Kvantová komunikace

Quantum – based Communications

Kateřina Šedivá

Bakalářská práce
2018

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2017/2018

ZADÁNÍ BAKALÁŘSKÉ PRÁCE
(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Kateřina Šedivá**
Osobní číslo:	**A15763**
Studijní program:	**B3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Forma studia:	**kombinovaná**
Téma práce:	**Kvantová komunikace**
Téma anglicky:	**Quantum-based Communications**

Zásady pro vypracování:

1. Vypracujte literární rešerši na dané téma.
2. Popište základní principy kvantových jevů využívaných v kryptografických komunikačních protokolech.
3. Uveďte příklady a principy jednotlivých dostupných protokolů.
4. Analyzujte dosavadní pokroky v oblasti kvantové kryptografie.
5. Popište možnosti dalšího budoucího rozvoje.

Rozsah bakalářské práce:

Rozsah příloh:

Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam odborné literatury:

1. KATZ, Jonathan a Yehuda LINDELL. Introduction to modern cryptography. Second edition. Boca Raton: CRC Press/Taylor & Francis Group, 2015, xx, 583. Chapman & Hall/CRC cryptography and network security. ISBN 978-1-4665-7026-9.
2. BURDA, Karel. Úvod do kryptografie. Brno: Akademické nakladatelství CERM, 2015, 108 s. ISBN 978-80-7204-925-7.
3. CAO, Zhenfu. New directions of modern cryptography. Boca Raton: CRC Press, c2013, xvii, 384 s. ISBN 978-1-4665-0138-6.
4. LEK, Kamol a Naruemol RAJAPAKSE. Cryptogaphy: protocols, desing, and applications. New York: Nova Science Publishers, c2012, ix, 242 s. Cryptography, steganography and data security. ISBN 978-1-62100-779-1.
5. BURDA, Karel. Aplikovaná kryptografie. Brno: Vutium, 2013, 255 s. ISBN 978-80-214-4612-0.
6. SKÁLA, Lubomír. Úvod do kvantové mechaniky. Praha: Karolinum, 2011, 297 s. ISBN 978-80-246-2022-0.
7. KULHÁNEK, Petr. Vybrané kapitoly z teoretické fyziky. Praha: AGA, 2016, 409 s. ISBN 978-80-904582-8-4.

Vedoucí bakalářské práce: **doc. Ing. Roman Šenkeřík, Ph.D.**
Ústav informatiky a umělé inteligence

Datum zadání bakalářské práce: **8. prosince 2017**

Termín odevzdání bakalářské práce: **24. května 2018**

Ve Zlíně dne 12. prosince 2017

doc. Mgr. Milan Adámek, Ph.D.
děkan

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky
L.S.

Ing. Jan Valouch, Ph.D.
ředitel ústavu

Jméno, příjmení:

Název bakalářské/diplomové práce:

Prohlašuji, že

- beru na vědomí, že odevzdáním diplomové/bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že diplomová/bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk diplomové/bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl/a jsem seznámen/a s tím, že na moji diplomovou/bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – diplomovou/bakalářskou práci nebo poskytnout licenci k jejímu využití jen připouští-li tak licenční smlouva uzavřená mezi mnou a Univerzitou Tomáše Bati ve Zlíně s tím, že vyrovnání případného přiměřeného příspěvku na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše) bude rovněž předmětem této licenční smlouvy;
- beru na vědomí, že pokud bylo k vypracování diplomové/bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky diplomové/bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem diplomové/bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na diplomové/bakalářské práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně, dne 23. 5. 2018

.....
podpis diplomanta

ABSTRAKT

Tato bakalářská práce se zabývá přenosem informace s využitím přírodních jevů, jako je kvantová mechanika.

V teoretické části je popsán úvod do kryptologie a dále jsou zde popsány základní principy kvantové mechaniky, jako je superpozice, spin, kvantová korelace. Dále je zde uvedený popis přenosu informace pomocí kvantových protokolů.

V praktické části jsou uvedené dostupné produkty, které využívají principy kvantové fyziky. Je zde uvedena analýza trhu pro firmy a státní instituce. Náhled na pokroky kvantových technologií ve světě a jejich výhled do možného budoucího rozvoje.

Klíčová slova: kvantová mechanika, kvantová kryptografie, kvantová korelace, polarizace fotonů

ABSTRACT

This bachelor thesis deals with the transmission of information using natural phenomena such as quantum mechanics.

The theoretical part describes basic principles of quantum mechanics such as superposition, spin, quantum correlation. Then there is the description of information transmission using quantum protocols and cryptography history.

In the practical part is lists of available products that use the principles of quantum physics. Also is here a market analysis for companies and state institutions. Description of progress in quantum technology in the world and their potential for future development.

Keywords: quantum mechanics, quantum cryptography, quantum correlation, polarization photons

Chtěla bych poděkovat svému vedoucímu práce doc. Ing. Romanovi Šenkeříkovi, Ph.D. za odborné vedení, trpělivost a ochotu, kterou mi v průběhu zpracování mé bakalářské práce věnoval.

Dále bych chtěla poděkovat svojí rodině a nejbližším za podporu, pomoc nejen při tvorbě bakalářské práce, ale také během celého studia.

Prohlašuji, že odevzdaná verze bakalářské/diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

OBSAH

ÚVOD

V dnešní době se technologie neustále vyvíjejí dopředu. Už nějaký čas se mluví o rozvíjení kvantových počítačů. Přičemž jejich vývoj se neustále zlepšuje a zdokonaluje. Dalším aspektem je kvantová kryptografie. Která v případě zhotovení kvantového počítače a jeho rozšíření, bude nedílnou součástí pro bezpečnost. Momentálně používané symetrické a asymetrické šifry budou proti kvantovým počítačům ohroženy. Například pro symetrickou šifru je potřeba dvakrát delší symetrický klíč pro poloviční ochranu před kvantovým počítačem. Vývoj kvantových systémů spočívá na přírodních jevech, jako je kvantová mechanika.

Kvantová mechanika je část fyziky, která se řídí jinými zákony, než na které jsme zvyklí z běžného makroskopického života. Neboť u makroskopických těles víme, jak se jejich chování bude vyvíjet v určité dané situaci, například pokud vyhodíme míček do vzduchu, víme, že po určitém časovém intervalu opět spadne na zem. V kvantové fyzice to ovšem takto nefunguje, neboť se řídí jinými fascinujícími zákony. Díky těmto zákonům nám jejich objasnění a následné využití v praxi dává nové využití a vývoj dosavadních technologií. Využití kvantové mechaniky je skvělé například při komunikaci v utajení. Neboť díky fyzikálním pravidlům kvantové mechaniky je zcela nehacknutelné.

Tato práce se zabývá především kvantovou komunikací. Protokoly, kterými kvantová komunikace probíhá a úvodem do samotné kvantové fyziky jako takové.

Teoretická část se zabývá úvodem do historie kryptologie a jejími principy. Dále pak kvantovou mechanikou a funkcí kvantové komunikace.

V praktické části se seznámíme s dostupnými produkty pro kvantovou komunikaci, které se zaměřují na využití kvantových fyzikálních zákonů s uvedením do praxe. Je zde i uvedená analýza pro možnosti firem a státních institucí tuto technologii využívat. Dále pak se budeme zabývat pokroky a nadhledem do možného budoucího rozvoje kvantových technologií.

I. TEORETICKÁ ČÁST

1 ZÁKLADNÍ POJMY

Kryptografie (šifrování) – Slovo pocházející z řečtiny kde, kryptós znamená skrytý a gráphein znamená psát. Zabývá se metodami utajování zpráv, které jsou převedeny do podoby, která je čitelná jen se speciální znalostí.

Transpoziční šifra – Je šifra, u které se využívá principů přeskládání symbolů zprávy jiným způsobem. Vstupem přeskládání musí být vždy blok o dané délce, přičemž dlouhé zprávy musejí být rozděleny na bloky dané délky. Následně se pak šifruje každý blok zvlášť.

Substituční šifra – Je šifra, u které se symboly zprávy zamění za jiné symboly. Podle konkrétní šifry to pak mohou být buď písmena, nebo jiné zástupné symboly.

WEP – Zastaralé zabezpečení bezdrátových sítí, které bylo prolomeno v roce 2001.

WPA – Zabezpečení bezdrátových sítí, které nahradilo jeho předchůdce WEP.

Moorov zákon – Předpověď, kterou v roce 1965 publikoval Gordon E. Moore, spoluzakladatel firmy Intel. Tato předpověď předpovídá, že se počet tranzistorů v procesoru zdvojnásobí zhruba každé dva roky a to má platit, jak pro celé odvětví mikroelektroniky, tak i pro všechny počítače.

Mikroskopický svět – Zcela jiný svět, než který známe, nedá se popsat názornými modely makrosvěta. Skládá se například z molekul, atomů. Z krátkých časových intervalů v řádech milisekund. Ale také se zabývá rozměry galaxií, pohybem objektů, které se pohybují rychlostí o velikosti blížící se rychlosti světla atd.

Makroskopický svět – Svět, který vnímáme svými smysly, dokážeme ho do jisté míry vysvětlit svým rozumem, má běžné rozměry, na které jsme zvyklý z každodenního života. Běžný časový interval, rychlost, energii, práci. Platí zde zákony klasické fyziky.

De Brogliova vlna - Je projevem vlnových vlastností pohybujících se částic. Udává že, krátké vlnové délky mají větší energii než delší vlnové délky.

Planckova konastanta - Konstanta úměrnosti kvanta záření, která je přímo úměrná jeho energii a nepřímo úměrná jeho frekvenci.

Relativistická hmotnost – Je taková hmotnost, která není stejná pro všechny pozorovatele, ale závisí na tom, jakou rychlostí se těleso pohybuje vůči pozorovateli.

Kvantová kryptografie – Obor kryptografie, který využívá poznatků kvantové mechaniky. Umožňuje spolehlivou detekci odposlechu. Zabývá se problémem bezpečné distribuce klíčů mezi odesílatelem a příjemcem**.**

Bellova nerovnost – Udává že, neslučitelnost kvantové mechaniky s lokálním realismem jde prokázat na dvojici kvantově provázaných částicích. Zaměřuje se na spin obou částic. Protože spin má vždy stejnou absolutní hodnotu a mění se jen jeho znaménko, musí se pro další vysvětlení principu předpokládat opakované měření více párů částic a statistické vyhodnocení výsledků. Jedná se tedy o takovou nerovnost, kterou splňují určité spinové korelace v lokálně realistických teoriích.

Sociální inženýrství - je způsob manipulace lidí za účelem provedení určité akce nebo získání určité informace.

Kvantová distribuce klíčů – Slouží pro výrobu a zároveň distribuci náhodného klíče přes kryptografický kanál.

Qubit – Neboli kvantový bit je jednotkou kvantové informace odvozené od klasického bitu. Nachází se v superpozici.

Kvantový počítač – Je mnohonásobně efektivnější než klasický počítač, neboť nese současně informace o všech možných hodnotách spinu a tím uskutečňuje paralelní výpočet všech možností, které mohou nastat.

2 HISTORIE KRYPTOLOGIE

Základní vlastností každého člověka je schopnost se dorozumívat. A díky tomu, že se lidé už spolu dorozumívají velmi dlouho, tak v některých případech bylo potřeba informaci, kterou si chtěli sdělit zabezpečit. Díky těmto snahám již vzniklo několik postupů, takzvaných algoritmů, které mají zapříčinit, aby informaci pochopil jen chtěný příjemce a nikoliv třetí strana, která by ji mohla nějakým způsobem zneužít.

V následujících odstavcích je proveden úvod do pojmů souvisejících s kryptologií a náhled do historie, jak si naši předci snažili co nejlépe střežit své tajemství.

2.1 Počátky kryptologie

Počátky kryptologie jsou stejně staré jako první tajemství, které si chtěli dva lidé mezi sebou sdělit s co nejmenší možností toho, aby je někdo třetí mohl odposlechnout. Proto nelze s určitostí sdělit nějaký aspoň přibližný letopočet.

Nicméně bylo objeveno, že již ve starém Egyptě byly některé texty psány atypickými hieroglyfy, kterým rozuměl jen člověk, který s nimi byl seznámen a tak tímto způsobem bylo zajištěno šifrování tajné zprávy.

2.2 Rozvoj kryptologie

Za prokazatelný rozvoj v oblasti kryptologie stáli staří Řekové. Vojevůdce Aeneus Tacticus zavedl vojenskou zabezpečenou komunikaci na ochranu proti nepřátelům a jako první začal rozdělovat kryptografické metody na transpoziční a substituční. Ve starém Řecku také vznikla první rozšířená kryptografická metoda skytala a polypova šifrovací mřížka.

Další významná šifra z tohoto období vznikla na Apeninském poloostrově a stál za ní jeden z nevýznamnějších římských císařů sám Julius Ceasar. Po němž se tato šifra jmenuje Ceasarova. Tuto šifru používal pro vojenskou komunikaci a popsal ji v Zápiscích o válce galské.

2.2.1 Skytala

Skytala je dřevěná hůl o přesně daném průměru, na který se navine tenká kožená nebo pergamenová páska viz Obr. 1. Poté se na pásku napíše tajná zpráva a sundá se z hole. Pouze člověk, který vlastní hůl o průměru stejném jako hůl na které byla zpráva napsaná, ji může po navinutí znovu přečíst. Pro ostatní je to pouze hromada písmen. [1]

Obr. 1. Skytala. [2]

2.2.2 Polybiova šifrovací mřížka

Polybiova šifrovací mřížka je tvořena mřížkou která má očíslované řádky a sloupce. Do nich je vepsána abeceda případně i jiné znaky a každý znak či písmeno je reprezentováno dvojicí čísel, na jejichž průsečíku řádku a sloupce se nachází, viz Tab. 1.

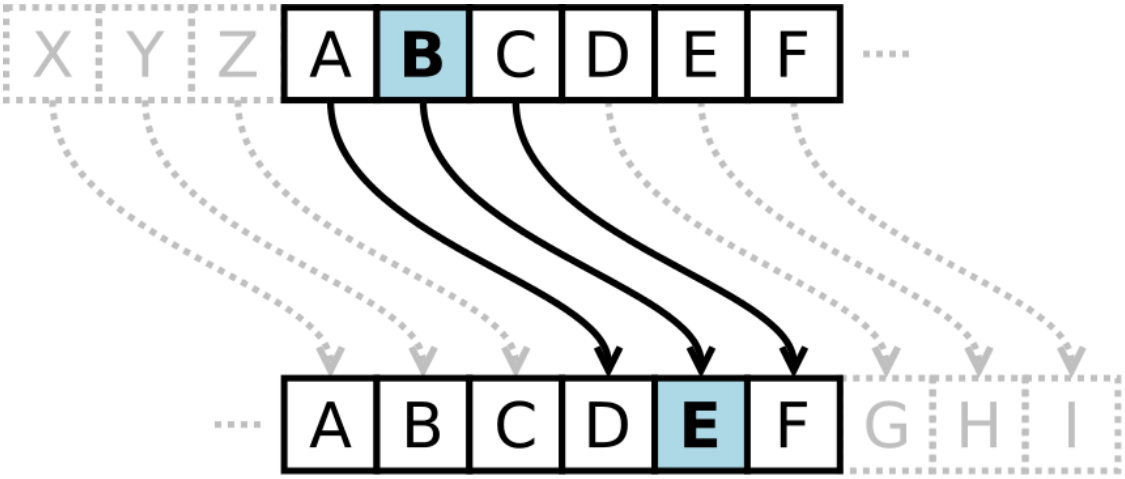
Tab. 1. Polybiova šifrovací mřížka.

	1	**2**	**3**	**4**
1	A	B	C	D
2	E	F	G	H
3	I	J	K	L
4	M	N	O	P
5	Q	R	S	T
6	U	V	W	X
7	Y	Z		

Při použití uvedené mřížky je slovo „SIFRA“ reprezentováno číselným řetězcem 5331225211.

2.2.3 Caesarova šifra

Princip Caesarovy šifry je velice jednoduchý. Všechna písmena jsou během šifrování zaměněna za písmeno, které se abecedně nachází o pevně určený počet míst, dále viz Obr. 2. Počet možných variant klíče této šifry je o jedna menší než počet písmen (znaků) v použité abecedě. [3]



Obr. 2. Princip Caesarovy šifry. [4]

2.3 Modernější kryptologie

Za průkopníka modernější kryptografie můžeme považovat Johannes Tritheim, což byl opat v klášteře v Sponheim. Ten napsal roku 1518 knihu Stenografie, ve které uvedl i princip stenografické šifry. Stenografická šifra využívá algoritmu, ve kterém je každé písmeno nahrazeno slovem v předem určené tabulce.

Významnou roli ve vývoji šifrovacích metod sehrála také Vignerova šifra, která používá 26 odlišných šifrových abeced. Z této šifry později vznikla Vernamova šifra, která se považuje za nerozluštitelnou. Podobnou váhu lze dát i šifrovacímu stroji, používanému za druhé světové války Německou armádou, který se nazýval Enigma.

2.3.1 Vernamova šifra

Vernamova šifra vznikla v roce 1917 a nechal jsi ji patentovat Gilbert Sandford Vernam. Funguje na principu posunu každého znaku zprávy o náhodně zvolený počet míst v abece-

dě. Z toho nám vyjde náhrada zcela náhodných písmen a díky tomuto faktu se stává šifra v principu zcela nerozluštitelná.

2.3.2 Enigma

Enigma je šifrovací stroj, který si nechal patentovat německý inženýr **Arthur Scherbius.** Je založen na kombinaci elektrického a mechanického systému. Mechanický systém je složen z klávesnice, sady rotujících disků (rotory), jež jsou řazeny za sebou na jedné ose a krokového mechanismu, který otáčí postupně jedním nebo několika rotory s každým stiskem klávesy viz Obr. 3. Tudíž, je při stisku stejné klávesy vícekrát stroj vždy jinak nastaven a výsledná šifra je tedy jiná.

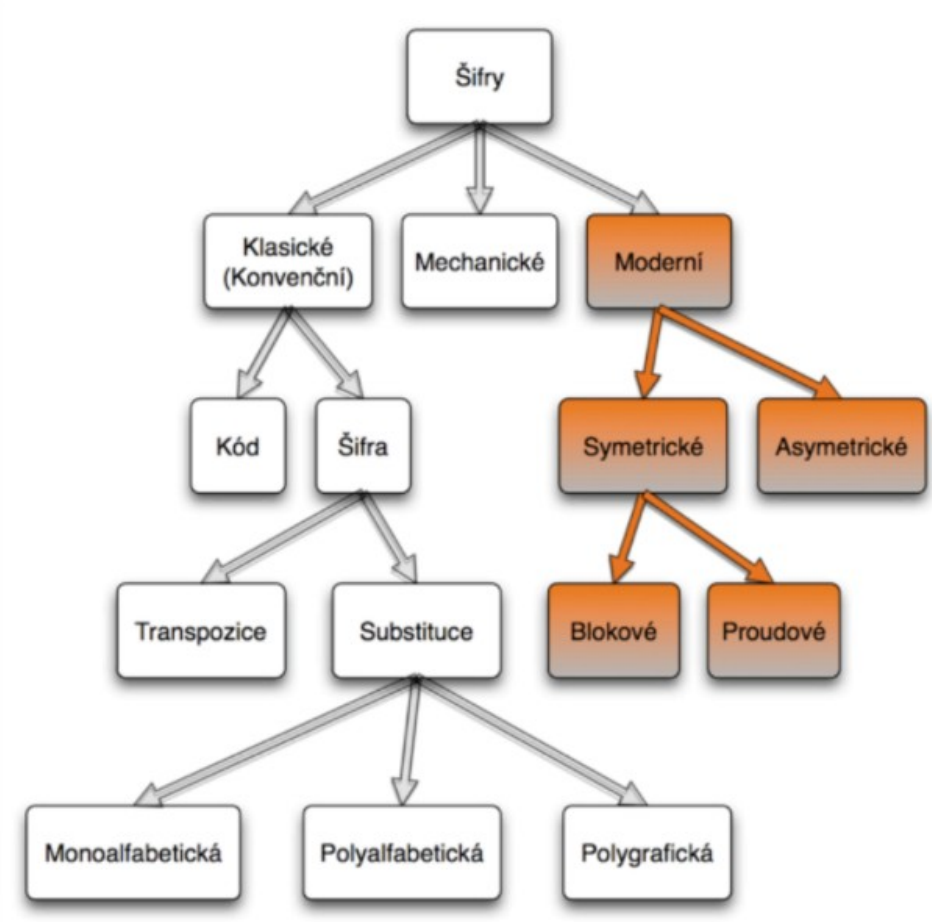
Šifrování probíhá takto: po stisku klávesy se uzavře elektrický obvod. Proud prochází různými komponenty, až se nakonec rozsvítí jedna z mnoha žárovek na panelu, čímž indikuje výsledné zašifrované písmeno. Tento šifrovací stroj byl nejvíce používán za druhé světové války. Nutnost o jeho prolomení nastartovalo éru počítačů, tak jak je známe v dnešním světě.

Obr. 3. Enigma. [5]

3 MODERNÍ KRYPTOLOGIE

V dnešním světě se s některým druhem šifrování setkáme každý den. Při používání naprosto běžných věcí jako chytrý telefon, platební karta, osobní počítač. Například při běžném používání chytrého telefonu je použito šifrování už od připojení na Wi-Fi až po načtení webové stránky a přihlášení se do e-mailové schránky. Tudíž se dá říct, že šifrování se stalo nedílnou součástí fungování dnešní společnosti.

Moderní kryptologie se rozděluje podle toho, jakým způsobem je prováděno šifrování a to buď pomocí symetrické či asymetrické šifry. Přičemž symetrická šifra se dále ještě dělí na blokovou a proudovou šifru viz Obr. 4. Kde bloková šifra pracuje s bloky o pevně dané délce, zatímco proudová šifra je tvořena zašifrovaným datovým tokem, který je tvořen kombinací vstupního datového toku a pseudonáhodným proudem bitů vytvořeným z šifrovacího klíče a šifrovacího algoritmu většinou pomocí funkce Exkluzivní disjunkce (XOR).

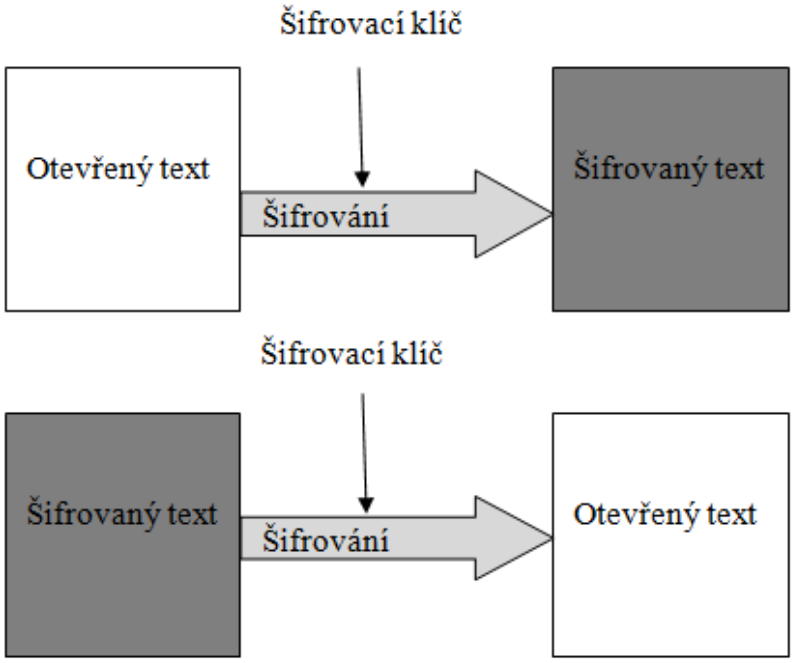


Obr. 4. Rozdělení moderních šifer. [6]

3.1 Symetrická kryptologie

Používá k šifrování i dešifrování stejný klíč. Výhodou těchto šifer je jejich nízká výpočetní náročnost. Nevýhodou je využití stejného klíče, což vede k tomu, že se odesílatel a příjemce musí předem domluvit na tajném klíči.

Symetrická šifra funguje tedy tak, že odesílatel zašifruje text předem domluveným tajným klíčem. Pošle jej příjemci a ten ho pomocí stejného klíče dešifruje, viz Obr. 5.



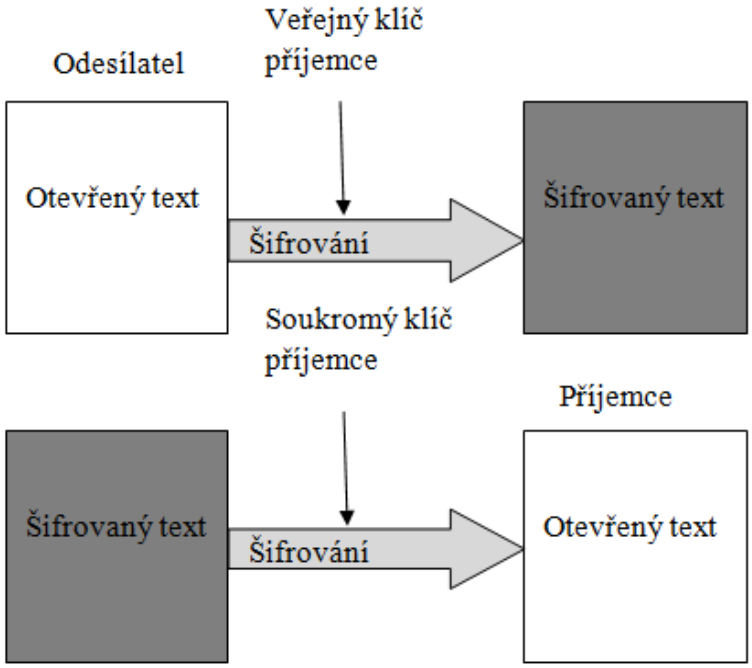
Obr. 5. Princip symetrického šifrování.

3.1.1 AES šifra

Je symetrická bloková šifra, která je rozdělena do bloků o pevně dané délce. Používá se například pro bezdrátové Wi-Fi sítě. Byla uznána Národní bezpečnostní agenturou k šifrování nejtajnějších dokumentů a je to šifra, která je volně dostupná široké veřejnosti. Šifra AES má tři velikosti klíče a to 128, 192 nebo 256 bitů a velikost bloku, která je pevně daná na 128 bitů.

3.2 Asymetrická kryptologie

Používá pro šifrování a dešifrování odlišné klíče. Používá se zde takzvaný soukromý a veřejný klíč, kde veřejný klíč majitel volně uveřejní a kdokoliv jím může šifrovat jemu určené zprávy. Poté je tu soukromý klíč, který je privátní a majitel ho drží v tajnosti, pomocí něj může zprávy dešifrovat, viz Obr. 6. Princip asymetrického šifrování.. Výhodou asymetrické šifry je, že ten kdo šifruje, nemusí s dešifrujícím příjemcem zprávy sdílet žádné tajemství, čímž se eliminuje potřeba výměny klíčů. Používá se například v RSA šifře.



Obr. 6. Princip asymetrického šifrování.

3.2.1 RSA šifra

Jedná se o šifru, která se používá pro šifrování dat a podepisování dokumentů. Patří do rodiny asymetrických šifer. Princip této šifry je postaven na tom, že rozložit velké číslo na součin prvočísel je časově náročný úkol. Podepisování dokumentů touto šifrou nám umožňuje ověřit, zda nebylo se zašifrovanou zprávou jakkoliv manipulováno a zda ji skutečně poslal odesílatel.

4 DALŠÍ VÝVOJ

Postupem času se díky narůstajícímu výpočetnímu výkonu počítačů musely šifrovací metody zdokonalovat, aby zvládaly odolávat pokusům o jejich rozluštění. S narůstající výpočetní silou se mohly zkoušet kombinace o jejich prolomení mnohokrát rychleji. Dnes se už díky tomu například šifrování pomoci WEP a WPA nepovažuje za bezpečné. Výkon počítačů však stále narůstá velmi rychle, podle donedávna platícího Moorova zákona, který říká, že počet tranzistorů v integrovaných obvodech se zdvojnásobí přibližně každé dva roky. Kryptologie na tento fakt reagovala vývojem moderních blokových a proudových šifer a následně se vývoj zaměřil k šifrování chaosem, fraktálním šifrováním, využití umělé inteligence a také kvantových jevů.

Následující kapitoly, budou zaměřeny na podrobnější popis využití kvantových jevů v kryptografii. Stručný popis principů kvantové mechaniky a dále pak její využití v kvantových protokolech.

5 KVANTOVÁ MECHANIKA

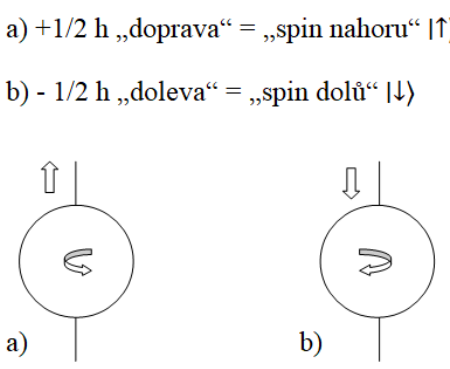
Zabývá se objasněním a popisem jevů v mikroskopickém světě, která fungují na jiném principu, než je fyzika makroskopických těles. Staví na nových poznatcích moderní fyziky a ukazuje nám rozmanitost přírody a jejích fascinujících jevů. Kvantová mechanika má takové fyzikální zákony, které jsou odlišné od normálních makroskopických zákonů. K jejím objasněním se nejčastěji používají matematické operátory. I když je kvantová mechanika zcela odlišná od té klasické, přesto se tu určitá spojitost mezi kvantovou a klasickou mechanikou nachází. Ta spočívá v tom že, pokud budeme přecházet od částic k makroskopickým tělesům, budou se vlnové délky de Broglieových vln a Planckova konstanta *h* jevit nekonečně malé a zákony kvantové fyziky by měly následně přecházet v zákony klasické mechaniky. [7]

5.1 Základní vlastnosti

Z běžného makroskopického světa, jsou již tedy známé fyzikální zákony, které lze logicky vysvětlit a jejichž principy se projevují v každodenním životě jako zcela běžné funkce v podobě například rychlosti jedoucího automobilu, dráhy po které se kutálí míč či času potřebnému k upečení dortu. Ve světě částic mikrosvěta tomu však takto není, tyto velmi malé částice se projevují jinými fyzikálními vlastnosti, než které jsou známé z běžného života a proto je důležité je zde zmínit.

5.1.1 Spin

Je jakási vlastní „točivost“, moment hybnosti částice, který se nedá zastavit. Má kvantové vlastnosti. Může nabývat dvou možných hodnot momentu hybnosti, které se značí (+1) pro $|\uparrow\rangle$ a (-1) pro $|\downarrow\rangle$. Například, elektron o hybnosti ½ má spin viz Obr. 7.



Obr. 7. Spin elektronu.

5.1.2 Princip superpozice

Princip superpozice spočívá v odlišnosti stavu měření, které dává s jistotou hodnotu (+1) pro $|\uparrow\rangle$ a (-1) pro $|\downarrow\rangle$. Potom se objekt může nacházet ve stavu,

$$|\Psi\rangle = \alpha_{\uparrow}|\uparrow\rangle + \alpha_{\downarrow}|\downarrow\rangle \qquad (1)$$

což nám značí lineární kombinaci = **superpozice,** přičemž platí že $\alpha_{\uparrow}, \alpha_{\downarrow} \in C$. Kde $\alpha_{\uparrow}, \alpha_{\downarrow}$ jsou libovolné komplexní koeficienty (v kvantové mechanice jsou fundamentálně za potřebí komplexní čísla). Měřením rozlišující oba stavy pak dává výsledek pro,

$$(+1)\ P_{\uparrow} = \frac{|\alpha_{\uparrow}|^2}{|\alpha_{\uparrow}|^2 + |\alpha_{\downarrow}|^2} \qquad (2)$$

$$(-1)\ P_{\downarrow} = \frac{|\alpha_{\downarrow}|^2}{|\alpha_{\uparrow}|^2 + |\alpha_{\downarrow}|^2} \qquad (3)$$

přičemž jiná hodnota než $P_{\uparrow}+P_{\downarrow}=1$ být naměřená nemůže. Po naměření se objekt ihned nachází v naměřeném stavu $|\uparrow\rangle$ nebo $|\downarrow\rangle$. Neboť pokud by, jsme se na daný objekt podívali, tak zkolabuje superpozice (vlnová funkce) a předmět se nachází pouze v jednom ze dvou stavů. Pravděpodobnost je pak určena kvadráty koeficientů $\alpha_{\uparrow}, \alpha_{\downarrow}$.

5.1.3 Kvantová korelace (provázanost)

Pokud budeme mít dvě částice se spinem například ½ (označené čísly 1 a 2) a budeme na nich provádět měření spinu. Přičemž při provedení měření, nám vyjde vždy buď kladná, nebo záporná vlastnost viz Tab. 2.

Dostaneme kombinace:

Tab. 2. Kombinace při měření spinu částic.

$(+)_1(+)_2$	$(+)_1(-)_2$
$(-)_1(+)_2$	$(-)_1(-)_2$

Kombinace pak odpovídají stavům v tabulce Tab. 3:

Tab. 3. Kombinace pro odpovídající stavy.

$\|\uparrow_1\uparrow_2\rangle$	$\|\uparrow_1\downarrow_2\rangle$
$\|\downarrow_1\uparrow_2\rangle$	$\|\downarrow_1\downarrow_2\rangle$

Všechny stavy následně můžeme dát do superpozice, čili můžeme vytvořit stav ze všech možných stavů. Celý systém může být tedy v libovolném stavu superpozice, kde,

$$|\Psi\rangle = \alpha_{\uparrow\uparrow}|\uparrow_1\uparrow_2\rangle + \alpha_{\uparrow\downarrow}|\uparrow_1\downarrow_2\rangle + \alpha_{\downarrow\uparrow}|\downarrow_1\uparrow_2\rangle + \alpha_{\downarrow\downarrow}|\downarrow_1\downarrow_2\rangle \quad (4)$$

přičemž předpokládáme, že součet kvadrátu je roven jedné,

$$|\alpha_{\uparrow\uparrow}|^2 + |\alpha_{\uparrow\downarrow}|^2 + |\alpha_{\downarrow\uparrow}|^2 + |\alpha_{\downarrow\downarrow}|^2 = 1 \quad (5)$$

kvadráty koeficientů pak udávají pravděpodobnosti přímo toho, že spiny jsou v těchto stavech.

Pokud si na jedné straně naměříme spin nahoru, na druhé musíme naměřit spin dolů, z toho následně můžeme sestavit tabulku s pravděpodobnostmi výsledků, viz Tab. 4:

Tab. 4. Pravděpodobnosti výsledků.

	↑ #1 ↓	
↑ #2 ↓	$\|\alpha_{\uparrow\uparrow}\|^2$	$\|\alpha_{\uparrow\downarrow}\|^2$
	$\|\alpha_{\downarrow\uparrow}\|^2$	$\|\alpha_{\downarrow\downarrow}\|^2$

U konkrétního příkladu to může například vypadat takto, kde budeme uvažovat dva spiny označené čísly 1 a 2 a vezmeme například takovouto superpozici

$$|\Psi\rangle = \frac{1}{\sqrt{2}}|\uparrow_1\downarrow_2\rangle - \frac{1}{\sqrt{2}}|\downarrow_1\uparrow_2\rangle \quad (6)$$

kde,

$$|\Psi\rangle = 0\ |\uparrow_1\uparrow_2\rangle + \left(\frac{1}{\sqrt{2}}\right)|\uparrow_1\downarrow_2\rangle + \left(-\frac{1}{\sqrt{2}}\right)|\downarrow_1\uparrow_2\rangle + 0\ |\downarrow_1\downarrow_2\rangle \tag{7}$$

potom pravděpodobnosti výsledků jsou na tabulce Tab. 5:

Tab. 5. Konkrétní pravděpodobnosti výsledků.

	↑ #1 ↓	
↑ #2 ↓	0	1/2
	1/2	0

Částice jsou tedy v provázaném stavu, kdy žádná nemá svoji vlnovou funkci, což je podstata provázanosti. Jakmile se provede měření jedné částice, následně jsou částice separované (oddělené) a každá je ve svém stavu, pak už to provázaný stav není.

5.2 Foton

Foton je stabilní elementární částice, popisována kvantem elektromagnetické energie. Může se chovat jako částice a zároveň i jako vlna. Tomuto jevu se říká korpuskulárně – vlnový dualismu. Mezi veličiny, které ho popisují, patří, frekvence *f*, vlnová délka λ, hybnost *p* a energie *E*. Má nekonečný poločas rozpadu, z tohoto aspektu je jeho životnost zcela nekonečná. Má nulový elektrický náboj a jeho spin je roven 1, jedná se tedy o boson.

5.2.1 Energie fotonu

Jeho energie *E* je podle speciální teorie relativity pro energii pohybující se částice zapsána vztahem.

$$E = c\sqrt{(m_0^2c^2 + p^2)} \tag{8}$$

Přičemž, *p* je hybnost fotonu, *c* je rychlost světla ve vakuu a m_0 je klidová hmotnost fotonu, která je nulová, platí tedy $m_0 = 0$. Celková energie fotonu je pak dána vztahem,

$$E = mc^2 \tag{9}$$

kde relativistická hmotnost *m* je vyjádřena vztahem,

$$m = \frac{m_0}{\sqrt{1-\frac{v^2}{c^2}}} \tag{10}$$

avšak, na rozdíl od běžného tělesa, u kterého považujeme jeho hmotnost za konstantní, u relativistické hmotnosti *m* nám záleží na jeho rychlosti, neboli relativistická hmotnost je taková hmotnost, která se vzhledem k dané vztažné soustavě pohybuje rychlostí *v*, což je patrné ze vzorce (10). Platí tedy, že hmotnost každého tělesa se s rostoucí rychlostí zvyšuje, tedy čím rychleji se bude těleso pohybovat rychlostí blížící se rychlosti světla *c*, tím bude těžší a m_0 je hmotnost tělesa, které je vzhledem k dané vztažné soustavě v klidu.

5.2.2 Hybnost fotonu

Pro elektromagnetické vlny je stanoven vztah mezi energií *E* a hybností *p*,

$$E = cp \tag{11}$$

přičemž, aby tato rovnice platila i pro foton, musí mít nulovou klidovou hmotnost. Z toho co tedy víme, můžeme ze vztahu (11) vyjádřit hybnost fotonu při jeho nulové klidové hmotnosti,

$$p = \frac{E}{c} = \frac{hf}{c} = \frac{h}{\lambda} \tag{12}$$

kde *h* je Planckova konstanta pro $h = 6{,}626\ 070\ 040(81)\times10^{-34}$ J·s a *c* je rychlost světla ve vakuu. Závorka s číslem 81 značí nepřesnost stanovení odchylkou v řádu poslední platné číslice.

5.3 Heisenbergovy relace neurčitosti

Heisenbergovy relace neurčitosti nám říkají, že polohu a hybnost jedné částice nemůžeme zjistit současně s nekonečnou přesností. Neboť pokud budeme chtít, určit polohu nějaké částice použijeme k tomu světelný zdroj (fotony) o vlnové délce λ . Přičemž abychom mohly určit, kde se částice nachází, musí mít tato částice aspoň velikost $\frac{\lambda}{2}$. U menších částic než $\frac{\lambda}{2}$ se světelná vlna vyhne a tím pádem se neodrazí od detekované částice a my nemůžeme zjistit její polohu Δx . Přesnost polohy měřené částice je tedy stanovená,

$$\Delta x \geq \frac{\lambda}{2} \tag{13}$$

při dopadu fotonů na částici, ji fotony předají hybnost ve stejném směru. Nejmenší předání hybnosti p dochází v případě, kdy na částici dopadne pouze jeden foton, který má velikost hybnosti rovnou $p = \frac{h}{\lambda}$. Díky tomu se po srážce fotonu s částicí (která byla předtím v klidu), změní hybnost částice o velikost

$$\Delta p = \frac{h}{\lambda} \tag{14}$$

z dosazení rovnice (13) a (14) dostáváme vztah $\Delta x \Delta p \geq \frac{\lambda}{2}\frac{h}{\lambda} = \frac{h}{4\pi}$. Přičemž jsme danou relaci neurčitosti odvodily pro operátory souřadnice x a impulzu p_x proto tedy $\Delta x \Delta p_x \geq \frac{\lambda}{2}\frac{h}{\lambda} = \frac{h}{4\pi}$, analogická relace by platila i pro operátory y a p_y respektive z a p_z.

V kvantové mechanice se také často používá zlomek $\frac{h}{2\pi}$, proto bylo zavedeno značení $\hbar = \frac{h}{2\pi}$. Konečnou rovnici Heisenbergovy relace neurčitosti píšeme tedy ve tvaru,

$$\Delta x \Delta p_x \geq \frac{\hbar}{2} \tag{15}$$

Přičemž $\hbar = 1,0545 \cdot 10^{-34}$ J·s.

5.4 Schrödingerova rovnice

Nám určuje jak vlastnosti kvantového objektu, tak i jeho chování v daných obecně časově proměnných podmínkách. Vychází z determinismu, což značí to, že každá událost či stav, jak už věcí, tak i lidského rozhodnutí je důsledkem předchozích událostí a stavů. Pokud zadáme hodnotu vlnové funkce v daném časovém okamžiku, tak můžeme přesně předpovědět, které hodnoty bude mít vlnová funkce v budoucnu, nebo které měla v minulosti. Rovnice slouží tedy k popisu časového vývoje stavu částic, neboli nám udává popis kvantového procesu. Tuto rovnici píšeme ve tvaru,

$$i\hbar \frac{\partial \psi(r,t)}{\partial t} = \hat{H}(t)\,\psi(r,t) \tag{16}$$

přičemž $\hat{H}$ je Hamiltonův operátor a ψ je vlnová funkce pro kterou platí,
$\psi(r, t=t0) \rightarrow \psi(r, t> t0)$

Z toho nám vyplívá, že pro nalezení řešení Schrödingerovy rovnice, nám stačí zadat jako jedinou počáteční podmínku tvar vlnové funkce v počátečním časovém okamžiku, tedy pro $\psi(r, t = t0)$. [8]

5.4.1 Schrödingerova kočka

Je jedním z nejznámějších paradoxu, který nám říká vlastnosti vlnové funkce a jejího kolapsu. Tento paradox spočívá v tom, že uzavřeme kočku do jakési neprůhledné krabice spolu s radioaktivním materiálem a lahvičkou jedu (kyanovodík). Přičemž víme, že radioaktivní materiál je takový materiál, který se řídí kvantovou mechanikou jako takovou a jeho poločas rozpadu můžeme zjistit pouze z hlediska určité pravděpodobnosti.

Funguje to tedy následovně, pokud se v radioaktivním materiálu rozpadne atom, zaregistruje to zařízení v krabici, které následně rozbije lahvičku s jedem a kočka zemře. My ovšem nevíme, kdy došlo k rozpadu atomu v radioaktivním materiálu, můžeme se pouze domnívat. Pokud pak vezmeme v úvahu, že systém může být pouze v jednom ze dvou kvantově mechanických stavů, je kočka živá a mrtvá zároveň. Dokud nám někdo (kdo dokáže posoudit po otevření krabice stav kočky) neřekne verdikt, zda je kočka živá či mrtvá. Schrödingerova rovnice nám tedy říká, že časový vývoj života kočky je matematicky popsán jako fyzicky nepopsatelná kombinace obou zmíněných stavů. Tak jako elektron není ani vlna, ani částice do té doby, než provedeme příslušné měření, kočka není ani živá ani mrtvá do té doby, dokud se někdo nepodívá dovnitř a neřekne výsledek.

6 KVANTOVÁ KRYPTOLOGIE

V kvantové kryptologii se využívá přírodních jevů z hlediska kvantové mechaniky. To poskytuje nepodmíněnou bezpečnost pro tajné informace, která díky garanci přírodních zákonů není podmíněna žádnými předpoklady na schopnosti útočníka.

Tedy bezpečnost kvantové kryptologie nespočívá v utajení procedury ani ve výpočetní náročnosti. Základem bezpečnosti jsou fundamentální fyzikální vlastnosti. V první řadě jde o kolaps kvantového stavu. Kvantová kryptologie má hned několik dostupných protokolů. Využívajících těchto vlastností kvantové fyziky.

Toto jsou dva nejznámější typy protokolů:

- Prepare and measure protocol (**BB84 protokol**)
  - používá polarizaci fotonů

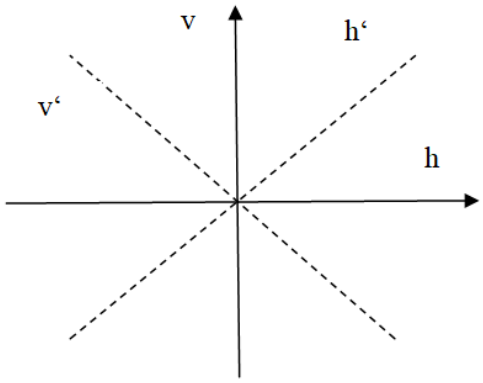
- Entaglement based protocol (**E91 protokol**)
  - používá korelaci spinu fotonů

6.1 Protokoly

Nejdříve se seznámíme s hlavními postavami, které se používají pro znázornění kvantových kryptografických protokolů. Hlavními aktéry jsou (dle anglického značení) **Alice** a **Bob**. Kde Alice chce poslat šifrovanou zprávu Bobovi, který si ji chce následně přečíst. Pak je tu narušitel **Eva** (eavesdropper), která chce jejich tajnou konverzaci odposlouchávat. Dalšími jmény, která se používají při tvorbě kvantových sítí nebo při sdílení kvantového klíče více uživateli jsou: Ali – Baba, Alex a Barbara, Anna a Boris, Charlie.

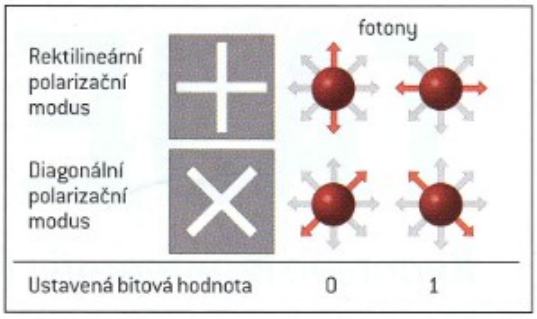
6.1.1 Protokol BB84

Protokol využívá polarizaci fotonů. Jednou z možností je lineární polarizace, která funguje tak, že se nejdříve Alice s Bobem domluví na způsobu, kterým si budou bity posílat. Následně si musí určit dvě polarizované báze, ve kterých mohou fotony kmitat a stanový k nim binární hodnoty 0 a 1 viz Obr. 8.



Obr. 8. Polarizační báze pro
h, h‘ pro bit 1 a v, v‘ pro bit 0.

Přičemž to může být například takto kdy pro 90º (↕) nebo 45º (↗) bude přiřazena hodnota 0 a pro polarizace pod úhlem 0^0(↔) a 135^0(↖) bude přiřazena hodnota 1, viz Obr. 9.

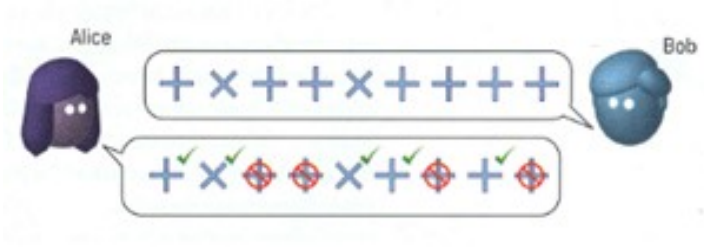


Obr. 9. Polarizované báze. [9]

Poté Alice generuje náhodnou sekvenci bitů. Následně zvolí náhodnou polarizační bázi a pomocí zdroje světla (laser) přes ni posílá foton, díky tomuž daný foton zpolarizuje a on tak získá pomyslnou bitovou hodnotu. Vše si zaznamená.

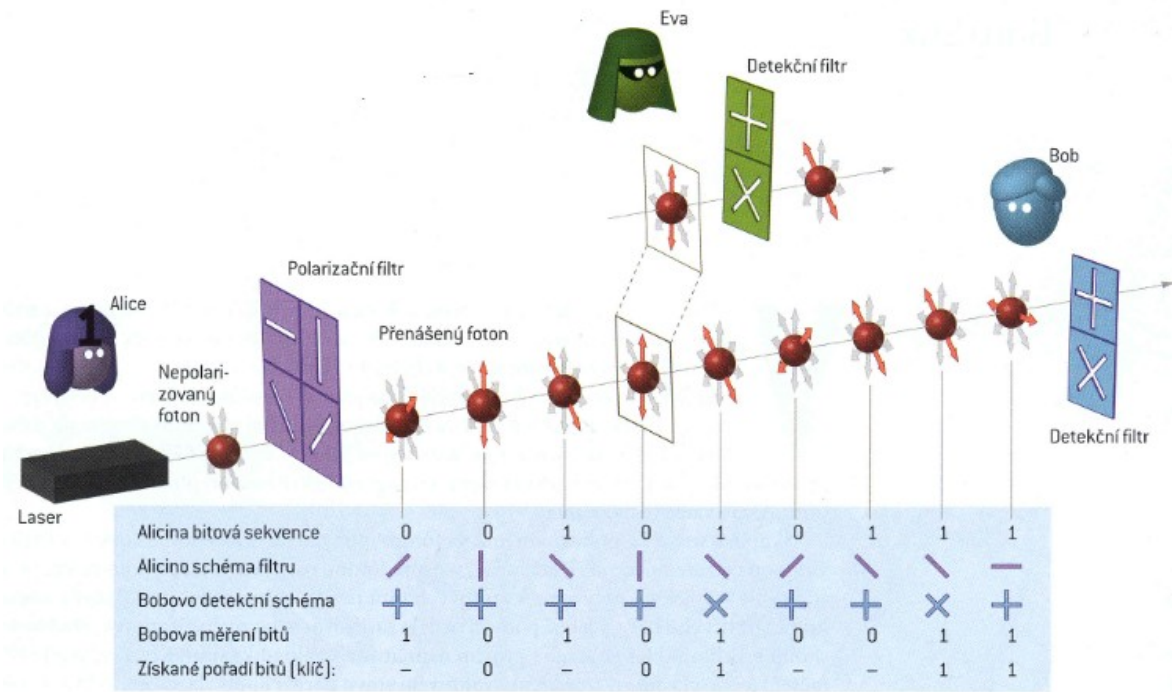
Následně Bob pro každý příchozí foton náhodně vybere polarizační bázi a podle dohodnutých bitových hodnot si zaznamená, jaká hodnota mu vyšla a jaký polarizační filtr použil.

Poté co Bob obdrží všechny příchozí fotony, sdělí Alici veřejným kanálem třeba telefonem či e-mailem pořadí použitých filtrů. Následně Alice sdělí Bobovi, jaké filtry použil správně. Na základě této výměny informací si vyberou bity k vytvoření klíče, kterým budou poté šifrovat své zprávy, viz Obr. 10.



Obr. 10. Sdělení Alice správného použití filtrů. [9]

Výhoda takového to přenosu je v tom že, pokud by se narušitel Eva pokusila sledovat tok fotonů, kvantová mechanika, díky Heisenbergovým relacím neurčitosti jí zabrání použít ke zjištění orientace fotonu oba filtry. Pokud si totiž vybere nesprávný filtr, může vytvořit chyby změnou polarizace fotonů, viz Obr. 11.



Obr. 11. Průběh získání bitů pro šifrovací klíč, pomocí polarizace fotonů. [9]

6.1.2 Protokol E91

Tento protokol navrhl Artur Ekert v roce 1991. Je založen na propletení párů fotonů. Mezi jejichž některé vlastnosti patří kvantová korelace. Fotony pak popisujeme, jedním společně kvantovým stavem.

Budeme mít zdroj propletených stavů, který vytvoří pár fotonů, který má zcela provázanou vzájemně pravoúhlou polarizaci. Tento stav můžeme zapsat jako,

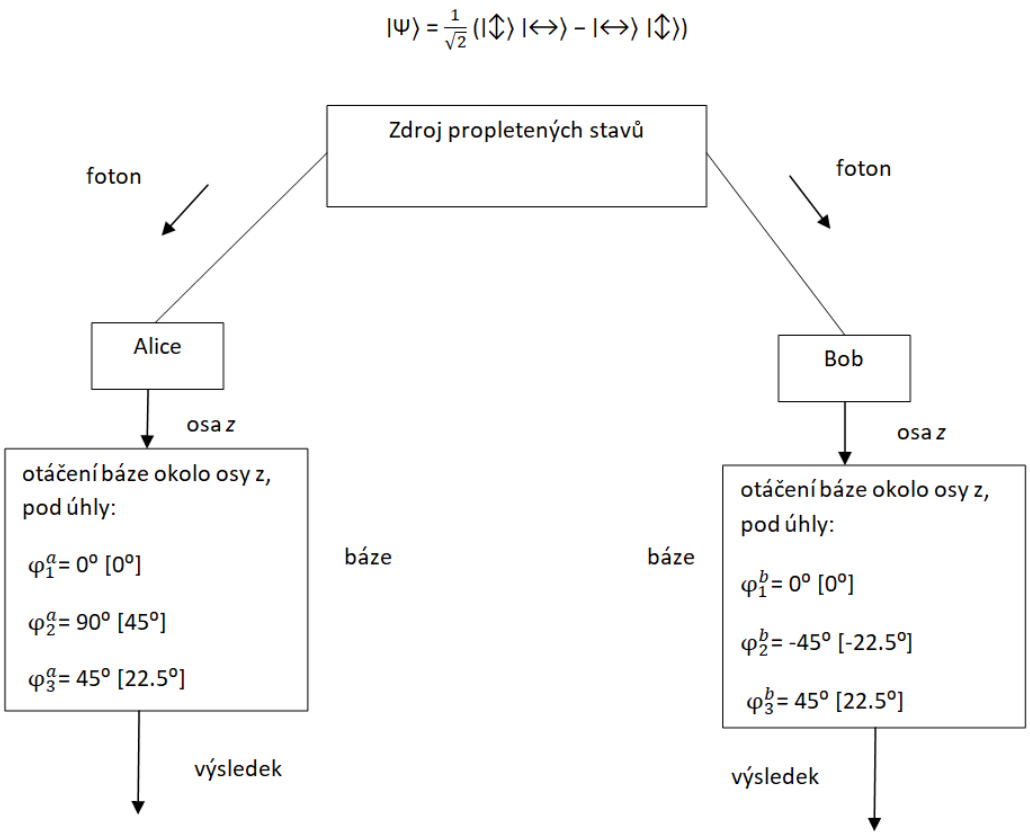
$$|\Psi\rangle = \frac{1}{\sqrt{2}}(|\updownarrow\rangle\,|\leftrightarrow\rangle - |\leftrightarrow\rangle\,|\updownarrow\rangle) \qquad (17)$$

přičemž jeden z fotonů letí k Alici a druhý k Bobovi viz Obr. 12. Alice měří polarizaci částic pomocí báze $\oplus$, kterou otáčí kolem osy z, podél které přilétávají fotony, pod úhly:

φ_1^a= 0º [0º], φ_2^a= 90º [45º] a φ_3^a= 45º [22.5º]

Bob měří pomocí otáčení báze, kolem osy z, pod úhly:

φ_1^b= 0º [0º], φ_2^b= -45º [-22.5º] a φ_3^b= 45º [22.5º]



Obr. 12. Měření polarizace částic pomocí báze.

Tedy poté, co Alice s Bobem naměří dostatečné množství fotonů, sdělí Alice a Bob pomocí veřejného kanálu které rotace báze zvolili. Pokud oba zvolí stejnou bázi, vědí, že nutně naměřili opačné hodnoty. U fotonů, pro které použili různé báze, si sdělí i výsledek měření.

Přičemž každé měření má dva možné výsledky:

$$\langle \mathrm{a}\,(\varphi_i^a)\mathrm{b}\,(\varphi_j^b)\rangle \tag{18}$$

kde a (φ_i^a) je proměnná, která udává (+1) pro měření horní orientace (horizontální polarizace) Alice a (-1) pro měření dolní orientace (vertikální polarizace). U b (φ_j^b) obdržíme podobné hodnoty podle Bobových měření. [10]

Kde kvantový výpočet poskytuje:

$$\langle \mathrm{a}\,(\varphi_i^a)\mathrm{b}\,(\varphi_j^b)\rangle = -\cos(\varphi_i^a - \varphi_j^b) \tag{19}$$

$$[\langle \mathrm{a}\,(\varphi_i^a)\mathrm{b}\,(\varphi_j^b)\rangle = -\cos(2(\varphi_i^a - \varphi_j^b))] \tag{20}$$

Stejně jako při porušování Bellovy nerovnosti dokládáme množství S, složené s korelačními koeficienty měření v různých základech:

$$\mathrm{S} = |\langle \mathrm{a}(\varphi_1^a)\mathrm{b}(\varphi_3^b)\rangle + \langle \mathrm{a}(\varphi_1^a)\mathrm{b}(\varphi_2^b)\rangle + \langle \mathrm{a}(\varphi_2^a)\mathrm{b}(\varphi_3^b)\rangle - \langle \mathrm{a}(\varphi_2^a)\mathrm{b}(\varphi_2^b)\rangle| \tag{21}$$

Použitím výsledků pro $\langle \mathrm{a}\,(\varphi_i^a)\mathrm{b}\,(\varphi_j^b)\rangle$ a příslušných úhlů dostame pro,

$$\mathrm{S} = 2\sqrt{2} \tag{22}$$

pokud Alice s Bobem dojdou k výsledku (22) tak ty fotony, které byly naměřeny se stejnou rotací báze, tvoří společný tajný klíč. Pokud by se narušitel Eva snažila získat informace o orientaci částic, sníží tím množství zapletení částic, a tím sníží hodnotu S, díky tomu Alice a Bob zjistí, že jsou odposlouchávání. [11]

6.2 Výhody kvantového šifrování

Šifrování představuje nejlepší obrannou linii proti narušení dat - zajišťuje, že samotná data jsou zbytečná, pokud padnou do neoprávněných rukou. Šifrování je ve skutečnosti stále více podmíněno novými pravidly ochrany údajů. Všechna řešení šifrování však nejsou vytvořena stejně. Jednou z výhod kvantového šifrování je princip superpozice, neboť díky němu je možné paralelně zpracovávat velké množství kvantových bitů. Díky tomu je mnohem snadnější a rychlejší provedení výpočtu některých časově náročných výpočetních

úloh, jako je faktorizace velkých čísel nebo vyhledávání v databázi. Další výhodou je jeho bezpečnost z hlediska odposlouchávání. Díky kvantové mechanice se tak stává téměř bezpečný i při nástupu kvantových počítačů, na rozdíl od klasických šifer.

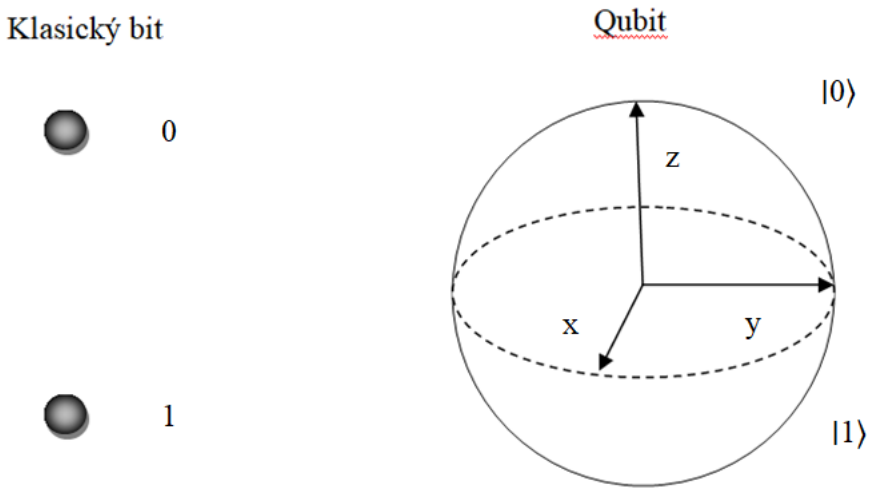
7 DALŠÍ ROLE KVANTOVÝCH JEVŮ

Tato kapitola bude zaměřena na další využití principů kvantové fyziky. Které se dále využívají v dnes už poměrně známém kvantovém počítači, s kterým se setkáváme v mnoha odborných článcích. Přičemž to není jen pouhá myšlenková úvaha o tom, jak by mohl takovýto počítač fungovat, ale díky se neustále vyvíjejícím technologiím, už v dnešní době existují i první kvantové počítače pro komerční sféru. [12]

7.1 Kvantový počítač

Počítače jsou nedílnou součástí každodenního života. Jejich rozvoj jde v poslední době neustále dopředu. Podle takzvaného Moorova zákona se počítačové součástky razantně miniaturizovaly mnoho desítek let, za ta léta se vyvinuly až do míry, kdy jednotlivé prvky mají velikost mikroskopických částic. Přičemž chování mikroskopických částic je ovlivněno zákony kvantové fyziky. Ty nám zde ale nejsou na obtíž, jak by se na první pohled mohlo zdát, ale naopak je můžeme využít k zhotovení nového typu počítačů, viz

Obr. 13. [13] V těchto nových počítačích jsou nahrazeny dnešní křemíkové obvody kvantovými částicemi. V současné době se na jejich vývoji účastní mnoho špičkových laboratoří.



Obr. 13. Klasický bit a kvantový qubit.

Funkce

Kvantový počítač využívá k zápisu informací kvantově mechanické vlnové částice jako je například spin elektronů, který umíme měřit díky jím generovaným magnetickým účinkům. Nejjednodušší měření je založeno na průletu částice nehomogenním magnetickým polem.

Částice se spinem $|\uparrow\rangle$ se vychýlí na jednu stranu, zatímco částice se spinem $|\downarrow\rangle$ se vychýlí na opačnou stranu. Částice s různou projekcí spinu, které prolétly magnetickým polem, pak dopadají do různých míst (detektorů). Jeho srdcem je objekt mikrosvěta takzvaný qubit(kvantový bit) což je základní jednotka informace. U klasického počítače je informace uložena do nul a jedniček. Ty mohou být realizovány určitým napětím na elektrodě nebo orientací magnetické domény v magneticky aktivním materiálu harddisku či jiného média.

S těmito nulami a jedničkami se pak následně dělají základní operace jako je například logický součet (OR), logický součin (AND), logická negace (NOT). Přičemž pro určitou kombinaci nul a jedniček na vstupu je dána konkrétní kombinace nul a jedniček na výstupu viz [14]

Tab. 6., kde operace NOT má jeden vstup a jeden výstup a operace AND je realizována dvěma vstupy a jedním výstupem. [14]

Tab. 6. Ukázka klasických operací NOT a AND pomocí hradel.

operace s bity	vstup 1	vstup 2	výstup
NOT	1	-	0
	0	-	1
AND	1	1	1
	1	0	0
	0	1	0
	0	0	0

U kvantového počítače je informace uložena pomocí qubitu, ten je na rozdíl od klasického bitu v superpozici dvou nebo více stavů viz Tab. 7. Superpozici je možné navodit laserovým nebo mikrovlnným impulzem. Při nichž se mění amplituda a fáze koeficientů superpozice.

Tab. 7. Ukázka kvantových operací s jedním Qubitem.

operace s qubitem	**vstup**	**výstup**
Pauliho x hradlo (NOT)	(α, β)	(β, α)
Pauliho y hradlo	(α, β)	$(i\beta, -i\alpha)$
Pauliho z hradlo (flip)	(α, β)	$(\alpha, -\beta)$
Hadamard	(α, β)	$(\alpha + \beta, \alpha - \beta)/\sqrt{2}$

Díky využití kvantových vlastností je kvantový počítač mnohonásobně efektivnější než klasický, neboť nese současně informace o všech možných hodnotách spinu a tím uskutečňuje paralelně výpočet všech možností, které mohou nastat.

II. PRAKTICKÁ ČÁST

8 MOŽNOSTI KOMERČNÍHO VYUŽITÍ KVANTOVÉ TECHNOLOGIE

Každou technologii provází vývoj, který se musí zaplatit. Z toho důvodu se už musí uvažovat o kvantové technologii jako o službě, která může být nabízena koncovým zákazníkům k použití v jejich aplikacích. V případě kvantového provázání fotonů lze uvažovat o této technologii jako o naprostém zvýšení bezpečnosti v ochraně dat a soukromí uživatelů. Tento fakt nemůže opomíjet žádná firma, která má takzvané vlastní „know how“, které jí stálo roky vývoje vlastních produktů a technologických řešení na kterých staví své portfolio. Pokud by firma při nějakém úniku dat, ať už kvůli sociálnímu inženýrství nebo díky externímu útoku takzvaných hackeru přišla o část nebo v nejhorším případě o celé své „know how“, což v technologických firmách můžou být schémata plošných spojů a k nim spojené dokumentace. Předčasné vyzrazení nového produktu, na který může konkurence tudíž dříve reagovat, nebo třeba i jen databáze jejich zákazníků. Mohlo by to mít pro danou firmu likvidační následky z důsledku ztráty důvěry zákazníků, případně v horším scénáři i technologického náskoku před konkurencí. Z tohoto důvodu by své podnikání měla každá firma co nejlépe chránit a kvantová technologie ji v tom může být skvělou pomocí.

Svět ale nejsou pouze firmy, je také rozdělen na státy, v kterých firmy své podnikání provozují. A v těch firmách především pracují lidé, kteří tomu státu přísluší. Státní instituce vlastní obrovské množství citlivých dat o svých občanech. Tudíž tu největší ochranu by měl poskytovat samotný stát. Z tohoto hlediska by se neměla kvantová technologie a její obrovská bezpečností výhoda vztahovat pouze k firmám, ale i ke státním institucím, které by se měli snažit všechna svoje data o svých občanech uchovávat co nejbezpečněji.

Existuje již několik technologických firem, které mají své produkty založené na kvantové technologii uvedené na trh, a tudíž jsou k dispozici pro použití firmám, které na nich můžou postavit své bezpečností opatření. V následujících kapitolách jsou představeny produkty dostupné na trhu a následná analýza výhod či nevýhod použiti kvantové technologie v daném segmentu.

9 PRODUKTY UVEDENÉ NA TRH

V případě, že dojde k masivnímu nástupu kvantových počítačů, bude zapotřebí kvantového šifrování, které odolá jejich výkonu. Momentálně používané asymetrické šifrování používá faktorizaci a další algoritmy, které bude případný kvantový počítač zpracovávat velmi rychle. Proto by vlády a podniky měli začít investovat do vývoje kvantové kryptografie a zařízení pracujících na tomto principu.

Kapitola je členěna na zařízení pro kvantově bezpečnou komunikaci, dále na zařízení plně využívající kvantovou distribuci klíče a pro hlavní komunikační kanál standardizovanou blokovou symetrickou šifru. Také jsou zde uvedeny doplňkové prvky využívajících kvantových jevů.

9.1 Kvantově zabezpečené síťové šifrování

Tato zařízení jsou určena k zabezpečení a splňují nejvyšší požadavky, a to i pokud jde o certifikace. Prostředí systému je uzavřené a je prokázáno jako bezpečné. Procesy a řízení jsou jednoduché, přímočaré a zcela optimalizované. Jsou vysoce výkonné a mají velmi dobré zabezpečení dat. Co se týče dlouhodobého dopadu, jsou flexibilní a mají vysokou životnost.

9.1.1 Centauris CN9000 Series

- Vysokorychlostní šifrování dat v okruhu 100 Gb / s
- Vysoká jistota, s velmi nízkou latencí šifrování
- Robustní, škálovatelné a jednoduché
- QRNG-powered 100Gb/s šifrování

Obr. 14. Centauris CN9000 Series. [15]

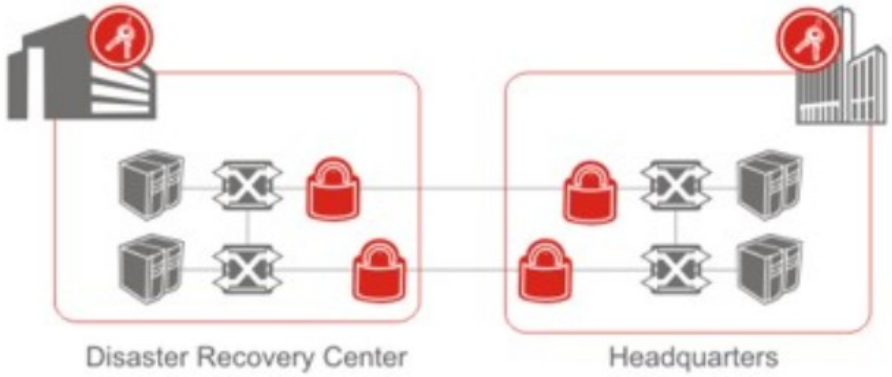
Je prvním komerčně dostupným certifikovaným 100Gb/s ethernetovým šifrováncím zařízením s vysokým stupněm utajení, který podporuje nejkomplexnější topologie což umožňuje 100% zabezpečení pro ultrarychlé sítě Big Data, Cloud a datová centra viz Obr. 14.

9.1.2 Centauris CN8000

- Kvantově bezpečný šifrátor multi-link (10x10Gb/s)
- Nekompromisní výkon, flexibilita a škálovatelnost
- QRNG-powered, multi-link šifrování
- Šifrování pro více uzlů na Ethernet a Fibre kanálech

Aplikace:

Šifrovací program Centauris CN8000 pracuje přes síťové topologie typu point-to-point viz Obr. 15., point-to-multipoint a full-mesh.



Obr. 15. Síťová topologie typu point-to-point. [16]

9.2 Kvantová distribuce klíče (QKD)

V praxi se QKD kombinuje s konvenčním symetrickým šifrováním, jako je AES, a často se používá k aktualizaci šifrovacích klíčů. Dvě zařízení QKD jsou propojena prostřednictvím optického vlákna a průběžně distribují klíčový materiál, který ukládají, dokud není požadován šifrovacím zařízením. Tato řešení pracují až do vzdálenosti 100 km (optický útlum odpovídající 20 dB) a jsou tak nasazena v sítích metropolitní oblasti. Mezi typické aplikace patří rozšíření zabezpečené sítě LAN v podnikových kampusech nebo propojení datových center.

9.2.1 Cerberis QKD Blade

- První platforma QKD na světě viz Obr. 16
- Prokazatelně bezpečná výměna klíčů na základě distribuce kvantových klíčů
- Kvantové klíče zajišťují dlouhodobou ochranu a utajení
- Plně automatizovaná výměna a nepřetržitá obnova klíčů
- Integrovaný zdroj entropie založený na Generátoru náhodných čísel

Obr. 16. Cerberis QKD Blade. [17]

9.2.2 Clavis3 QKD Platform for R&D

- Slouží pro distribuování kvantových klíčů pro aplikace výzkumu a vývoje
- Otevřená platforma QKD pro vysokorychlostní generování klíčů pro aplikace výzkumu a vývoje do vzdálenosti až 100km
- Hardwarově založený protokol pro destilační klíč (FPGA) viz Obr. 17

Obr. 17. Clavis3 QKD Platform for R&D. [18]

9.3 Další dostupné produkty

Zde jsou zmíněny některé z dalších produktů využívajících kvantových jevů uvedené na trhu. Je zde uveden generátor náhodných čísel od společnosti ID Quantiqu, a miniaturní vícekanálový fotonový čítač.

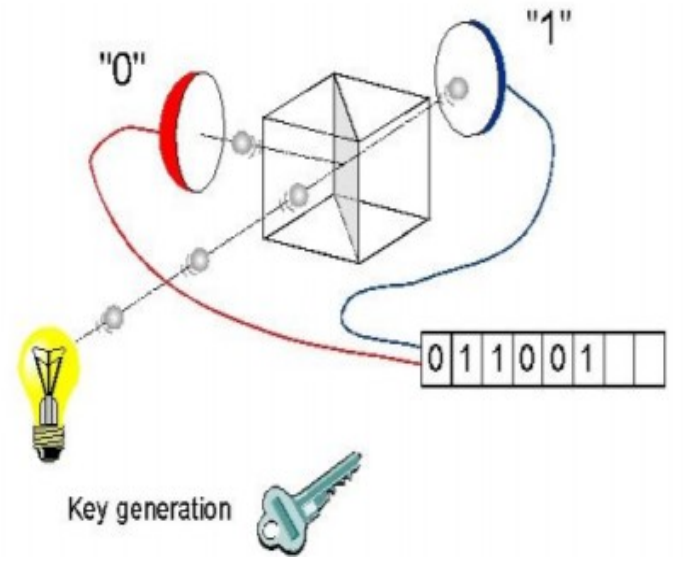
9.3.1 Quantis Random Number Generator

- Pravý generátor náhodných čísel využívající náhodnost kvantové fyziky
- Pravý hardwarový generátor náhodných čísel (RNG)
- Důvěryhodný a ověřený zdroj kvantové náhodnosti
- Průběžná kontrola stavu a zjišťování selhání mechanismus
- Instantní entropie, škálovatelná pro různé aplikace
- Pokročilé funkce, jako je měřítko a extrakce náhodnosti

Obr. 18. Quantis Random Number Generator. [19]

Je založen na principech kvantové fyziky. Jeho uplatnění najdeme hned v několika průmyslových odvětvích, včetně bezpečnosti, her či loterií. Patří do rodiny hardwarových generátorů náhodných čísel (RNG), které využívají elementární kvantové optické procesy, jako zdroj skutečné náhodnosti viz Obr. 18.

Fotony (lehké částice) jsou posílány jeden po druhém na poloprůhledné zrcadlo a detekovány. Exkluzivní události (odraz nebo přenos) jsou přiřazeny hodnotám bitů "0" nebo "1". Takové kvantové procesy poskytují okamžitou a nevyčerpatelnou entropii viz Obr. 19.



Obr. 19. Princip generátorů náhodných čísel. [20]

Provoz Quantis QRNG je průběžně monitorován, aby se zajistilo okamžité zjištění poruchy a v případě potřeby i vypnutí náhodného bitového toku. Má výhodu oproti konvenčním zdrojům náhodnosti, tím že je nezranitelný vůči ekologickým perturbacím a umožňuje ověření živého stavu.

9.3.2 ID150 Visible 8 Channel SPAD

- Miniaturní 8 kanálový fotonový čítač pro OEM aplikace
- Volný běh
- 35% kvantová účinnost
- Nízká míra chybného vyhodnocení
- 8 kanálů

Obr. 20. ID 150 Visble 8
Channel SPAD.[21]

Je jediný vícekanálový detektor s jednosložkovými stabilními polovodiči na trhu. Má vynikající časové rozlišení menší než 60 ps, které umožňuje měření s vysokou přesností. Čip je umístěn na desce s plošnými spoji na prvním stupni termoelektrického chladiče viz Obr. 20. Termistor lze použít k měření teploty čipu. Pro provoz v režimu počítání fotonů jsou zapotřebí pouze dva nízké napájecí zdroje +5 V a -25 V.

10 ANALÝZA

V této části se zaměříme na analýzu zařízení pro kvantové šifrování, jako je jejich cena, výhody, nevýhody, zda jsou vhodné spíše pro malé firmy či státní organizace atd. Do analýzy však nelze zahrnout přímé srovnání technologických řešení založených na kvantové fyzice, které jsou momentálně na trhu. A tudíž srovnání jejich výhod a nevýhod vůči sobě. Produkty a na nich založené řešení pro daného zákazníka je vždy tvořeno individuálně podle jeho potřeb a nejsou o tom vedeny žádné veřejné záznamy ani recenze.

Cena

Není sama o sobě určující pro celkovou cenu za zabezpečení informací pomocí kvantové kryptografie, neboť zde hraje roli zaprvé cena zařízení a zadruhé TCO. Je však násobně vyšší proti klasické kryptografii, přičemž ale cena chráněných informací může být ve srovnání s touto cenou neporovnatelná.

Platí tedy, že cena zařízení a celkové realizace je vždy tvořena na daného zákazníka a je ovlivněna poptávkou trhu a dalšími faktory, proto nelze uvést konkrétní čísla. Všeobecně se dá však říct, že momentálně se cena pohybuje na minimálně sedmi ciferných číslech v Českých korunách.

Použitelnost zařízení

Uvedená zařízení v předešlé kapitole jsou vhodné jak pro firmy, tak i pro státní sféru. Avšak z hlediska ceny jsou spíše určeny pro státní sféru či nadnárodní společnosti. V České republice použití kvantové technologie pro daný segment působnosti zprostředkovává například česká distribuční firma L2K spol. s r.o.

Potřeba kvantové kryptografie v dnešní době

Bezpečnost dnešní kryptografie veřejného klíče spočívá především na předpokladu, že některé matematické funkce jsou složité na výpočet nebo dekódování bez přístupu k výpočetnímu výkonu dnešních klasických počítačů.

Nicméně, s nástupem masivně silných kvantových počítačů v příštím desetiletí, takové předpoklady již nebudou stačit. Hodně dnešních šifrování bude zranitelné. Navíc, informace, které byly staženy dnes, mohou být dešifrovány offline v příštích letech (uložit, dešifrovat později).

Proto musí vlády a podniky začít investovat do "kvantově zabezpečené kryptografie" - včetně klíčových distribučních řešení jako je QKD - která odolává kvantovým počítačům. Všechny vlády a podniky by měly uskutečnit přechod ke kvantovému zabezpečení jako nedílnou součást plánování rizik a měly by být přijaty nové investice do infrastruktury a bezpečnosti.

Stručný nadhled nad problematiku kvantové komunikace lze shrnout takto:

Výhody

- výkon
- zabezpečení

Nevýhody

- cena
- dostupnost

11 POKROKY A VÝHLED DO BUDOUCNA

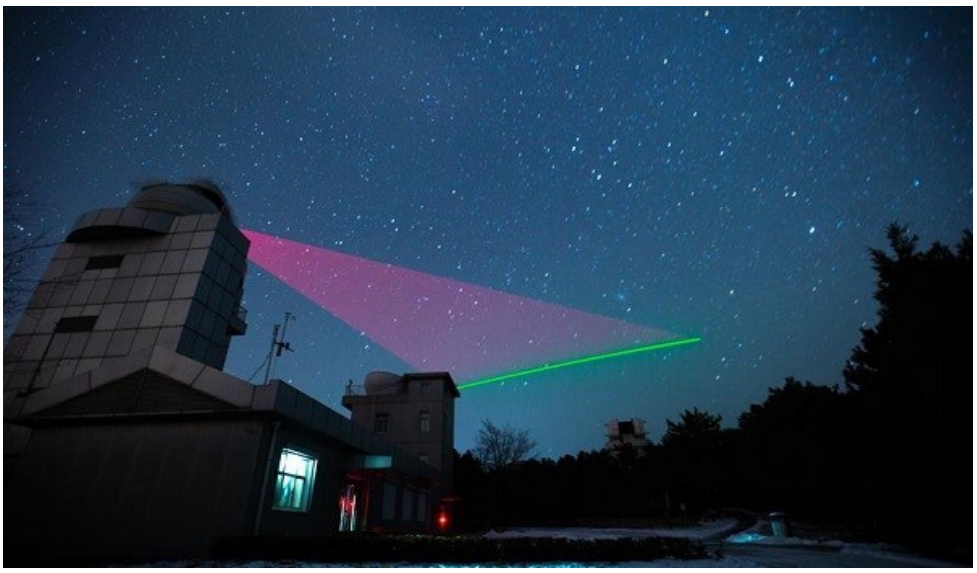
Technologie se neustále vyvíjejí a zdokonalují i co se kvantových technologií týče. Přičemž ve světě patří úspěšný průlom v oblasti kvantové komunikace nemalým podílem Číně. Která v této oblasti pokročila směrem dopředu.

Tato část je zaměřená na doposud uskutečněné průlomové úspěchy v kvantové komunikaci, dále pak je tu zmíněn jejich plánovaný budoucí vývoj a také vývoj v oblasti kvantových počítačů.

11.1 Kvantová komunikace

Obor kvantové distribuce klíčů (Quantum Key Distribution) slouží za pomoci kvantového provázání fotonů k přenosu kryptografických klíčů. V dnešní době je to rychle se rozvíjející odvětví.

Jeden z přenosu se uskutečnil 29. 09. 2017, kdy Čína provedla první kvantovou videokonferenci. Tento přenos se odehrával mezi Pekingem a Vídní viz Obr. 21. Kvantová komunikace probíhala za pomoci čínského satelitu Micius, který obíhá Zemi ve výšce cca 500 kilometrů. Jeho palubu obsahují tři ústřední přístroje, vysílač kvantových klíčů pro QKD, zdroj kvantově provázaných fotonů a zařízení k příjmu a analýze kvantové teleportace. Pomocí optických vláken, je satelitní kvantová síť na obou stranách napojená na pozemní kvantové sítě.



Obr. 21. Fotografie čínské pozemní stanice komunikující s družicí Micius. [22]

Při komunikaci přes satelit pak procházejí kvantově provázané fotony téměř prázdným prostorem a mají to tím pádem snazší.

A to není jediný z průlomových úspěchů čínských vědeckých pokroků, který jde dopředu v oblasti kvantové komunikace a teleportace. Mezi další se může řadit přenos entanglovaných částic skrz vodu, které by mohly časem sloužit jako komunikace mezi ponorkami.

Budoucí vývoj

Budoucí vývoj v QKD se soustředí na zvýšení rozsahu systémů a poskytnutí globální QKD sítě. Za účelem překročení důvěryhodných uzlů, které omezují systém QKD na pozemní systémy, kde uzly mohou být zřízeny každých několik desítek kilometrů. Další možností je zbavit se optického vlákna. To je možné výměnou klíče pomocí kvantové kryptografie ve volném prostoru, mezi pozemní stanicí a nízkou pozemní orbitální družicí.

Absorpce v atmosféře probíhá převážně během několika prvních kilometrů. Pokud je vybrána odpovídající vlnová délka, optické spojení mezi zemí a družicemi se může vytvořit v nadmořské výšce zhruba 800 km. Taková družice se pak pohybuje s ohledem na zemský povrch. Při přechodu na druhou stanici, která se nachází tisíce kilometrů od první stanice, se může znovu vysílat klíč, viz Obr. 22. [20]

Obr. 22. Kvantová distribuce klíče z vesmíru. [20]

Satelit je implicitně považován za bezpečnou zprostředkovatelskou stanici. Tato technologie je méně zralá než technologie založená na optických vláknech. Výzkumné skupiny již

provedly předběžné testy tohoto systému. Pokročilý výzkum se provádí v Číně, který zahájil první QKD satelit nazvaný Micius viz informace výše.

Dalším pokrokem v kvantovém světě by mohly být kvantové opakovače, které by sloužily k rozšíření klíče výměnou přes libovolně dlouhé vzdálenosti. V praxi však takové kvantové opakovače ještě neexistují, ale jsou předmětem intenzivního výzkumu.

11.2 Kvantové informatika

Kvantová informatika slibuje, hned několik velmi zajímavých směrů, mezi které bez pochyby patří například vysokorychlostní kvantové počítače. V letošním roce (10. 1. 2018) se společnost Intel pochlubila svým nejnovějším univerzálním kvantovým počítačem, který obsahuje celkem 49 qubitů.

Co se však qubitů týče, jsou nesmírně křehké a náchylné. Ztrátu dat totiž může způsobit nechtěné sledování či sebemenší rušení. Proto je nezbytné je provozovat při teplotě 20 milikelvinů, což je jen nepatrně nad absolutní nulou. Je to jeden z důvodů proč nejdou tak rychle rozšířit. A protože zatím neexistuje tak malý a výkonný chladící zařízení, musí pracovat ve velkých sálech. Stejně jako první počítače. Zatím se ani neočekává, že by jejich velikost v dohledné době spočinula na velikost dnešních desktopů. Intel se však zabývá ještě jiným typem qubitů, jsou to tak zvané spinové qubity. Tyto qubity mohou být teoreticky mnohem menší. Avšak zda budou moct být, tvořeny s využitím křemíkových technologií se teprve ukáže. Teoreticky by to jít mělo. Procesory budou tedy zkoušet vyrábět ve svých moderních továrnách využívající 300mm křemíkových waferů. [23]

ZÁVĚR

V dnešní době jsou technologie nedílnou součástí každodenního života. Skoro veškeré informace, platby, komunikace atd. se dnes provádějí online, přičemž šifrování v nich hraje důležitou roli. V tomto směru může vývoj kvantových počítačů, na němž se v současné době pracuje, ohrozit v některých případech každodenně používané technologie a tudíž i velkou měrou snížit soukromí. V situaci, kdyby došlo k úspěšnému vývoji a rozšíření kvantových počítačů. Budou informace ohroženy, neboť kvantové počítače pracují s qubity, což jsou kvantové bity v superpozici, které fungující na principu kvantové mechaniky. Díky tomuto principu využití kvantových vlastností jsou kvantové počítače mnohonásobně efektivnější než klasické, neboť nesou současně informace o všech možných hodnotách spinu a tím uskutečňují paralelní výpočet všech možností, které mohou nastat. A tak jsou z hlediska prolomitelnosti dnešních šifer mnohem efektivnější.

Proto je nutné sehrát roli i z hlediska bezpečnosti, k tomu slouží kvantová kryptografie, která využívá fascinujících zákonů přírody a staví převážně na kvantové mechanice. Díky níž nám vznikají šifrovací protokoly, které jsou téměř nehacknutelé.

V dnešní době už toho tedy víme o fyzice mikrosvěta mnohem více a umíme některé její vlastnosti i využít, ale pořád je ještě co dolaďovat a prozkoumávat. Fyzikální zákony kvantové fyziky nejsou totiž, tak jednoduše objasnitelné jako jsou zákony klasické fyziky a jak bylo řečeno v jedné fyzikální přednášce o kvantové fyzice: „Pokud si někdo myslí, že kvantovou fyziku pochopil, tak ji zaručeně nepochopil.“

Nicméně kvantové technologie se i přes náročnost pochopení kvantové fyziky neustále vyvíjí směrem dopředu a je jen otázkou času, kdy naplno bude lidstvo schopno využít její potenciál.

SEZNAM POUŽITÉ LITERATURY

[1] HISTORIE KRYPTOLOGIE [online]. [cit. 2018 – 05 – 19]. Dostupné z: http://www.fi.muni.cz/usr/jkucera/pv109/2003/xbitto.htm

[2] Skytala. In: Wikimedia Commons [online]. [cit. 2018-05-19]. Dostupné z: https://commons.wikimedia.org/wiki/File:Skytala%26EmptyStrip-Shaded.png

[3] Caesarova šifra. Wikipedie [online]. [cit. 2018-05-19]. Dostupné z: https://cs.wikipedia.org/wiki/Caesarova_šifra

[4] Caesarova šifra. In: Wikipedie [online]. [cit. 2018-05-19]. Dostupné z: https://cs.wikipedia.org/wiki/Caesarova_šifra#/media/File:Caesar3.svg

[5] Enigma. In: Wikipedie [online]. 2003 [cit. 2018-05-19]. Dostupné z: https://cs.wikipedia.org/wiki/Soubor:Enigma.jpg

[6] prezentace

[7] Vznik a základy kvantové mechaniky. Encyklopedie fyziky [online]. Jaroslav Reichl a Martin Všetička, 2018 [cit. 2018 – 03 – 10]. Dostupné z: http://fyzika.jreichl.com/main.article/view/732-vznik-a-zaklady-kvantove-mechaniky

[8] SKÁLA, Lubomír. Úvod do kvantové mechaniky. Praha: Karolinum, 2011. ISBN 978-80-246-2022-0.

[9] STIX, Gary. NEJLÉPE STŘEŽENÁ TAJEMSTVÍ. SCIENTIFIC AMERICAN ČESKÉ VYDÁNÍ. 2005, 2005(6), 5.

[10] The physics of quantum information: quantum cryptography, quantum teleportation, quantum computation [online]. New York: Springer, 2001 [cit. 2018-03-12]. ISBN 978-3540667780.

[11] Kvantová kryptografie [online]. Praha, 2008 [cit. 2018-03-28]. Dostupné z: http://quantum.karlov.mff.cuni.cz/archiv_praci/strasky/BPTX_2007_1_11320_NSZZ027_228462_0_49010.pdf. Bakalářská práce. Univerzita Karlova v Praze - Matematicko-fyzikální fakulta.

[12] První kvantový počítač stojí deset milionů dolarů. VTM [online]. [cit. 2018-05-23]. Dostupné z: http://vtm.e15.cz/prvni-kvantovy-pocitac-stoji-deset-milionu-dolaru

[13] Teorie a perspektiva kvantových počítačů [online]. ČVUT PRAHA, Fakulta elektrotechnická, Vojtěch Kupča, 2001 [cit. 2018-04-12]. Dostupné z: http://www.karlin.mff.cuni.cz/~holub/soubory/qc/qc.html

[14] How Quantum Computers Work. HowStuffWorks [online]. [cit. 2018-05-12]. Dostupné z: https://computer.howstuffworks.com/quantum-computer.htm

[15] Centauris CN9000 Series. ID Quantique [online]. Genève - Switzerland: ID Quantique, 2018 [cit. 2018-04-12]. Dostupné z: https://www.idquantique.com/quantum-safe-security/products/centauris-cn9000-series/

[16] Centauris CN8000. ID Quantique [online]. Genève - Switzerland: ID Quantique, 2018 [cit. 2018-04-12]. Dostupné z: https://www.idquantique.com/quantum-safe-security/products/centauris-cn8000-series/

[17] Cerberis QKD Blade. ID Quantique [online]. Genève - Switzerland: ID Quantique, 2018 [cit. 2018-04-21]. Dostupné z: https://www.idquantique.com/quantum-safe-security/products/cerberis-qkd-blade/

[18] Clavis3 QKD Platform for R&D. ID Quantique [online]. Genève - Switzerland: ID Quantique, 2018 [cit. 2018-04-25]. Dostupné z: https://www.idquantique.com/quantum-safe-security/products/clavis3-qkd-platform-rd/

[19] Quantis Random Number Generator. ID Quantique [online]. Genève - Switzerland: ID Quantique, 2018 [cit. 2018-05-12]. Dostupné z: https://www.idquantique.com/random-number-generation/products/quantis-random-number-generator

[20] Understanding Quantum Cryptography. QUANTUM - SAFE SECURITY WHITE PAPER[online]. 2017, 14 [cit. 2018-05-12]. Dostupné z: https://marketing.idquantique.com/acton/attachment/11868/f-020d/1/-/-/-/-/Understanding%20Quantum%20Cryptography_White%20Paper.pdf

[21] ID150 Visible 8 Channel SPAD. ID Quantique [online]. Genève - Switzerland: ID Quantique, 2018 [cit. 2018-05-11]. Dostupné z: https://www.idquantique.com/single-photon-systems/products/id150/

[22] Fotografie čínské pozemní stanice komunikující s družicí Micius. In: The Brics Post[online]. 2017 [cit. 2018-05-19]. Dostupné z: http://thebricspost.com/chinese-satellite-sends-unbreakable-code-from-space/)

[23] Intel Unveils ‘Breakthrough’ Quantum Computer. EXTEMETECH [online]. 2018 [cit. 2018-05-24]. Dostupné z: https://www.extremetech.com/computing/261734-intel-unveils-new-quantum-computer-declares-quantum-breakthrough

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

WPA Wi-Fi Protected Access.

WEP Wired Equivalent Privacy.

TCO Total Cost of Ownership.

RSA Rivest, Shamir, Adleman.

RNG Random number generation.

QRNG Quantum random number generator.

QKD Quantum key distribution.

OEM Original Equipment Manufacturer.

LAN Local Area Network.

FPGA Field Programmable Gate Array.

AES Advanced Encryption Standard.

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM PŘÍLOH

CD s textem práce