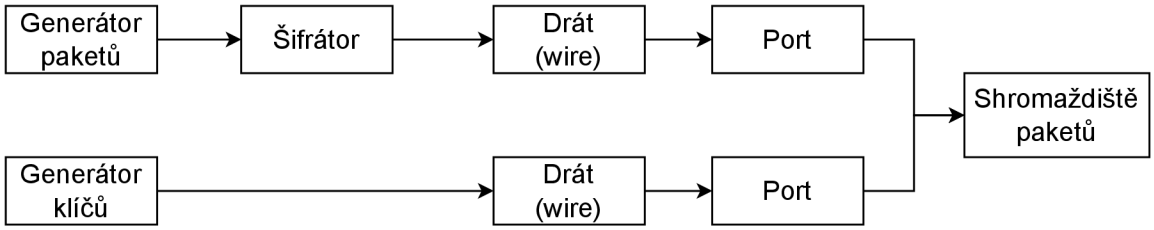


Obrázek 8.2: Zobrazení procentuálního pokrytí oblačností jednotlivých výškových vrstev v Brně 1. června 2022

Každý typ mraku ovlivňuje laserový paprsek jinak. Záleží vždy na vlastnostech oblaku. Z výškové klasifikace mraků, zmíněné zde 3.2.4 lze usoudit, že nízko položená oblaka ovlivňují paprsky laseru více než ty výše položené. Je to dáno tím, že nízká oblaka obsahují více kapek vody a mají větší hustotu, což zvyšuje šanci na roztříštění nebo pohlcení paprsku. Naopak vysoká oblaka jsou více průsvitná, a tedy lze předpokládat, že budou méně vychylovat laserové paprsky. K odsimulování vlivu oblačnosti na přenos kvantové a normální informace laserem lze tedy namapovat výsledky měření, zmíněné v předchozí kapitole 7.3, v níž byl nasazen simulátor útočníka. Ten odkláněl data z kanálu, a narušoval tak koherenci dat. Největší narušení bylo pro 45 %, to lze tedy namapovat na nízká oblaka. Naopak nejmenší narušení 30 % lze namapovat na vysoká oblaka, 40% narušení pak pro střední oblaka. Vliv oblak na laserový paprsek je komplexní záležitost, která je ovlivněna mnoha faktory a vlastnostmi mraků. Simulace tak vychází ze zjednodušeného modelu. Pro potřeby simulace se předpokládá, že oblaka alespoň částečně propustí laserový paprsek a umožňují i malý přenos dat.

8.2 Simulační nástroj

Pro simulování laserových přenosů byla použita Python knihovna `SimPy` s nadstavbou `ns.py`. `SimPy` umožňuje modelování stochastických procesů s diskrétním výskytem událostí. Rozšíření `ns.py` přidává objekty a mechanismy pro simulaci síťové komunikace. Některé byly použity nebo upraveny tak, aby seděly do podoby laserové komunikace. Na diagramu 8.3 je schéma bloků, ze kterých se skládá běh simulace:



Obrázek 8.3: Blokové schéma zapojení jednotlivých bloků simulace

Popis jednotlivých bloků:

- Generátory – Generátor paketů slouží pro simulaci přenosu klasických dat. Vytváří pakety o velikosti, která je generována z exponenciálního rozdělení s hodnotou $\lambda = 0,001$. Pakety jsou zarovnávány tak, aby jejich minimální velikost byla alespoň 21 bajtů (minimum paketu na internetu je 20 B hlavička a 1 B dat). Maximální velikost je poté omezena na 1 506 bajtů (typická velikost MTU). Interval pro generování nových paketů je dán normálním rozdělením se střední hodnotou $\mu = 0,1$ a směrodatnou odchylkou $\sigma = 0,01$.

  Generátor klíčů simuluje QKD systém, tedy samotné vytváření klíčů. Vytváří pakety, jejichž velikost je dána normálním rozdělením se střední hodnotou $\mu = 2\,506$ a směrodatnou odchylkou $\sigma = 389$. Data vychází z tabulky 7.1 naměřených parametrů pro kvantový kanál v klidovém (běžném provozu). Střední hodnota je průměr a směrodatná odchylka vychází z výpočtu $(MAX - MIN)/2$. Velikost je následně nutné interně převést na bajty. Tyto „pakety“ jsou generovány každou jednou jednotkou

simulačního času. Tento jeden paket tedy reprezentuje rychlost generování klíče na kvantovém spoji za dobrých podmínek.

- Šifrátor – do schématu byl vytvořen objekt reprezentující šifrovací algoritmus. Zanáší umělé zpoždění paketů, což představuje dobu šifrování. Ta je dána konkrétním algoritmem a velikostí paketu, který se šifruje. Objekt si také pamatuje množství spotřebované energie, která je nutná pro zašifrování dat. Je nutno dodat, že schéma neobsahuje dešifrování. Dešifrátor se dá do schématu snadno přidat, jakožto další objekt na konci, který je identický se šifrátorem. Implementovány byly všechny šifry, které jsou zmíněné v tabulce 6.1. Je tedy možné vybrat kteroukoliv šifru.

- Drát (angl. objekt `Wire`) – přidává zpoždění. Reprezentuje zpoždění daného kanálu. Zpoždění je dáno exponenciální distribuční funkcí s hodnotou $\lambda = 0,12$. Hodnota vychází z [76], v čemž se měří průměrné zpoždění kanálu. Volitelně lze přidat i určitou ztrátovost kanálu.

- Port – modeluje výstupní port spoje. Tento objekt umožňuje modelovat propustnost kanálu. Jedná se o důležitý prvek zapojení. Skrz něj lze ovlivňovat rychlost spojení, a tedy měnit rychlost, s jakou se přenáší kvantově zabezpečené klíče a klasická data. Propustnost se udává v bitech za sekundu. Pro kvantový kanál je výchozí hodnota 3 000 bit/s, z měření 7.1 nebyla rychlost přenosu vyšší. Pro klasická data má přenos pomocí laseru nastavenu propustnost 100 Mb/s. Takové hodnoty by jednotlivá spojení měla pouze za předpokladu čisté oblohy, a tedy téměř nulového narušení signálu.

- Shromaždiště paketů – jak název napovídá, je to koncový blok, v němž se shromažďují vygenerované pakety a klíče. Tento objekt slouží ke sběru informací. Především počítá zpoždění paketů, množství přenesených bajtů nebo to, jak dlouho čekaly pakety při zahlcení linky. U simulace je v této práci důležitý počet přijatých bajtů, z čehož se poté odvodí propustnost jednotlivých kanálů.

Samotný běh simulace se děje po jednotlivých krocích. `SimPy` je jako většina jiných knihoven a frameworků jednovláknová a deterministická. Pokud by se například nepoužily distribuční funkce pro generování paketů nebo klíčů, výsledek běhu simulace by byl pokaždé naprosto identický. Výsledek simulace je tedy stochastický a může pro různé běhy udávat lehce odlišné hodnoty. Nikoliv však drasticky odlišné, vždy bude záležet na dané specifikaci počasí a přenosových rychlostech. Daný kanál (`wire`) je možné propojit do jednoho, přičemž se kvantový i klasický kanál spojí dohromady. V rámci spouštění běhů simulace jsem tuto variantu nebral v potaz.

8.3 Popis simulace

Běh nástroje začíná načtením vstupních dat z CSV souboru. Formát dat je popsán v příloze A. Data udávají informace o oblačnosti během dne. Každý řádek reprezentuje jeden simulační blok (10 časových jednotek). Tento blok je rozdělen procentuálně mezi dané rychlosti přenosu podle celkového pokrytí oblohy oblačností. Ty se střídají sekvenčně, neboť simulační systém provádí vždy jednu událost po druhé. Zde je menší příklad: Celkové pokrytí oblačností je 60 %. Nízká oblačnost tvoří 50 % a střední oblačnost 80 %, vysoká oblaka se nevyskytují. Postup je následující:

- Jestliže je celková oblačnost 60 %, pak u 4 z 10 kroků bude mít simulace maximální možnou přenosovou rychlost, tedy takovou, u níž spoj není ovlivněn žádným útlumem.
- 60 % bude rozděleno poměrově mezi jednotlivé vrstvy oblačnosti, které ji tvoří. Zde 2 kroky (20 %) připadnou nízké oblačnosti a poslední 4 kroky (40 %) střední oblačnosti. Poměry se vypočítají následovně:

$$60/(50+80) = 0,461 \tag{8.1}$$
$$0,461 * 5 = 2,305 \tag{8.2}$$
$$0,461 * 8 = 3,688 \tag{8.3}$$

  Výsledky se zaokrouhlí na celá čísla. Každý typ oblačnosti ovlivňuje rychlost jiným způsobem. Ty byly představeny v sekci o klasifikaci mraků 3.2.4.

Tento princip je aplikován na každý řádek souboru dat. Vždy po deseti krocích se zaznamenají údaje z jednotlivých bloků a zapíší se do výstupního CSV souboru, jehož formát je popsán v příloze A.

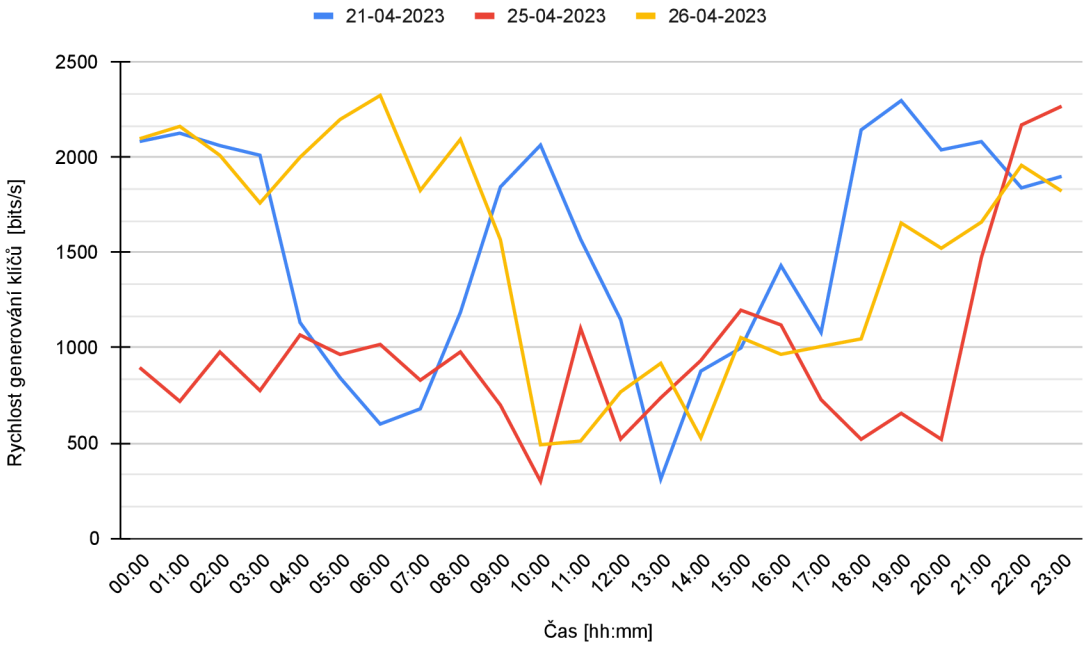
Šifrování dat probíhá pouze pro klasická data. Hodnoty pro šifrátor vychází z tabulky 6.1. Spotřeba baterie je pro zašifrování 5 MiB souboru, bylo tedy nutné tuto hodnotu v simulačním systému upravit tak, aby hodnoty odpovídaly jednomu bajtu dat. Propustnost šifry je také dána v MiB, muselo tedy dojít i k jejímu převodu na bajty. Do výstupního CSV souboru je zaznamenána pouze celková spotřeba (v μAh) a celkové zpoždění za daný simulační blok (10 jednotek času pro jeden řádek dat).

8.4 Výsledky simulace

V této sekci jsou prezentovány výsledky simulace pro letní a zimní měsíce a pro tři dny v dubnu. Každý den byl odsimulován 5krát. Návod na spuštění simulačního nástroje je uveden v příloze C. Výsledky jsou zobrazeny vždy pro poslední běh. Pro dubnové dny, které mají rozlišení 1 hodiny, je zobrazena rychlost kvantového klasického kanálu a celkové odhadované spotřeby vybraných šifrovacích algoritmů. U letních a zimních měsíců je zde zobrazen pouze graf rychlosti generování kvantových klíčů. Grafy klasického kanálu lze nalézt v příloze B.

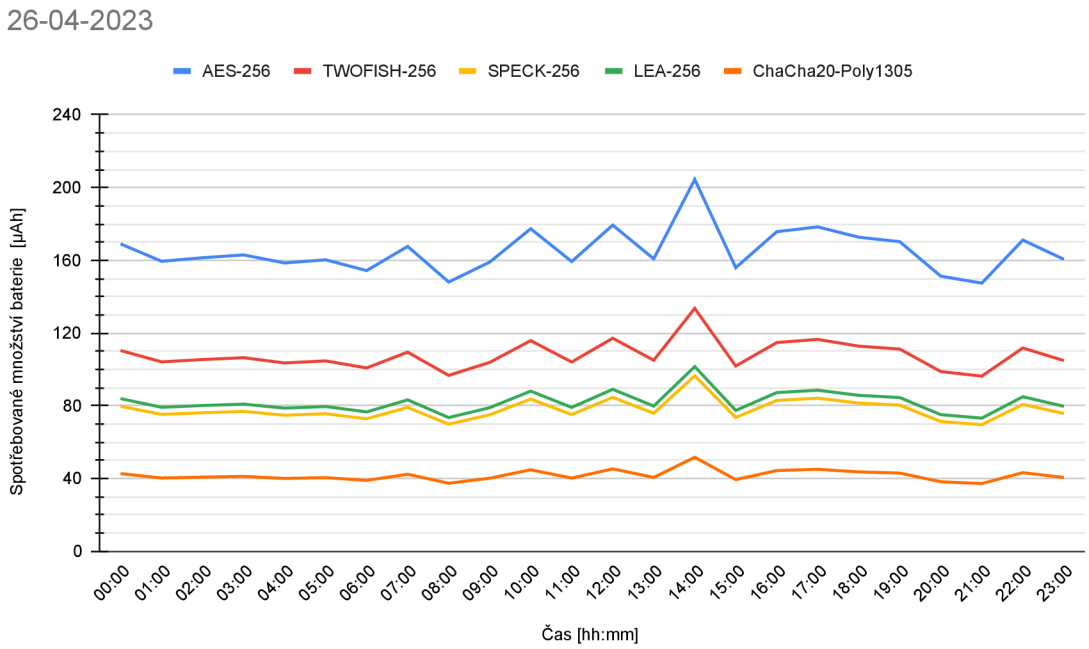
8.4.1 Jarní oblačnost

Výsledky simulace pro následující dny (21., 25. a 26. dubna). Časové rozestupy jsou po jedné hodině:

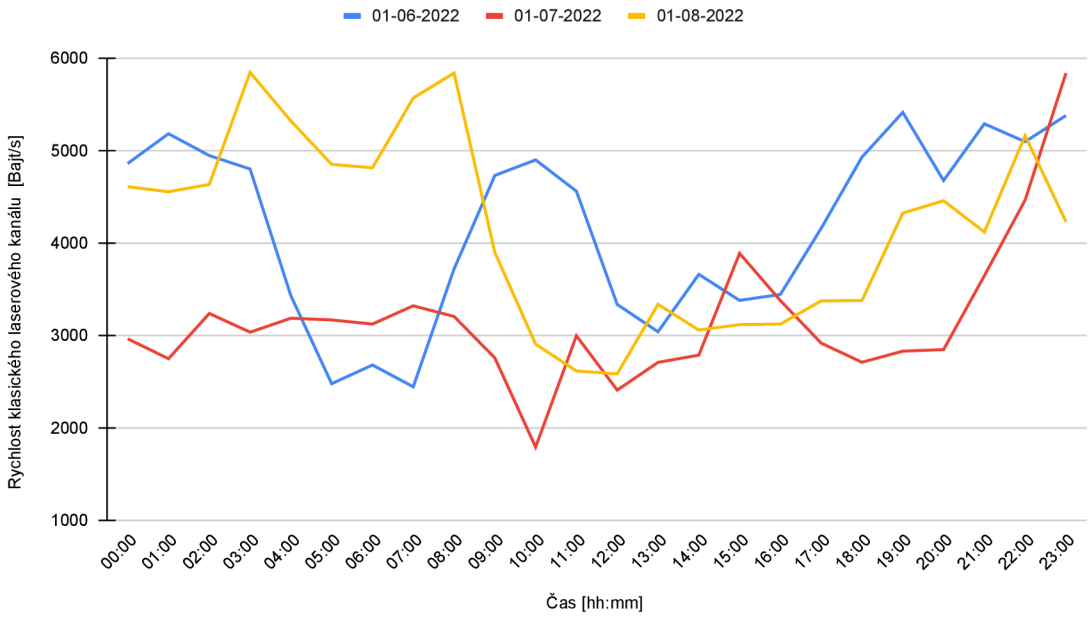


Obrázek 8.4: Rychlost kvantového kanálu během vybraných tří dnů v dubnu 2023

Výstupy simulačního nástroje pro šifrovací algoritmy (na obrázku 8.5 reprezentují pouze 10 sekund z dané hodiny. Proto hodnoty do grafu byly roznásobeny hodnotu $6 * 60$, aby odpovídaly jedné hodině.



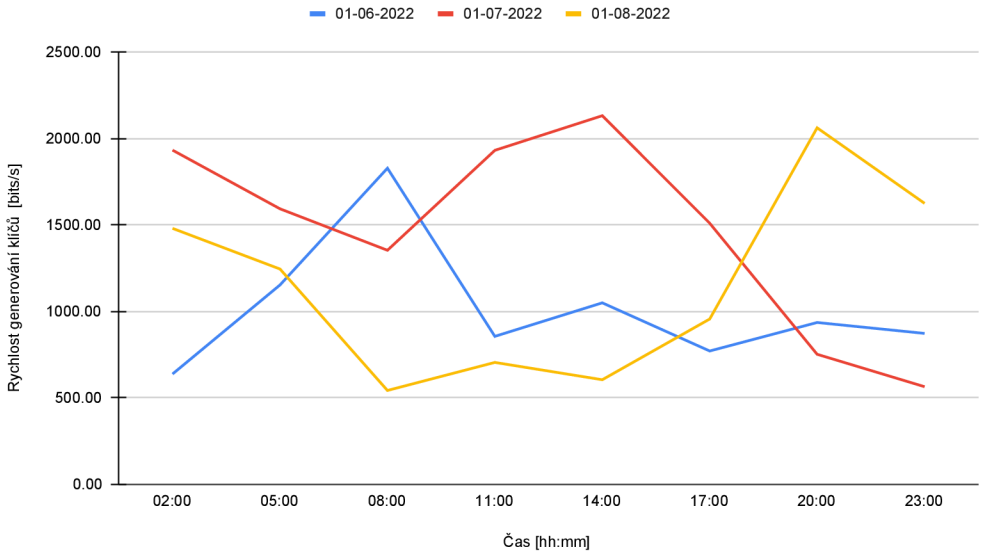
Obrázek 8.5: Odhadovaná spotřeba baterie v μAh pro dané šifrovací algoritmy během jednoho dne (26. dubna 2023)



Obrázek 8.6: Rychlost klasického laserového kanálu během vybraných tří dnů v dubnu 2023

8.4.2 Letní oblačnost

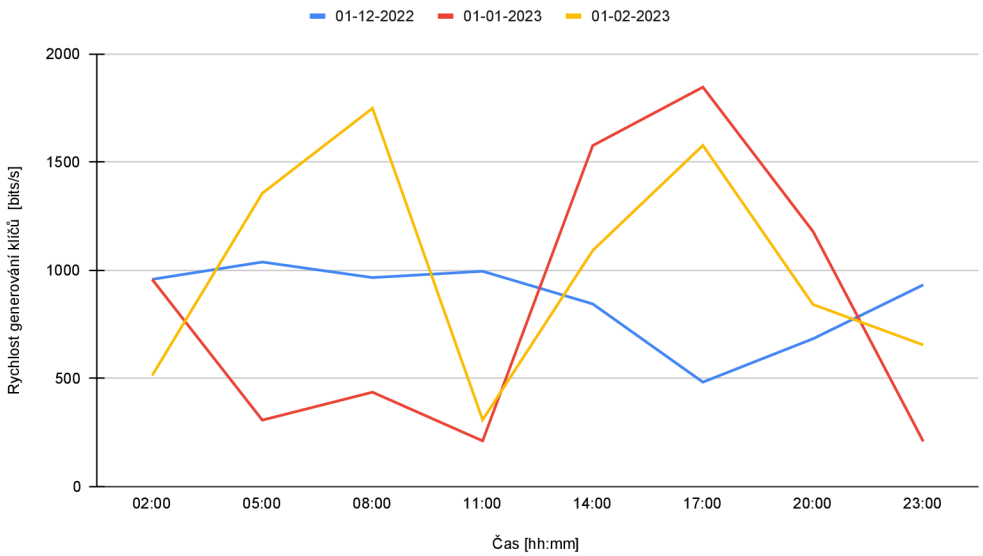
Výsledky simulace pro letní měsíce:



Obrázek 8.7: Rychlost kvantového kanálu v letních měsících

8.4.3 Zimní oblačnost

Výsledky simulace pro zimní měsíce:



Obrázek 8.8: Rychlost kvantového kanálu v zimních měsících

8.5 Vyhodnocení simulace

Simulace, která byla provedena během dnů, které měly časový rozestup jedné hodiny, dává nejpřesnější výsledky. Jak lze vidět na obrázku 8.4, rychlost kvantového kanálu se může značně měnit v závislosti na dané oblačnosti. Krasně to lze spatřit na prvním dnu (21. dubna, modrá barva), u kterého byla rychlost v ranních hodinách kolem 750 bitů/s, kolem poledne opět vzrostla na průměrnou rychlost přes 2 kbit/s a následně zase klesla. Toto přináší otázky, zda má pro nízké rychlosti smysl data přenášet, nebo počkat až budou lepší podmínky, a neriskovat tedy zbytečnou ztrátu dat během přenosu a plýtvat energií.

Na dalším obrázku je vidět 8.5 odhadovaná spotřeba energie pro šifrování dat na klasickém kanále pro den 26. dubna. Zajímavá je asociace s rychlostmi přenosu dat na 8.4 a 8.6. Můžeme vidět, že největší spotřeba byla ve chvílích, v nichž rychlost kanálu byla nejnižší (žlutá křivka na 8.6), tedy kolem 14. hodiny. Spotřeba jednotlivých šifer koreluje s informacemi z tabulky 6.1. Lze si též povšimnout, že spotřeba u algoritmů, které jsou více náročné na spotřebu (AES), v kritických chvílích roste daleko rychleji, než v případě těch méně náročných (ChaCha20-Poly1305). Během velké ztrátovosti kanálu narůstá bitová chybovost. Což způsobuje ztrátu paketů nebo jejich poškození[2]. V reálném nasazení to může vyústit ve ztrátu synchronizace mezi šifrováním na jedné straně a dešifrováním na straně druhé. To se často řeší opakovanými pokusy o resynchronizaci, což dále zatěžuje kanál a zvyšuje energetickou spotřebu během šifrování. Zvlášť pro proudové šifry může být synchronizace náročnější, stejně tak pro blokové šifry. Proto může být na místě nasadit blokovou šifru v momentě, kdy očekáváme větší ztrátovost kanálu, a to i přesto, že bloková šifra může být náročnější na spotřebu. Více je toto rozvedeno ve studii zde [133].

Pokud by to zařízení umožňovalo, mohlo by být možné mezi jednotlivými šiframi i dynamicky přepínat. V případě dobrých přenosových rychlostí stačí použít šifry, u kterých je bezpečnost dostatečně prokázána (např. AES nebo Twofish). Pokud by přenosové rychlosti kanálu byly nízké, mohou rychlejší šifry ChaCha20-Poly1305 nebo Speck být efektivnější, a to jak z hlediska spotřeby, tak i samotné zátěže kanálu. Záleží také na tom, jak moc jsou přenášená data citlivá na šifrování. V případě, že chceme mít jistotu naprosté bezpečnosti, je lepší počkat na dobré přenosové podmínky a šifrovací algoritmus dynamicky neměnit

Porovnání mezi zimním a letním obdobím dopadlo podle očekávaní. V zimě je daleko větší míra oblačnosti a rychlost se může měnit daleko více. Vždy ale záleží na konkrétních dnech a na stavu počasí. I v zimě může být krásné počasí, a naopak v létě bývají bouřky. Nicméně obecně lze předpokládat v zimě menší přenosovou rychlost a větší útlum.

Nutno ovšem podotknout, že výsledky jsou pouze simulace nad daným modelem, který nezahrnuje všechny možné parametry reálného světa a atmosféry. Nelze tedy říci, že by odpovídala realitě jedna ku jedné. Dává ale solidní odhad, jak se může měnit rychlost v závislosti na dané oblačnosti, jež se může rapidně měnit. Simulační systém se dá libovolně upravit tak, aby odpovídal jiným hodnotám přenosů kvantových kanálů. Hodnoty pro rychlost generování klíčů a útlum kvantových kanálů vychází z měření QKD systému *Clavis*[3].

[2] Zde je dobré upřesnit, že toto simulační nástroj nedokáže.

Kapitola 9

Závěr

Cílem této diplomové práce bylo prozkoumat různé protokoly pro kvantovou distribuci klíčů, změřit přenosové vlastnosti a navrhnout simulační nástroj. Tento cíl práce byl splněn.

Pro navržení simulačního nástroje bylo potřeba nastudovat dostupnou literaturu o kvantové distribuci klíčů a protokoly, které se k tomuto účelu využívají, což je popsáno v kapitole 2. Dále bylo nutné nastudovat různá existující řešení QKD systémů a to včetně bezdrátových laserových řešení, viz kapitola 3. Vytvořené klíče kvantové komunikace odebírají šifrovací algoritmy, které byly popsány v kapitole 4. Nad vybranými algoritmy byla provedena analýza jejich bežečnosti, rychlosti a spotřeby elektrické energie, výsledky jsou sepsány na konci kapitoly 6. Algoritmy ChaCha20-Poly1305, LEA a Speck vyšly jako nejefektivnější pro různá vestavěná zařízení s omezenou baterií. Parametry přenosu QKD systému byly změřeny na existujícím spoji mezi fakultami FEKT a FIT univerzity VUT v Brně. Pro klidový stav se rychlost generování klíčů na kvantovém kanále pohybuje v průměru kolem 2,5 kbit/s. Na změření útlumu kvantového kanálu bylo do spoje zapojeno zařízení simulující útočníka, který se snaží kanál odposlouchávat. Rychlost tak může extrémně klesnout až na 400 bit/s. Výsledky měření jsou popsány v kapitole 7.

V práci jsem poté vytvořil simulační nástroj, který využívá naměřená data kvantového kanálu tak, aby simuloval přenos dat za pomoci laserů. Bylo dále nutné zajistit data o oblačnosti během dne. Různé vrstvy oblak mohou měnit danou rychlost laserového spoje. V momentech špatného počasí, při němž je přenosová rychlost malá, může být lepší přenos zcela přerušit a vyčkat na lepší atmosférické podmínky než se snažit přenášet data, šifrovat je a plýtvat energií. Záleží, jak dlouho bude velká oblačnost přetrvávat. Rychlosti za špatného počasí se mohou pohybovat kolem 700 bit/s. Více je možné nalézt v poslední kapitole 8.

Zadání této diplomové práce jsem si vybral, jelikož mi téma kvantové kryptografie přišlo zajímavé a málo prozkoumané. Vypracování mě naučilo mnoho o principech kvantové mechaniky a o jejím aplikování pro distribuci kryptografických klíčů po kvantovém kanále, na kterém je bezpečnost založena na fyzikálních principech. Dále mě práce obohatila o jednotlivé možnosti laserových přenosů, především pak ve spojení s bezdrátovým kanálem, který je realizován pomocí satelitních družic. Dozvěděl jsem se také mnoho o symetrických šifrách, které vznikly pro zařízení s omezeným zdrojem energie.

Budoucí práce na toto téma by mohly být zaměřené na možná další využití QDK systémů, jako jsou například generátory náhodných dat. Dále by se dal zlepšit simulační nástroj, který by bral v potaz konkrétní typy mračen. Další zajímavou možností by bylo skutečné změření a vyhodnocení laserových přenosů se satelitem.

Literatura

[1] Alagic, G., Cooper, D., Dang, Q., Dang, T., Kelsey, J. M. et al. *Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process*. Gaithersburg, Maryland, USA: National Institute of Standards and Technology, 05. července 2022. DOI: https://doi.org/10.6028/NIST.IR.8413. Dostupné z: https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=934458.

[2] Alrowaithy, M. a Thomas, N. Investigating the Performance of C and C++ Cryptographic Libraries. In:. New York, USA: Association for Computing Machinery, 2019, s. 167–170. VALUETOOLS 2019. DOI: 10.1145/3306309.3306335. ISBN 9781450365963. Dostupné z: https://doi.org/10.1145/3306309.3306335.

[3] Assche, G. v. *Quantum Cryptography and Secret-Key Distillation*. Cambridge, Anglie: Cambridge University Press, 2006. 10-12 s. ISBN 9780511617744.

[4] Avanzi, R., Bos, J., Ducas, L., Kiltz, E., Lepoint, T. et al. *CRYSTALS-Kyber: Algorithm Specifications And Supporting Documentation (version 3.02)* [online]. PQ-Crystals, 04. srpna 2021. Dostupné z: https://pq-crystals.org/kyber/data/kyber-specification-round3-20210804.pdf.

[5] Bai, S., Ducas, L., Kiltz, E., Lepoint, T., Lyubashevsky, V. et al. *CRYSTALS-Dilithium: Algorithm Specifications and Supporting Documentation (Version 3.1)* [online]. PQ-Crystals, 08. února 2021. Dostupné z: https://pq-crystals.org/dilithium/data/dilithium-specification-round3-20210208.pdf.

[6] Baritompa, W. P., Bulger, D. W. a Wood, G. R. Grover's Quantum Algorithm Applied to Global Optimization. *SIAM Journal on Optimization*. 2005, sv. 15, č. 4, s. 1170–1184. DOI: 10.1137/040605072. Dostupné z: https://doi.org/10.1137/040605072.

[7] Beaulieu, R., Treatman Clark, S., Shors, D., Weeks, B., Smith, J. et al. The SIMON and SPECK lightweight block ciphers. In: *2015 52nd ACM/EDAC/IEEE Design Automation Conference (DAC)*. San Francisco, USA: IEEE, červen 2015, s. 1–6. DOI: 10.1145/2744769.2747946. ISBN 978-1-4799-8052-9. Dostupné z: https://ieeexplore.ieee.org/document/7167361.

[8] Bedington, R., Arrazola, J. M. a Ling, A. Progress in satellite quantum key distribution. *NPJ Quantum Information*. Springer Science and Business Media LLC. Srpen 2017, sv. 3, č. 1. DOI: 10.1038/s41534-017-0031-5. Dostupné z: https://doi.org/10.1038%2Fs41534-017-0031-5.

[9] Biham, E. A Fast New DES Implementation in Software. In: *Fast Software Encryption Workshop*. 4th International Workshop. Haifa, Izrael: Springer, 1997, sv. 1267, s. 260–272. Lecture Notes in Computer Science. DOI: 10.1007/BFb0052352.

[10] Biham, E. a Shamir, A. Differential Cryptanalysis of DES-like Cryptosystems. *Journal of Cryptology*. 1991, sv. 4, s. 3–72. DOI: 10.1007/BF00630563.

[11] Biryukov, A. a Grossschädl, J. Cryptanalysis of the Full AES Using GPU-Like Special-Purpose Hardware. *IACR Cryptology ePrint Archive*. Leden 2011, sv. 2011, s. 710. DOI: 10.3233/FI-2012-626. Dostupné z: https://eprint.iacr.org/2011/710.pdf.

[12] Branciard, C. *Distributed phase reference schemes for QKD: Explicit attacks and security considerations*. Université de Genève, Švýcarsko: Perimeter Institute, červen 2007. DOI: 10.48660/07060011. PIRSA:07060011. Dostupné z: https://pirsa.org/07060011.

[13] Branciard, C., Gisin, N., Lutkenhaus, N. a Scarani, V. Zero-Error Attacks and Detection Statistics in the Coherent One-Way Protocol for Quantum Cryptography. arXiv. 2006. DOI: 10.48550/ARXIV.QUANT-PH/0609090. Dostupné z: https://arxiv.org/abs/quant-ph/0609090.

[14] Branciard, C., Gisin, N. a Scarani, V. Upper bounds for the security of two distributed-phase reference protocols of quantum cryptography. *New Journal of Physics*. IOP Publishing Ltd. Leden 2008, sv. 10, č. 1, s. 013031. DOI: 10.1088/1367-2630/10/1/013031. Dostupné z: https://iopscience.iop.org/article/10.1088/1367-2630/10/1/013031/pdf.

[15] Bub, J. Quantum Entanglement and Information. In: Zalta, E. N. a Nodelman, U., ed. *The Stanford Encyclopedia of Philosophy* [online]. Summer 2023. Stanford, Kalifornie, USA: Metaphysics Research Lab, Stanford University, 2023 [cit. 2023-05-05]. Archiv (URL) bude dostupný až od 21. Června 2023. Dostupné z: https://plato.stanford.edu/archives/sum2023/entries/qt-entangle/.

[16] Cao, Y., Li, Y.-H., Yang, K.-X., Jiang, Y.-F., Li, S.-L. et al. Long-Distance Free-Space Measurement-Device-Independent Quantum Key Distribution. *Physical Review Letters*. American Physical Society. Prosinec 2020, sv. 125, č. 26, s. 260503–260509. DOI: 10.1103/PhysRevLett.125.260503. Dostupné z: https://journals.aps.org/prl/pdf/10.1103/PhysRevLett.125.260503.

[17] Chefles, A. Unambiguous discrimination between linearly independent quantum states. *Physics Letters A*. 1998, sv. 239, č. 6, s. 339–347. DOI: https://doi.org/10.1016/S0375-9601(98)00064-4. ISSN 0375-9601. Dostupné z: https://www.sciencedirect.com/science/article/pii/S0375960198000644.

[18] Chen, Y.-A., Zhang, Q., Chen, T.-Y., Cai, W.-Q., Liao, S.-K. et al. An integrated space-to-ground quantum communication network over 4,600 kilometres. *Nature*. Leden 2021, sv. 589, s. 214–219. DOI: https://doi.org/10.1038/s41586-020-03093-8. Dostupné z: https://www.nature.com/articles/s41586-020-03093-8.pdf.

[19] Cherckesova, L. V., Safaryan, O. A., Beskopylny, A. N. a Revyakina, E. Development of Quantum Protocol Modification CSLOE-2022, Increasing the Cryptographic Strength of Classical Quantum Protocol BB84. *Electronics*. 2022, sv. 11, č. 23. DOI: 10.3390/electronics11233954. ISSN 2079-9292. Dostupné z: https://www.mdpi.com/2079-9292/11/23/3954.

[20] Choi, I., Young, R. J. a Townsend, P. D. Quantum information to the home. *New Journal of Physics*. New Journal of Physics. Červen 2011, sv. 13, č. 6, s. 063039. DOI: 10.1088/1367-2630/13/6/063039. Dostupné z: https://iopscience.iop.org/article/10.1088/1367-2630/13/6/063039/pdf.

[21] *Clavis*^{3} *QKD Platform Brochure* [online]. Carouge, Ženeva, Švýcarsko: ID Quantique, leden 2020 [cit. 2022-11-28]. Dostupné z: https://marketing.idquantique.com/acton/attachment/11868/f-0216/1/-/-/-/-/Clavis3%20QKD%20Platform_Brochure.pdf.

[22] Crane Casey. *Block Cipher vs Stream Cipher: What They Are & How They Work* [online]. HashedOut, 14. ledna 2021 [cit. 2023-03-05]. Dostupné z: https://www.thesslstore.com/blog/block-cipher-vs-stream-cipher/.

[23] Cruz, R. J., Guimarães, A. a Aranha, D. F. *Efficient and secure software implementations of Fantomas* [online]. 2019. Cryptology ePrint Archive, Paper 2019/906. Dostupné z: https://eprint.iacr.org/2019/906.pdf.

[24] *Cryptography in a post-quantum world* [online]. Carouge, Ženeva, Švýcarsko: Accenture Technology, 04. října 2018 [cit. 2023-03-01]. Dostupné z: https://www.accenture.com/content/dam/accenture/final/a-com-migration/manual/r3/pdf/Accenture-809668-Quantum-Cryptography-Whitepaper-v05.pdf.

[25] *CVE-2016-2183* [online]. CVE - Mitre, 31. srpna 2016 [cit. 2023-03-08]. Dostupné z: https://nvd.nist.gov/vuln/detail/CVE-2016-2183.

[26] Daemen, J. a Rijmen, V. *AES Proposal: Rijndael*. National Institute of Standards and Technology, USA, 09. dubna 2003. Dostupné z: https://csrc.nist.gov/csrc/media/projects/cryptographic-standards-and-guidelines/documents/aes-development/rijndael-ammended.pdf.

[27] Daniel Dinu, D. K. Triathlon of lightweight block ciphers for the Internet of things. *Journal of Cryptographic Engineering* [online]. Červenec 2018, sv. 9. DOI: https://doi.org/10.1007/s13389-018-0193-x. Dostupné z: https://link.springer.com/article/10.1007/s13389-018-0193-x.

[28] Delfs, H. a Knebl, H. *Introduction to Cryptography: Principles and Applications*. 2. vyd. Springer Berlin, Heidelberg, 2007. ISBN 978-3-642-08040-1. Dostupné z: https://link.springer.com/book/10.1007/3-540-49244-5.

[29] Derbez, P. a Fouque, P.-A. Exhausting Demirci-Selçuk Meet-in-the-Middle Attacks Against Reduced-Round AES. In:. Březen 2013. DOI: 10.1007/978-3-662-43933-3_28. ISBN 978-3-662-43932-6. Dostupné z: https://eprint.iacr.org/2015/259.pdf.

[30] Dey, S., Garai, H. K. a Maitra, S. *Cryptanalysis of Reduced Round ChaCha-New Attack and Deeper Analysis* [online]. International Association for Cryptologic Research, 2023. DOI: https://doi.org/10.46586/tosc.v0.i0.0-0. Cryptology ePrint Archive, Paper 2023/134. Dostupné z: https://eprint.iacr.org/2023/134.pdf.

[31] Diffie, W. a Hellman, M. New directions in cryptography. *IEEE Transactions on Information Theory*. 1976, sv. 22, č. 6, s. 644–654. DOI: 10.1109/TIT.1976.1055638. Dostupné z: https://ieeexplore.ieee.org/document/1055638.

[32] Dinur, I. Improved Differential Cryptanalysis of Round-Reduced Speck. In: Joux, A. a Youssef, A., ed. *Selected Areas in Cryptography – SAC 2014*. Cham: Springer International Publishing, 2014, s. 147–164. ISBN 978-3-319-13051-4.

[33] *Eavesdropping simulator: principle and implementation*. Carouge, Ženeva, Švýcarsko: ID Quantique, květen 2020 [cit. 2023-02-17]. Soubor je možné nalézt na přiloženém paměťovém médiu.

[34] Elminaam, D. S. A., Kader, H. M. A. a Hadhoud, M. M. Evaluating The Performance of Symmetric Encryption Algorithms. *International Journal of Network Security*. Egypt: [b.n.]. Květen 2010, sv. 10, č. 3, s. 213–219. Dostupné z: http://ijns.jalaxy.com.tw/contents/ijns-v10-n3/ijns-2010-v10-n3-p213-219.pdf.

[35] Erven, C. *On Free Space Quantum Key Distribution and its Implementation with a Polarization-Entangled Parametric Down Conversion Source*. Waterloo, Ontario, Kanada, 2007. Diplomová práce. University of Waterloo. Dostupné z: https://uwspace.uwaterloo.ca/handle/10012/3021.

[36] Ferguson, N. Impossible dierentials in Twofish. Červen 2000. Dostupné z: https://www.schneier.com/wp-content/uploads/2016/02/paper-twofish-impossible.pdf.

[37] Figueroa Hernandez, J. *A Comparison of Lightweight Ciphers Meeting NIST Lightweight Cryptography Requirements to the Advanced Encryption Standard*. Pomona, US, 2019. Diplomová práce. California State Polytechnic University. Dostupné z: https://scholarworks.calstate.edu/concern/theses/dr26z024c?locale=en.

[38] Gaidash, A. A., Egorov, V. I. a Gleim, A. V. Revealing of photon-number splitting attack on quantum key distribution system by photon-number resolving devices. *Journal of Physics*. IOP Publishing. Srpen 2016, sv. 735, č. 1, s. 012072. Conference Series. DOI: 10.1088/1742-6596/735/1/012072. Dostupné z: https://iopscience.iop.org/article/10.1088/1742-6596/735/1/012072/pdf.

[39] Gaj, K. a Chodowiec, P. Comparison of the Hardware Performance of the AES Candidates Using Reconfigurable Hardware. In: *AES Candidate Conference*. New York, USA: [b.n.], Duben 2000, s. 40–54.

[40] Gao, R.-Q., Xie, Y.-M., Gu, J., Liu, W.-B., Weng, C.-X. et al. Simple security proof of coherent-one-way quantum key distribution. *Optics Express*. Nanjing University, China: Optica Publishing Group. Červen 2022, sv. 30, č. 13, s. 23783–23795. DOI: 10.1364/oe.461669. Dostupné z: https://doi.org/10.1364%2Foe.461669.

[41] Gisin, N., Ribordy, G., Zbinden, H., Stucki, D., Brunner, N. et al. *Towards practical and fast Quantum Cryptography*. Ženeva, Švýcarsko: arXiv, 2004. DOI: 10.48550/ARXIV.QUANT-PH/0411022. Dostupné z: https://arxiv.org/pdf/quant-ph/0411022.pdf.

[42] Halmos, P. R. *A Hilbert Space Problem Book*. Springer New York, NY, 1982. ISBN 978-0-387-90685-0. Dostupné z: https://link.springer.com/book/10.1007/978-1-4684-9330-6.

[43] Harrison, D. M. *Mach-Zehnder Interferometer*. University of Toronto, Canada: Physics Virtual Bookshelf, 15. října 2018 [cit. 2022-12-28]. Dostupné z: https://faraday.physics.utoronto.ca/PVB/Harrison/MachZehnder/MachZehnder.html.

[44] Hercigonja, Z. Comparative Analysis of Cryptographic Algorithms. *International Journal of Digital Technology and Economy* [online]. Prosinec 2016, sv. 1, č. 2, s. 127–134, [cit. 2023-03-08]. Dostupné z: https://hrcak.srce.hr/en/file/262162.

[45] Heyde, K. a Wood, J. L. A theory of polarized photons. In: *Quantum Mechanics for Nuclear Structure, Volume 1*. IOP Publishing, 2019, kap. 1, s. 1–9. 2053-2563. DOI: 10.1088/978-0-7503-2179-2ch1. ISBN 978-0-7503-2179-2. Dostupné z: https://iopscience.iop.org/book/mono/978-0-7503-2179-2.pdf.

[46] Hong, D., Lee, J.-K., Kim, D.-C., Kwon, D., Ryu, K. H. et al. LEA: A 128-Bit Block Cipher for Fast Encryption on Common Processors. In: Kim, Y., Lee, H. a Perrig, A., ed. *Information Security Applications*. Cham: Springer International Publishing, 2014, s. 3–27. Dostupné z: https://link.springer.com/chapter/10.1007/978-3-319-05149-9_1.

[47] Huang, L. S. Z. a Yang, Q. Automatic Differential Analysis of ARX Block Ciphers with Application to SPECK and LEA. In: *Proceedings, Part II, of the 21st Australasian Conference on Information Security and Privacy*. Berlin, Heidelberg: Springer-Verlag, 2016, Volume 9723, s. 379–394. DOI: 10.1007/978-3-319-40367-0_24. ISBN 9783319403663. Dostupné z: https://doi.org/10.1007/978-3-319-40367-0_24.

[48] Ilic, N. The Ekert Protocol. *Journal of PHY334*. University of Waterloo, Kanada: Information Institute Publishing. Červenec 2007, sv. 1. Dostupné z: https://www.ux1.eiu.edu/~nilic/Nina%27s-article.pdf.

[49] Inoue, K., Takesue, H. a Honjo, T. DPS quantum key distribution and related technologies. *Proceedings of SPIE - The International Society for Optical Engineering*. Leden 2009, sv. 7236. DOI: 10.1117/12.808590.

[50] Inoue, K., Waks, E. a Yamamoto, Y. Differential Phase Shift Quantum Key Distribution. *Physical Review Letters*. American Physical Society. Červen 2002, sv. 89. DOI: 10.1103/PhysRevLett.89.037902. Dostupné z: https://journals.aps.org/prl/pdf/10.1103/PhysRevLett.89.037902.

[51] *International cloud atlas*. 2. vyd. Ženeva, Švýcarsko: World Meteorological Organization, 1987. ISBN 9263124078. Dostupné z: https://digitallibrary.un.org/record/6948.

[52] *IQuantum Key Distribution System Clavis*^{3} *User Guide*. 2.8. Ženeva, Švýcarsko: ID Quantique SA, listopad 2021 [cit. 2023-02-15]. Soubor je možné nalézt na přiloženém paměťovém médiu.

[53] Jelen, J. O interpretaci kvantové mechaniky: O čem vlastně je kvantová fyzika? Fakulta elektrotechnická ČVUT, Praha: [b.n.]. 2006. Dostupné z: http://aldebaran.feld.cvut.cz/vyuka/moderni_fyzika_pro_kybernetiku/clanky/kvantmech.pdf.

[54] Juels, A. a Weis, S. A. Authenticating Pervasive Devices with Human Protocols. In: Shoup, V., ed. *Advances in Cryptology – CRYPTO 2005*. Berlin, Heidelberg: Springer Berlin Heidelberg, Srpen 2005, sv. 3621, s. 293–308. DOI: 10.1007/11535218_18. ISBN 978-3-540-28114-6.

[55] Karen Martin. *Waiting for quantum computing: Why encryption has nothing to worry about* [online]. TechBeacon, 15. srpna 2018 [cit. 2023-03-03]. Dostupné z: https://techbeacon.com/security/waiting-quantum-computing-why-encryption-has-nothing-worry-about.

[56] Khatri, N. BLOWFISH ALGORITHM. *International Journal of Engineering Sciences & Management Research*. Říjen 2015. ISSN 2349-6193. Dostupné z: https://www.academia.edu/16734455/BLOWFISH_ALGORITHM.

[57] Klíčník, O. *Kvantová distribuce klíčů přes optickou vláknovou infrastrukturu*. Brno, CZ, 2021. Bakalářská práce. Vysoké učení technické v Brně, Fakulta Elektrotechniky a Komunikačních Technologií. Vedoucí práce Ing. Petr Münster Ph.D. doc. Dostupné z: http://hdl.handle.net/11012/197922.

[58] Kronberg, D. A., Nikolaeva, A. S., Kurochkin, Y. V. a Fedorov, A. K. Quantum soft filtering for the improved security analysis of the coherent one-way quantum-key-distribution protocol. *Physical Review A*. American Physical Society (APS). Březen 2020, sv. 101, č. 3. DOI: 10.1103/physreva.101.032334. Dostupné z: https://journals.aps.org/pra/pdf/10.1103/PhysRevA.101.032334.

[59] Lance, A., Leiseboer, J. a Symul, T. Quantum Key Distribution Systems Compared. In: QuintessenceLabs. [online]. 1.1. Deakin University, Austrálie: [b.n.], Duben 2018. Dostupné z: https://info.quintessencelabs.com/hubfs/PDFs/Whitepaper_QKD_Systems-Compared.pdf.

[60] Lavie, E. a Lim, C. C. Improved Coherent One-Way Quantum key Distribution for High-Loss Channels. *Physical Review Applied*. American Physical Society (APS). Prosinec 2022, sv. 18, č. 6. DOI: 10.1103/physrevapplied.18.064053. Dostupné z: https://journals.aps.org/prapplied/pdf/10.1103/PhysRevApplied.18.064053.

[61] Leal Junior, A. a Frizera Neto, A. Chapter 4 - Optical fiber fundaments and overview. In: Leal Junior, A. a Frizera Neto, A., ed. *Optical Fiber Sensors for the Next Generation of Rehabilitation Robotics*. Academic Press, 2022, s. 67–91. DOI: https://doi.org/10.1016/B978-0-32-385952-3.00013-5. ISBN 978-0-323-85952-3. Dostupné z: https://www.sciencedirect.com/science/article/pii/B9780323859523000135.

[62] Lee, O. a Vergoossen, T. *An updated analysis of satellite quantum-key distribution missions.* arXiv, 2019. DOI: 10.48550/ARXIV.1909.13061. Dostupné z: https://arxiv.org/pdf/1909.13061.pdf.

[63] Liao, S.-K., Cai, W.-Q., Handsteiner, J., Liu, B., Yin, J. et al. Satellite-Relayed Intercontinental Quantum Network. *Physical Review Letters.* American Physical Society. Leden 2018, sv. 120, č. 3, s. 030501–030505. DOI: 10.1103/PhysRevLett.120.030501. Dostupné z: https://journals.aps.org/prl/pdf/10.1103/PhysRevLett.120.030501.

[64] Liyana Chew, N. A. Randomness Analysis on Speck Family Of Lightweight Block Cipher. *International Journal of Cryptology Research.* Kuala Lumpur, Malajsie: Malaysian Society for Cryptology Research. 2015, sv. 5, s. 44–60. Dostupné z: https://www.cybersecurity.my/data/content_files/53/1660.pdf.

[65] Luka Komljenovic and Jonathan Wright and Timothy Szeltner and David Aloi . *Theoretical and Practical Significance of One-Time-Pad Cryptography* [online]. [cit. 2023-03-03]. Dostupné z: https://www.csuohio.edu/sites/default/files/75%20A.pdf.

[66] Lustro, R. A. F. Modified Key Derivation Function for Enhanced Security of Speck in Resource-Constrained Internet of Things. In: [online]. MECS PRESS, Srpen 2021, sv. 4, s. 14–25. DOI: 10.5815/ijcnis.2021.04.02. Dostupné z: https://www.mecs-press.org/ijcnis/ijcnis-v13-n4/IJCNIS-V13-N4-2.pdf.

[67] Luykxl, A., Mennink, B. a Paterson, K. Analyzing Multi-key Security Degradation. In: Tsuyoshi, T. a Thomas, P., ed. *Advances in Cryptology – ASIACRYPT 2017.* Cham, Německo: [b.n.], Listopad 2017, sv. 10625, s. 575–605. Lecture Notes in Computer Science. DOI: 10.1007/978-3-319-70697-9_20. ISBN 978-3-319-70696-2. Dostupné z: https://link.springer.com/chapter/10.1007/978-3-319-70697-9_20.

[68] Mafu, M., Marais, A. a Petruccione, F. A Necessary Condition for the Security of Coherent- One-Way Quantum Key Distribution Protocol. *Applied Mathematics & Information Sciences.* Natural Sciences. 2014, sv. 8, č. 6, s. 2769–2773. Dostupné z: https://www.naturalspublishing.com/files/published/08jfv709wm6fx4.pdf.

[69] Mallick, S. a Malacara, D. Common-Path Interferometers. In: *Optical Shop Testing.* John Wiley & Sons, Ltd, 2007, kap. 3, s. 97–121. DOI: https://doi.org/10.1002/9780470135976.ch3. ISBN 9780470135976. Dostupné z: https://onlinelibrary.wiley.com/doi/pdf/10.1002/9780470135976.ch3.

[70] Menezes, A. J., Oorschot, P. C. van a Vanstone, S. A. Handbook of applied cryptography. In:. 1. vyd. CRC Press, 1996, kap. 8, s. 283–319. ISBN 978-0849385230. Dostupné z: https://cacr.uwaterloo.ca/hac/about/chap8.pdf.

[71] Micciancio, D. Shortest Vector Problem. In: Tilborg, H. C. A. van, ed. *Encyclopedia of Cryptography and Security.* Boston, Maryland, USA: Springer US, 2005, s. 569–570. DOI: 10.1007/0-387-23483-7_392. ISBN 978-0-387-23483-0. Dostupné z: https://doi.org/10.1007/0-387-23483-7_392.

[72] Miralem Mehic, P. F. a Voznak, M. *Quantum Key Distribution Networks: A Quality of Service Perspective*. 1. vyd. Springer Cham, 2022. ISBN 978-3-031-06607-8.

[73] Moradi, A., Poschmann, A., Ling, S., Paar, C. a Wang, H. Pushing the Limits: A Very Compact and a Threshold Implementation of AES. In: *Advances in Cryptology - EUROCRYPT 2011 - 30th Annual International Conference on the Theory and Applications of Cryptographic Techniques*. Springer, 2011, sv. 6632, s. 69. Lecture Notes in Computer Science. DOI: 10.1007/978-3-642-20465-4_6. Dostupné z: https://www.iacr.org/archive/eurocrypt2011/66320067/66320067.pdf.

[74] Moroder, T., Curty, M., Lim, C. C. W., Thinh, L. P., Zbinden, H. et al. Security of Distributed-Phase-Reference Quantum Key Distribution. *Physical Review Letters*. American Physical Society (APS). Prosinec 2012, sv. 109, č. 26. DOI: 10.1103/physrevlett.109.260501. ISSN 1079-7114. Dostupné z: https://journals.aps.org/prl/pdf/10.1103/PhysRevLett.109.260501.

[75] Mouha, N., Mennink, B., Herrewege, A. V., Watanabe, D., Preneel, B. et al. *Chaskey: An Efficient MAC Algorithm for 32-bit Microcontrollers* [online]. International Association for Cryptologic Research, 2014. Cryptology ePrint Archive, Paper 2014/386. Dostupné z: https://eprint.iacr.org/2014/386.pdf.

[76] Newman, D., Sizemore, N., Carreras, B. a Lynch, V. Growth and propagation of disturbances in a communication network model. In: *Proceedings of the 35th Annual Hawaii International Conference on System Sciences*. Big Island, Havaj, USA: IEEE, únor 2002, s. 867– 874. DOI: 10.1109/HICSS.2002.993977. ISBN 0-7695-1435-9.

[77] Nie, T., Zhou, L. a Lu, Z.-M. Power evaluation methods for data encryption algorithms. *IET Software*. 2014, sv. 8, č. 1, s. 12–18. DOI: https://doi.org/10.1049/iet-sen.2012.0137. Dostupné z: https://ietresearch.onlinelibrary.wiley.com/doi/pdf/10.1049/iet-sen.2012.0137.

[78] Nir, Y. a Langley, A. *ChaCha20 and Poly1305 for IETF Protocols* [RFC 8439]. RFC Editor, červen 2018. DOI: 10.17487/RFC8439. Dostupné z: https://www.rfc-editor.org/rfc/pdfrfc/rfc8439.txt.pdf.

[79] Novák, M. *Návrh stabilizovaného optického zdroje*. Brno, CZ, 2011. Bakalářská práce. Vysoké učení technické v Brně, Fakulta Elektrotechniky a Komunikačních Technologií. Vedoucí práce Ing. Miloslav Filka, C. prof. Dostupné z: https://www.vut.cz/www_base/zav_prace_soubor_verejne.php?file_id=42499.

[80] Ntanos, A., Lyras, N. K., Zavitsanos, D., Giannoulis, G., Panagopoulos, A. D. et al. LEO Satellites Constellation-to-Ground QKD Links: Greek Quantum Communication Infrastructure Paradigm. *Photonics*. 2021, sv. 8, č. 12. DOI: 10.3390/photonics8120544. ISSN 2304-6732. Dostupné z: https://www.mdpi.com/2304-6732/8/12/544.

[81] Nurhadi, A. I. a Syambas, N. R. Quantum Key Distribution (QKD) Protocols: A Survey. In: *2018 4th International Conference on Wireless and Telematics (ICWT)*. Bali, Indonésie: IEEE, červenec 2018, s. 1–5. DOI: 10.1109/ICWT.2018.8527822. Dostupné z: https://ieeexplore.ieee.org/document/8527822.

[82] Omowa, E. *Performance and Power Consumption Analysis of Symmetric Encryption Algorithms in Wireless Devices*. Nssuka, Nigérie, 2010. Diplomová práce. University of Nigeria. Vedoucí práce Nwodoh, T. Dostupné z: https://www.academia.edu/40390022/Performance_and_Power_Consumption_Analysis_of_Symmetric_Encryption_Algorithms_in_Wireless_

[83] Ortu, A., Holzäpfel, A., Etesse, J. a Afzelius, M. Storage of photonic time-bin qubits for up to 20 ms in a rare-earth doped crystal. *NPJ Quantum Information* [online]. Březen 2022, sv. 8, č. 29. DOI: https://doi.org/10.1038/s41534-022-00541-3. Dostupné z: https://www.nature.com/articles/s41534-022-00541-3.pdf.

[84] *Y.3800: Overview on networks supporting quantum key distribution* [online]. Ženeva, Švýcarsko: International Telecommunication Union, říjen 2019 [cit. 2022-11-20]. Dostupné z: https://www.itu.int/rec/T-REC-Y.3800-201910-I.

[85] Paschotta, R. Photon Counting. In: *Encyclopedia of Laser Physics and Technology*. 1. vyd. Wiley-VCH, říjen 2008. ISBN 978-3-527-40828-3. Dostupné z: https://www.rp-photonics.com/photon_counting.html.

[86] Podolský, J. *Dvojštěrbinové experimenty v kvantové teorii* [online]. MFF UK, Praha: [b.n.], 10. listopadu 1998. Dostupné z: http://utf.mff.cuni.cz/~podolsky/Kvant/Dvojster.htm.

[87] Prakasam, Kumar, S. a Nandakumar, V. Efficient power distribution model for IoT nodes driven by energy harvested from low power ambient RF signal. *Microelectronics Journal*. 2020, sv. 95, s. 104665. DOI: https://doi.org/10.1016/j.mejo.2019.104665. ISSN 0026-2692. Dostupné z: https://www.sciencedirect.com/science/article/pii/S0026269219307190.

[88] Prakasam, Madheswaran, Sujith a Sayeed, M. S. An Enhanced Energy Efficient Lightweight Cryptography Method for various IoT devices. *ICT Express*. 2021, sv. 7, č. 4, s. 487–492. DOI: https://doi.org/10.1016/j.icte.2021.03.007. ISSN 2405-9595. Dostupné z: https://www.sciencedirect.com/science/article/pii/S2405959521000400.

[89] Přichystal, J. *Úvod do teorie informace* [online]. PEF MZLU v Brně: [b.n.], 24. září 2007 [cit. 2023-02-17]. Dostupné z: https://akela.mendelu.cz/~jprich/predn/teoinf.pdf.

[90] *Quantis QRNG Chips* [online]. Carouge, Ženeva, Švýcarsko: ID Quantique, říjen 2022 [cit. 2023-02-17]. Dostupné z: https://marketing.idquantique.com/acton/attachment/11868/f-025e/1/-/-/-/-/Quantis%20QRNG%20Chip_Brochure.pdf.

[91] *Quantis QRNG USB* [online]. Carouge, Ženeva, Švýcarsko: ID Quantique, srpen 2022 [cit. 2023-02-17]. Dostupné z: https://marketing.idquantique.com/acton/attachment/11868/f-021f/1/-/-/-/-/Quantis%20QRNG_Brochure.pdf.

[92] *Quantum Key Distribution (QKD); Orchestration Interface for Software Defined Networks* [online]. ETSI GS QKD 018 v1.1.1. Francie: European Telecommunications Standards Institute, duben 2022 [cit. 2023-02-15]. Dostupné z:

https://www.etsi.org/deliver/etsi_gs/QKD/001_099/018/01.01.01_60/gs_QKD018v010101p.pdf.

[93] *Quantum Key Distribution Training CerberisXG presentation.* V3.1.0. Ženeva, Švýcarsko: ID Quantique SA, duben 2022 [cit. 2023-02-15]. Soubor je možné nalézt na přiloženém paměťovém médiu.

[94] Rachmat, N. a Samsuryadi. Performance Analysis of 256-bit AES Encryption Algorithm on Android Smartphone. *Journal of Physics.* IOP Publishing. Březen 2019, sv. 1196, č. 1, s. 012049. Conference Series. DOI: 10.1088/1742-6596/1196/1/012049. Dostupné z: https://iopscience.iop.org/article/10.1088/1742-6596/1196/1/012049/pdf.

[95] Radhika Rani Chintala, S. V. Design and implementation of energy efficient lightweight encryption (EELWE) algorithm for medical applications. *Information technology in industry.* Auricle Technologies, Pvt., Ltd. Březen 2021, sv. 9, č. 1, s. 461–471. DOI: 10.17762/itii.v9i1.152. Dostupné z: http://it-in-industry.org/index.php/itii/article/view/152/136.

[96] Ray Beaulieum, J. S. *Simon and Speck: Block Ciphers for the Internet of Things.* NIST Interagency/Internal Report (NISTIR), National Institute of Standards and Technology, Gaithersburg, MD, 09. července 2015. Dostupné z: https://csrc.nist.gov/csrc/media/events/lightweight-cryptography-workshop-2015/documents/papers/session1-shors-paper.pdf.

[97] Regev, O. On Lattices, Learning with Errors, Random Linear Codes, and Cryptography. In: *Proceedings of the Thirty-Seventh Annual ACM Symposium on Theory of Computing.* New York, USA: Association for Computing Machinery, 2005, s. 84–93. STOC '05. DOI: 10.1145/1060590.1060603. ISBN 1581139608. Dostupné z: https://doi.org/10.1145/1060590.1060603.

[98] Relyea, R. *Post-quantum cryptography: Hash-based signatures* [online]. USA: Red Hat, 27. října 2022 [cit. 2023-03-01]. Dostupné z: https://www.redhat.com/en/blog/post-quantum-cryptography-hash-based-signatures.

[99] Rinn, E. *IDQ QKD Cerberis^3, Clavis^3 & Cerberis XG/XGR QNET User Guide.* 1.7. Ženeva, Švýcarsko: ID Quantique SA, únor 2022 [cit. 2023-02-15]. Soubor je možné nalézt na přiloženém paměťovém médiu.

[100] Rizvi, S., Hussain, S. Z. a Wadhwa, N. Performance Analysis of AES and TwoFish Encryption Schemes. In: *2011 International Conference on Communication Systems and Network Technologies.* Katra, Indie: [b.n.], 2011, s. 76–79. DOI: 10.1109/CSNT.2011.160. Dostupné z: https://ieeexplore.ieee.org/document/5966408.

[101] Robinson, B. S., Boroson, D. M., Schieler, C. M., Khatri, F. I., Guldner, O. et al. TeraByte InfraRed Delivery (TBIRD): a demonstration of large-volume direct-to-Earth data transfer from low-Earth orbit. In: Hemmati, H. a Boroson, D. M., ed. *Free-Space Laser Communication and Atmospheric Propagation XXX.* San Francisco, Kalifornie, USA: SPIE, 2018, sv. 10524, s. 105240V. DOI: 10.1117/12.2295023. Dostupné z: https://doi.org/10.1117/12.2295023.

[102] Saraiva, D., Leithardt, V. R. Q., Paula, D. de, Sales, A. M., González, G. V. et al. PRISEC: Comparison of Symmetric Key Algorithms for IoT Devices. *Sensors*. Basilej, Švýcarsko: [b.n.]. 2019, sv. 19, č. 19. DOI: 10.3390/s19194312. ISSN 1424-8220. Dostupné z: https://www.mdpi.com/1424-8220/19/19/4312.

[103] Schimmel, G., Produit, T., Mongin, D., Kasparian, J. a Wolf, J.-P. Free space laser telecommunication through fog. *Optica*. Optica Publishing Group. Říjen 2018, sv. 5, č. 10, s. 1338–1341. DOI: 10.1364/OPTICA.5.001338. Dostupné z: https://opg.optica.org/optica/abstract.cfm?URI=optica-5-10-1338.

[104] Schneier, B. *Description of a New Variable-Length Key, 64-Bit Block Cipher (Blowfish)* [online]. Prosinec 1993 [cit. 2023-03-10]. Dostupné z: https://www.schneier.com/academic/archives/1994/09/description_of_a_new.html.

[105] Schneier, B. *The Twofish Encryption Algorithm* [online]. Dr. Dobb's Journal, prosinec 1998 [cit. 2023-03-10]. Dostupné z: https://www.schneier.com/academic/archives/1998/12/the_twofish_encrypti.html.

[106] Security Analysis of ChaCha20-Poly1305 AEAD. In: KDDI Research, Inc. *CRYPTREC-EX-2601-2016*. únor 2017. Dostupné z: https://www.cryptrec.go.jp/exreport/cryptrec-ex-2601-2016.pdf.

[107] Seo, H., Liu, Z., Choi, J., Park, T. a Kim, H. Compact Implementations of LEA Block Cipher for Low-End Microprocessors. In: *Information Security Applications*. 1. vyd. Springer Cham, Leden 2016, sv. 9503, s. 28–40. DOI: 10.1007/978-3-319-31875-2_3. ISBN 978-3-319-31874-5. Dostupné z: https://eprint.iacr.org/2015/732.pdf.

[108] Shannon, C. E. Communication Theory of Secrecy Systems*. *Bell System Technical Journal*. 1949, sv. 28, č. 4, s. 656–715. DOI: https://doi.org/10.1002/j.1538-7305.1949.tb00928.x. Dostupné z: https://onlinelibrary.wiley.com/doi/pdf/10.1002/j.1538-7305.1949.tb00928.x.

[109] Shor, P. W. a Preskill, J. Simple Proof of Security of the BB84 Quantum Key Distribution Protocol. *Physical Review Letters*. American Physical Society (APS). Červenec 2000, sv. 85, č. 2, s. 441–444. DOI: 10.1103/physrevlett.85.441. Dostupné z: https://journals.aps.org/prl/pdf/10.1103/PhysRevLett.85.441.

[110] Shor, P. Algorithms for quantum computation: discrete logarithms and factoring. In: *Proceedings 35th Annual Symposium on Foundations of Computer Science*. Santa Fe, USA: [b.n.], 1994, s. 124–134. DOI: 10.1109/SFCS.1994.365700. Dostupné z: https://ieeexplore.ieee.org/document/365700.

[111] Sibleyras, F. *Security of Modes of Operation and other provably secure cryptographic schemes*. 2020. Disertační práce. Sorbonne Université. Dostupné z: https://hal.science/tel-03058306.

[112] Singh, H., Gupta, D. a Singh, A. Quantum Key Distribution Protocols: A Review. *IOSR Journal of Computer Engineering*. Leden 2014, sv. 16, s. 01–09. DOI: 10.9790/0661-162110109. Dostupné z: https://www.iosrjournals.org/iosr-jce/papers/Vol16-issue2/Version-11/A0162110109.pdf.

[113] *Six-State Protocol Offers Advantages for Quantum Cryptography* [online]. University of Illinois Urbana-Champaign, USA: News wise, 25. července 2002. Dostupné z: https://www.newswise.com/articles/six-state-protocol-offers-advantages-for-quantum-cryptography.

[114] Sleem, L. a Couturier, R. Speck-R: An ultra light-weight cryptographic scheme for Internet of Things. *Multimedia Tools and Applications*. v1. Springer Verlag. 2021, sv. 80, č. 11, s. 17067 – 17102. Dostupné z: https://hal.science/hal-03359990v1/document.

[115] Stoilov, M. *A classical attack on the coherent one way protocol for quantum key distribution*. Sofia, Bulharsko: arXiv, 2020. DOI: 10.48550/ARXIV.2003.07198. Dostupné z: https://arxiv.org/pdf/2003.07198.pdf.

[116] Stucki, D., Barreiro, C., Fasel, S., Gautier, J.-D., Gay, O. et al. Continuous high speed coherent one-way quantum key distribution. *Optics Express*. The Optical Society. Červenec 2009, sv. 17, č. 16, s. 13326. DOI: 10.1364/oe.17.013326. Dostupné z: https://doi.org/10.1364%2Foe.17.013326.

[117] Stucki, D., Brunner, N., Gisin, N., Scarani, V. a Zbinden, H. Fast and simple one-way Quantum Key Distribution. *Applied Physics Letters*. Ženeva, Švýcarsko: AIP Publishing. Prosinec 2005, sv. 87, č. 19, s. 194108 – 194108. DOI: 10.1063/1.2126792. Dostupné z: https://arxiv.org/pdf/quant-ph/0506097.pdf.

[118] Subandi, A., Lydia, M. S. a Sembiring, R. W. Analysis of RC6-Lite Implementation for Data Encryption. In: INSTICC. *Proceedings of the 3rd International Conference of Computer, Environment, Agriculture, Social Science, Health Science, Engineering and Technology - Volume 1: ICEST,*. SciTePress, 2018, sv. 1, s. 42–47. DOI: 10.5220/0010037500420047. ISBN 978-989-758-496-1.

[119] Sudip Sengupta. *Block Cipher vs. Stream Cipher* [online]. Crashtest Security, 3. února 2022 [cit. 2023-03-05]. Dostupné z: https://crashtest-security.com/block-cipher-vs-stream-cipher/.

[120] Trényi, R. a Curty, M. Zero-error attack against coherent-one-way quantum key distribution. *New Journal of Physics*. IOP Publishing. Září 2021, sv. 23, č. 9, s. 093005. DOI: 10.1088/1367-2630/ac1e41. Dostupné z: https://iopscience.iop.org/article/10.1088/1367-2630/ac1e41/pdf.

[121] Tsai, C.-W., Yang, C.-W., Lin, J., Chang, Y.-C. a Chang, R.-S. Quantum Key Distribution Networks: Challenges and Future Research Issues in Security. *Applied Sciences*. 2021, sv. 11, č. 9. ISSN 2076-3417. Dostupné z: https://www.mdpi.com/2076-3417/11/9/3767.

[122] Tsonev, D., Videv, S. a Haas, H. Light fidelity (Li-Fi): towards all-optical networking. In: Dingel, B. B. a Tsukamoto, K., ed. *Broadband Access Communication Technologies VIII*. San Francisco, Kalifornie, USA: SPIE, 2014, sv. 9007, s. 900702. DOI: 10.1117/12.2044649. Dostupné z: https://doi.org/10.1117/12.2044649.

[123] Vlastimil Klíma. *Základy moderní kryptologie – Symetrická kryptografie I.* [online]. 1.3. 2005 [cit. 2023-03-04]. Dostupné z: http://crypto-world.info/klima/mffuk/Symetricka_kryptografie_I_2005.pdf.

[124] Wang, J. a Huberman, B. *A Guide to Global Quantum Key Distribution Networks*. arXiv, 2020. DOI: 10.48550/ARXIV.2012.14396. Dostupné z: https://arxiv.org/pdf/2012.14396.pdf.

[125] *What Is Entanglement and Why Is It Important?* [online]. Pasadena, Kalifornie, USA: Science Explained, California Institute of Technology (Caltech) [cit. 2023-05-05]. Dostupné z: https://scienceexchange.caltech.edu/topics/quantum-science-explained/entanglement.

[126] Whiting, D. a Schneier, B. *Improved Twofish Implementations* [online]. Schneier, 02. prosince 1998 [cit. 2023-03-24]. Dostupné z: https://www.schneier.com/wp-content/uploads/2016/02/paper-twofish-speed.pdf.

[127] Wolf, E. *Introduction to the theory of coherence and polarization of light*. Cambridge, Anglie: Cambridge University Press, 2007. ISBN 9780521822114. Dostupné z: https://www.worldcat.org/title/149011826.

[128] Wolf, R. Eavesdropping Strategies. In: *Quantum Key Distribution*. 1. vyd. Srpen 2021. Lecture Notes in Physics. ISBN 978-3030739904. Dostupné z: https://link.springer.com/book/10.1007/978-3-030-73991-1.

[129] Woods, S. a Baumgartner, K. The Heisenberg Uncertainty Principle. In: *Quantum Chemistry* [online]. LibreText, Březen 2020, kap. 1.9 [cit. 2023-05-02]. Dostupné z: https://batch.libretexts.org/print/url=https://chem.libretexts.org/Courses/Pacific_Union_College/Quantum_Chemistry/01%3A_The_Dawn_of_the_Quantum_Theory/1.09%3A_The_Heisenberg_Uncertainty_Principle.pdf.

[130] Wootters, W. K. a Zurek, W. H. A single quantum cannot be cloned. *Nature*. Říjen 1982, sv. 299, s. 802–803. Dostupné z: https://www.nature.com/articles/299802a0.

[131] Zahorski, A. *Everything You Need to Know About the Twofish Encryption Algorithm* [online]. MakeUseOf, 06. července 2022 [cit. 2023-03-10]. Dostupné z: https://www.makeuseof.com/twofish-encryption-algorithm-explained/.

[132] Zetie, K., Adams, S. F. a Tocknell, R. M. *How does a Mach–Zehnder interferometer work?* [online]. Westminster School, Londýn, Anglie: Westminster Schoo, Physics Department, červenec 1999 [cit. 2022-12-28]. Dostupné z: https://www.cs.princeton.edu/courses/archive/fall06/cos576/papers/zetie_et_al_mach_zehnder00.pdf.

[133] Zhang, X., Heys, H. a Li, C. Energy efficiency of symmetric key cryptographic algorithms in wireless sensor networks. In: *2010 25th Biennial Symposium on Communications*. Kingston, Kanada: [b.n.], 2010, s. 168–172. DOI: 10.1109/BSC.2010.5472979. Dostupné z: https://ieeexplore.ieee.org/document/5472979.

Příloha A

Formát CSV souborů

V této příloze je popsán formát vstupních a výstupních CSV souborů, které jsou použity pro běh simulačního nástroje. Formát vstupního souboru musí být striktně dodržen.

Vstupní CSV soubor

Soubor obsahuje postupně tyto sloupce:

- `time` – čas, slouží pouze pro informaci uživatele. S touto hodnotou se nikterak nepracuje. Simulace probíhá řádek po řádku
- `total-cloud-cover` – celkové pokrytí oblohy oblačností. Hodnota je v procentech (znak procenta – % se neuvádí)
- `low-clouds` – celkové pokrytí oblohy nízkou oblačností. Hodnota je v procentech (znak procenta – % se neuvádí)
- `middle-clouds` – celkové pokrytí oblohy střední oblačností. Hodnota je v procentech (znak procenta – % se neuvádí)
- `high-clouds` – celkové pokrytí oblohy vysokou oblačností. Hodnota je v procentech (znak procenta – % se neuvádí)

Výstupní CSV soubor

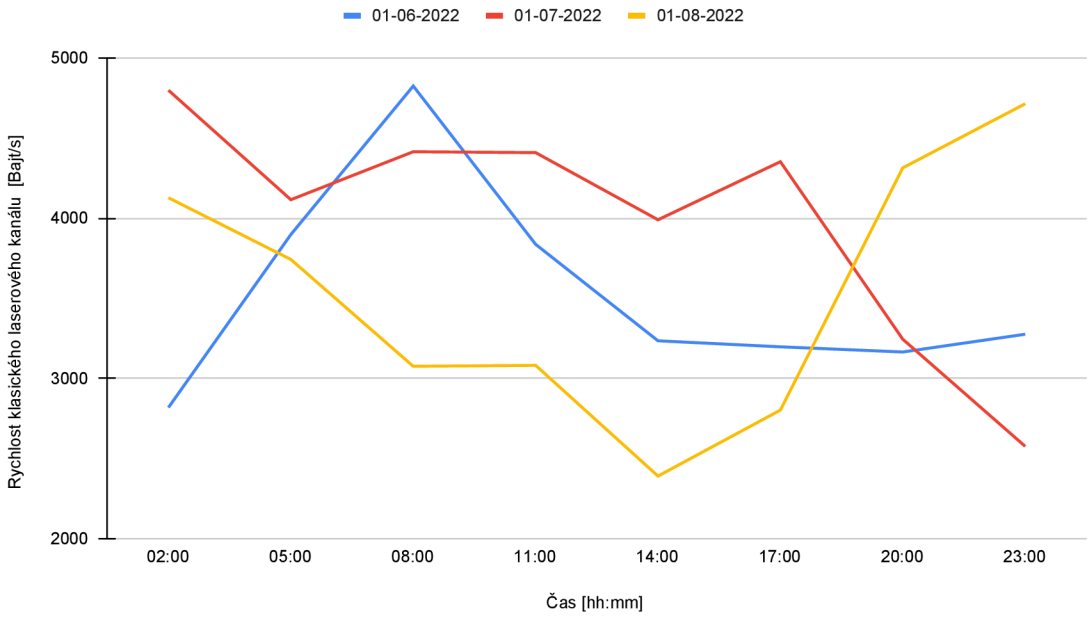
Soubor obsahuje postupně tyto sloupce:

- `time` – jedná se o počet odsimulovaných kroků od začátku simulace. Ve výchozím nastavení se simulační data zaznamenávají po 10 krocích.
- `regular-traffic-delays` – zpoždění paketů klasického spoje. Hodnota se počítá od doby vzniku po příchod paketů do *shromaždiště paketů*. Je ovlivněna zpožděním kanálu (tedy dobou přenosu) a rychlostí šifrování. Jedná se o simulační čas.
- `regular-traffic-throughput` – propustnost kanálu, který přenáší klasická data. Je vypočítán jako celkový počet přenesených bajtů děleno 10 simulačními kroky. Hodnota tedy nemusí nutně znamenat maximální hodnotu, kterou je schopen kanál přenášet data. Pokud bylo generováno malé množství dat, bude propustnost menší.
- `keys-delays` – zpoždění klíčů kvantového spoje. Tedy kolik jednotek simulačního času proběhlo od jeho vygenerování až po jeho příchod do *shromaždiště paketů*.
- `key-throughput` – propustnost kvantového kanálu. Udává tedy rychlost, s jakou bylo možné generovat klíče. Je vypočítán jako celkový počet přenesených bitů během 10 simulačních kroků.
- `total-encryption-delay` – celkové zpoždění paketů klasické komunikace, které bylo zapříčiněno šifrovacím algoritmem pro daný simulační blok (po 10 jednotkách simulačního času). Doba je v jednotkách simulačního času.
- `total-encryption-battery-drain` – celková spotřeba energie vynaložena na zašifrování dat. Jedná se o hodnotu pro daný simulační blok (po 10 jednotkách simulačního času). Hodnota je v μAh.

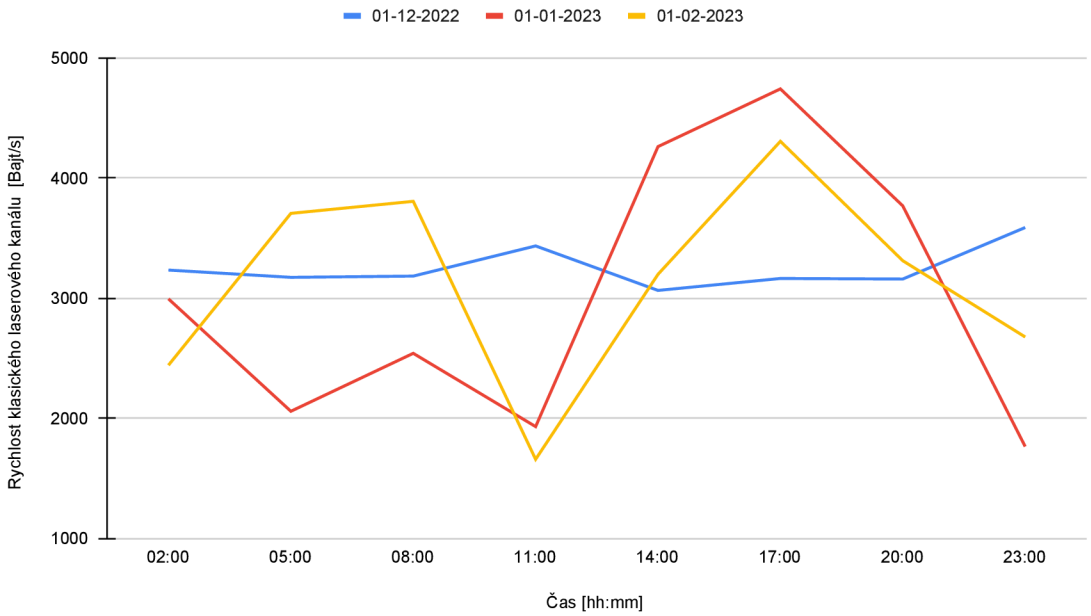
Příloha B

Grafy simulace

Výsledné grafy simulace pro klasické laserové kanály během letních a zimních měsíců.



Obrázek B.1: Rychlost klasického laserového kanálu v letních měsících



Obrázek B.2: Rychlost klasického laserového kanálu v zimních měsících

Příloha C

Simulační nástroj

Použití hlavního nástroje `sim_day_weather.py`:

```
usage: sim_day_weather.py [-h] [-o OUTPUT] [-i INPUT] [-a]

optional arguments:
-h, --help            show this help message and exit
-o OUTPUT, --output OUTPUT
                      Name of the output CSV file
-i INPUT, --input INPUT
                      Path to the input CSV file
-a, --all-ciphers     Use all ciphers in sequence and save
                      the data output to all.csv
-d, --debug           Enable debug mode
```

Potřeba nainstalovat Python knihovny `SimPy` a `ns.py`[1].

[1] Dostupné zde: https://github.com/TL-System/ns.py

Příloha D

Struktura adresáře

Níže je struktura adresáře na odevzdaném médiu:

```
/
├── ns.py/
├── qkd-documents/
└── sim/
    ├── cipher.py
    ├── data/
    │   ├── data-01-01-2023.csv
    │   ├── data-01-02-2023.csv
    │   ├── data-01-06-2022.csv
    │   ├── data-01-07-2022.csv
    │   ├── data-01-08-2022.csv
    │   ├── data-01-12-2022.csv
    │   ├── data-21-04-2023.csv
    │   ├── data-25-04-2023.csv
    │   ├── data-26-04-2023.csv
    │   └── simulation-good-weather-one-channel.csv
    ├── output/
    │   ├── all-ciphers.csv
    │   ├── simulation-day-weather-01-01-2023.csv
    │   ├── simulation-day-weather-01-02-2023.csv
    │   ├── simulation-day-weather-01-06-2022.csv
    │   ├── simulation-day-weather-01-07-2022.csv
    │   ├── simulation-day-weather-01-08-2022.csv
    │   ├── simulation-day-weather-01-12-2022.csv
    │   ├── simulation-day-weather-21-04-2023.csv
    │   ├── simulation-day-weather-25-04-2023.csv
    │   └── simulation-day-weather-26-04-2023.csv
    ├── sim_day_weather.py
    ├── sim_good_weather_one_channel.py
    └── utils.py
```

Stručný popis jednotlivých souborů:

- Složka `ns.py` obsahuje knihovní funkce nutné pro běh simulace[1].
- Složka `qkd-documents` obsahuje podpůrné prezentace firmy IDQ ohledně fungování QKD Clavis[3].
- Složka `data` obsahuje data o oblačnosti pro jednotlivé dny, která byla použita pro simulaci.
- Složka `output` obsahuje výsledky simulace k daným dnům. Tyto hodnoty byly použity v grafech při vyhodnocení.
- Soubor `sim_day_wather.py` simulační nástroj
- Soubor `utils.py` obsahuje pomocné funkce a specifikace kvantových kanálů. Pokud by někdo chtěl upravit hodnoty přenosů pro kvantové a laserové kanály, lze to upravit zde.
- Soubor `cipher.py` obsahuje třídy simulující jednotlivé kryptografické algoritmy.
- Soubor `sim_good_weather_one_channel.py` slouží jako příklad možného spojení klasického a kvantového kanálu do jednoho společného kanálu. V práci toto nebylo nikterak využito nebo vyhodnoceno.

[1] Lze stáhnout i z repozitáře projektu https://github.com/TL-System/ns.py