Ochrana utajovaných informací pomocí kvantové kryptografie

Protection of classified information by quantum cryptography

Bc. David Tříska

Diplomová práce
2011

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2010/2011

ZADÁNÍ DIPLOMOVÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Bc. David TŘÍSKA**
Osobní číslo:	**A09408**
Studijní program:	**N 3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Téma práce:	**Ochrana utajovaných informací pomocí kvantové kryptografie**

Zásady pro vypracování:

1. **Zpracujte formou manuálu pro použití v PKB.**
2. **Charakteristika a systematizace kvantové kryptografie.**
3. **Porovnání kryptografické ochrany a kvantové kryptografie z hlediska bezpečnosti.**
4. **Vysvětlete pojem ochrana utajovaných informací.**
5. **Problematika hackingu v kvantové kryptografii.**
6. **Praktická využitelnost kvantové kryptografie v bezpečnostní komunitě.**

Rozsah diplomové práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **POLKINGHORNE, John. Kvantová teorie. Praha : Dokořán, 2007. 119 s. ISBN 978-80-7363-084-3.**
2. **LAUCKÝ, Vladimír. Speciální bezpečnostní technologie. 1. vyd. Zlín : [s.n.], 2009. 223 s. ISBN 978-80-7318-762-0.**
3. **Zákon číslo 412/2005 Sb. O ochraně utajovaných informací a bezpečnostní spolehlivosti.**
4. **LAUCKÝ, Vladimír. Technologie komerční bezpečnosti II. Zlín 2007. ISBN 978-80-7318-631-9.**
5. **LAMBROPOULOS, Peter; PETROSYAN, David. Fundamentals of Quantum Optics and Quantum Information. 1. Heraklion : Springer, 2007. 326 s. ISBN 978-3-540-34571-8.**
6. **PIPER, Fred, MURPHY, Sean. Kryptografie : Průvodce pro každého. Pavel Mondschein. 1. vyd. Praha : Dokořán, 2006. 157 s. ISBN 80-7363-074-5.**
7. **VERTON, Dan. Black Ice : Neviditelná hrozba kyberterorismu. 1. [s.l.] : Helion, 2004. 264 s. ISBN 83-7361-564-4.**

Vedoucí diplomové práce: **JUDr. Vladimír Laucký**
Ústav bezpečnostního inženýrství

Datum zadání diplomové práce: **25. února 2011**

Termín odevzdání diplomové práce: **27. května 2011**

Ve Zlíně dne 25. února 2011

L.S.

prof. Ing. Vladimír Vašek, CSc.
děkan

doc. RNDr. Vojtěch Křesálek, CSc.
ředitel ústavu

ABSTRAKT

Diplomová práce je zaměřena na popis kvantové kryptografie jako prostředku k ochraně informací. Postupně se budu zabývat popisem kvantové kryptografie, porovnáním kvantové kryptografie a „klasické kryptografie“, utajovanými informacemi, problematikou hackingu v kvantové kryptografii a průzkumem zařízení využívajících kvantovou kryptografii. Práce může najít uplatnění jako příručka, jak chránit informace s využitím kvantové kryptografie, nebo pomoci při výběru způsobu zabezpečení informací.

Klíčová slova: kvantová kryptografie, utajované informace, kryptografická ochrana, bezpečnostní přenos, ochrana informací, kvantový bit, QKD.

ABSTRACT

The thesis is focused on description of quantum cryptography as a means to protect information. I will deal with the description of quantum cryptography, comparing quantum cryptography and „classical cryptography“, classified information and problems of hacking in quantum cryptography and sensing device using quantum cryptography. The work can be used as a guide to how to protect information by quantum cryptography or assistance in selecting the method of information security.

Keywords: quantum cryptography, classified information, cryptographic protection, transmission security, protection of information, quantum bit, QKD.

Děkuji vedoucímu diplomové práce, panu JUDr. Vladimíru Lauckému, za odborné vedení, drahocenné rady a věcné připomínky, které vedly ke zdokonalení práce. Cením si pomoci Bc. Lucie Pochobradské za kontrolu pravopisu. Velké díky patří boršické knihovnici, mé tetě, Petře Víchové, za distribuci literatury. Dále bych rád poděkoval za konzultace panu Zdeňku Kladivovi ze společnosti L2K, panu doc. Ing. Karlu Burdovi, CSc., z VUT Brno. Svým rodičům, přítelkyni a kamarádům za podporu při psaní 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 s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- 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 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 16. května 2011 …….

podpis diplomanta

OBSAH

ÚVOD

Diplomová práce se zaměřuje na kvantovou kryptografii[1] jako metodu ochrany informací. Práce pojednává o oblastech historie kryptografie, seznámení s kvantovou kryptografií, popis a příklady protokolů, porovnání „klasické“ kryptografie s kvantovou kryptografií. Budu popisovat výhody a nevýhody jednotlivých metod k ochraně informací. V další části následuje vysvětlení pojmu „ochrana utajovaných informací“. Součástí práce je také problematika hackingu v kvantové kryptografii a pokusy o prolomení. Závěrečná část diplomové práce je zaměřena na praktické využití kvantových technologií. Charakterizuji vybrané společnosti, které dodávají kvantová zařízení, a popis jejich produktů.

Diplomovou práci jsem zpracoval formou příručky, která bezpečností manažery, firmy, společnosti a zájemce o kryptografii seznámí s kvantovou kryptografií a související problematikou. Práci jsem rozdělil na kapitoly podle určeného zadání a v jednotlivých kapitolách jsem řešil zadaný úkol.

Při posílání psaní zpravidla použijeme obálku a pečlivě ji zalepíme. A to z důvodu, aby zprávu či určitou informaci četla jen osoba, které je určena. Mluvím o tom z důvodu, že i psaní v obálce představuje ochranu informací. Jedná se o velmi primitivní způsob ochrany, avšak hojně používaný.

Informace typu „tajné“, „přísně tajné“ a podobně si ovšem nevystačí jen s obyčejnou obálkou. Při přenosu a manipulaci s těmito informacemi je nutné dodržovat přesná pravidla, o kterých mluví zákon č. 412/2005Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti a další vyhlášky.

Při přenosu informace po síti, například emailem, nebo práci s digitálními daty využíváme k ochraně informací kryptografii. V podstatě existují dva základní typy utajení informace pomocí kryptografie, první druh je „klasická kryptografie“ na matematické bázi a druhý druh představuje kvantová kryptografie založena na fyzikálních zákonech. Podrobněji se budu zabývat rozdílem mezi těmito typy kryptografie, jejich výhodami a nevýhodami.

---

[1] Kryptografie – šifrování zpráv. Kryptografie se dělí na „klasickou“ kryptografii, která je založena na matematických principech. Patří sem symetrická a asymetrická kryptografie (viz dále). Další druh kryptografie je kvantová kryptografie, která se řadí do nejmladšího odvětví kryptografie. Založena na fyzikálních zákonech.

Práce samozřejmě není zaměřena na ochranu zprávy obálkou, ale na nejmladší druh ochrany informací, a to pomocí kvantové kryptografie. Kvantovou kryptografii můžeme chápat jako způsob distribuce klíče, nejedná se přímo o zabezpečení zprávy pomocí kvantové kryptografie. Kvantová kryptografie využívá přírodní zákony, přesněji zákony fyziky, kvantové mechaniky a zákonů částic. Zjednodušeně řečeno jde o chování jednotlivých fotonů. „Klasická“ kryptografie, symetrická a asymetrická, používá k zabránění zjištění obsahu zprávy nejrůznější matematické klíče, transpozice a kódování.

Kvantovou kryptografii používá řada bank a ve Švýcarsku byla dokonce tato forma šifrování použita při volbách.

I. TEORETICKÁ ČÁST

1 ÚVOD DO KRYPTOGRAFIE

Na úvod bych stručně vysvětlil základní pojmy, které se týkají šifrování a pojmů s šifrováním spojených.

Kryptografie – vědní obor, který se zabývá šifrováním zpráv. Převádí zprávu do podoby, která je čitelná jen se speciální znalostí. Taková znalost se nazývá klíč. Slovo kryptografie pochází z řeckého slova „kryptós“, které znamená „skrytý“, a „gráphein“ znamená psát. Spojením slov dostaneme spojení „skryté psaní“. Osoba zabývající se šifrováním se nazývá kryptograf.

Kryptoanalýza – opak kryptografie. Zabývá se způsoby, jak zjistit původní informaci ze zašifrované zprávy, a to bez použití klíče. Slovo kryptoanalýza pochází také z řečtiny. „Kryptós“ znamená „skrytý“ a „analýein“ představuje „rozvázat“. Osoba, která se zabývá kryptoanalýzou, se nazývá kryptoanalytik.

Kryptologie – věda, která zahrnuje jak kryptografii, tak kryptoanalýzu. Zabývá se jak šifrováním zpráv, tak také dešifrováním zpráv.

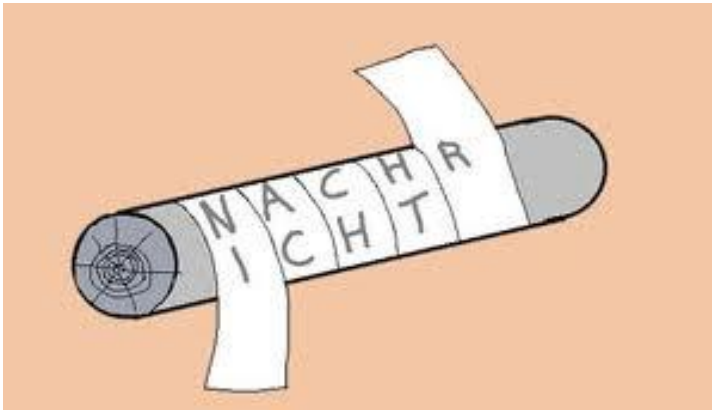
Nepodmíněná bezpečnost – představuje nejvyšší míru bezpečnosti kryptografického systému. Bezpečnost není závislá na žádných předpokladech o schopnostech a technických možnostech útočníka. To znamená, že útočník nezná informace o klíčích. Útočník nemá šanci se dostat k tajným informacím, tyto vlastnosti garantují zákony fyziky a matematiky.

Nutnost utajovat komunikaci provází lidi už tisíce let. Kryptografové vymýšleli složitější a složitější šifry a kryptoanalytici je úspěšně prolamovali. Vznikl souboj kryptografů a kryptoanalytiků, díky němuž vznikají nové způsoby šifrování. Kvantová kryptografie představuje nejmladší způsob předání klíče k zašifrování zprávy.

1.1 Historie kryptografie

Vznik kryptografie můžeme hledat v období vzniku písma, asi před 4000 lety. Kryptografie nachází rozmanité uplatnění v podnikatelském sektoru i v osobním využití. Na obrovský rozmach kryptografie má vliv celá řada faktorů. Nejzásadnější je rozmach internetového obchodování a využívání internetu jako komunikačního kanálu. Elektronické obchodování patří do obliby stále většímu množství lidí po celém světě. Jedna ze zásadních překážek je obava o bezpečnost.

Kryptografie se vyvíjela po staletí, její základy můžeme hledat v Řecku a v Egyptě. Za zmínku stojí jedna z prvních šifrovacích metod, která vznikla právě v Řecku – Skytale. Na dnešní dobu se jednalo o velmi primitivní způsob utajení zprávy. Princip spočíval, že na hůl o určitém průměru se namotal pásek kůže, kde byla napsána zpráva. Poté bylo možné zprávu přečíst jen na holi o stejném průměru. Kdo tento způsob šifrování neznal, pro něj byl na pásku kůže jen shluk náhodných písmen.



Obr. 1. Skytale

[15]

Další významná šifrovací metoda počátečního vývoje byla Caesarova šifra. Rozluštění těchto šifrovacích metod v současné době znamená práci na několik minut.

1.1.1 Vývoj ve 20. století

Kryptografie se vyvíjela po staletí, ovšem až na začátku 20. století došlo k velmi prudkému rozvoji. Tento prudký rozvoj je přisuzován vynalezení telegrafu. Do konce 50. let 20. století se objevila velká řada mechanických šifrovacích přístrojů. V mnoha muzeích a historických výstavách jsou tyto přístroje k nahlédnutí. Velmi oblíbený je anglický Bletchley Park[2], kde prolomil Alan Turing šifrovací stroj Enigmu[3]. Význam dekódování můžeme pozorovat i v řadě současných filmů s tématikou 2. světové války. Pozornost je soustředěna na dopad rozluštění Enigmy a dekódování zpráv před útokem na Pearl Harbor.

[2] Bletchley Park – známý také jako Station X, hlavní dekódovací stanice v Anglii během 2. světové války.
[3] Enigma – Přenosný šifrovací stroj. Používaný od počátku 20. let 20. století, nejdříve pro civilní účely a později ho začaly používat armády (Německo ve 2. světové válce).

V historii byly mnohokrát distribuce a ukládání klíče podceněny. Chyby pramenily z důvodu slabého kryptografického vzdělání nebo podcenění útočníka. Zvláště v období 2. světové války si každý o svém způsobu šifrování myslel, že je neprolomitelný a dokonalý. Mezi nejznámější selhání uložení klíče patří opakované získání kryptografických klíčů z poškozených německých ponorek pro šifrovací stroj Enigma.

Purpurový kód, nazývaný také Purpur, představuje japonský kódovací systém. Japonci používali Purpurový kód od roku 1937 a v průběhu 2. světové války. Byl využívaný ministerstvem zahraničí jako nejspolehlivější kódovací systém určený pro nejtajnější zprávy. Krátce od nasazení Purpuru začal americký kryptolog W. F. Friedman[4] purpurový kód odposlouchávat. Z části jej spolu s manželkou (Elizabeth Smithovou Friedmanovou) prolomil, a to v roce 1940. Bylo nutné shromáždit dostatek informací k částečnému prolomení, neboť rozluštění vyžadovalo vysoké intelektuální požadavky. Po rozluštění Američané měli možnost znát japonské plány a vytvořit účinnou taktiku. Přístroj produkující Purpurový kód se skládal z baterie, stupňovitého přepínače a z rozvodové desky. Stroj měl obsluhu, která zapisovala klíče na daný den. Purpurový kód se později v roce 1939 pokoušeli rozluštit i námořní kryptografové.

S nástupem počítačů si kryptografie prošla velkou změnou. Dříve se šifrování převážně používalo pro vojenské a státní účely, pro jednotlivce a firmy byla kryptografie prakticky nedostupná. V současné době tohle tvrzení neplatí. Kryptografie se stala veřejně používanou v soukromém i státním sektoru za účelem zajištění důvěrnosti a integrity informací. Každý měl a má zájem, aby zprávu dostal jen ten, komu je určena. Vzniká celá řada šifrovacích algoritmů, zejména pro bankovní sektor. Algoritmy jako DES, RSA, DSA a další. Zásluhy na vzrůstající oblibě kryptografie a jejím historickém významu nemá pouze literatura.

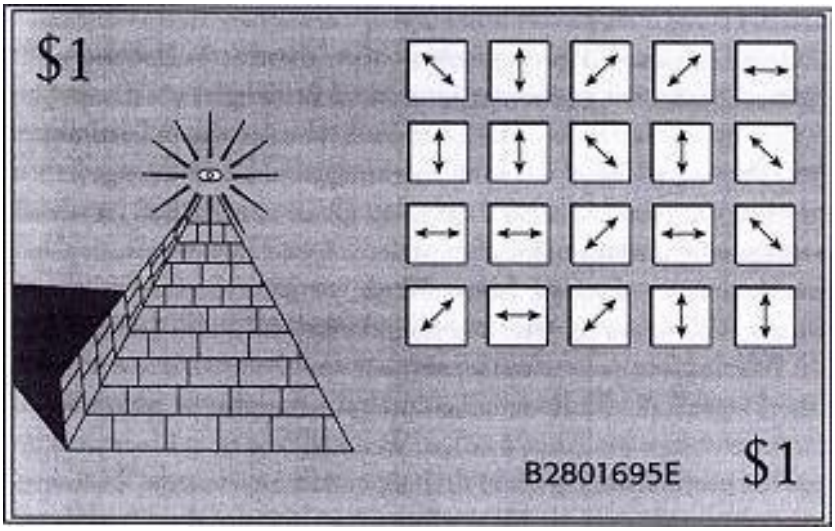
1.1.2 Éra kvantové kryptografie

Objev moderní kvantové teorie v polovině 20. let minulého století byl, jak se ukázalo velmi významný. Přinesl jednu z nejzásadnějších změn fyzikálního světa od doby Isaaca

[4] W. F. Friedman – úspěšný americký kryptolog, narozen 1891 v Kišiněvě (Moldavská SSR). V roce 1892 se s otcem přestěhovali do USA. Pracoval pro NSA (National Security Agency). Zemřel 12. listopadu 1969.

Newtona[5]. Kvantovou teorii lze označit za jeden z nejvýznamnějších objevů 20. století a její přínos za revoluci v chápání fyzikálních procesů. V průběhu 80 let zkoumání a vývoje, které následovalo po objevení kvantové mechaniky, se teorie ukázala jako velmi užitečná v mnoha odvětvích.

Základní kámen kvantové kryptografie položil Stephen Wiesner[6] v 70. letech dvacátého století. Snažil se publikovat své myšlenky pomocí „kvantových peněz“. Jeho přínos byl revoluční, ale sotva někdo pochopil velký potenciál pro budoucí vývoj. Neměl žádnou podporu, aby na svém výzkumu mohl dále pracovat. Nesměl ani publikovat své myšlenky v odborných časopisech. V koncepci Stephena Wiesnera šlo o to, že každá dolarová bankovka obsahovala 20 světelných pastí. Příklad takové bankovky můžeme vidět na obr. 2. Každá z 20 pastí obsahovala foton, který byl polarizován jedním ze čtyř možných způsobů. Každý záznam byl označen jako unikátní sériové číslo. Následně fotony mohly být snímány a obnoveny bankou, která zná exaktní posloupnost polarizovaných filtrů. Tyto filtry potřebují být použity ke čtení sériového čísla. Wiesnerova koncepce byla brilantní, až do dneška nikdo neuspěl ve stavbě robustních fotonových pastí.



Obr. 2. Ukázka kvantové bankovky od Stephena Wiesnera

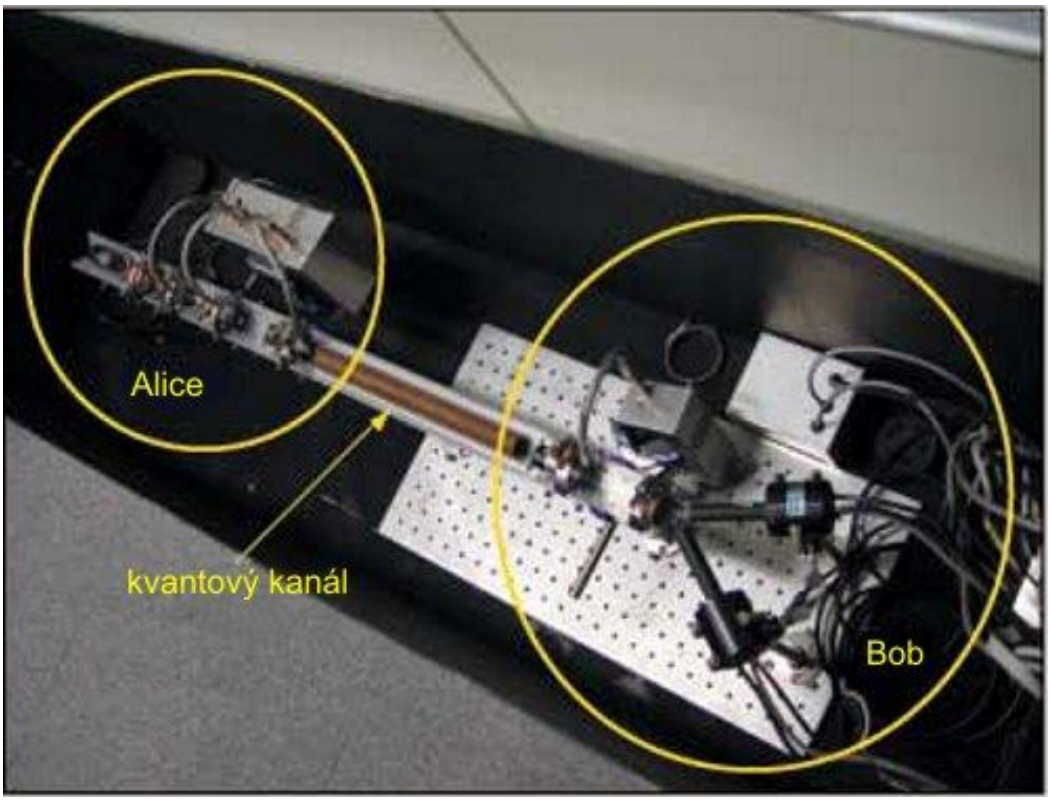
[15]

[5] Isaac Newton – anglický fyzik, matematik, astronom. Považován za jednu z nejvlivnějších osob v dějinách lidstva.

[6] Stephen Wiesner – narozen v roce 1942, vystudoval Columbia University v New Yorku, jako první přišel s nápadem kvantové distribuce klíče.

Další pokrok se datuje roku 1984, kdy Bennett[7] a Brassard[8] navrhli první kvantový kryptografický protokol BB84 [viz 1.5.1]. Komunikační protokol se dočkal vylepšení v podobě verze B92 [viz 1.5.3] v roce 1992. Navrhl jej autor předešlého protokolu Ch. H. Bennett.

Kvantová kryptografie od té doby prochází řadou technických zlepšení. Dnes se aplikuje kvantová kryptografie komerční cestou, jedná se o poměrně drahou záležitost. K přenosu fotonů slouží optická vlákna a k měření polarizace se využívá krystal $CaCO_3$ (uhličitan vápenatý).



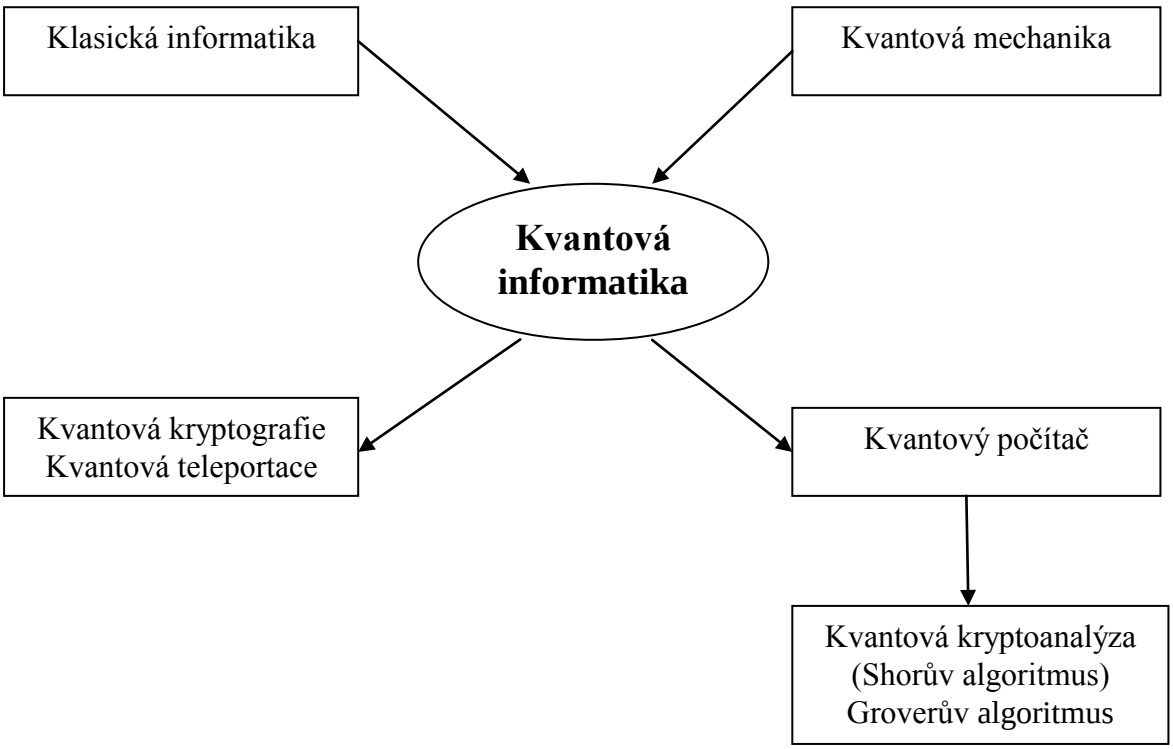
Obr. 3. První systém kvantové kryptografie

[16]

Na obrázku můžeme vidět první systém kvantové kryptografie. Odesílatel a příjemce (Alice a Bob) spolu komunikují prostřednictvím kvantového kanálu, který je v tomhle případě dlouhý 30cm.

[7] Charles H. Bennett – narozen v roce 1943, zaměstnanec IBM, objevitel základů kvantové kryptografie.
[8] Gilles Brassard – narozen v Montrealu v roce 1955, objevitel protokolu pro kvantovou kryptografii.

Rád bych zmínil i historii kvantových počítačů. První zmínka o kvantových počítačích je skloňována se známým fyzikem Richardem Feynmannem[9]. Všiml si, že při simulaci kvantových systémů na klasickém osobním počítači rostou požadavky na výpočetní čas. Tento růst je exponenciální s délkou vstupu. Uvažoval nad otázkou, zda by toho nešlo využít obráceně, což by mohlo vést k podstatnému urychlení chodu některých algoritmů. Definice kvantového počítače se přičítá Davidu Deutschovi[10] v roce 1985. Rozmach odvětví kvantových počítačů nastal v roce 1994, kdy Peter Shor navrhl kvantové algoritmy pro faktorizaci velkých čísel. Do té doby se faktorizace velkých čísel pokládala za principiálně neřešitelnou a na tomhle způsobu fungovaly kryptografické metody. Společnost IBM se řadu let zabývá výzkumem kvantových počítačů. Tyto počítače využívají princip superpozice a linearity kvantové mechaniky.



Obr. 4. Oblasti kvantové informatiky

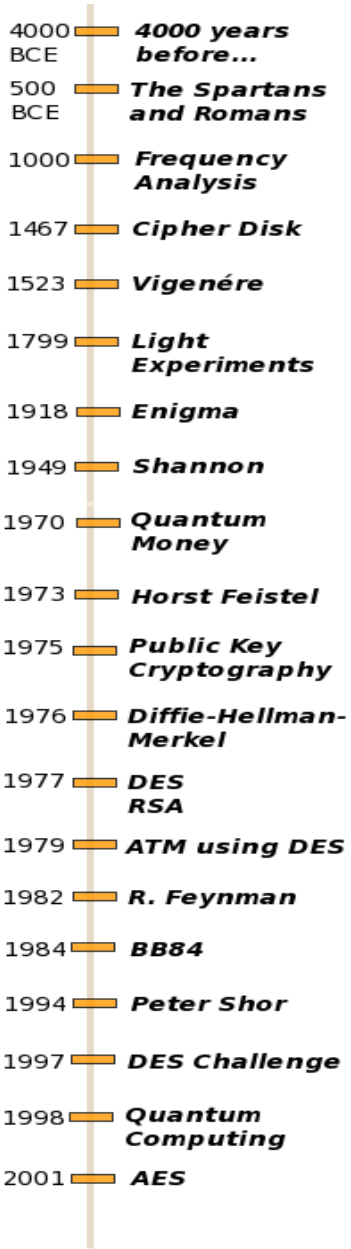
[9] Richard Feynmann – (1918 – 1988), americký fyzik, patřil k největším fyzikům 20. stol.. Pracoval na vývoji jaderné bomby, tzv. projekt Manhattan. V roce 1965 mu byla udělena Nobelova cena. Pracoval na způsobu popisu reakcí elementárních částic poskytujících alternativní náhled na chápání kvantové fyziky.

[10] David Deutsch – narozen 1953, formuloval v roce 1985 první algoritmus navržený pro útok na kvantový počítač. Jeden ze zakladatelů kvantové teorie počítání.

Kvantová kryptografie je oddělená část kvantové informatiky a není přímo závislá na existenci kvantového počítače. Následující schéma ukazuje, jakým způsobem jsou jednotlivé oblasti vzájemně propojeny.

1.1.3 Historický přehled

Na následujícím obrázku můžeme vidět postupný vývoj kryptografie, se zaměřením také na kvantové oblasti, od prvopočátku až do současnosti.

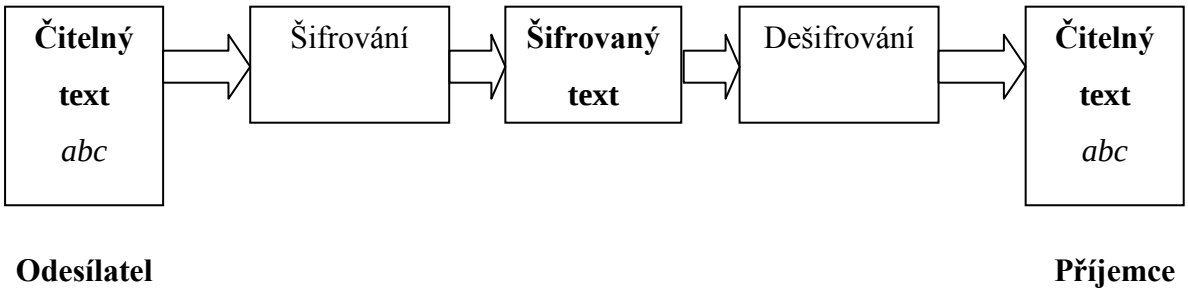


Obr. 5. Milníky kryptografie

[15]

1.2 Seznámení s kryptografií

Pro pochopení slova kryptografie uvedu jednoduchý obrázek. Zjednodušeně lze obrázek popsat následovně. Zprávu, kterou chceme odeslat, zašifrujeme, z původní zprávy vznikne zašifrovaný text. Poté příjemce zprávu dešifruje a dostává původní zprávu. Pojem šifra představuje kryptografický algoritmus, ten převádí čitelný text na šifrovaný text. Obrázek popisuje základní princip kryptografie. Kryptografie se dělí na symetrickou a asymetrickou. Symetrická šifra používá k šifrování i dešifrování stejný klíč, který se nazývá tajný klíč. Asymetrická šifra používá veřejný klíč pro šifrování zprávy a soukromý klíč pro dešifrování. Podrobněji tyto typy kryptografie popíšu později.



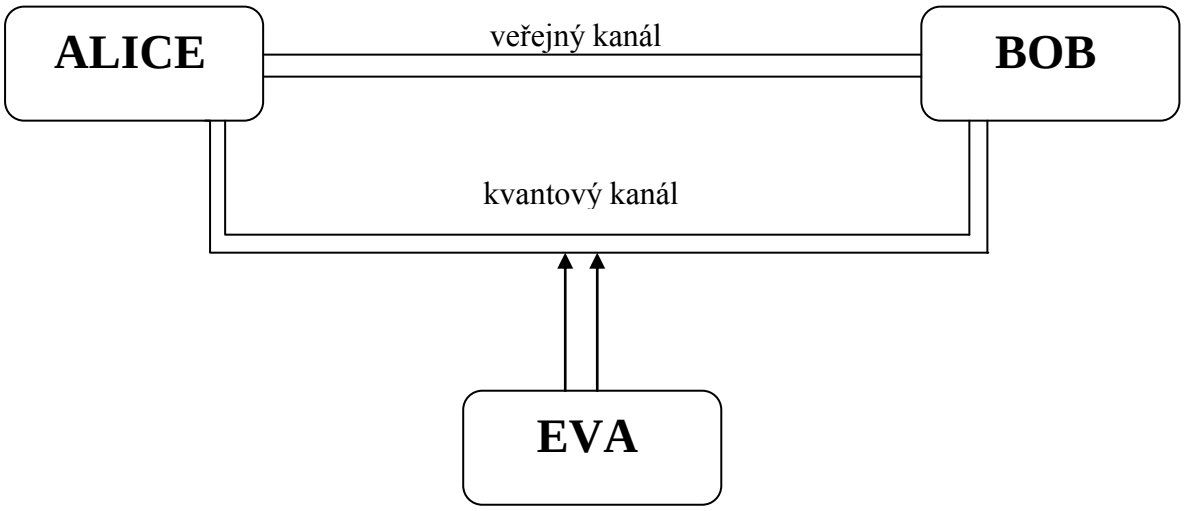
Obr. 6. Princip kryptografie

Slovní spojení „kvantová kryptografie“ představuje metodu pro bezpečný přenos klíče. Její garance bezpečnosti stojí na zákonech fyziky. Kvantová teorie informace v současné době přitahuje obrovský zájem pro její potenciálně revoluční aplikace pro výpočet a bezpečnou komunikaci.

V klasické kryptografii se k zamezení zjištění obsahu přenášené zprávy využívají různé matematické metody. Kvantová kryptografie pracuje na bázi zákonů fyziky, konkrétně na kvantovém chování jednotlivých fotonů světla, a nespoléhá na sílu kryptografického algoritmu. Tento způsob zajišťuje, že informace přenášená fotony se při jakémkoli způsobu odposlechu změní a útok je možné lehce detekovat. Odposlech útočníkovi nepřinese dostatečnou informaci pro efektivní narušení bezpečnosti. Kvantovou mechaniku lze využít k samotnému vysílání informací, ale i pro zjišťování, zda se toto vysílání snaží někdo zachytit. Z důvodu těchto vlastností se kvantová kryptografie převážně používá k distribuci klíčů. Vytvoření tajného a bezpečného klíče mezi dvěma stranami umožňuje tok jednotlivých fotonů. Při zřízení klíče vyšle jeden uživatel druhému uživateli náhodnou

sekvenci. Jestliže dojde k narušení přenosu, bude toto narušení odhaleno a celý cyklus začne znovu. Sekvence, která nebyla zachycena, je použita jako základ klíče.

Kvantová distribuce klíče funguje na přenosu klíče pomocí jednotlivých fotonů. Účastníky komunikace v kryptografii a v kvantové kryptografii zpravidla představují Alice, Bob a Eva. Alice odesílá klíč, Bob klíč přijímá a Eva představuje narušitele, snaží se odposlechnout klíč, aniž by byla odhalena. Alici a Boba spojují dva kanály. První kanál je kvantový, který posílá klíč. Druhý kanál se nazývá veřejný a slouží pro testování dosažených výsledků. Důležitou informací je, že veřejný kanál může být kýmkoliv monitorován, ale musí být v tomto kanále zajištěna autentizace[11]. Úkolem autentizace v tomto případě je, jak zajistit, aby Alice a Bob věděli, že komunikují spolu.



Obr. 7. Komunikace v kvantové kryptografii

1.3 Kvantové zpracování informace

Kvantové zpracování informace představuje další a velmi významnou tendenci v oblasti zpracování informace, komunikace a bezpečnosti. Použitím zákonů kvantové fyziky je

[11] Autentizace – představuje proces nebo samotné ověření identity. Využití především v oblasti počítačů a internetových serverů. Ověřuje, kdo je daný návštěvník stránky nebo systému, a jaké mu přísluší pravomoce a oprávnění.

možné dosáhnout cílů, které nejdou řešit klasickými metodami. Nebo popřípadě úlohy řešit efektivněji.

Kvantová logika pozměnila způsob použití základních spojek „a“ a „nebo“. Ve 30. letech 20. stol. začal kvantový svět nabízet jiný typ logiky. Například elektron může být v bodě „1“ a v bodě „2“, ale také v libovolném stavu superpozice mezi „1“ a „2“. Tento kvantový pohled představuje tzv. prostřední, třetí možnost. Od toho se také někdy používá název tříhodnotová logika. Klasická logika zformulovaná Aristotelem žádný třetí stav nezná. Konkrétní formu kvantové logiky vypracovali Garrett Birkhoff[12] a John von Neumann[13].

Oblasti kvantového zpracování informace:

- Distribuce kryptografických klíčů (tímto tématem se budu později zabývat podrobněji).
- Exponenciální zrychlení některých algoritmů, např. vyhledání v databázích a faktorizace čísel[14].
- Navýšení kapacity komunikačního kanálu atd.

1.3.1 Klasické vs. kvantové zpracování informace

„Zatímco základním prvkem při klasickém zpracování informace je bit, který může nabývat dvou hodnot, u kvantového zpracování je to kvantový bit (qubit), který může nabývat nespočetně mnoha hodnot. Při kvantovém zpracování informace, komunikaci a v kryptografii se využívají speciální, a často zdánlivě magické kvantové jevy jako jsou entanglování a nelokální efekty. Jednou ze zajímavých aplikací kvantových jevů je kvantová teleportace.“[15]

---

[12] Garrett Birkhoff – (1911 – 1996). Americký matematik, zajímal se o konstruování prvních elektronických počítačů, pracoval například pro společnost General Motors.

[13] John von Neumann – (1903 – 1957). Maďarský matematik, přispěl značnou měrou do oborů kvantová fyzika, ekonomika, informatika a dalších matematických disciplín.

[14] Faktorizace čísel – rozložení čísla na součin menších čísel. Nejčastější použití je rozklad celého čísla na součin prvočísel. Využití v matematice a jejích aplikacích.

[15] Prof. RNDr. GRUSKA, DrSc. Josef. Kvantové zpracování informace a kryptografie [online]. 1. Brno : [cit. 2011-01-13]. Fakulta informatiky Masarykovy univerzity. Dostupné z WWW: <http://www.fi.muni.cz/research/formal-methods/quantum.xhtml>.

Fyzikální popis:

- Klasické vyjádření: Klasická fyzika je založena na principech vytvořených před vznikem kvantové fyziky. Tuto oblast popisují rovnice.
- Kvantové vyjádření: Postavené na teoriích, kde hlavním pojmem je kvantum[16]. Oproti klasické fyzice se zde nepopisuje stav systému přiřazením daných hodnot fyzikálních veličin. Předpokládá se i existence stavů, kde je výsledek měření znám jenom v oblasti pravděpodobnosti.

Nositel informace:

- Klasické vyjádření: Makroskopické veličiny[17], např. proud, napětí, délka atd.
- Kvantové vyjádření: Kvantový stav (foton) je stav systému popsaný vlnovou funkcí. Tato vlnová funkce je vlastní funkcí operátoru patřící dané fyzikální veličině.

Jednotka informace:

- Klasické vyjádření: Reprezentováno jednotkou bit (stav 0 nebo 1).
- Kvantové vyjádření: Tzv. qbit (libovolná kombinace 0 a 1).

Klasické informace lze libovolně kopírovat, lze vytvořit zcela identickou kopii dané zprávy. Naopak z kvantové informace nelze vytvořit identickou kopii neznámého kvantového stavu.

1.3.2 Předpoklady kvantového zpracování informace

Klasické zpracování informace je dnes technologicky dostupné, a tudíž velmi rozšířené. Kvantové zpracování informace nabízí efektivnější algoritmy a vyšší bezpečnost přenášených dat. Představuje také rozmanitou oblast s mnoha tématy pro výzkum.

[16] Kvantum – množství.
[17] Makroskopické veličiny – označení pro veličiny, které jsou pozorovatelné pouhým okem.

Existuje několik podstatných argumentů, proč je kvantové zpracování informace důležitá součást vědy:

a) Kvantové zpracování informace má předpoklad, že bude podstatou pro pochopení složitých kvantových systémů a jevů.

b) Kvantové zpracování informace se v mnoha případech jeví jako efektivnější pro řešení známých problémů.

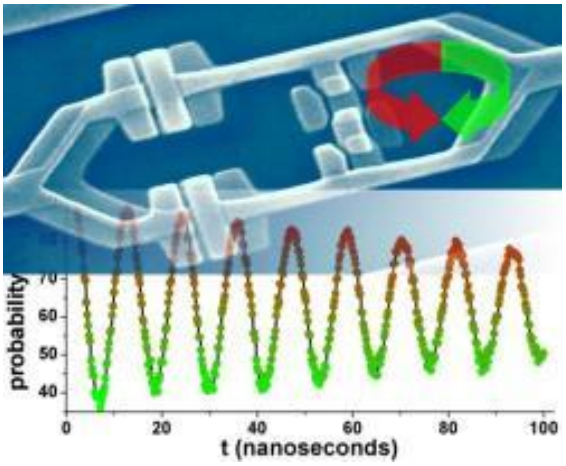
c) Předpokládá se, že zkoumání kvantového zpracování informace povede k novým a pravděpodobně přínosným technologiím.

d) Řada vědních disciplín a vývoj technologií spějí do stavu, který bude vyžadovat znalosti manipulace, izolování a přenos mikroskopických předmětů.

e) A především, o čem v téhle práci jde, že nabízí zcela novou úroveň bezpečnosti kvantové kryptografie. Velký rozmach se očekává v nejbližších letech.

1.3.3 Kvantový bit

Základní stavební jednotka běžného osobního počítače je tranzistor, který představuje dva stabilní stavy (zapnuto, vypnuto). Jeden z těchto stavů odpovídá dvojkové číslici, bitu „0“, a druhý bitu „1“. V kvantovém počítači se mohou základní jednotky (např. atomy) vyskytovat v superponovaných stavech. To znamená, mohou představovat zároveň 0 nebo 1. Kvantový systém v superponovaném stavu není ani ve stavu 0 nebo 1, ale ani mezi nimi. Přesnější tvrzení je, že systém je ve stavu 0 a zároveň stavu 1. Měřením qubitu získáme hodnotu odpovídající právě jednomu vlastnímu stavu. Pro jednoznačné rozlišení od klasických bitů nesou název kvantové bity (qubity). Posloupnost několika kvantových bitů se nazývá kvantový registr. Osm spojených qubitů tvoří qubyte, jedná se o stejné názvosloví jako u klasických bitů.



Obr. 8. Schéma q-bitu

[15]

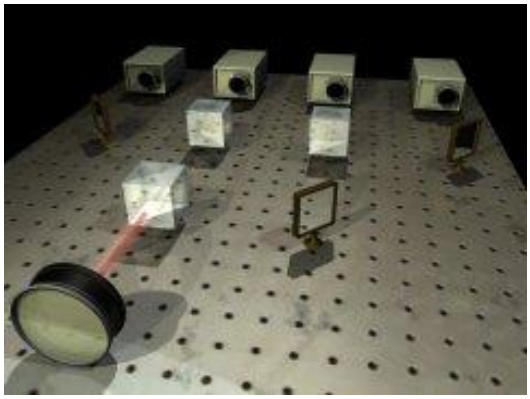
Jeden qubit může nabývat dvou stavů – 0 nebo 1. Dva qubity čtyři stavy (00, 01, 10 nebo 11), tři qubity osm stavů (000, 001, 010, 100, 011, 101, 110, 111) atd. Tady je důležité si uvědomit, že pomocí jednoho qubitu lze provést dva výpočty zároveň. Se dvěma qubity jsou to čtyři výpočty. Celkově tak počet současných stavů je roven 2^n, kde *n* představuje počet qubitů. Na první pohled to není nic zvláštního. Ovšem při použití například 100 qubitů dostaneme obrovské číslo v řádech miliard výpočtů. Měřením jednoho qubitu získáme nejvýše jeden bit klasické informace. I malý počet kvantových bitů poskytuje velké výpočetní možnosti. Tohle už je velmi zajímavé a slibné pro vývoj kvantových počítačů.

1.4 Vzdálenost v kvantové kryptografii

Problém, který omezuje kvantovou kryptografii, je v omezené vzdálenosti mezi odesílatelem a příjemcem. Šifrovací klíče mezi odesílatelem a příjemcem je možné odesílat jen na relativně krátkou vzdálenost, což činí kvantovou kryptografii částečně omezenou. Zaznamenaný rekord byl 148,7km v březnu roku 2007 v Los Alamos. Vzdálenost byla dosažena po optickém vlákně.

Před dvěma lety vědci z Toshiba´s European laboratory v Cambridge přišli s „průlomovým“ řešením. Zkonstruovali zařízení, které by mělo být schopné posílat šifrovací klíče na prakticky neomezenou vzdálenost. Princip je založen na pravidelném zesilování fotonového kvantového signálu.

Technologie je stále ve vývoji, ale řada odborníků jí předpovídá slibnou budoucnost. Uplatnit by se měla ve špionážních službách a vojenských operacích.



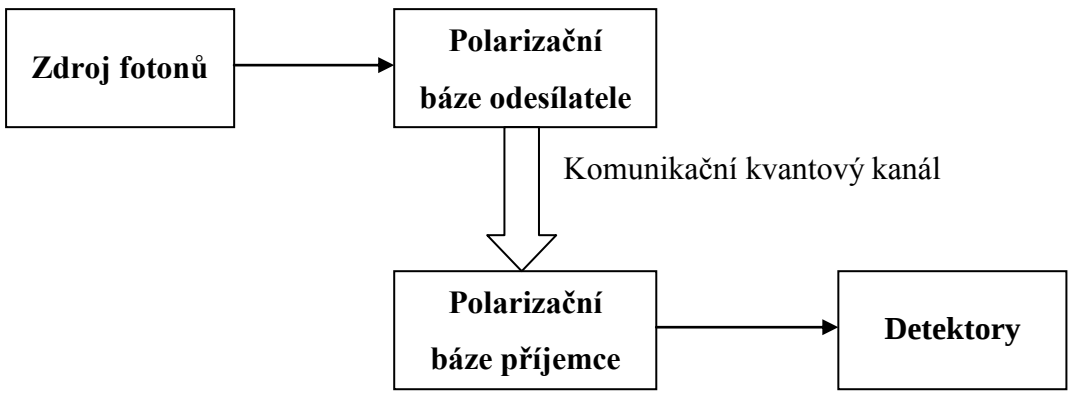
Obr. 9. Animace kvantové kryptografie

[www.osel.cz]

1.5 Protokoly v kvantové kryptografii

Klíč v kvantové kryptografii je sestaven pomocí kvantových stavů fotonů. Bezpečnost je založena převážně na nemožnosti dělení fotonu na více částí a nemožnost současného měření určitých veličin.

V následující části budou zmíněny některé existující protokoly kvantové kryptografie. Od nejznámějšího protokolu BB84 až po méně známé a používané protokoly. Kvantové protokoly nejsou sestaveny jen na teoretickém principu. Provádí se i prakticky, některé ovšem na krátké vzdálenosti nebo optickým kabelem. Každý protokol zobrazuje základní prvky jako zdroje fotonů, polarizační báze odesílatele, polarizační báze příjemce a detektory. Polarizační báze odesílatele a příjemce spojuje kvantový komunikační kanál.

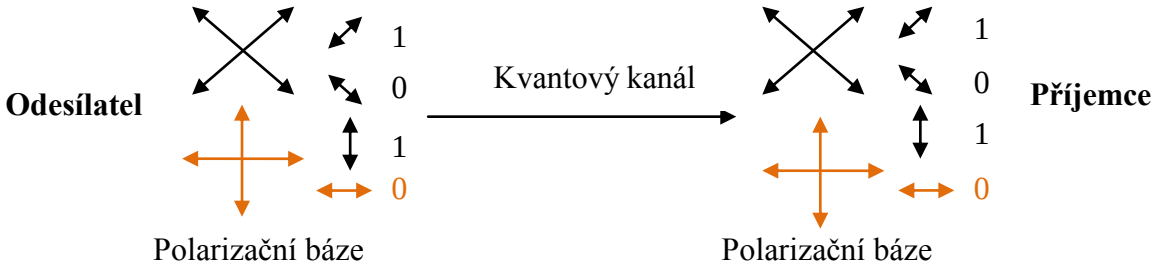


Obr. 10. Obecné schéma kvantového systému

1.5.1 Kvantový protokol BB84

Navržen v roce 1984 americkými vědci Ch. H. Bernettem a G. Brassardem. Jak jsem již zmínil, název vznikl z prvních písmen autorů a roku vytvoření (BB84). Protokol BB84 vychází z tzv. „kvantových peněz“ od Stephena Wiesnera (viz kapitola 1.1.2).

Princip funkce protokolu BB84 využívá lineárních a diagonálních polarizačních bází (možnost využít i kruhovou polarizaci fotonů).



Obr. 11. Princip protokolu BB84

Ukázka principu protokolu BB84 v případě, že odesílatel a příjemce použijí stejnou polarizační bázi.

Pravděpodobnost ***p*** odhalení útočníka u protokolu BB84:

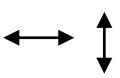
$$p = 1 - \left(\frac{3}{4}\right)^n$$

Kde *n* je počet obětovaných bitů

Lineární báze

Označení: +

Odklon 0º nebo 90º



Diagonální báze

Označení: x

Odklon 45º nebo 135º

Při kódování je možné využít jednu bázi, ale pro větší bezpečnost se používají dvě báze. Přenos klíče protokolu BB84 jsem podrobněji popsal v kapitole [2.2.4].

1.5.2 Protokol E91

S protokolem E91 přišel Artur Ekert v roce 1991, tento protokol se také nazývá EPR protokol. EPR protokol využívá zapletené páry fotonů. Tyto páry fotonů jsou vytvořeny odesílatelem nebo nějakým odděleným zdrojem.

Činnost protokolu je založena na dvou vlastnostech zapletení. Nejprve jsou zapletené fotony korelované (po naměření jakékoliv polarizace na jedné částici naměříme opačnou polarizaci na druhé částici). Odesílatel a příjemce měří, zda mají fotony vertikální nebo vodorovnou polarizaci. Vždy dostanou stejnou odpověď s pravděpodobností 100%. Stejná pravděpodobnost nastane, když oba měří jiný doplňkový pár (orthogonal). Výsledky jsou náhodné, odesílatel nemůže předpovídat, zda obdrží vertikální nebo vodorovnou polarizaci.

Pokus o naslouchání naruší korelace a odesílatel i příjemce odposlech odhalí. Pravděpodobnost ***p*** odhalení útočníka:

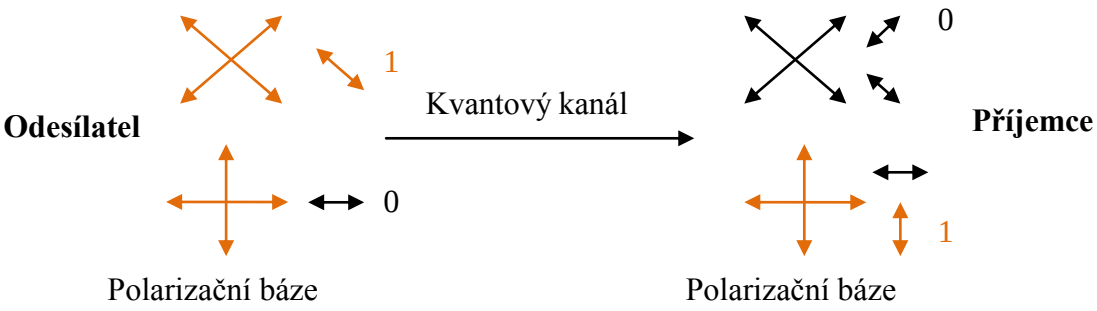
$$p = 1 - \left(\frac{2}{3}\right)^n$$

Kde *n* je počet obětovaných bitů

1.5.3 Protokol B92

V roce 1992 navrhl Charles H. Bennett, autor předešlého protokolu BB94, protokol s názvem B92. Využívá 2 neortogonální stavy polarizace fotonu, je klasifikován jako dvoustavový protokol.

1. Odesílatel vybere polarizační schémata a bity a sdělí je příjemci.
2. Následuje vysílání fotonů.
3. Odesílatel náhodně vygeneruje klíč a po kvantovém kanálu klíč posílá příjemci.
4. Příjemce náhodně volí polarizační báze a zaznamenává výsledky svých měření. Celkem jsou možné 4 typy výsledků.
5. Odeslání celého klíče. Komunikace přes veřejný kanál. Příjemce informuje odesílatele, kde byl schopen rozpoznat fotony. Sdělením několika bitů z klíče zjistí, jestli jejich komunikace byla či nebyla odposlouchávána.



Obr. 12. Princip protokolu B92

Odesílatel volí opačnou bázi než příjemce. Výhoda protokolu oproti protokolu BB84 spočívá v mnohem jednodušší komunikaci. Příjemce oznamuje jen správně obdržené qubity. Teoretické podklady prezentují protokol jako 100% bezpečný. V praktickém použití vzniká větší výskyt chyb, nutné počítat s určitými ztrátami, které vzniknou ve vlákně. Toto může zapříčinit složitější odhalení útočníka.

Výpočet pravděpodobnosti ***p*** odhalení útočníka u protokolu B92:

$$p = 1 - \left(\frac{7}{8}\right)^{n}$$

Kde **n** je počet obětovaných bitů

1.5.4 Šestistavový protokol

Šestistavový protokol vychází z protokolu BB84. Liší se tím, že polarizace je možná v 6 směrech. Lineární a diagonální polarizace, známá z protokolu BB84, a také kruhová polarizace.

Druh polarizovaného fotonu	Hodnota polarizovaného fotonu
	0
	1
↗	0
↖	1
↔	0
↕	1

Tab. 1. Polarizace fotonu u šestistavového protokolu

Přenos klíče je obdobný jako u protokolu BB84. Odesílatel si zvolí bity pro jednotlivé polarizace, jak můžeme vidět v Tab. 2. Následuje náhodná změna podle polarizace vygenerovaného klíče. Příjemce náhodně vybírá polarizace a obdržené bity si ukládá. Po přenosu klíče komunikace probíhá pomocí běžného kanálu. Příjemce oznámí odesílateli pořadí, jak použil báze. Odesílatel reaguje, ve kterých bitech se společně shodli. Zbylé bity již netvoří klíč. I zde funguje obětování bitů pro případné zjištění odposlechu. Pokud hodnoty obětovaných bitů jsou stejné, útok není odposloucháván. Vyskytne se jen malé procento chybných bitů, které je způsobeno chybami v kvantovém kanále.

Šestistavový protokol disponuje pravděpodobností ***p*** odhalení útočníka:

$$p = 1 - \left(\frac{2}{3}\right)^n$$

Kde **n** je počet obětovaných bitů

1.5.5 Protokol SARG04

V roce 2004 navrhli Valerio Scarani, Antonio Acín, Grégoire Ribordy a Nicolas Gisin čtyřstavový protokol SARG04. Název protokolu vznikl od počátečních písmen svých objevitelů a roku navržení. Protokol SARG04 vychází z protokolu BB84, jedná se o modifikovanou verzi. Kvantový přenos pracuje na stejném principu, rozdíl v protokolech je ve veřejné diskuzi.

Pravděpodobnost ***p*** odhalení útočníka je dána vztahem:

$$p = 1 - \left(\frac{3}{4}\right)^n$$

Kde **n** je počet obětovaných bitů

2 SROVNÁNÍ „KLASICKÉ“ A KVANTOVÉ KRYPTOGRAFIE

Abychom „klasickou“ (matematickou) kryptografii a kvantovou kryptografii mohli srovnat, je třeba si oba pojmy vysvětlit. Hlavní rozdíl spočívá, jak již bylo řečeno, že klasická kryptografie využívá k utajení zprávy matematické metody. Například Vernamova šifra je založena na posunu písmen o několik pozic v abecedě. Naopak kvantová kryptografie stojí na přírodních zákonech.

2.1 Matematická kryptografie

Kryptografie s veřejným klíčem pracuje na jednoduchém principu, ale objevena byla teprve v 90. letech minulého století. Předtím platilo pravidlo, že se používal jeden a ten samý klíč k zašifrování i rozšifrování zprávy. Tomuto druhu kryptografie se říká symetrická kryptografie. S nástupem asymetrické kryptografie vznikla kryptografie se dvěma klíči. Z toho vychází, že kryptografii z pohledu použití dělíme na symetrickou a asymetrickou.

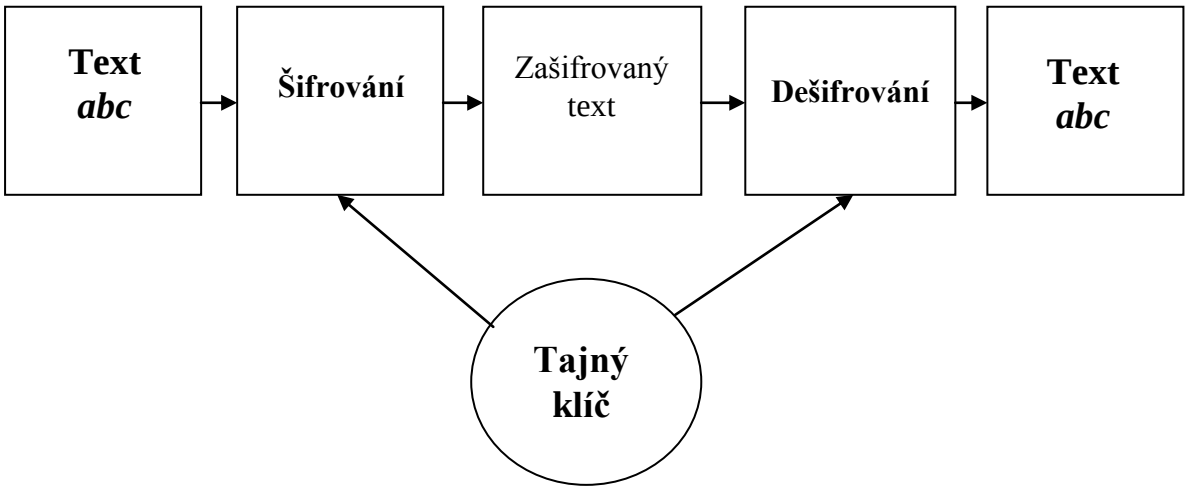
2.1.1 Symetrická kryptografie

Symetrickému šifrování se také někdy říká konvenční šifrování. Pro šifrování i dešifrování zprávy používá jeden šifrovací klíč (tajný klíč), který musí být znám oběma uživatelům (odesílateli i příjemci). Mezi výhody symetrických šifrovacích algoritmů patří rychlost. Algoritmy jsou velmi rychlé, rychlejší než asymetrické šifrovací algoritmy. Další velká výhoda spočívá v nenáročnosti na výpočetní výkon. Měřením bylo zjištěno, že zatížení je až 1000x menší než při použití asymetrického šifrování. Využití zpravidla pro zabezpečení ukládaných dat (na HDD, přenosná média atd.). Největší „nevýhoda“ symetrické kryptografie je především použití jednoho klíče k šifrování i dešifrování zprávy. Nějakým způsobem se musí tajný klíč dostat od odesílatele k příjemci. Jako řešení se nabízí poslat klíč zabezpečeným přenosem. Ovšem existuje-li zabezpečený přenos mezi odesílatelem a příjemcem, potom není třeba zprávu nebo informaci šifrovat. Nastává možnost využít zabezpečený přenos pro odeslání zprávy a data nešifrovat. Symetrické algoritmy se často používají společně v kombinaci s asymetrickými, aby byly využity jejich jednotlivé výhody.

Bezpečná komunikace řešená symetrickou šifrou:

- jednoduchá implementace,

- rychlé a „rozumné“ délky klíče.



Obr. 13. Princip funkce symetrického šifrování

Symetrická kryptografie se dělí na proudové šifry a blokové šifry.

Jak již plyne z názvu, u proudových šifer probíhá šifrování postupně bit po bitu. Každý bit je zvlášť zašifrován a poté také dešifrován. Na závěr jsou bity složeny do výchozí podoby. Například soubor s dokumentem.

Proudové šifry:

a) RC4 – Navrhl Ronald Rivest (RC je zkratka pro **R**ivest´s **C**ipher). Vstupem pro RC4 může být klíč o libovolné délce až 256 bajtů.

b) FISH – Vznikla ve společnosti Siemens v roce 1993. Poměrně rychlý šifrovací algoritmus, s dostatečnou délkou klíče.

Další druh symetrického šifrování představují blokové šifry, které jsou více rozšířené než proudové. Pracují na principu, že původní bitový sled rozdělí na tzv. bitová slova. Všechna slova musí mít stejnou velikost, popřípadě jsou vhodně doplněna bitovou šifrou. Nejvíce rozšířené jsou verze šifrování 64 bitů, 128 bitů a 256 bitů.

Vybrané příklady blokových šifer:

a) DES – **D**ata **E**ncryption **S**tandard. Byl vyvinut firmou IBM a schválen vládou USA jako oficiální šifrovací standard. Šifra DES využívá bloky o velikosti 64 bitů a délka klíče je 56 bitů. DES byl prolomen v roce 1997 útokem hrubou silou. Nejvhodnější využití DES je šifrování souborů na pevném disku. Používá se již málo, nedostatečné zabezpečení.

b) IDEA – Klíč délky 128 bitů a pracuje po 64 bitových blocích. Pravděpodobně nejbezpečnější blokový algoritmus. IDEA je patentována v řadě evropských zemích a USA. Přibližně dvakrát rychlejší než algoritmus DES a zároveň nabízí vyšší úroveň bezpečnosti.

c) Blowfish – 64 bitový šifrovací algoritmus s proměnnou délkou klíče. Jedná se o velmi silný a bezpečný šifrovací algoritmus. Bezpečnost byla prověřena mnoha testy.

d) AES – Advanced Encryption Standard. Délka klíče může být 128, 192 nebo 256 bitů. Šifruje data postupně v blocích s pevnou délkou 128 bitů. Výhoda je vysoká rychlost šifrování a není veřejně známo žádné úspěšné prolomení této metody.

e) Další blokové šifry např.: GOST, RC2, Triple DES, Twofish.

2.1.2 Asymetrická kryptografie

U symetrického šifrování byl problém s výměnou klíče. Řešila se otázka, jak šifrovací klíč doručit k příjemci. Situace se stala kritická při nástupu elektronické komunikace. Na tento popud vzniká asymetrická kryptografie.

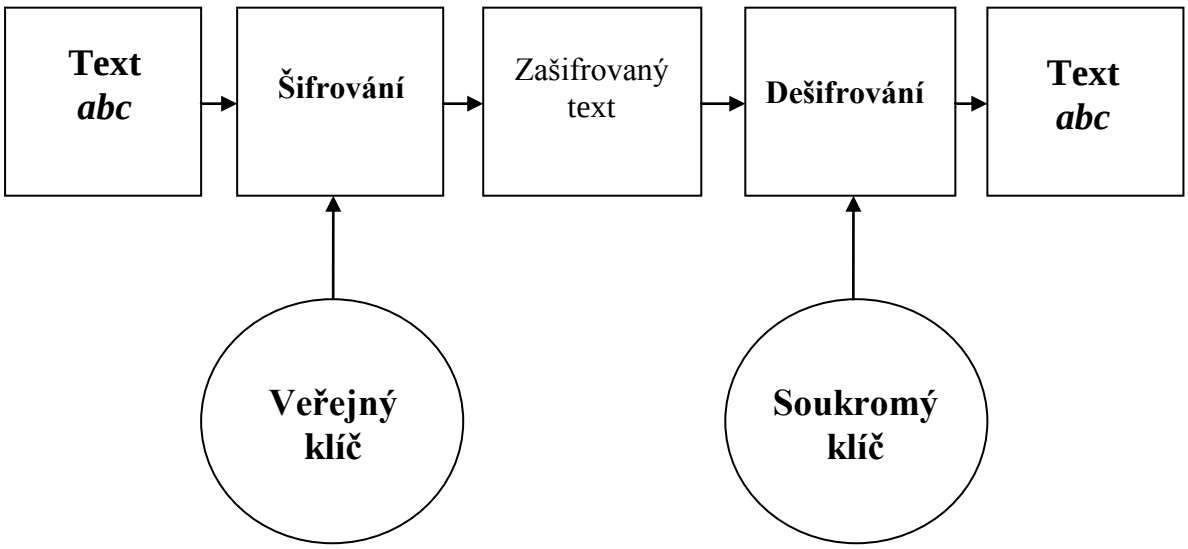
Asymetrické šifrování v roce 1975 navrhl Whitfield Diffie[18]. Princip asymetrického šifrování spočívá v použití dvou odlišných klíčů, veřejného a soukromého. Veřejný a soukromý klíč se dohromady nazývají klíčový pár. Toto je základní rozdíl oproti symetrické kryptografii. Veřejný klíč poskytujeme veřejnosti, ke klíči má přístup každý, a

[18] Whitfield Diffie – americký kryptograf, narozen v roce 1944.

soukromý klíč si chráníme, slouží pro naše používání. Při zaslání zprávy šifrované asymetrickým algoritmem musím znát veřejnou část klíče příjemce. Klíč veřejný je určen k šifrování. Tento klíč majitel veřejně umístí, například na své internetové stránky, a kdokoliv může tento klíč použít k šifrování zprávy pro vlastníka tohoto klíče. Soukromý klíč je dešifrovací. Vlastník klíč musí držet v tajnosti a pomocí tohoto klíče dešifruje zprávy zašifrované jeho veřejným klíčem.

Fungování asymetrického šifrování spočívá v jednocestných funkcích. Tyto funkce jsou v jednom směru lehce proveditelné. Například při práci s velkými čísly jde snadno spočítat součin dvou prvočísel, ale vypočítat z výsledku původní prvočísla zabere více času.

Výhody asymetrického šifrování spočívají v možnostech klíč přenášet i nezabezpečeným kanálem. Počet klíčů roste lineárně s počtem komunikujících dvojic. Asymetrické šifrování je vhodné pro elektronické podepisování dokumentů. Nevýhoda spočívá v o mnohem nižší rychlosti než u symetrického šifrování.



Obr. 14. Princip funkce asymetrického šifrování

Asymetrické šifrování se používá společně v kombinaci se symetrickým šifrováním, aby bylo využito jednotlivých výhod. Data se zašifrují rychlou symetrickou šifrou a otisk dat je zašifrován asymetrickým algoritmem.

Nejpoužívanější asymetrické algoritmy a protokoly:

a) RSA – Vynalezen v roce 1978 Ronem **R**ivestem, Adi **S**hamirem a Lenem **A**dlemanem. Název odvozen z počátečních písmen příjmení zakladatelů. Do roku 2000 byla šifra patentována pro Severní Ameriku. Matematickým problémem spojeným s šifrou RSA je rozložit velké číslo na prvočísla. Velikost bloků i klíčů bývá mnohem větší než u symetrických šifer. Typická velikost bloku je 640 bitů, 1024 bitů nebo dnes běžně používaná a doporučená velikost 2040 bitů. Uplatnění najdou pro šifrování digitálních podpisů nebo pro šifrování klíčů symetrických algoritmů.

b) DSA – Představuje zkratku **D**igital **S**ignature **A**lgorithm. Standard americké vlády pro digitální podpis. Vznikl v srpnu roku 1991 v americkém institutu NIST[19]. Vhodný pro využití ke generování digitálních podpisů, ne ovšem k šifrování dat.

c) Diffie Hellman – Vynalezli v roce 1976 Whitfield Diffie a Martin Hellman. První praktické využití metody vytvoření tajných sdílených informací na nechráněném komunikačním kanále. Umožňuje vytvořit přes nezabezpečený kanál mezi komunikačními stranami šifrované spojení, a to bez předchozího dohodnutí šifrovacího klíče. Základní myšlenkou je, že i kdyby někdo dokázal zachytit komunikaci potřebnou pro dohodu na klíči, nebyl by schopen klíč vypočítat. Známá nevýhoda protokolu je proražení útokem typu Man in the middle[20] z důvodu neumožnění autentizace[21] účastníků.

[19] NIST – National Institute of Standards and Technology. Jedná se o Národní institut standardů a technologie. Laboratoř měřících standardů pod ministerstvem obchodu USA. Úkolem je podpora konkurenceschopnosti USA a inovace. Zaměstnává asi 2900 vědců, techniků atd.

[20] Man in the middle – V překladu „člověk uprostřed“. Odposlouchává komunikaci mezi účastníky, stane se aktivním prostředníkem komunikace.

[21] Autentizace – Ověření identity. Proběhne – li proces autentizace, pak nastává autorizace, to je schválení, ověření přístupu atd.

2.2 Kvantová kryptografie

Kvantová kryptografie představuje poslední článek ve vývoji odvětví kryptografie. Nástup kvantové kryptografie se před 10 lety odhadoval ve větší míře rozšíření a použití. V dnešní době používá kvantovou kryptografii spousta bank a ve Švýcarsku, jak již jsem zmínil, byla použita při volbách jako forma šifrování. V soukromém sektoru kvantová kryptografie nedosahuje zatím zdaleka rozšíření „klasické“ kryptografie.

Vadim Makarov z univerzity v norském Trondheimu tvrdí: „Většina podob používané kvantové kryptografie na dnešním trhu je zranitelná. Vychází z názoru, že nejde o zpochybnění teoretických základů, ale o existující problém konkrétních systémů. Konkrétní uspořádání detektorů laserových pulzů.“

2.2.1 Kvantová teorie

Zrod kvantové teorie se datuje na počátek 20. století. Existuje řada experimentů a jevů, které předcházely objevení kvantové teorie. Patří sem jev záření absolutně černého tělesa[22], fotoelektrický jev[23], ohyb elektronů[24], Bohrův paradox[25], nekomutativnost aktu měření[26] a neurčitost měření[27]. Vznikla na popud výsledků některých pokusů na jedné straně a jejich popisem na druhé straně. Významným impulzem k rozvoji byla de Broglieho hypotéza pojednávající o dualitě částicových a vlnových vlastností klasických částí. Kvantová teorie popisuje chování a znaky subatomárních částic[28] a fyzikálních polí. Základem kvantové teorie je kvantová mechanika zabývající se pohyby elementárních částic.

---

[22] S myšlenkou přišel M. Planck v roce 1901. Dokázal, že shoda mezi experimentálně naměřenými křivkami záření těles a teorií jde docílit pomocí energie záření, která je kvantována.

[23] Objeven fyzikem Albertem Einsteinem v roce 1905. Pokusné výsledky s trháním elektronů z vrchní části kovů za účasti záření lze vysvětlit, je-li záření složeno z oddělených částic (kvant), které pojmenoval fotony. Energie fotonu je spotřebovaná vytržením elektronu na jeho kinetickou energii.

[24] Částice se mohou jevit v některých situacích jako vlnění.

[25] Podle Maxwellových rovnic elektrony obíhající v atomech kolem jádra by měly ztrácet energii zářením a po spirále se přibližovat k jádru.

[26] Měření ve světě atomů je závislé na pořadí. Dostáváme různé výsledky závislé na pořadí měření.

[27] Existují veličiny, které nejde současně měřit s neomezenou přesností. Příkladem je poloha a rychlost.

[28] Subatomární částice – pojmenování pro částice menší než atom. Takové částice jsou např. nukleony, z nich se skládá atomové jádro. Nukleon představuje název pro proton a neutron.

Kvantová teorie neposkytuje přesné hodnoty měření, pouze předvídá možné hodnoty. Při charakterizování jevů je nutné použít klasické fyziky, ta vyjadřuje fakta, z kterých vycházíme.

Kvantová teorie a její součásti, jako kvantová mechanika, kvantová teorie pole atd., jsou stále rozvíjeny a zdokonalovány. Vědecká pracoviště na celém světě se každodenně zabývají zdokonalováním a objevováním neobjeveného. Kvantová teorie se jeví jako mimořádně úspěšná při popisu různých jevů probíhajících zejména ve světě částic.

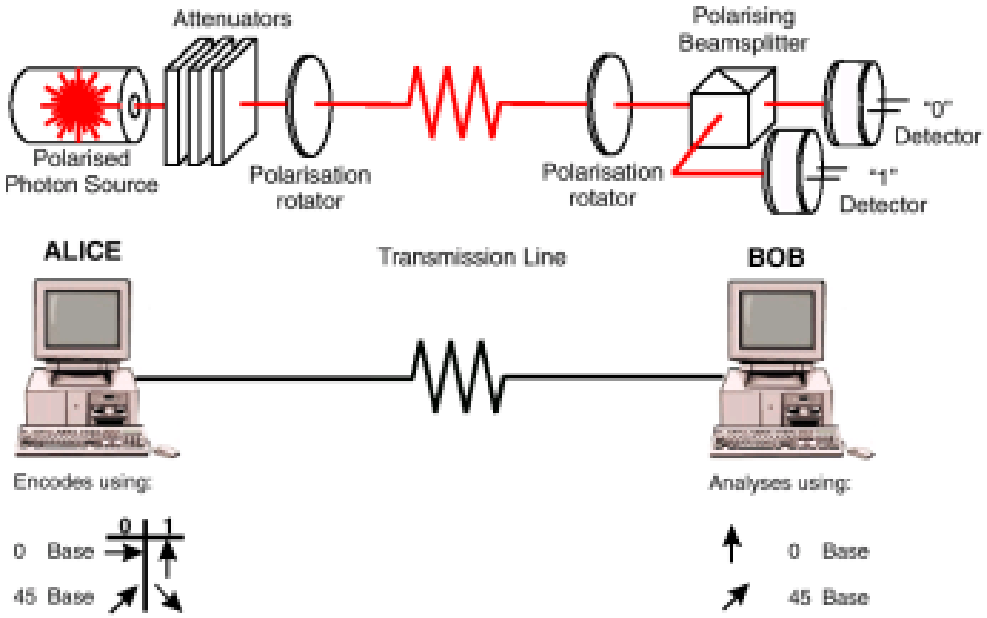
2.2.2 Kvantová distribuce klíče

Kvantová distribuce klíče se často označuje QKD (Quantum key distribution). Problém bezpečné distribuce kryptografického klíče představuje zásadní problém kryptografie od jejích počátků. Nejdůležitějším faktem bezpečnosti kryptografického systému je, že nejméně bezpečný článek systému tvoří celý systém. Například použijeme bezpečný šifrovací systém, ale šifrovací klíč bude generován nejslabším kryptografickým algoritmem nebo protokolem. Tak vznikne nevhodná kombinace, kterou rozhodně nedoporučuji použít. Před nástupem kvantové kryptografie jako jedna z nejbezpečnějších distribucí byla doručit klíč kurýrem. Kurýr musel být důvěryhodný, sledovaný a klíč umístěn v zabezpečeném kufříku nebo obalu. Řešení bylo charakteristické pro vládní organizace a velké společnosti.

Kvantová kryptografie představuje vhodný nástroj pro distribuci klíčů. Tok jednotlivých fotonů umožňuje spolehlivě a bezpečně vytvořit tajný klíč. Pojem systém kvantové kryptografie vyjadřuje systém distribuce klíče[29]. Princip spočívá, že odesílatel (Alice) zajistí přípravu fyzického systému do známého kvantového stavu a odešle jej příjemci (Bob). Příjemce vykoná měření jedné ze dvou určitých veličin systému přijatého od odesílatele. Výměny a měření jsou provedeny v dostatečném množství, obě strany komunikace budou mít dostatek hodnot, které se dají využít jako klíč.

Jako veličina pro měření se v nejčastějších případech používá polarizace fotonů, kterou můžeme vidět na obrázku.

[29] Systém distribuce klíče – QKD (**Q**uantum **K**ey **D**istribution).



Obr. 15. Polarizace fotonů

[http://www.lupa.cz]

K přenosu informace se využívá fotonů s různou polarizací. Rozlišujeme 4 roviny, tzv. polarizační stavy. V Tab. 3. můžeme vidět, že první a třetí polarizační stav reprezentuje bit s hodnotou 1 a zbylé dva stavy bit s hodnotou 0.

Polarizační stav	Bitová hodnota	Báze
→	**0**	+
↑	**1**	+
↗	**0**	x
↖	**1**	x

Tab. 2. Polarizace fotonu

Informace o veličině, kde Alice nastavila a poté Bob měřil hodnotu, byly veřejné. Konkrétní naměřené hodnoty se ovšem nikde nezveřejňovaly. Teoreticky by musel útočník zkoušet získat informace z kvantového systému. Funkce je založena na principu nejistoty, došlo by k naměření odlišné hodnoty, než která byla nastavena odesílatelem. Z toho

vyplývá, že odesílatel a příjemce by se o odposlechu dozvěděli pouhým porovnáním hodnot.

Distribuce klíče umožní odesílateli a příjemci získat sdílený klíč. Odesílatel (Alice) vysílá fotony v jedné polarizaci. Rozlišujeme čtyři typy polarizací podle úhlu, a to 0º, 45º, 90º a 135º. Příjemce (Bob) zaznamenává polarizaci v kolmém směru, to jsou hodnoty 0º a 90 º nebo diagonální 45º a 135 º. Podrobněji distribuci klíče popíšu v kapitole [2.2.4].

2.2.3 Protokol BB84

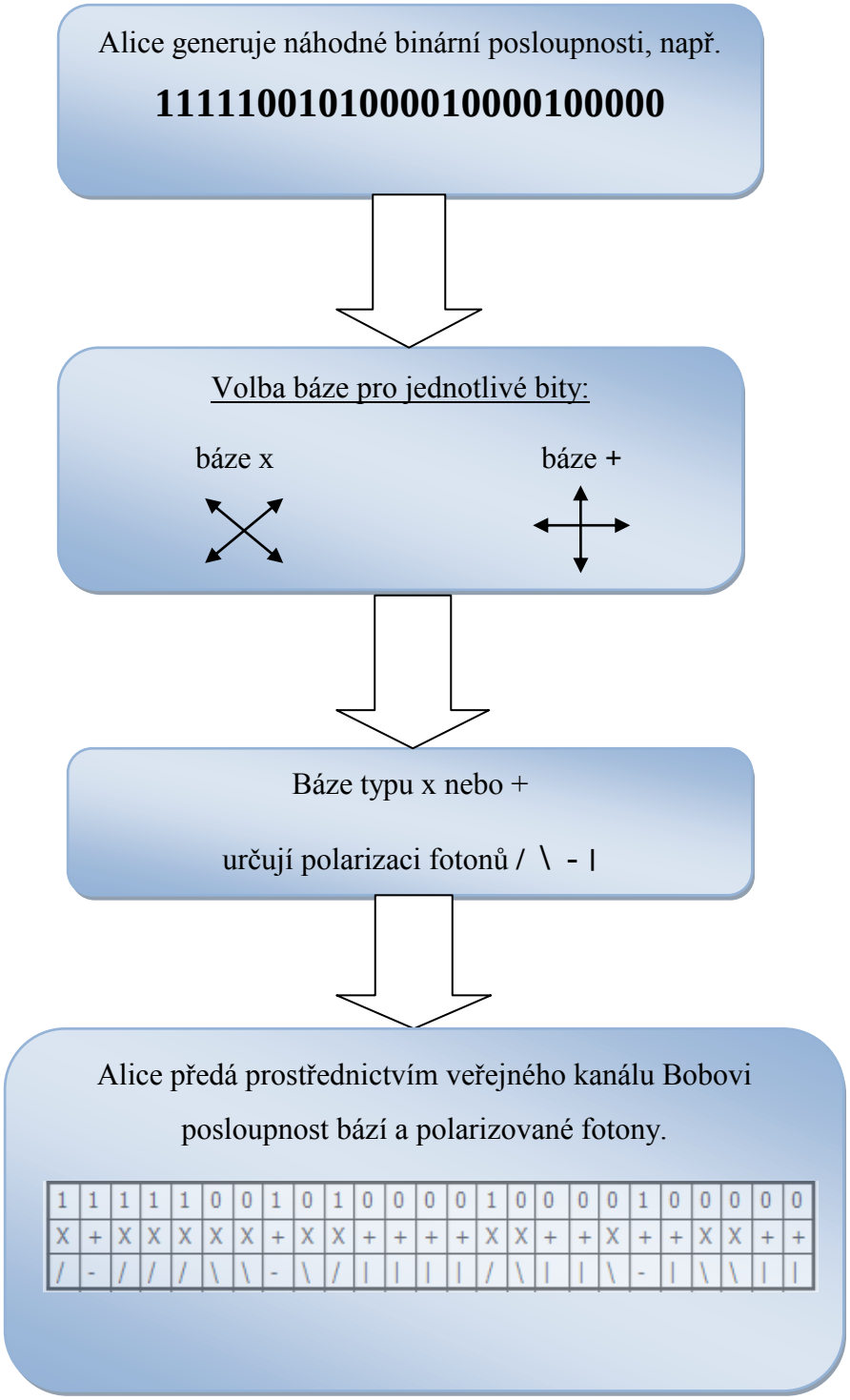
BB84 představuje zkratku odvozenou od příjmení autorů Bennett a Brassard a číslo 84 rok, kdy protokol vytvořili. Jedná se o nejstarší protokol kvantové kryptografie. O pět let později Bennet se svým studentem protokol poprvé uskutečnili v laboratoři. Tento protokol slouží k dohodě na symetrickém klíči. Protokol BB84 byl založen na Heisenbergovém principu neurčitosti ve spojení s polarizačním kódováním. Praktické využití protokolu se po jeho objevení zdálo nemožné, zcela mimo hranice tehdejších technologií. S mírnými obměnami se BB84 používá dodnes. Dnes jsou tyto systémy dostupné i v komerční sféře. Např. USB komerční zařízení pro kvantovou distribuci klíče, které nabízí několik firem. Pracují s využitím optických vláken na vzdálenost přes 100km. Ceny se pohybují v řádech sta tisíc USD.

2.2.4 Způsob komunikace protokolu BB84

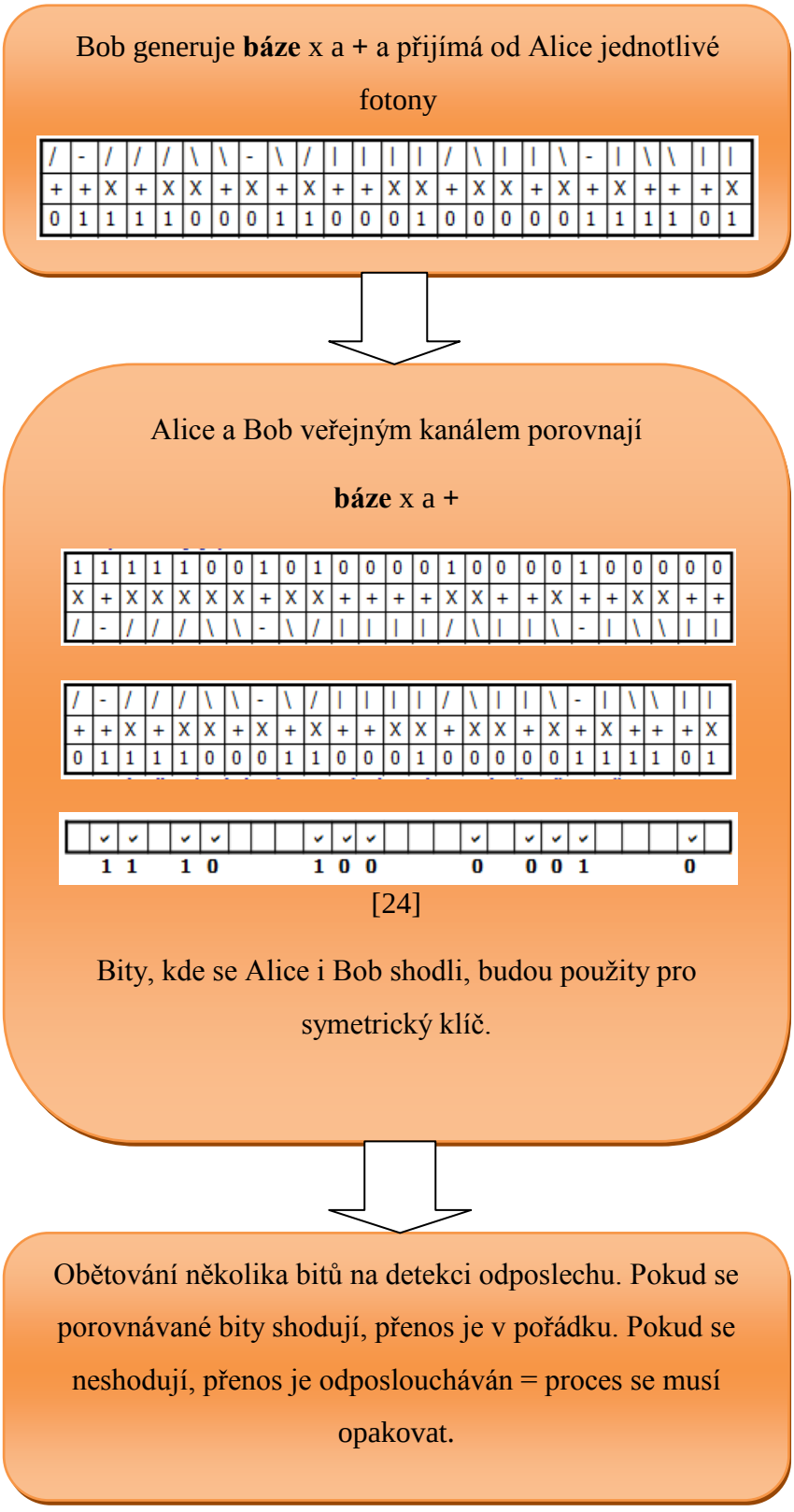
V následující kapitole znázorním princip komunikace a možný způsob odposlechu u nejpoužívanějšího protokolu BB84. Pro lepší představu uvedu grafické a tabulkové znázornění, doplněné vysvětlujícím textem.

Příklad průběhu komunikace protokolu BB84. Odesílatel (Alice) a příjemce (Bob) se chtějí dohodnout na klíči. Útočník (Eva) chce klíč odposlechnout. Názvosloví Alice, Bob a Eva se používá v řadě odborné literatury a zdrojích o kryptografii, tudíž ho v této ukázce uvedu také.

Obecný postup:



Obr. 16. Postup odesílatele (Alice)



[24]

Obr. 17. Postup příjemce (Boba) a dohoda na klíči

Postup kvantového protokolu výměny klíče:

Ukázka principu detekce přítomnosti odposlechu.

1. Odesílatel (Alice) produkuje fotony ve 4 možných rovinách. Dále odesílá fotony kvantovým kanálem příjemci (Bob). Důležité je, že množství odeslaných fotonů musí přesáhnout minimálně dvojnásobek bitů utajované zprávy.
2. Poté Bob dělá měření na fotonech, náhodně střídá báze.
3. Alice předá Bobovi prostřednictvím veřejného kanálu posloupnost bází, kde byly jednotlivé fotony polarizovány. Konkrétní výsledky si ponechá pro sebe.
4. Bob zaznamená hodnoty polarizací pro fotony, které měřil ve správné bázi. Právě z těchto bitů bude později vytvořen klíč. Ostatní výsledky nebudou použity, v příkladu níže asi 60%.
5. V následujícím kroku Bob veřejným kanálem Alici sdělí, jaké fotony měřil ve správné bázi. Alice zná polarizaci posílaných fotonů, tudíž zná bity klíče. Bob bez chyby měřil a z toho vyplývá, že zná také klíč.
6. Část bitů klíče musí být obětováno na detekci odposlechu. Tyto obětované bity jsou náhodně voleny. Dále si Alice a Bob navzájem tyto bity pošlou a porovnají své hodnoty. V pořádku, pokud se shodují, pokud se ovšem neshodují, linka je odposlouchávána. V případě odposlechu je klíč nepoužitelný, musí být zapomenut! Celý postup bude proveden znovu od začátku.

Alice generuje náhodnou binární posloupnost (1. řádek tabulky). Volí náhodně báze (2. řádek tabulky). Poté kóduje všechny bity do polarizace fotonů a na závěr bity odesílá Bobovi (3. řádek).

0	1	1	1	1	0	1	1	0	0	1	1	1	0	1	1
x	x	+	x	+	+	x	+	+	x	+	x	x	+	+	x
/	/	-	/	|	|	\	-	|	\	-	\	\	/	|	\

Tab. 3. Odesílatel (Alice)

Bob dekóduje přijaté fotony (1. řádek) dle náhodně zvolené báze (2. řádek). Dekódování bitů (3. řádek).

/	/	-	/	ǀ	ǀ	\	-	ǀ	\	-	\	\	/	ǀ	\
+	x	+	x	+	+	+	+	+	x	+	x	+	+	+	x
0	1	1	0	1	0	0	1	0	1	1	1	0	0	1	1

Tab. 4. Příjemce

Alice oznámí Bobovi (veřejně a s autentizací původní zprávy), kde a jakou bázi použila. Alice také ohlásí informace o bázi. Bity, kde se Alice i Bob shodli, můžeme vidět v tabulce. Tyto bity budou použity pro symetrický klíč.

	ᵛ	ᵛ		ᵛ	ᵛ		ᵛ	ᵛ		ᵛ	ᵛ		ᵛ	ᵛ	ᵛ
	1	**1**		**1**	**0**		**1**	**0**		**1**	**1**		**0**	**1**	**1**

Tab. 5. Bity pro klíč

ᵛ – symbol představuje OK (souhlas).

Dále je nutné provést tzv. obětování bitů na detekci odposlechu. Útočník (Eva) případným odposlechem ovlivní stav procházejících bitů. Alice a Bob obětují některé bity a porovnají konkrétní výsledné hodnoty. „Všechny“ obětované bity se shodují, můžeme tvrdit, že útočník neposlouchá. Odposlech by se projevil jako chyba v přenosu.

Eva může získat klíč v podstatě jedním způsobem. Bude odposlouchávat kvantový komunikační kanál (měřit odesílatelovy fotony). Měření je možné pouze ve stejných dvou bázích jak postupoval Bob, potom z fotonů může dekódovat potřebné bity pro klíč. Pro Evu je stěžejní, že nejde změřit jeden foton zároveň v obou bázích. Jedná se o

tzv. nekomutující operátory[30]. Tipne-li Eva správnou bázi, dostane správný výsledek. Stav fotonu se nezmění a Alice ani Bob nezaregistrují narušení. Ovšem vyskytne-li se foton v nesprávně zvolené bázi, přemění se jeho kvantový stav. Kdyby se jednalo o správný výsledek Bobova měření, byl by výsledek pouze náhodný. Z toho vyplývá, že asi 50% případů útoku se neodhalí a to z důvodu, že Bob dostane čistě náhodou správný výsledek. Závěrem lze doporučit, čím více bitů Alice a Bob veřejně porovnávají, tím se zvětšuje pravděpodobnost odhalení Evy.

Při zvoleném počtu obětovaných bitů *N*, dostáváme vztah pro pravděpodobnost ***p*** detekce soustavného odposlechu: $p = 1 - (3/4)^N$

V mém případě bych za *N* dosadil číslo 3 (obětoval jsem 3 bity, viz *Tab. 6.*).

$$p = 1 - (3/4)^N = 0{,}578 \Rightarrow 57{,}8\%$$

Ve zvoleném příkladě vyšla pravděpodobnost detekce soustavného odposlechu 57,8% při 3 obětovaných bitech. Výsledek se odvíjí od počtu zvolených bitů. Například při obětovaní 32 bitů bychom dostali výsledek pravděpodobnosti 99,9%. Příklad jsem zvolil jen na ukázku k vysvětlení principu výměny klíče, a tudíž jsem nedosáhl nejideálnějšího výsledku pravděpodobnosti.

Zbylé bity, které můžeme vidět ve 3. řádku v *Tab. 6.*, tvoří tajný klíč.

V našem případě bude klíč: **1 1 0 0 1 0 1 1.**

	1						**1**				**1**				
	∨						∨				∨				
		1		**1**	**0**			**0**		**1**			**0**	**1**	**1**

Tab. 6. Obětované bity a bity pro klíč, úspěšný přenos

[30] Nekomutující operátory – reprezentují nekompatibilní, tzv. komplementární pozorovatelné veličiny.

Ukázka simulace odposlechu Evy, která narušila komunikaci mezi Alicí a Bobem. Odposlech se projeví změnou polarizace některých fotonů. Postup na straně Alice a Boba již nebudu popisovat, jedná se o stejný postup, který je popsán výše u nenarušeného přenosu útočníkem.

ALICE

0	1	1	1	1	0	1	1	0	0	1	1	1	0	1	1
x	x	+	x	+	+	x	+	+	x	+	x	x	+	+	x
/	/	-	/	|	|	\	-	|	\	-	\	\	/	|	\

BOB

/	/	-	/	|	|	-	-	|	/	-	\	\	/	|	\
+	x	+	x	+	+	x	+	+	x	+	x	+	+	+	x
0	1	1	0	1	0	0	1	0	1	1	1	0	0	1	1

Obětované bity – označeny modře, mají za úkol zjistit případný odposlech.

	1	**1**		**1**	**0**	**1**	**1**	**0**	**1**	**1**	**1**		**0**	**1**	**1**

Při použití velké sekvence bitů je odhalení odposlechu velmi pravděpodobné. Bity, které byly použity k obětování, již nebudou tvořit výsledný klíč. V našem případě klíč bude následující: **1 1 0 0 1 1 1**.

V reálném přenosu počet obětovaných bitů představuje minimální počet vzhledem k celkovému počtu přenášených bitů.

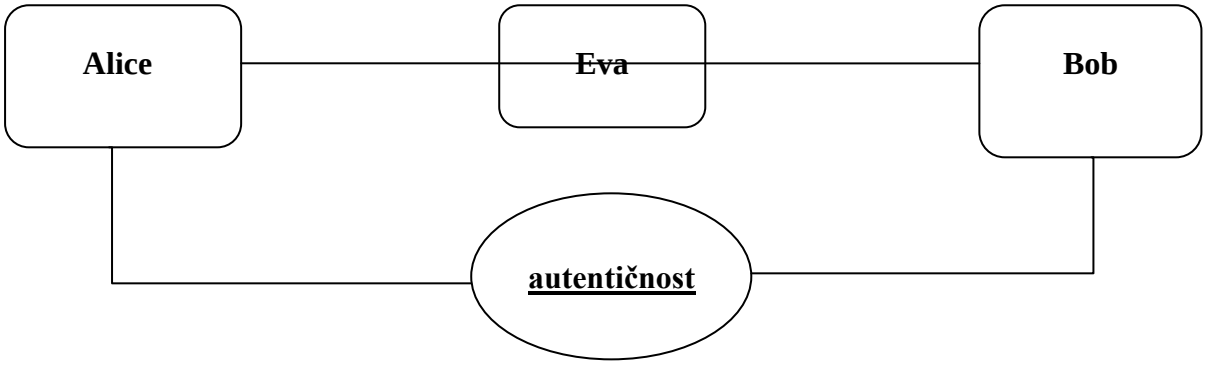
	˅	**1**		**1**	**0**	**X**	˅	**0**	**X**	**1**	˅		˅	**1**	**1**

Tab. 7. Přenos narušený odposlechem

2.2.5 Nedostatky kvantové kryptografie

První problém je, poslouchá-li Eva na lince nepřetržitě. Pokud se porovnávané bity neshodují, linka je odposlouchávána, klíč je zapomenut a postup se opakuje znovu a znovu. To znamená, že Alice s Bobem by se na klíči nikdy nedohodli. Tahle slabina je spíše technického charakteru než kryptografického, protože například je možné komunikační kanál ochromit fyzickým zásahem. Z toho vyplývá, čím vícekrát se bude opakovat generování klíče, tím se zvyšuje Evina šance, že klíč odposlechne. Doporučení na úspěšnou obranu spočívá v použití dostatku kontrolních bitů.

Další problém představuje, že protokol na veřejném kanále neřeší autentičnost. Bob veřejně sděluje Alici, jaké fotony měřil ve správné bázi. Alice v tomto případě nemusí s určitostí vědět, zda komunikuje skutečně s Bobem a nekomunikuje s Evou. Chybí zde proces ověření identity na straně příjemce a odesílatele. Popsaný protokol kvantové kryptografie nemá ošetřenu autentičnost (pravost, původnost). Tato absence u popsaného protokolu se může stát zranitelným místem.



Obr. 18. Autentičnost

Dále bych se zastavil ještě u komunikace Alice a Boba. Určitý problém nastává, že foton, který vygenerovala Alice, musí být doručen Bobovi. Na spojovací trase mezi Alicí a Bobem musí být pouze optické vlákno. Nesmí mezi nimi být žádný aktivní prvek (přepínač nebo opakovač). Uvažujeme-li **n** koncových uživatelů, tak musí být každý uživatel (uzel) propojen samostatným vláknem s (n-1) ostatními uzly. Výsledkem je složitá síť skládající se z **N** vláken, která spojuje každý uzel se všemi ostatními uzly systému.

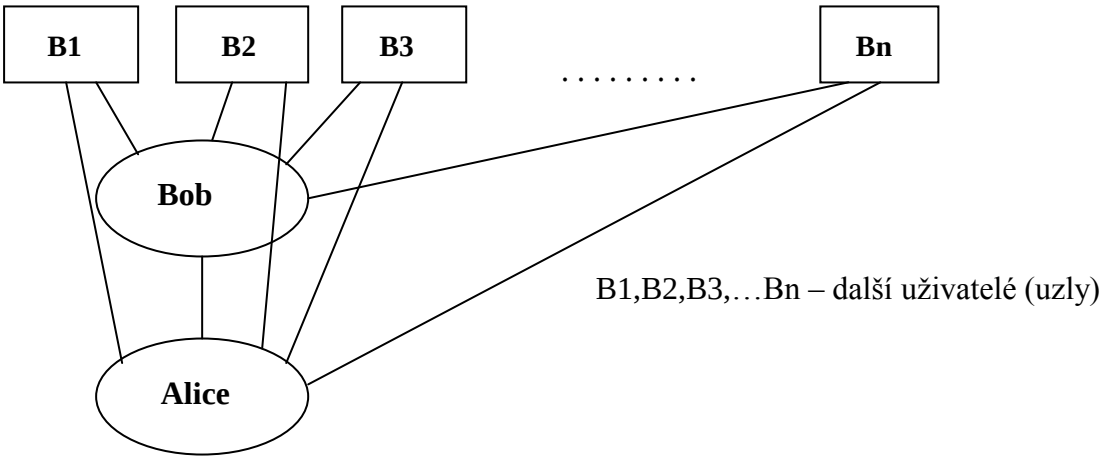
To lze vyjádřit následujícím vztahem:

$$N = n(n-1)/2$$

N… počet vláken

n… počet koncových uzlů (uživatelů)

Při velkém počtu uživatelů je popsané řešení finančně i provozně neakceptovatelné.



Obr. 19. Příklad topologie kvantové kryptografie

Poměrně velký problém spatřuji v omezeném dosahu přenosu po optickém vlákně. Jak již víme, nemůžeme zde použít opakovače nebo přepínače. Vzdálenost mezi uzly je omezena délkou spojovací trasy. Tato délka se obvykle pohybuje v řádech desítek až stovek kilometrů (max. zjištěná délka je 148,7km). Přičemž, když uvažujeme vzdálenost např. mezi Brnem a Prahou 200km, tak nasazení kvantové kryptografie je zde nemožné. O globálním využití v tomto případě nemůžeme uvažovat. V řadě odvětví je uvedené omezení neakceptovatelné.

Rychlost distribuce klíče se pohybuje v řádu 10^2 Kb/s, ve srovnání s dnešními jinými typy přenosových rychlostí je tato rychlost pomalá.

2.2.6 Porovnání klasické a kvantové kryptografie

Klasická kryptografie:

- Jen omezená možnost kopírování nosičů klasické informace.

- Spoléhá na výpočetní složitost šifrovacích algoritmů.
- Dělí se na symetrické a asymetrické šifrovací algoritmy.
- Pracuje s klíči o extrémních délkách (princip one-time-pad[31]).
- Většina současných systémů je založena na klasické kryptografii.

Kvantová kryptografie:

- Teoretické předpoklady dokazují bezpečné fungování bez ohledu na teoretické znalosti a prostředky potenciálního útočníka.
- Odborníci předpokládají, že bezpečnost kvantové kryptografie nebude ohrožena ani s případným nástupem kvantových počítačů.
- Nemožnost vytvoření stejných kopií neznámého kvantového stavu.
- Princip spočívá v tom, že se nejprve přenese klíč, který se v případě pozitivní detekce odposlechu nepoužije. Bude se mezi odesílatelem a příjemcem generovat nový klíč.
- Finančně náročné pořizovací náklady.

Kvantová kryptografie představuje bezpečnou distribuci klíče. Myslím si ale, že „klasickou“ kryptografii pravděpodobně nikdy plně nenahradí. Výše zmíněné nevýhody (nedostatky) [2.2.5] mě o tom přesvědčují.

Kryptografická ochrana, která se dělí na symetrickou a asymetrickou, má některé algoritmy, které již nelze použít. Zkrátka jsou málo bezpečné a při dnešní výpočetní rychlosti počítačů jsou lehce prolomitelné. Ostatní šifrovací algoritmy symetrické i asymetrické kryptografie jsou zastoupeny ve všech odvětvích spojených s komunikací a manipulací s informacemi.

V komerčním a státním sektoru je kvantová kryptografie jednoznačně méně zastoupena než „klasická“ kryptografie.

[31] One-time-pad – často používaný anglický název pro Vernamovu šifru. V překladu „jednorázová tabulková šifra“. U šifry je dokázáno, že je zatím nerozluštitelná.

3 UTAJOVANÉ INFORMACE

Do vlastnictví každé společnosti, ať již soukromé nebo státní, patří informace (obchodní tajemství, dovednosti, recepty apod.). Ochrana utajovaných informací hraje významnou roli i v činnosti PKB. Ochrana informací v PKB se prováděla i v minulosti, ovšem nyní má jinou podobu. Představuje náročný proces obsahující právní normy, které praví, jak ochranu realizovat.

Informace představují zásadní roli v každé společnosti a jejím vlastnictví. V prostředí tržního hospodářství má velkou výhodu pro soutěžící společnosti. Informace se stávají zbožím s vysokou tržní hodnotou. Problematiku ochrany utajovaných informací řeší zákon č. 412/2005 Sb.[32] o ochraně utajovaných informací a o bezpečnostní způsobilosti.

„Utajované informace[33] jsou takové informace, na jejichž utajení má vždy zájem buď nějaká fyzická osoba, nebo právnická osoba (instituce, stát). Tento zájem vyplývá z faktu, že při zneužití takovéto utajené informace vznikne nějaká újma. Svůj zájem na utajení tento subjekt dává zpravidla najevo tím, že činí řadu opatření, aby utajení bylo zachováno a nepovolaná osoba se s takovou informací neseznámila. Tato opatření mají různý charakter a patří mezi ně i možnost sankce proti tomu, kdo se s takovou informací neoprávněně seznámí nebo ji vyzradí.“[34]

Každá organizace musí stanovit stupeň utajení informací a místo, kde se utajované informace vyskytují. Organizace musí vždy mít vlastní ochranný systém vyplývající z konkrétních podmínek.

Mezi podmínky organizace především patří:

- Druhy informací, které se nacházejí v organizaci nebo se kterými se bude manipulovat.

---

[32] Zákon č. 412/2005 Sb. o ochraně utajovaných informací a o bezpečnostní způsobilosti. Ze dne 21. září 2005. Zákon byl již devětkrát novelizován: zákonem č. 119/2007 Sb., zákonem č. 177/2007 Sb., zákonem č. 296/2007 Sb., zákonem č. 32/2008 Sb., zákonem č. 124/2008 Sb., zákonem č. 126/2008 Sb., zákonem č. 250/2008 Sb., zákonem č. 41/2009 Sb. a zákonem č. 227/2009 Sb. (od 1. července 2010).

[33] Autor použil slovo „skutečnosti“, které je nově nahrazeno slovem informace. Informace = skutečnost.

[34] LAUCKÝ, Vladimír. *Technologie komerční bezpečnosti II*. 2. vyd. Zlín : [s.n.], 2007. 83 s. ISBN 978-80-7318-631-9.

- Stanovena a vyznačena místa, kde se s utajovanými informacemi pracuje.
- Určené personální funkce, kdo s informacemi může přijít do styku, popřípadě s jakým druhem informace.

Důležitý je výběr spolehlivých zaměstnanců, kteří budou určeni a oprávněni se seznamovat s utajovanými informacemi. Další důležitý aspekt je rozhodnutí o ochranném opatření pro každý druh informace. Musí být chráněny zájmy organizace, ale zároveň splněny požadavky právních norem (zákon č. 412/2005 Sb. a další příslušné vyhlášky).

Ochrana informací je stejně důležitá pro soukromé organizace, tak i pro stát. Všechny státy chrání své informace související s bezpečností státu, ochranou zájmů, strategicky důležité informace apod. Stát chrání tyto informace především proto, že vyzrazení nebo ohrožení informací by mohlo způsobit státu určitou újmu.

3.1 Národní bezpečnostní úřad

Národní bezpečnostní úřad (NBÚ) představuje orgán výkonné moci. Vznikl na základě zákona č. 148/1998 Sb., o ochraně utajovaných skutečností a o změně některých zákonů. Začal fungovat od 1. srpna roku 1998 se sídlem v Praze. NBÚ vykonává činnost podle zákona č. 412/2005 Sb. Více informací je možné nalézt na stránce: www.nbu.cz.

Obr. 20. Sídlo NBÚ

[www.nbu.cz]

Spravuje oblasti:

- ochrany utajovaných informací,
- bezpečností způsobilosti.

NBÚ, orgán státní správy, vykonává tyto hlavní úkoly:

- provádí certifikace,
- výkon státního dozoru,
- jednotné provádění ochrany utajovaných informací v ČR,
- vykonávání bezpečnostních prověrek (fyzických osob, podnikatelů, organizací),
- vydává osvědčení, potvrzení a certifikáty,
- vyvíjí a schvaluje národní šifrové algoritmy,
- vytváří národní politiku kryptografické ochrany,
- zajišťuje činnost Národních středisek: pro měření kompromitujícího elektromagnetického vyzařování, pro bezpečnost informačních systémů, komunikační bezpečnosti, pro distribuci kryptografického materiálu.
- Další činnosti stanovené zákonem: vydávání vyhlášek, vydává Věstník (periodická publikace určená veřejnosti, vychází dle potřeb NBÚ), povoluje poskytování utajovaných informací v mezinárodním styku, evidování případů neoprávněného nakládání s utajovanými informacemi apod.

V čele NBÚ je ředitel, kterého jmenuje a odvolává vláda ČR. Předseda vlády ČR dohlíží na fungování NBÚ a je v roli nadřízeného ředitele NBÚ.

3.2 Zákon o ochraně utajovaných informací

Ochrana utajovaných informací se řídí podle zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti. „Tento zákon upravuje zásady pro stanovení informací jako informací utajovaných, podmínky pro přístup k nim a další požadavky na jejich ochranu, zásady pro stanovení citlivých činností a podmínky pro jejich výkon a s tím spojený výkon státní správy.“[35] Přijetí zákona na ochranu utajovaných informací zajišťuje kompatibilitu se zákony užívanými v zemích EU a NATO.

[35] § 1 zákona č. 412/2005 Sb. O ochraně utajovaných informací a bezpečnostní spolehlivosti.

Zákon č. 412/2005 Sb. řeší problematiku utajovaných informací v celém rozsahu. Důraz je kladen na personální bezpečnost a průmyslovou bezpečnost, které byly v minulých právních úpravách řešeny nedostatečně. Jednotlivé druhy bezpečnosti dále stanovují vyhlášky Národního bezpečnostního úřadu.

Přístup k systému ochrany je založen na dvou základních principech:

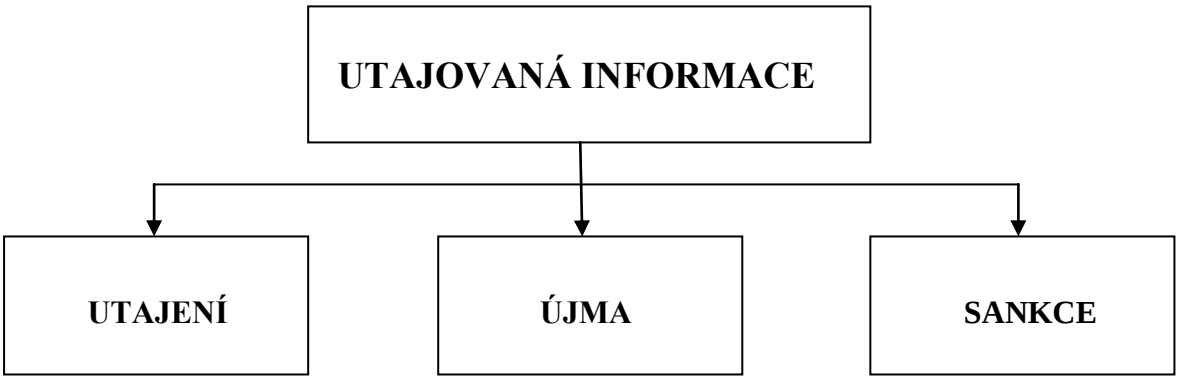
1. Informace utajovat co nejméně, ale co nejkvalitněji. Využít efektivní řešení.
2. S utajovanými informacemi by se měly seznamovat osoby, které informace potřebují znát k výkonu funkce apod. Těchto osob by mělo být pokud možno co nejméně.

3.3 Znaky utajovaných informací

Základní znaky utajované informace jsou:

- Utajení – Zvláštní režim (režim utajení), který zabraňuje, aby utajovaná informace byla známa nepovoleným osobám. Režim omezuje znalost obsahu informace jen na stanovený počet pracovníků. Režim utajení obsahuje nařízení a opatření, které zamezují nepovoleným osobám seznámení s utajovanými informacemi.
    - Utajení zajišťuje:
        - Důvěrnost utajované informace – neoprávněná osoba k informaci nepronikne, nemůže s utajovanou informací neoprávněně nakládat. Neoprávněné nakládání s utajovanou informací znamená vyzrazení informace, zničení, znehodnocení nebo ztrátu. Neoprávněné nakládání představuje také neoznačení utajované informace příslušným stupněm utajení a špatné určení stupně utajení utajované informace.
        - Integrita utajované informace – utajovaná informace nemůže být jakýmkoliv způsobem změněna (upravena).
        - Dostupnost utajované informace – pro určené osoby komplexní a rychlý přístup k utajované informaci.

- Újma – V případě, že je tajemství informace porušeno, může vzniknout újma. Například při neoprávněné manipulaci s utajovanou informací. Na základě újmy se utajované informace dělí na příslušné stupně utajení, které zmíním později. Zákon č. 412/2005 Sb. definuje, co která újma způsobuje. Například finanční újmu, materiálovou škodu, ztráty na životech nebo zdraví.
- Sankce – Když dojde k porušení ochrany tajemství, jsou stanoveny sankce pro osobu, která tajemství porušila nebo se pokusila porušit. Zákon trestá porušení utajení bez ohledu na to, zda skutečně nastala újma související s porušením tajemství informace. Sankce představuje nástroj, kterým stát prosazuje svůj zájem na ochraně utajovaných informací. Sankce se dělí na finanční a majetkové. V ostatních případech mohou být hodnoceny dle trestního zákona.



Obr. 21. Znaky utajované informace

3.4 Klasifikace utajovaných informací

Zákon č. 412/2005 Sb. stanovil rozsah vzniklé újmy a charakterizoval pojem chráněného zájmu s pomocí klasifikace utajovaných informací do čtyř stupňů utajení. Každá utajovaná informace musí být označena předepsaným způsobem a příslušným stupněm utajení.

Utajované informace klasifikujeme stupni utajení:

- Přísně tajné – PT
- Tajné – T
- Důvěrné – D

- Vyhrazené - V

Klasifikace je stanovena na základě intenzity újmy, která může vzniknout v případě neoprávněného nakládání s informací. Stupně utajení jsou seřazeny od nejvyššího stupně utajení po nejnižší.

Členění utajovaných informací ve vztahu k možné újmě:

Stupeň utajení	Charakteristika újmy
Přísně tajné	Nejvyšší stupeň utajení. Vyzrazení nebo zneužití informace tohoto stupně utajení může způsobit mimořádně vážnou újmu zájmům ČR.
Tajné	Druhý nejvyšší stupeň utajení. Vyzrazení neoprávněné osobě nebo zneužití může způsobit vážnou újmu zájmům ČR.
Důvěrné	Neoprávněné nakládání s utajovanou informací může způsobit prostou újmu zájmům ČR.
Vyhrazené	Nejnižší stupeň utajení. Vyzrazení neoprávněné osobě nebo zneužití informace může být nevýhodné pro zájmy ČR.

Tab. 8. Členění utajovaných informací

Od klasifikace utajovaných informací do jednotlivých stupňů se odvíjí rozdílné postupy pro ochranu informací (bezpečnostní prověrka organizace a osoby).

3.5 Druhy zajištění ochrany utajovaných informací

Ochranu informací zajišťuje více aspektů. Tato ochrana ve společnostech je důležitá například k ochraně proti průmyslové špionáži. Průmyslová špionáž představuje specifický druh získávání informací. Řadí se do nejstarší špionážní činnosti. Charakteristická je především tím, že společnost má zájem získat od jiné společnosti tajné informace. Mezi tyto informace patří informace spojené s konkrétní společností, např. recepty, výrobní postupy, návody, know-how, firemní tajemství apod.

Podstata ochrany informací řeší způsob, jak seznámit určitý okruh lidí s utajovanými informacemi. Zároveň se zabývá způsoby, aby se s utajovanými informacemi neseznamovaly osoby, které k tomu nejsou určeny. Toto opatření se jako celek nazývá bezpečnostní politika podniku ve smyslu ochrany utajovaných informací.

3.5.1 Bezpečnostní politika utajovaných informací

Důležitou součástí strategie společností jsou úvahy, jak své informace chránit. Společnost pomocí stanovených cílů rozvrhuje oblast řešení bezpečnosti. Bezpečnost je nutné pojmout jako celek, od úrovně celé společnosti až po jednotlivé sektory. Proč společnosti chrání své informace? V případě ztráty nebo odcizení informací může dojít v krajním případě k ukončení činnosti společnosti, značným finančním ztrátám, ztráty zakázek apod. I přes narůstající počty útoků na data nebo informace může společnost oblast zabezpečení informací podcenit. Každá organizace, kde se vyskytují utajované informace, vypracovává bezpečnostní politiku ochrany utajovaných informací. Bezpečnostní politika zahrnuje bezpečnostní projekt, ve kterém se popisuje použití prostředků ochrany. Bezpečnostní politika ochrany utajovaných informací jako celek se skládá z jednotlivých druhů bezpečností (fyzická bezpečnost, personální bezpečnost, bezpečnost IS apod.). Požadavky jsou stanoveny zákonem č. 412/2005 Sb. a dalšími zmíněnými právními předpisy.

Bezpečnostní politika představuje:

- cíle společnosti v oblasti ochrany utajovaných informací,
- popisuje utajované informace:
    - rozsah,
    - místa výskytu,
    - rizika jejich možného ohrožení.
- nasazení prostředků ochrany.

V počátku tvorby bezpečnostní politiky se jedná o stanovení bezpečnostních požadavků, tzn. bezpečnostní cíle, kterých je třeba dosáhnout. Cíle vychází v první řadě z legislativy a finančních možností společnosti a také z bezpečnostních rizik. Správné stanovení bezpečnostních rizik vytváří podklad pro odpovídající bezpečnostní opatření. Vhodně zpracovaná bezpečnostní rizika tvoří základ bezpečnostní politiky požadované úrovně.

3.5.2 Bezpečnostní projekt

Stanovené požadavky a přechod k jejich řešení obstarává bezpečnostní projekt. Obsahuje způsob realizace bezpečnostní politiky, patří sem oblasti personální, průmyslová, administrativní, fyzická, informační a komunikační systémy a kryptografická ochrana. Technická opatření je nutné aplikovat do společnosti, vybrat vhodné komponenty informačních technologií, správná volba zabezpečení, netechnická forma (personální) apod. Bezpečnostní projekt se tvoří ve spolupráci svých IT útvarů, popřípadě externích, a externím dodavatelem. Nezbytná součást bezpečnostního projektu musí být stanovení bezpečnostní struktury organizace a definování základních rolí, odpovědnosti a povinností v oblasti bezpečnosti. Bezpečnostní projekt společnosti představuje dokument, který je posuzován NBÚ při bezpečnostní prověrce organizace.

Bezpečnostní projekt především obsahuje:

- výskyt utajovaných informací – budovy, pracoviště a místa,
- druh, rozsah a stupeň utajení utajovaných informací, které budou ve společnosti vznikat nebo se v ní vyskytovat,
- určená možná rizika utajovaných informací,
- možnosti použití prostředků k ochraně utajovaných informací,
- kontrolní opatření,
- časový plán realizace bezpečnostního projektu,
- organizační rozdělení úkolů pro realizaci bezpečnostního projektu,
- materiální, personální a finanční požadavky.

Vypracovaný bezpečnostní projekt je poté nutné implementovat do společnosti. Jedná se především o manažerské úsilí, při kterém se společnost snaží přeměnit bezpečnostní projekt do každodenního fungování společnosti. Celá implementace musí být dobře sledována a vedena.

Společnost dokládá spolu s bezpečnostním projektem další dokumenty, které stanovují vyhlášky NBÚ.

Dokumenty související s procesem ochrany utajovaných informací:

- Provozní řád objektu,
- bezpečnostní projekt ochrany objektu,
- spisový řád,
- skartační řád,
- technická dokumentace fyzické bezpečnosti,
- vyhodnocení rizik,
- krizový plán ochrany objektu,
- dokument o bezpečnosti informačních systémů pracujících s utajovanými informacemi.

Po zavedení do provozu je bezpečnostní systém pravidelně kontrolován, zda realizovaná bezpečnostní politika pracuje v souladu se záměrem, jak byla původně navržena. Případné objevené nedostatky jsou dokumentovány, vyhodnoceny a následně odstraněny.

Cíle v oblasti ochrany informací:

- Nepovolené osobě zabránit styku (seznámení) s utajovanými informacemi,
- vytvořit opatření pro ochranu utajovaných informací při jejich manipulaci, tvorbě, příjmu, ukládání apod.,
- s utajovanými informacemi se budou seznamovat jen osoby splňující podmínky zákona č. 412/2005 Sb.,
- prostor s utajovanými informacemi zabezpečit vhodnými prostředky (MZS, EZS apod.),
- při nasazení technických prostředků, kryptografických metod a informačních systémů používat jen certifikované prvky NBÚ.

Bezpečnostní politika společnosti se společně s bezpečnostním projektem překládá NBÚ a poté se žádá o vykonání bezpečnostní prověrky. Bezpečnostní politika ochrany utajovaných informací představuje správně vytvořené každodenní fungování společnosti v oblasti bezpečnosti utajovaných informací.

3.6 Zabezpečení společností

„Společnost Symantec Corp. zveřejnila výsledky své globální studie 2010 State of Enterprise Security. Studie zjistila, že 42% organizací považuje zabezpečení za svůj hlavní problém. Nejedná se o překvapení, když vezmeme v úvahu, že 75% organizací zaznamenalo v uplynulých 12 měsících počítačové útoky. Tyto útoky stály velké podniky v průměru 2 mil. USD ročně. Organizace uváděly, že zabezpečení je stále obtížnější kvůli nedostatku zaměstnanců, novým iniciativám v oblasti IT, které stupňují potíže se zabezpečením, a kvůli problémům se zajištěním souladu IT s předpisy. Studie vychází z průzkumu provedeného v lednu 2010 ve 27 zemích mezi 2 100 podnikovými vedoucími pracovníky z řad CIO, CISO a manažery IT.“[36]

Závěry studie:

- Bezpečnost společností ovlivňuje několik faktorů. Důležitý faktor je, že se zabezpečení nevěnuje potřebný počet zaměstnanců. Nejrizikovější oblasti představují zabezpečení sítí (44% úspěšných útoků), zabezpečení koncových bodů (44% úspěšných útoků) a zabezpečení příjmu a odesílání zpráv (39% úspěšných útoků).
- Všechny prozkoumané společnosti registrovali v roce 2009 ztráty v oblasti IT. Nejčastější krádeže představovaly: ztrátu duševního vlastnictví, informace o kreditních kartách zákazníků, jiné finanční údaje a osobní údaje zákazníků. V 92% byly ztráty spojeny s finanční újmou. Následky pro společnosti se poté odráží na produktivitě, tržbě a ztrátě důvěry zákazníků.
- V roce 2009 75% společností zaregistrovalo počítačové útoky. 36% společností vyhodnotilo útoky jako nebezpečné a vysoce úspěšné. Další nepříjemná statistika uvádí, že u 29% společností se během roku 2009 počet útoků zvýšil.
- Bezpečnosti informací je ve společnostech kladen nemalý význam. Zajímavostí je, že v 42% případů hodnotí společnosti počítačovou kriminalitu jako svůj největší problém.

---

[36] *Chip online : Elektronický archiv časopisu Chip* [online]. Praha : Burda, 05-2010 [cit. 2011-03-05]. Dostupné z WWW: < http://earchiv.chip.cz/cs/earchiv/vydani/r-2010/chip-05-2010/google-chyby.html >.

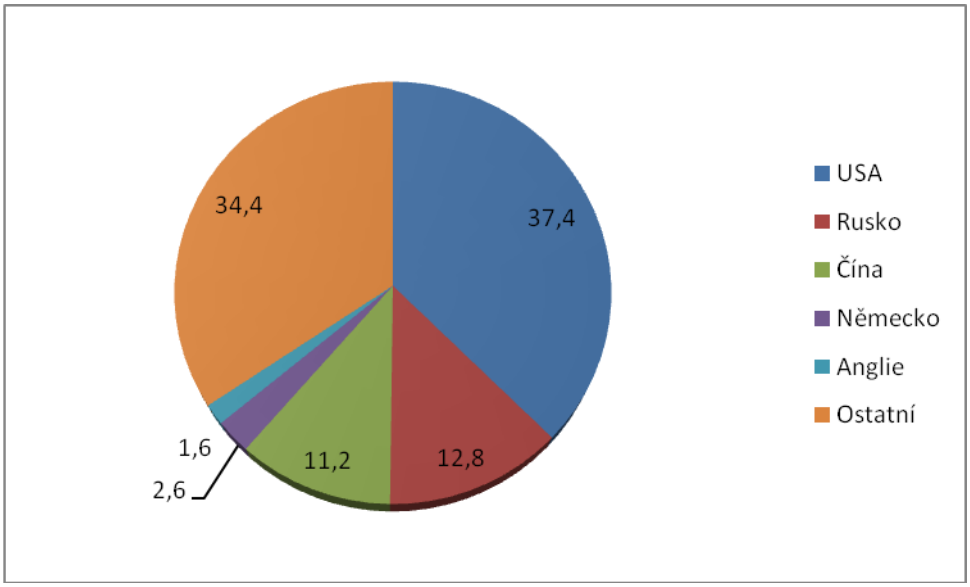
4 HACKING V KVANTOVÉ KRYPTOGRAFII

V budoucnu hrozí, že se teroristé rozhodnou kombinovat kybernetický terorismus s fyzickým útokem. Teroristé si budou volit za cíle elektronickou infrastrukturu s využitím ničivých počítačových programů, zahlcení internetu nebo telekomunikační sítě. Zahlcení obrovským množstvím informací, které by zmíněné sítě učinily nepoužitelnými. Dále je nutné počítat, že existují útoky s pomocí elektromagnetické energie nebo vysokoenergetických radiových vln. Tyto typy útoků na dálku zničí data v počítačových sítích. Elektronický útok v kombinaci s fyzickým často fyzický útok maskuje a zhoršuje. Zdvojený útok by mohl totálně ochromit např. nejdůležitější vládní orgány nebo celé společnosti.

V dnešní době mnohačetných počítačových útoků na různé systémy se začalo říkat lidem, kteří se nabourávají do systému, „Hackeři“. Jsou to počítačoví specialisté s výbornými znalostmi fungování systému. V systému se dovedou výborně orientovat a upravit ho podle svých představ. Slovo „hacking“ je odvozeno od anglického slova „hack“, což v doslovném překladu znamená „hákovat“ neboli proniknout. Proniknutí do cizích počítačových systémů a získat přístup k informacím.

Počítačový virus můžeme chápat jako program, který se sám šíří (vytváří své kopie). Chová se podobně jako biologický virus, který vkládá bakterie do živých buněk. Většina virů je uzpůsobena rychlému množení, ukládají se do souborů nebo dokumentů. Posouzení programu jako viru je využití k šíření jiného hostitele. Vir se mezi počítači šíří tak, že někdo přenese celého hostitele (soubor na CD-ROM, DVD-ROM, HDD, prostřednictvím počítačové sítě apod.). Počítačové viry se dělí na cíleně ničivé, které smažou data na HDD. Další typy virů nejsou přímo škodlivé, ale obtěžují uživatele např. otvíráním různých programů, složek apod.

Graf znázorňuje procentuální výskyt infikovaných webových stránek. V USA je výskyt největší, větší než v kterékoliv jiné zemi. Údaje pochází z časopisu Chip 05/2010 a jsou aktuální ke konci roku 2009.



Graf 1. Výskyt infikovaných webových stránek

Obecně způsobů prolomení systémů je mnoho, s vyspělým počítačovým vybavením a stále většími znalostmi hackerů počty útoků stále stoupají.

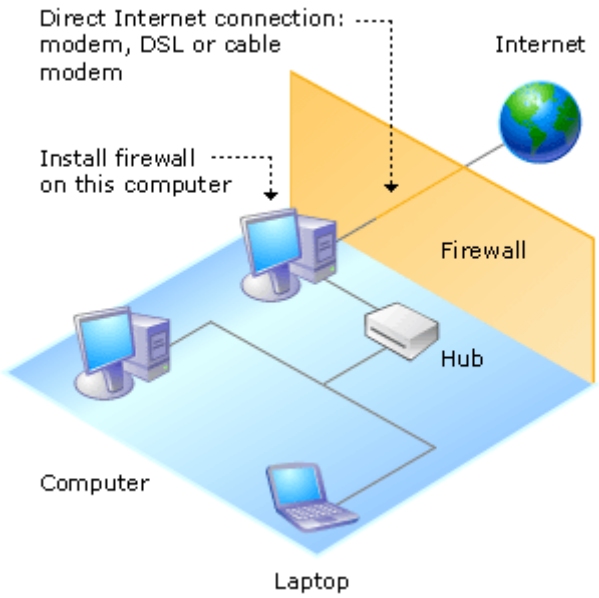
Metody prolomení systému:

- trojský kůň[37]- přes vzdálenou správu může být počítač ovládán hackerem, hacker pronikne do počítače,
- exploit[38] s určitým Payloadem,
- získání přístupových hesel do protokolů, např. FTP,

[37] Trojský kůň – pro uživatele skrytá část programu, ve většině případů se škodlivou činností. Pojmenování Trojský kůň je odvozeno z povídky o dobytí Tróje. Jedná se o samostatný program, který se může jevit neškodně (jednoduchý nástroj, hra, apod.). Trojský kůň sám není škodlivý, navržen k otevření a čekání na příkazy, které zadává útočník na konkrétní systém.

[38] Exploit – jedná se o program, zdrojový kód nebo posloupnost příkazů, které slouží k využití chyby v aplikaci. Tato chyba vzniká při tvoření programu. Kvůli systémovým nedostatkům („dírám“) autoři programů tvoří tzv. záplaty (patch), které slouží k vylepšení aplikace či programu.

- chybně nakonfigurovaná síť, nepoužívání firewallu[39] apod.



Obr. 22. Firewall

[http://www.microsoft.com]

4.1 Zranitelnost kvantové kryptografie

O prolomení kvantové kryptografie je řada článků, otázkou je, které se v celém rozsahu zakládají na pravdě. V mnoha případech se jedná o různá tvrzení a domněnky, které nejsou podloženy skutečným důkazem. Částečně tato tvrzení podléhají tlakům výrobců kvantových produktů. Svou roli zde hraje reklama a konkurence.

Ovšem jedno zajímavé tvrzení, které přinesl Vadim Makarov z univerzity v norském Trondheimu, říká, že velké množství současných implementací kvantové kryptografie je zranitelné. Nejde o fyzikální objev ani o zpochybnění teoretických základů. Jedná se o problém s uspořádáním detektorů laserových pulzů. Výsledkem je, že komunikaci lze odposlouchávat bez příjemcova zjištění. Cílem k úspěchu je ovládnout hardwarové zařízení, to zvyšuje úspěšnost útoku téměř na cokoliv. Odposlech je směřován na klíč

[39] Firewall – síťové zařízení používané k řízení a zabezpečení síťového provozu. Určuje pravidla pro komunikaci mezi sítěmi, ty navzájem od sebe odděluje.

posílaný nezabezpečeným kanálem. Názor odborníků zní, že typ útoku je spíše realizovatelný v teoretické rovině než použitelný v praxi.

Kvantová kryptografie funguje na principu sdílení tajného klíče. Každá číslice z tajného klíče je zakódovaná do polarizace jednotlivých fotonů. Odesílatel vysílá proud fotonů v binárním tvaru 0 nebo 1. Pro každou hodnotu si vybere jeden ze dvou způsobů, jak číslici zakódovat. Příjemce neví, který systém odesílatel používá, tudíž musí být schopný dekódovat oba typy. Pomocí dvou párů fotonových detektorů pro každý systém. Pokud foton dosáhne správné dvojice, je správně dekódovaný, pokud ne, dostane příjemce falešný výsledek. Když je přenos u konce, odesílatel sdělí příjemci nezabezpečeným kanálem, který systém používá pro každý foton. Bity dekódované nesprávně se odstraňují a vzniká konečný tajný klíč pro pozdější komunikaci. V praxi se tyto kroky provádějí automaticky s využitím počítačového systému. Při odposlechu útočníkem konečný tajný klíč obsahuje chyby a odhalí útočníkovu přítomnost.

Makarov a jeho kolegové ukázali, že útočník může kontrolovat příjemcovo zařízení. Útočník s příjemcem budou dekódovat přesně stejné bity vysílané od odesílatele. Při sdělení, které fotony jsou zakódovány chybně, může útočník zjistit klíč odposlechem nezašifrované zprávy. Přičemž nedojde k žádným dalším chybám v neshodě bitů.

Metoda využívá typ fotonů, který může jeho citlivost snížit o velmi jasný záblesk světla. Útok začíná, když útočník zasáhne pulsem světla na všechny čtyři detektory v zařízení na straně odesílatele. Poté může útočník poslat druhý pulz a cílem je jeden ze čtyř detektorů. Pulz je dávka mnoha jednotlivých fotonů, všechny kódované jedním ze dvou kvantových systémů a všechny nesou stejnou číslici.

Odesílatelův paprsek nejdříve posílá polovinu fotonů na každý pár detektorů. Fotony dopadnou na detektor a není-li tento detektor určen pro tento systém kódování, jsou fotony rozděleny opět dál mezi dvěma detektory.

Počáteční polovina impulsu, který dosáhne dvojice určené pro tento systém kódování, je zaměřena na jeden detektor. V tomto případě s takovou intenzitou, aby nepřekročil svůj práh, a to vede k zaznamenání číslice.

Způsobem zaslání sekvence zakódovaných fotonů, které jsou stejné s těmi, které dostává od odesílatele, může útočník bezpečně zachytit klíč. Přičemž nejsou detekovány kvantové chyby.

Makarov odhalil tyto chyby ve dvou ze tří typů běžně používaných kvantových zařízeních. Nyní se hledá způsob, jak vyřešit výše popsaný nedostatek.

Odborníci uznávají objevení chyby, ale zároveň poukazují, že použitý silnější světelný pulz na primární detektor může příjemce zaregistrovat a rozpoznat útok. Dále se shodují, že se nejedná o vážně nebezpečnou chybu. Závěrem lze říct, že se jedná spíše o teoretickou slabost, nikoliv praktickou.

4.2 Útok na kvantovou kryptografii

Níže popsaný útok je pravděpodobně nejefektivnější z útoků na protokol BB84. Jedná se o individuální útok, útočník manipuluje s každým přicházejícím qubitem. Opakem individuálních útoků jsou kolektivní útoky.

Funkce útoku spočívá, že útočník umístí do cesty kvantové hradlo. Prvním vstupem v hradle bude posílaný foton a druhým bude útočníkův připravený kvantový stav. Produktem interakce je kvantové provázání obou stavů, tzv. entanglement. Zjednodušeně řečeno jde o stav nesoucí nějakou informaci o posílaném stavu. Tuto informaci jde konkrétním měřením získat. Důležitá informace je, že si útočník může nastavit, jak interakce komunikaci ohrozí. Čím více se útočník objevuje, tím více chyb se vyskytuje na straně odesílatele a příjemce.

Zdroje fotonů, přenosový kanál a detektory vnáší do přenosu chyby. Takové chyby se nedají rozlišit od útočníkových pokusů o útok. Pokud by útočník produkoval menší počet útoků než počet nevynucených chyb, nelze ho teoreticky odhalit. Nutno dodat, že útočník by získal méně informací než je v principu možné.

Nabízí se tedy otázka: jde plnohodnotně odposlechnout klíč? V tomto konkrétním typu útoku odpověď zní ne. Kvantová distribuce klíče nepředstavuje jen kvantově – mechanickou část, ale i postprocesing[40] informací a komunikaci po klasické lince mezi odesílatelem a příjemcem. Řádově se neodesílají desítky qubitů, ale mnohonásobně více. V QKD existují tzv. důkazy bezpečnosti, které počítají, kolik je možné získat informací

[40] Postprocesing – v překladu: následné zpracování.

libovolným fyzikálním měřením. Výsledek nám řekne, jaká je přenosová rychlost klíče pro určitou vzdálenost.

V popsaném případě odposlechu na jednom qubitu má útočník informaci o klíči. Ovšem toto nepředstavuje QKD, protože teoreticky jednobitový klíč je nepoužitelný. O kvantovou distribuci klíče se jedná až v případě přenosu s mnoha qubity. Také zde má útočník informace o klíči po skončení první fáze, tzv. kvantové. Následný postprocesing útočníka o informaci o klíči připraví, a tudíž je přenos klíče bezpečný. Postprocesing sníží nepatrně délku výsledného klíče.

4.3 Pokus o prolomení QKD

Předností kvantové kryptografie je možnost rychle zjistit případný odposlech. Vědci Feihu Xu, Bing Qi a Hoi-Kwong Lo z Torontské univerzity v Ontariu v květnu v roce 2010 vydali zajímavý článek. „Důkazy nepodmíněné bezpečnosti různých protokolů distribuce kvantového klíče (QKD) jsou postaveny na zidealizovaných předpokladech. Jedním z klíčových předpokladů je: odesílatel [kvantového klíče] (Alice) může požadované kvantové stavy připravit bez chyb. Ovšem takový předpoklad může být narušen v reálných QKD systémech.“[41]

Citovaný úryvek lze shrnout, že reálný systém pro přípravu šifrovacích klíčů má určité vady. Slabiny mohou útočníkovi pomoci nabourat se do přenosu a odposlouchávat tak komunikaci. Útočníkovi přitom nehrozí odhalení. Vědci dále v článku popisují, jak simulovali útok, který by využil slabin systému pro QKD.

Všeobecně, co se týká odposlechu má kvantová kryptografie velkou výhodu. Odposlech systému (narušení odposlechem) se detekuje, tzn. útočník je odhalen. Co za tak zdánlivě jednoduchým způsobem stojí? Odposlech představuje z pohledu fyziky určitý způsob měření. Kvantová mechanika všechny měření (odposlechy) provedené na systému konkrétní systém narušuje, řekněme, že jej mění. Tyto změny nejsou nepatrné a jde si jich okamžitě všimnout.

---

[41] *Scinet* [online]. 2006-2008 [cit. 2011-03-06]. Selhala nejbezpečnější technika pro přenos informací? Dostupné z WWW: <http://www.scinet.cz/selhala-nejbezpecnejsi-technika-pro-prenos-informaci.html>. ISBN 1803-1277.

U protokolu BB84 se hranice šumu uvádí s tolerancí 20%. Registruje-li příjemce odchylky větší než 20%, je na místě mít podezření, že je komunikace odposlouchávána.

Výše zmíněný tým vědců jeden konkrétní komerční systém odposlouchával. Úroveň chyb splňovala hranici 20%. Konkrétně naměřená hodnota byla 19,7%. Pomyslná hranice šumu 20% „pracuje“ jen jedním směrem.

Pokud úroveň šumu překročí 20% → velká pravděpodobnost odposlechu.

Ovšem opačným směrem, tzn. pod hranici 20%, tvrzení neplatí.

Důležitý je zvolený přístroj, který poskytuje komunikaci (s jakou garancí). Hranice šumu v systému pod 20% může být také odposlouchávána.

Vědci přišli s nápadem, že zkusili napadnout zdroj šumu, který vzniká, když odesílatel připravuje pro příjemce kvantové stavy pro generování šifrovacího klíče. Tím pádem může útočník získat dostatečné množství informací o klíči, přičemž se nezvýší úroveň šumu přes důležitou hranici 20%. Útočník v tomto případě zůstane nezpozorován. Tento typ útoku byl konkrétně proveden na komerčním zařízení ID-500 od známé švýcarské společnost Id Quantique.

Po zveřejnění článku se okamžitě objevila řada reakcí. Většina odborníků tvrdí, že jde o nesmysl. Jedna z reakcí je zde: „S tím článkem to jaksi přepískli. Tvrzení, která ze svého výzkumu odvodili, jsou naprosto přehnaná,“ řekl pro Physics World Gregory Ribordy ze společnosti Id Quantique. Dále upozornil, že použitý systém pro distribuci klíče je zastaralý. Nevyrábí se od roku 2004. „Tento typ útoku by navíc v komerčních aplikacích vůbec nefungoval.“[42]

Zakladatel Id Quantique, Nicolas Gisin z Ženevské univerzity, má stejný názor. „Jejich tvrzení jsou velmi nadsazená, protože nalezená chybová míra 19,7% hodně převyšuje

[42] *Scinet* [online]. 2006-2008 [cit. 2011-03-07]. Selhala nejbezpečnější technika pro přenos informací? Dostupné z WWW: <http://www.scinet.cz/selhala-nejbezpecnejsi-technika-pro-prenos-informaci.html>. ISBN 1803-1277.

úroveň 8%, která je implementována do komerčních systémů. Tedy tvrzení, že komerční systém pro distribuci kvantového klíče byl hacknut, je prostě nesmyslné.“[43]

Zajímavé je, že řada fyziků nebo jen nadšenců zkouší prolomit systém založen na kvantové kryptografii. Osobně si myslím, že je to prospěšné, jelikož tvoří jakýsi hnací motor vývojářům kvantových systémů. A svým způsobem hledají chyby, systém testují, co vydrží. Výše zmíněný typ útoku nebo pokusu o prolomení byl jeden z mnoha, který se neúspěšně pokusil hacknout systém QKD. Z řady pokusů o prolomení kvantové kryptografie jsem nezaznamenal žádný plnohodnotný úspěšný útok. Z tohoto pozorování usuzuji, že komerční kvantové systémy, které jsou nasazovány v dnešní době, dostatečně splní požadované prvky ochrany.

[43] *Scinet* [online]. 2006-2008 [cit. 2011-03-07]. Selhala nejbezpečnější technika pro přenos informací? Dostupné z WWW: <http://www.scinet.cz/selhala-nejbezpecnejsi-technika-pro-prenos-informaci.html>. ISBN 1803-1277.

II. PRAKTICKÁ ČÁST

5 KRYPTOGRAFIE V PRAXI

Několikrát jsem již zdůraznil vliv kryptografie na moderní svět a běžný život. Služby, na které narážíme každý den, jsou určitým způsobem spojeny právě s kryptografií. Ať již komunikace přes internet, jako je email nebo všeobecná ochrana informací, vyžaduje šifrování. V současnosti se v praxi používá „klasická“ kryptografie zastoupená symetrickými a asymetrickými šiframi. V menším zastoupení se vyskytuje kvantová kryptografie.

Krátce po objevení kvantového protokolu BB84 se distribuce klíče prováděla na malé vzdálenosti (jednotky až desítky centimetrů) a při velmi malých přenosových rychlostech (jednotky bitů za sekundu). Z počátku všechny tyto pokusy probíhaly jen v laboratorních podmínkách a nebyly začleněny do praxe. Důvodem byla nedostatečná technická řešení a všeobecně malá znalost tohoto odvětví. Pokrok nastal s nástupem optických vláken a detektorů fotonů. Přenosová rychlost a vzdálenost distribuce klíče se zvýšila na úroveň použitelnou v praxi.

5.1 Činnost ČR v oblasti kvantové kryptografie

Ministerstvo vnitra (MV) se mimo jiné zabývá státní podporou výzkumu a vývoje. Podle zákona č. 130/2002 Sb., o podpoře výzkumu a vývoje z veřejných prostředků a o změně některých souvisejících zákonů. Na MV se v roce 1994 začal tvořit systém státní podpory výzkumu a vývoje, který se mimo jiné zabývá i kryptoanalytickým rozborem kvantové kryptografie.

Pro zajištění činnosti je stanoven řídící orgán odbor vzdělání a správy policejního školství. Zdroje financí výzkumu a vývoje pocházejí z:

a) účelového financování,

b) institucionálního financování.

Hlavní cíle:

- reakce na aktuální oblasti vnitřní bezpečnosti a veřejného pořádku,
- formulovat kroky v boji proti bezpečnostním rizikům,
- zavádět postupy, které omezují působnost kriminality,

- zaměření na problémové okruhy,
- posilování represivního a preventivního působení státu v minimalizaci kriminality a zároveň zvyšování bezpečnosti České republiky.

5.1.1 Kryptoanalytický rozbor kvantové kryptografie

Doba řešení tohoto projektu je 3 roky a byl řešen od roku 1995. Řadí se do sekce ochrany státního tajemství a utajovaných skutečností MV.

Projekt je založen na prototypu kvantového šifrátoru, zabývající se ochranou dat v komunikačních systémech. Z kryptoanalytického rozboru, fyzikálně-teoretického rozboru dat a technického rozboru aparatury byla prozkoumána platnost kvantové mechaniky z pohledu tzv. q-deformovaných optických stavů a případné q-deformace Heisenbergových relací neurčitosti[44]. Z výsledků měření se stanoví hranice bezpečnosti kvantové kryptografie v komunikačních systémech a šifrátorech s optickými vlákny.

5.1.2 Aplikace kvantové informace v kryptologii

Doba realizace 6 let, projekt řešen od roku 1998, v roce 1999 byl tento projekt zařazen pod NBÚ. Příjemcem tohoto projektu je ústav informatiky a výpočetní techniky AV ČR.

Tématem řešení je oblast kvantové a klasické teorie informace z hlediska aplikované matematiky. Plně navazuje na kryptologický výzkum. Další okruhy zahrnují kvantové počítání a kryptografii z pohledu kvantové fyziky. S vizí sledování fyzikální realizace kvantového počítače, testování možných fyzikálních principů, na kterých je stavěna kvantová kryptografie.

5.1.3 Kvantová kryptografie a kvantový přenos informace

Projekt řešený také od roku 1998 po dobu 6 let. Projekt byl od roku 1999 zařazen pod NBÚ. Příjemce tohoto projektu je společná laboratoř optiky UP Olomouc a FzÚ AV ČR.

---

[44] Heisenbergův princip neurčitosti – matematická vlastnost dvou kanonicky (standardních) konjugovaných veličin. Nejznámější zástupci veličin jsou poloha a hybnost elementární částice v kvantové fyzice.

Realizace projektu zahrnuje výzkum kvantové kryptografie a telekomunikace. Patří sem oblasti experimentálního prototypu kvantového kryptografu s polarizovanými fotony.

Na tomto prototypu je prováděno fyzikální měření a přenos kvantové informace.

5.1.4 Aplikace kvantového počítání v kryptologii

Doba řešení projektu je 3 roky také od roku 1998. Projekt přešel od roku 1999 pod NBÚ. Příjemce projektu je sekce ochrany státního tajemství a utajovaných skutečností MV.

Zaměření na zabezpečení výzkumu bezpečnosti dostupných šifrovacích algoritmů, založených na výpočetní složitosti. „Je protiváhou výzkumu v oblasti kvantové kryptografie a kvantově kryptografických protokolů, které jedině mohou ochránit utajenou informaci proti libovolnému kryptoanalytickému útoku i v budoucnu.“[45]

5.1.5 Kvantové počítače a kryptografie z hlediska kvantové fyziky

Projekt byl zařazen na listinu řešených projektů v roce 1998 a doba řešení je 6 let. Od roku 1999 přešel pod NBÚ. Projekt je určen Matematicko-fyzikální fakultě UK Praha.

Projekt má za cíl demonstrovat souvislost mezi informatikou a fyzikou. Dostupná kvantová kryptografická zařízení jsou vhodná pro ověřování základních fyzikálních zákonů. Tyto zákony musí kvantové kryptografické protokoly dodržovat. Jde o stanovení dostupné meze pro kvantová zařízení a možnosti jejich konstrukce. Zabývá se možnostmi napadení kvantových kryptografií.

5.1.6 Projekt GA202/95/0002

Informační systém výzkumu, experimentálního vývoje a inovací eviduje a shromažďuje informace o řešených projektech, které jsem výše zmínil. Na představu, co takový projekt obsahuje a vyžaduje, jsem si vybral projekt GA202/95/0002.

Informace o projektu:

Identifikační kód: GA202/95/0002

---

[45] *Odbor vzdělání a správy policejního školství* [online]. 2005 [cit. 2011-03-07]. Ministerstvo vnitra ČR. Dostupné z WWW: <http://aplikace.mvcr.cz/archiv2008/ministerstvo/vyzkum.html>.

Důvěrnost údajů: S – Úplné a pravdivé údaje nepodléhající ochraně podle zvláštních právních předpisů

Název v původním jazyce: Kryptoanalytický rozbor kvantové kryptografie

Poskytovatel: GA0 - Grantová agentura České republiky (GA ČR)

Program: GA - Standardní projekty (1993-…)

Hlavní obor: BE - Teoretická fyzika

Zahájení řešení: 1995

Ukončení řešení: 1997

Poslední stav řešení: K - Končící víceletý projekt, tj. projekt, který byl řešen již v předcházejícím roce, příslušný rok sběru dat je posledním rokem účinnosti smlouvy resp. vykonatelnosti rozhodnutí o poskytnutí podpory

Finance projektu:

Období	1995	1996	1997	za celou dobu řešení
Výše podpory ze státního rozpočtu	542 tis. Kč	793 tis. Kč	591 tis. Kč	1 926 tis. Kč
Celkové uznané náklady	542 tis. Kč	793 tis. Kč	591 tis. Kč	1 926 tis. Kč
Typ	plánované	plánované	přidělené	předpokládané

Cíle řešení v původním jazyce: Kryptoanalytický rozbor experimentálních dat na zkonstruovaném prototypu kvantového šifrátoru za účelem ochrany dat v komunikačních systémech. Fyzikální podstata spočívá v experimentálním ověření přenosu polarizovaných signálů optickým vláknem, stanovení chybovosti, prověření jednofotonové detekce při respektování kvantově mechanického principu neurčitosti konjugovaných veličin. Na základě kryptoanalytického rozboru a fyzikálně-teoretického rozboru dat a technického rozboru aparatury bude prověřena platnost kvantové mechaniky z hlediska

	q-deformovaných optických stavů a případné q-deformace Heisenbergových relací neurčitosti. Ze získaných experimentálních a teoretických výsledků se stanoví hranice bezpečnosti kvantové kryptografie v komunikačních systémech a šifrátorech s optickými vlákny
Rok dodání údajů do CEP:	1997
Systémové označení dodávky dat:	CEP/1997/GA0/GA07GA/V/9:7

Účastníci projektu:

Počet příjemců:	1
Počet dalších účastníků projektu:	1
Příjemce:	Národní bezpečnostní úřad ČR
Řešitel:	RNDr. Jaroslav Hrubý, CSc. (státní příslušnost: CZ - Česká republika)
Další účastník projektu:	Univerzita Palackého v Olomouci
Řešitel:	Doc. Ing. Václav Sochor, DrSc. (státní příslušnost: CZ - Česká republika)
Účastník – organizační jednotka:	České vysoké učení technické v Praze / Fakulta jaderná a fyzikálně inženýrská

Výsledky projektu v RIV:

Počet výsledkův RIV: 0[46]

[46] *Informační systém výzkumu, experimentálního vývoje a inovací :Výzkum, vývoj a inovace podporované z veřejných prostředků ČR* [online]. 1.6.0. Praha : MathAn Praha, s.r.o., 2009 [cit. 2011-03-07]. Dostupné z WWW: < http://www.isvav.cz/projectDetail.do?rowId=GA202%2F95%2F0002>.

6 SPOLEČNOSTI ZABÝVAJÍCÍ SE KVANTOVOU KRYPTOGRAFIÍ

Kolem roku 2000 začaly soukromé společnosti vyrábět a distribuovat první zařízení pro kvantovou distribuci klíče a kvantové generátory čísel.

V České republice jsou také společnosti, které se zabývají prodejem zařízení založenými na kvantové kryptografii. Všechny společnosti či firmy v České republice, na které jsem narazil, zmíněné produkty pouze prodávají. Nezabývají se přímo s výrobou, ale spolupracují se zahraničními výrobci a dodavateli.

6.1 Id Quantique

Švýcarská firma se sídlem v Ženevě, která patří k průkopníkům kvantové kryptografie. První společnost, která kvantovou kryptografii uvedla na trh a to v roce 2001. Jedná se o přední světovou společnost ve vývoji pokročilých řešení zabezpečení vysokorychlostních přenosů dat postavených na kvantové, ale i klasické kryptografii. Společnost se přesněji zabývá oblastí síťové bezpečnosti a oblastí optických přístrojů. Id Quantique dodává kvantové produkty pro soukromé podniky, ale i pro orgány státní správy.

Obr. 23. Logo společnosti Id Quantique

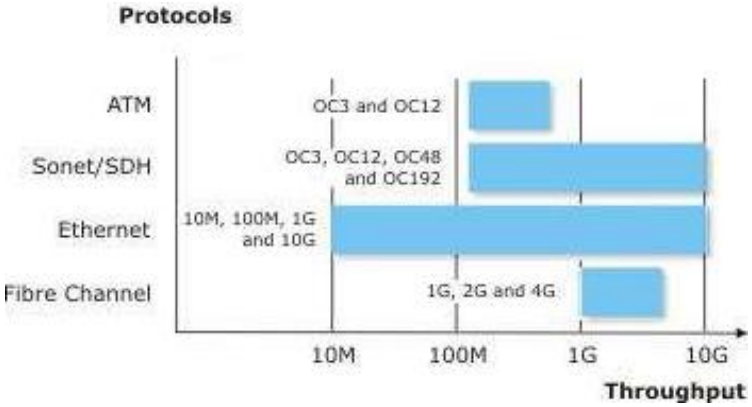
[http://www.idquantique.com]

6.1.1 Cerberis

Zařízení Cerberis nabízí nový přístup zabezpečení sítě. S využitím vysokorychlostního šifrování s kvantovou distribucí klíče (QKD). Pracuje na principu vysokorychlostního šifrovacího protokolu AES (Advanced Encryption Standard) a QKD. Zařízení se skládá ze serveru a šifrovacího zařízení.

Podporované protokoly:

- Ethernet až do 10Gbit/s
- Fibre Channel až do 4Gbit/s
- Sonet/SDH do 10Gbit/s
- ATM do 622Mbit/s



Obr. 24. Podporované protokoly

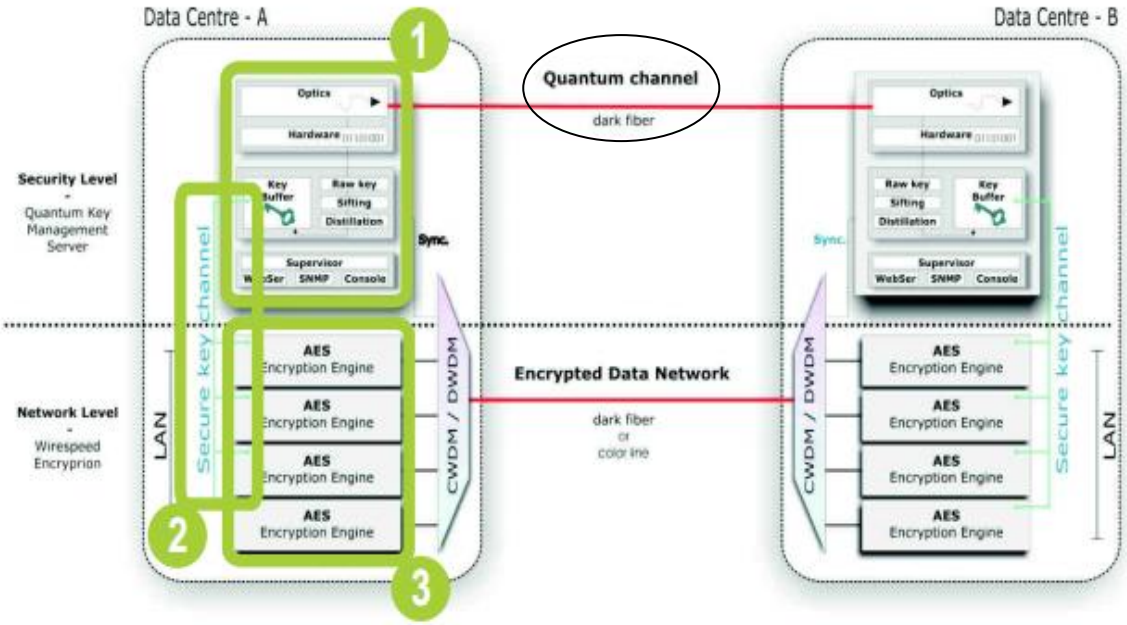
[http://www.idquantique.com]

Hlavní znaky:

- automatická obnova klíče
- univerzálnost – šifrátory pro různé protokoly
- bezpečná distribuce klíče prováděna přes optické vlákno (do vzdálenosti až 100 km).

Obr. 25. Zařízení Cerberis

[http://www.idquantique.com]



Obr. 26. Znázornění funkce zařízení Cerberis

[http://www.cryptodevice.com]

Jak můžeme vidět na obrázku, celé zařízení je rozděleno na 2 části. Security Level (QKD server) obstarává distribuci klíče kvantovým kanálem. Optika a příslušný hardware zajišťují distribuci klíče. Další část představuje Network Level, která se zabývá šifrovaným přenosem zprávy za využití standardu AES.

Podstatné na principu funkce je, že zařízení využívá pro přenos klíče jednu cestu a pro přenos zprávy cestu jinou. Po dohodnutí klíče a vyloučení odposlechu se začne přenášet zpráva.

1. QKD server:
    - Optická platforma Plug & Play
    - Protokol BB84/SARG
    - Dosah do 50km (větší dosah na vyžádání)
    - Přenosová rychlost větší než 1000bit/s
    - Server může vysílat až do 12 šifrátorů

2. Klíčový kanál (idQ3P):
    - Sériová linka
    - Šifrování AES-256
    - Autentizace HMAC-SHA-1
    - Rychlost výměny klíče: 1 klíč za minutu
3. Šifrovací zařízení:
    - Až do 10GB za sekundu
    - Protokoly (viz výše):
        i. Ethernet
        ii. Sonet/SDH
        iii. Fibre Channel (FC)
        iv. ATM

Zařízení Cerberis disponuje moderními technologiemi. Konkrétně zařízení Cerberis obstálo u zabezpečení švýcarských voleb (viz 6.4), což potvrzuje jeho kvalitu a demonstruje praktické využití.

Nedostatek spatřuji ve vzdálenosti distribuce klíče. Nejedná se o nedostatek u tohoto konkrétního zařízení, ale o současné možnosti kvantové kryptografie. Distribuce klíče u zmíněných voleb ve Švýcarsku probíhala na vzdálenost 4km, to je v pořádku. Ovšem např. kdyby se jednalo o volby v ČR a hlasovací místnosti by byly v krajských městech a datové centrum v Praze, již by vznikl problém ve velké vzdálenosti. Zabezpečení by se muselo poté řešit jiným způsobem, navrhoval bych využít „klasické kryptografie“.

6.1.2 Clavis

Systém Clavis slouží zejména k účelům výzkumu v oblasti kvantové kryptografie. Clavis je založen na optické platformě, která nabízí výbornou stabilitu a interferenční kontrast. Bezpečná výměna klíčů je možná do vzdálenosti 100km. Clavis se skládá ze dvou stanic.

Obr. 27. Systém Clavis

[http://www.idquantique.com]

Vlastnosti:

- Vynikající stabilita a kontrast
- Kompatibilní s WDM[47]
- Bezpečná výměna klíčů do100 km
- Protokoly BB84 a SARG
- Komplexní sada software, výkonný grafický nástroj pro analýzu (viz obr. 28.)
- C++ knihovna pro možnost programování systému

Obr. 28. Ukázka nástroje pro analýzu

[http://www.idquantique.com]

[47] WDM - Wavelength Division Multiplex. Vlnové multiplexování.

Využitelnost:

- Kryptografický a kvantový výzkum
- Aplikace nových protokolů
- Odborná příprava a vzdělání

Výhodu u tohoto zařízení spatřuji v integrovaném nástroji pro analýzu, který slouží k výukovým a výzkumným účelům. Přináší užitečné informace např. o rychlosti generování klíče a další informace o klíči. Tyto informace se dále zpracovávají a analyzují.

6.1.3 Quantis

Z kvantové teorie vychází i zařízení nesoucí název Quantis - Kvantový generátor náhodných čísel (Quantum Random Number Generator). Je založen na postupném vysílání fotonů na poloprůhledné zrcadlo. Přechod fotonu nebo odraz fotonu je zaznamenán jako hodnota 0 nebo 1. Zařízení disponuje ve své třídě nejlepší bitovou rychlostí generování náhodných čísel.

Vlastnosti:

- Náhodné generování čísel
- Přenosová rychlost až 16Mb/s
- Kompaktní a spolehlivý
- Snadná integrace do stávajících aplikací

Vyrábí se ve třech provedeních: jako PCI karta, USB zařízení a OEM modul.

Obr. 29. Quantis v provedení jako PCI karta, USB zařízení a OEM model

[http://www.idquantique.com]

Praktické využití:

- Kryptografie
- Hazardní hry, loterie
- Zabezpečený tisk
- Statistický výzkum

6.2 Společnost L2K

Název L2K představuje českou společnost založenou v roce 1995 zabývající se IT. V polovině roku 2001 byla společnost rozšířena o divizi DataSec, která se výhradně zaměřuje na počítačovou bezpečnost. Nabízí výrobky bezpečnostních technologií v oblasti IT Security. Společnost L2K spolupracuje se společností Id Quantique a prodává její produkty v České republice a zastupuje ji na českém trhu. Významnějšího distributora kvantových produktů jsem na českém trhu nenašel.

L2K je společností prověřenou NBÚ (potvrzení č. 2145) a je držitelem certifikátu ISO 9001:2001 pro systém managementu jakosti.

6.3 MagiQ

MagiQ je americká společnost založená v roce 1999. Společnost se zabývá např. vývojem optických vláken, optickými senzory a mimo jiné také zařízeními založenými na kvantové kryptografii.

Strategie společnosti je pochopit potřeby zákazníků a splnění jejich požadavků, spojeno s moderními řešeními. Proto patří mezi její zákazníky například NASA, DARPA, U.S. ARMY a další.

Obr. 30. Logo společnosti MagiQ

[http://www.magiqtech.com]

6.3.1 QPN™ Security Gateway (QPN – 8505)

Zařízení QPN 8505 představuje systém založený na kvantové kryptografii v kombinaci s klasickou kryptografií. Zařízení kombinuje ochranu pomocí VPN[48] a zároveň zabezpečení pomocí kvantové kryptografie. Zařízení je vybaveno optikou pro QKD s vysílačem a přijímačem.

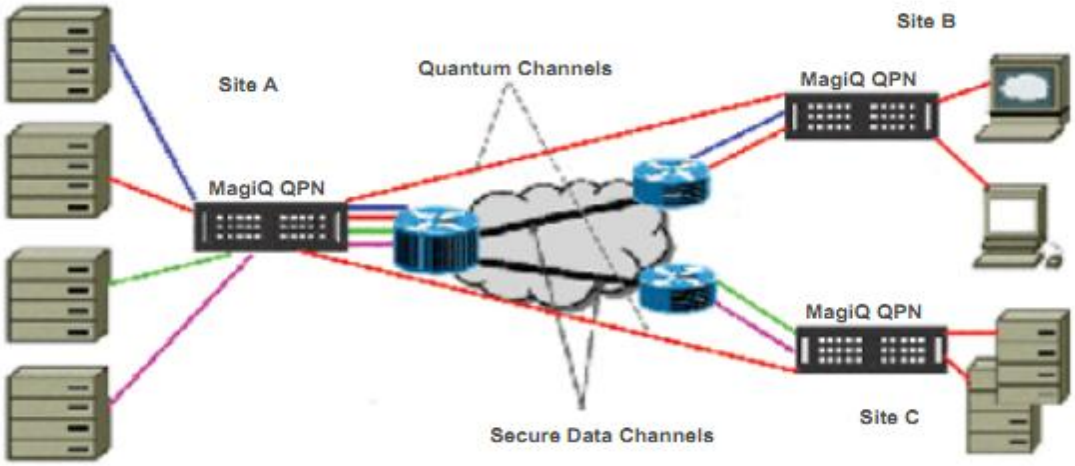
Obr. 31. QPN™ Security Gateway (QPN – 8505)

[http://www.magiqtech.com]

Vlastnosti:

- Generátor náhodných čísel
- Frekvence obnovy klíče: 100 klíčů/s
- Síťová kompatibilita
- Podporuje protokoly BB84, AES a 3DES
- Přenos na vzdálenost až 100km
- Rozhraní: až 16x RJ45 konektor, 10/100 Ethernet
- Další technické parametry v PŘÍLOZE P V: MagiQ QPN™ Security gateway 8505

[48] VPN – virtuální privátní síť (virtual private network). Propojení několika PC prostřednictvím veřejné sítě (internet), doprovází bezpečnostní riziko. Pomocí VPN lze propojit PC v rámci jedné uzavřené (důvěryhodné) sítě. Při tomto typu propojení je totožnost ověřována digitálními certifikáty, dochází k autentizaci.



Obr. 32. Přenos dat QPN™ Security Gateway (QPN – 8505)

[http://www.magiqtech.com]

Na obr. 32. můžeme vidět rozdělení komunikačních kanálů na zabezpečený VPN kanál (Secure Data Channels) a kvantový kanál (Quantum Channels) pro kvantovou distribuci klíče. Toto řešení zaručuje zvýšenou bezpečnost. Informace se přenáší až ve chvíli, kdy je detekce odposlechu klíče na kvantovém kanálu v pořádku.

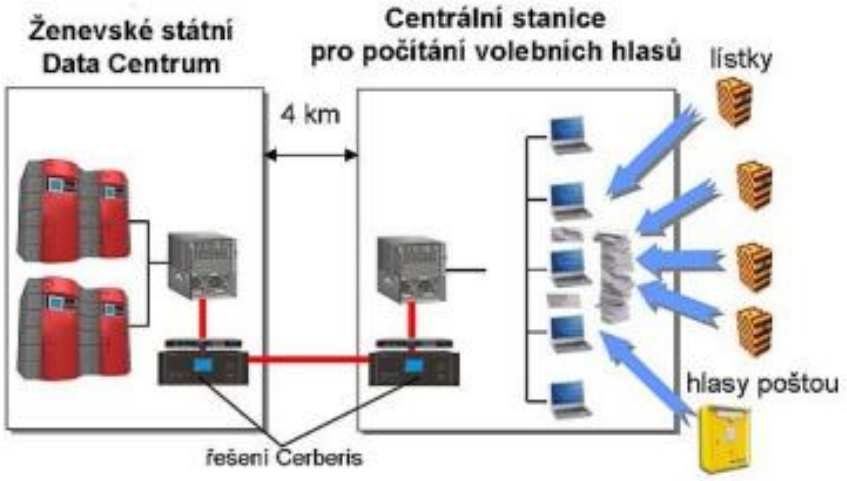
MagiQ QPN 8505 jt určen především pro vládní a vojenské oblasti a shromažďování zpravodajských informací. Zařízení lze využít i v komerční sféře např. finanční služby a vnitřní bezpečnost.

6.4 Zabezpečení voleb v Ženevě 2007

Dne 31. října 2007 se uskutečnili Federální volby v Ženevě. Na této větě není nic výjimečného. Ovšem poprvé v historii byla v parlamentních volbách použita kvantová kryptografie pro zabezpečení sčítání hlasů. Technické řešení zajišťovala již zmíněná švýcarská společnost Id Quantique.

„Chtěli bychom zabezpečit optimální bezpečnostní podmínky pro sčítání hlasů“, řekl státní kancléř Ženevy Robert Hensler.

Místnost pro sčítání volebních hlasů byla od datového centra vzdálena 4km. Přenos byl řešen optickou trasou.



Obr. 33. Schéma realizace zabezpečení

[http://www.cryptodevice.com/pdf/idquantique/Pripadova_studie-Swiss_National_Elections.pdf]

Praktickou implementací je systém Cerberis od firmy Id Quantique. Instalace zařízení a uvedení do provozu trvalo 30 minut.

Vzhledem k úspěšné implementaci je v plánu každé další volby v kantonu zabezpečovat kvantově kryptografickým řešením „Cerberis“. Bylo již např. použito pro volby „Constituante“ 19. října 2008. Pod vedením profesora Gisina z Ženevské university vznikl project „SwissQuantum“, v jehož rámci má v kantonu vzniknout např. vysokorychlostní páteřní zabezpečená síť v celé oblasti ženevského jezera, jejíž vznik experti významem přirovnávají ke vzniku prvních internetových linek v USA v 70-tých letech.“[49]

Toto řešení představuje implementaci zařízení Cerberis do konkrétního projektu. Nabízely se samozřejmě i jiné způsoby zabezpečení s menšími finančními nároky. Švýcarsko společně se společností Id Quantique tímto ukázali nový způsob zabezpečení oblastí, jako jsou volby. V případě důležitosti a utajení informací je určitě zvolené řešení správné a bezpečné.

[49] http://www.cryptodevice.com/pdf/idquantique/Pripadova_studie-Swiss_National_Elections.pdf

6.5 Zhodnocení kvantových produktů

Po prozkoumání nabízených produktů společností IdQuantique a MagiQ jsem dospěl k následujícím informacím. Americká společnost MagiQ se zabývá větší škálou produktů, již zmíněná výroba optických vláken, laditelných laserů a senzorů. V aktuální nabídce této společnosti jsem našel pravděpodobně jejich nejlepší současné zařízení MagiQ QPN™ Security gateway 8505. Společnost IdQuantique se mimo kvantově kryptografické produkty zabývá vědeckým vybavením. V nabídce této společnosti se nachází více produktů na bázi kvantové kryptografie a kvantových generátorů náhodných čísel (Cerberis, Clavis…).

Výše popsané kvantové produkty patří mezi nejmodernější zařízení, která jsou nyní na trhu k dispozici. Tyto produkty ve většině případů nacházejí uplatnění ve státním sektoru a v armádách vyspělých států. Slouží k zabezpečení nejdůležitějších informací, v naší právní normě informace typu přísně tajné nebo tajné. Např. česká společnost L2K dodala zařízení od společnosti Id Quantique ozbrojeným složkám státu ČR. Podrobnější informace jsem nezískal, jelikož se jedná o citlivé informace, které nelze sdělovat veřejnosti.

Rozhodně méně jsou tato zařízení rozšířená v soukromém sektoru. V PKB jsem nenašel žádnou implementaci kvantového produktu za účelem ochrany informací. Výjimku zde tvoří banky, kde není výskyt zanedbatelný. Za menším rozšířením v soukromém sektoru vidím převážně dvě příčiny. První překážka je ve vysoké pořizovací ceně. Ceny nejmodernější kvantových zařízení k bezpečné distribuci klíče se pohybují v desítkách až statisících amerických dolarů. Další překážku spatřuji v důvodu neměnit stávající zabezpečení s využitím „klasické“ kryptografie. Současné aplikované symetrické a asymetrické algoritmy jsou dostatečné k bezpečné distribuci informací. Např. šifra AES, u které doposud není známo úspěšné prolomení.

Kvantová kryptografie představuje nejmladší odvětví zabezpečení informací s vysokou garancí bezpečnosti. Ovšem tuto „dokonalou“ metodu omezují již zmíněné nevýhody (viz kapitola 2.2.5). Například všechny zmíněné zařízení disponují vzdáleností pro přenos klíče okolo 100km, což vidím jako problém pro globální nebo mezistátní komunikaci. Dále problém s topologií sítě.

Předpokládaný vývoj kvantové kryptografie se bude zaměřovat především na zvýšení vzdálenosti pro přenos klíče a přenosové rychlosti. Podaří-li se tento problém zlepšovat,

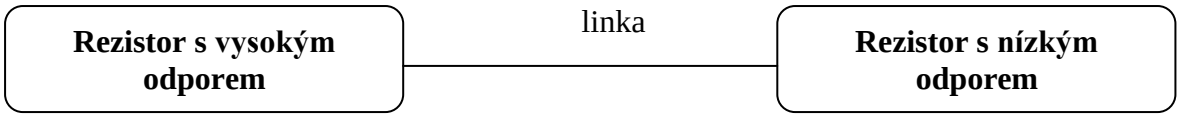
určitě QKD zařízení najdou větší uplatnění. Další rozhodující faktor pro větší rozšíření je cena. Myslím si, že pokud cena výrazněji neklesne, soukromý sektor nebude upřednostňovat tento typ zabezpečení.

Dle mého názoru je kvantová kryptografie se svým rozšířením na pomyslném vrcholu. Nepředpokládám, že by někdy zcela vytlačila „klasickou“ kryptografii nebo získala dominantní postavení. K takovému názoru mě přivedly zmíněné nevýhody a postoje odborníků.

6.5.1 Alternativa kvantové kryptografie

Jednu z možných budoucích alternativ kvantové kryptografie představili v roce 2007 američtí vědci. Jedná se o způsob šifrování zpráv založený na náhodném pohybu elektronů ve vodiči.

Metodu představil Laszlo Kish z texaské A&M University. Princip funkce spočívá v posílání dat v nepravidelných intervalech. Data jsou také maskována jako teplený šum. Šifrování i dešifrování vykonávají rezistory na každém konci linky. Oba rezistory produkují náhodný šum, mezi který se přiloží signály zprávy.



Obr. 34. Možná realizace metody

V případě pokusu o útok narušitel nerozezná střední úroveň signálu. To znamená, že nepozná přenášené data od šumu. Pokud by se útočníkovi signál podařilo od šumu oddělit, nepřevedl by jej do digitální podoby, protože nezná nastavení rezistorů.

Další obrana proti útoku je, že se změní úroveň šumu linky, a tím pádem se příjemce o narušení dozví.

Popsaná metoda doručila klíče na 2000km, jednalo se o test. Což je v porovnání s kvantovou kryptografií několikanásobně více. Porovnání kvantové kryptografie a výše popsané metody je zajímavé. Otázkou zůstává, zda se metoda dostane i do komerčního prostředí a nějakým způsobem zasáhne do konkurence v oblasti ochrany informací, nebo zůstane jen v laboratořích.

ZÁVĚR

V diplomové práci jsem popsal metody kvantové kryptografie, dostupné produkty, společnosti a vztah ČR k oblasti kvantové kryptografie. Snažil jsem se vysvětlit výhody a nevýhody spojené s nasazením kvantové kryptografie pro ochranu informací v praxi.

V teoretické části jsem charakterizoval kvantovou kryptografii, její historii, protokoly a principy. Porovnal jsem vlastnosti „klasické“ kryptografie s kvantovou kryptografií a tyto vlastnosti analyzoval. Uvedl jsem příklad kvantové distribuce klíče u protokolu BB84. Upozornil jsem na příčiny, které mě přesvědčily, že kvantovou kryptografii pravděpodobně nečeká velká budoucnost. Mnoho článků tvrdí opak, ale myslím si, že jsou ovlivněny částečně reklamou a snahou přesvědčit zákazníky o „dokonalosti“ kvantové kryptografie. Vysvětlil jsem pojem „utajované informace“ a proč je nutné tyto informace chránit před případným ohrožením.

V praktické části informuji o projektech České republiky spojených s kvantovou kryptografií. V další části se zabývám společnostmi, které se zaměřují na produkty založené na kvantové kryptografii. Na závěr jsem se věnoval zhodnocení kvantových produktů.

Diplomová práce přináší přehled o kvantové distribuci klíče a jejím praktickém využití. Práce může najít uplatnění a poskytnout informace při rozhodnutí společností nebo státních orgánů, zda využít k ochraně informací právě kvantovou kryptografii.

Kvantová kryptografie je stále ve stádiu výzkumu. Prvních několik společností zabývajících se kvantově kryptografickými zařízeními ukazuje současný směr a vývoj těchto produktů. Možná se za pár let ukáže, zda můj názor na vývoj kvantové kryptografie je pravdivý, či se mýlím. Na druhou stranu bych byl rád, kdyby se kvantová kryptografie v budoucnu více začlenila do ochrany informací.

Co nelze kvantové kryptografii upřít, je její vývoj. Donedávna se kvantová distribuce klíče řešila na papíře, v laboratořích nebo výzkumných ústavech. V dnešní době se již vyskytují zařízení QKD a generátory náhodných čísel, které poskytují kvalitní úroveň zabezpečení.

V současné době si zákazník v oblasti bezpečnosti informací může vybrat řešení s nasazením „klasické“ kryptografie nebo kvantové kryptografie. Důležité je si uvědomit výhody a nevýhody jednotlivých řešení a u výběru s nimi počítat.

ZÁVĚR V ANGLIČTINĚ

In the thesis I described methods of quantum cryptography, available products and companies in the field of quantum cryptography. I tried to explain advantages and disadvantages linked to setting of quantum cryptography for protection of information in practise.

In theoretical part I described quantum cryptography, its history, records and principles. I compared characters of „classical" cryptography with quantum cryptography and I also analysed those characters. I pointed out an example of quantum distribution of key at BB84 record. I refered to causes which persuaded me that quantum cryptography probably won't expand too much in future. Plenty of articles assert the contrary but I think they are partly influenced by advertisement and endeavour to persuade customers about „perfection" of quantum cryptography. I explained the concept „classified information" and why it's necessary to protect this information from contingent menace.

In practical part I inform about projects of Czech Republic connected with quantum cryptography. In the next part I deal with companies which focus on products based on quantum cryptography. In the last part I attended to evaluation of quantum products.

The thesis brings summary of quantum distribution of key and its practical usage. The thesis can find use and provide information during decisions of companies or state organs whether to use quantum cryptography to information protection.

Quantum cryptography has still been in research stage. First few companies dealing with quantum cryptographical equipment show present direction and development of those products. Maybe in few years my opinion about quantum cryptography development will turn out to be truth or not. On the other hand I would be glad if quantum cryptography gets more involved in protection of information in future.

What cannot be denied to quantum cryptography is its development. Until recently quantum distribution of key was solved on paper, in laboratories or research institutions. Nowadays the QKD equipment and generators of random numbers which provide high-quality level of security have occured.

At the present time customer in the field of protection of information can choose solution with „classical“ cryptography or quantum cryptography setting. It’s important to be aware of advantages and disadvantages of particular solutions and count on them while choosing.

SEZNAM POUŽITÉ LITERATURY

Literatura:

[1] POLKINGHORNE, John. *Kvantová teorie*. První vydání v českém jazyce. Praha : Dokořán, 2007. 119 s. ISBN 978-80-7363-084-3.

[2] Zákon číslo 412/2005 Sb. O ochraně utajovaných informací a bezpečnostní spolehlivosti.

[3] PIPER, Fred, MURPHY, Sean. *Kryptografie : Průvodce pro každého.* Pavel Mondschein. 1. vyd. Praha : Dokořán, 2006. 157 s. ISBN 80-7363-074-5.

[4] LAMBROPOULOS, Peter; PETROSYAN, David. *Fundamentals of Quantum Optics and Quantum Information.* 1. Heraklion : Springer, 2007. 326 s. ISBN 978-3-540-34571-8.

[5] LAUCKÝ, Vladimír. *Speciální bezpečnostní technologie*. 1. vyd. Zlín : [s.n.], 2009. 223 s. ISBN 978-80-7318-762-0.

[6] TŘÍSKA, David. *Kryptografická ochrana*. Zlín, 2009. 102 s. Bakalářská práce. Univerzita Tomáše Bati ve Zlíně. Dostupné z WWW: < http://dspace.knihovna.utb.cz/bitstream/handle/10563/10800/t%C5%99%C3%ADska_2009_bp.pdf?sequence=1>.

[7] CHOWN, Marcus. *Kvantová teorie nikoho nezabije : Průvodce vesmírem*. 1. Zlín : Kniha Zlín, 2010. 200 s. ISBN 978-80-87162-59-0.

[8] VERTON, Dan. *Black Ice : Neviditelná hrozba kyberterorizmu*. 1. Gliwice : Helion S.A., 2004. 278 s. ISBN 83-7361-565-2.

[9] PAJTINOVÁ, Mária. *Metody kvantové kryptografie*. Brno, 2009. 49 s. Bakalářská práce. Vysoké učení technické. Dostupné z WWW: <www.vutbr.cz/www_base/zav_prace_soubor_verejne.php?file_id=18607>.

[10] MUSIL, Rudolf. Ochrana utajovaných skutečností. 1. vyd. Praha : Eurounion, 2001. 379 s. ISBN 80-85858-93-2.

[11] LAUCKÝ, Vladimír. *Technologie komerční bezpečnosti II*. 2. vyd. Zlín : [s.n.], 2007. 123 s. ISBN 978-80-7318-631-9.

[12] ČERNÝ, Josef a kolektiv. *Systemizace bezpečnostního průmyslu. Ochrana utajovaných skutečností*. 6. díl. 26 s.

Internetové zdroje:

[13] JANČOVIČ, Jakub. *Http://www.agrospolvb.cz* [online]. 2005 [cit. 2011-01-06]. Šifrování na Internetu a PGP. Dostupné z WWW: <http://www.agrospolvb.cz/paja/download/site/index.html>.

[14] KLIMÁNEK, Oldřich. *Dsl.cz* [online]. 18.6.2010 [cit. 2011-01-05]. Dostupné z WWW: <http://www.dsl.cz/clanek/1828-selhala-nejbezpecnejsi-technika-pro-prenos-informaci>.

[15] Wikipedie : Otevřená encyklopedie [online]. 2001 , 10.1.2011 [cit. 20011-01-20]. Dostupný z WWW: <www.cs.wikipedia.org/>.

[16] HÁLA, Vojtěch. Kvantová kryptografie. *Aldebaran bulletin* [online]. 4.5.2005, 3, 14, [cit. 2011-01-09]. Dostupný z WWW: <http://aldebaran.cz/bulletin/2005_14_kry.php>. ISSN 1214-1674. <http://www.aldebaran.cz/studium/fyzika/kvantovka.html#kvanta>.

[17] *Slovník cizích slov online* [online]. 1. 2006-2010 [cit. 2011-01-12]. Dostupné z WWW: <http://www.slovnik-cizich-slov.net/>.

[18] Národní bezpečnostní úřad [online]. 2007- , 16.1.2011 [cit. 2011-02-07]. Dostupný z WWW: <http://www.nbu.cz>.

[19] prof. RNDr. GRUSKA, DrSc. Josef. *Kvantové zpracování informace a kryptografie* [online]. 1. Brno : [cit. 2011-01-13]. Fakulta informatiky Masarykovy univerzity. Dostupné z WWW: <http://www.fi.muni.cz/research/formal-methods/quantum.xhtml>.

[20] HOUSER, Pavel. *Http://scienceworld.cz* [online]. 1. 2001 [cit. 2011-01-17]. Kvantové počítače: kde zůstává zdravý rozum stát. Dostupné z WWW: <http://scienceworld.cz/matematika/kvantove-pocitace-kde-zustava-zdravy-rozum-stat-4435>.

[21] *SecurityWorld* [online].IDG, 2011 [cit. 2011-01-26]. Dostupné z WWW: <http://securityworld.cz/>.

[22] *Lupa* [online]. 1999-2011 [cit. 2011-01-27]. Dostupné z WWW: <http://www.lupa.cz/>. ISSN 1213-0702.

[23] *L2K* [online]. Praha : 2010 [cit. 2011-02-03]. Dostupné z WWW: <http://www.l2k.cz/index.php> <http://www.cryptodevice.com>.

[24] ROSA, Tomáš. *Matematicko-fyzikální fakulty UK v Praze* [online]. Praha : 2006 [cit. 2011-02-14]. Seznámení s kvantovou kryptografií. Dostupné z WWW: <www.karlin.mff.cuni.cz/~tuma/ciphers08/qc_uvod_v4.ppt>.

[25] MAREK, Rudolf; DASTYCH, Jiří. *Systemonline* [online]. 2003 [cit. 2011-02-15]. Bezpečnostní politika v organizaci. Dostupné z WWW: <http://www.systemonline.cz/clanky/bezpecnostni-politika-v-organizaci.htm>.

[26] *Osel : Objective Source E-Learning* [online]. Praha : 2007 [cit. 2011-02-21]. Kvantová kryptografie na dálku. Dostupné z WWW: <http://www.osel.cz/index.php?zprava=760>. ISSN 1214-6307.

[27] DOBŘÍŠEK, Miroslav. *Scycore* [online]. Praha : České vysoké učení technické v Praze, 19.3.2005 [cit. 2011-02-21]. Komerční výrobky pro kvantovou kryptografii. Dostupné z WWW: <http://www.scycore.com/papers/cryptofest05_slides.pdf>.

[28] *Special service international* [online]. Praha : 2008 [cit. 2011-02-21]. Dostupné z WWW: <http://www.ssi.cz/>.

[29] *Chip online : Elektronický archiv časopisu Chip* [online]. Praha : Burda, 2006-2010 [cit. 2011-03-05]. Dostupné z WWW: <http://earchiv.chip.cz/cs/earchiv>.

[30] *Osel : Objective Source E-Learning* [online]. Praha : 2007 [cit. 2011-03-06]. Dostupné z WWW: <http://osel.cz/>.

[31] *Scinet* [online]. 2006-2008 [cit. 2011-03-06]. Dostupné z WWW: <http://scinet.cz/>. ISBN 1803-1277.

[32] *Odbor vzdělání a správy policejního školství* [online]. 2005 [cit. 2011-03-07]. Ministerstvo vnitra ČR. Dostupné z WWW: <http://aplikace.mvcr.cz/archiv2008/ministerstvo/vyzkum.html>.

[33] *Informační systém výzkumu, experimentálního vývoje a inovací : výzkum, vývoj a inovace podporované z veřejných prostředků ČR* [online]. 1.6.0. Praha : MathAn Praha, s.r.o., 2009 [cit. 2011-03-07]. Dostupné z WWW: <http://www.isvav.cz/>.

[34] *IDQ : FROM VISION TO TECHNOLOGY* [online]. Switzerland : 2001 [cit. 2011-02-21]. Dostupné z WWW: <http://www.idquantique.com/>.

[35] *MagiQ* [online]. Boston : 2002-2009 [cit. 2011-04-04]. Dostupné z WWW: <http://www.magiqtech.com>.

[36] HOUSER, Pavel. *Computerworld* [online]. Praha : IDG, 31.5.2007 [cit. 2011-04-09]. Lepší kvantová kryptografie. Dostupné z WWW: <http://computerworld.cz/udalosti/lepsi-kvantova-kryptografie-2475>.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

Poznámka: zkratky jsou řazeny postupně podle výskytu v diplomové práci.

Č.	Číslo.
Sb.	Sbírky.
Např.	Například.
Atd.	A tak dále.
Stol.	Století.
USD	United States dollar.
USB	Universal Serial Bus.
Km	Kilometr.
Apod.	A podobně.
Tzv.	Tak zvané.
Viz	Rozkazovací způsob od slovesa vidět.
USA	United States of America.
LSD	Diethylamid kyseliny lysergové.
IT	Informační technologie.
s.r.o.	Společnost s ručením omezením.
PKB	Průmysl komerční bezpečnosti.
UT	Utajovaná informace.
EU	Evropská unie.
NATO	North Atlantic Treaty Organization.
NBÚ	Národní bezpečnostní úřad.
ČR	Česká republika.
CD	Compact Disc.
DVD	Digital Versatile Disc (Digital Video Disc).

HDD	Hard disk drive.
EZS	Elektronický zabezpečovací systém.
MU	Mimořádná událost.
MZS	Mechanické zábranné systémy.
KČ	Koruna česká.
QKD	Quantum key distribution.
MV	Ministerstvo vnitra.
AV	Akademie věd.
UP	Univerzita Palackého.
UK	Univerzita Karlova.
AES	Advanced Encryption Standard.
PC	Personal computer.

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM GRAFŮ

SEZNAM PŘÍLOH

PŘÍLOHA P I: PŘEHLED PRÁVNÍCH PŘEDPISŮ SOUVISEJÍCÍCH S OCHRANOU UTAJOVANÝCH INFORMACÍ

- Zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů.
- Zákon č. 413/2005 Sb., o změně zákonů v souvislosti s přijetím zákona o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů.

Prováděcí právní předpisy: [http://www.nbu.cz]

- Nařízení vlády č. 522/2005 Sb., kterým se stanoví seznam utajovaných informací, ve znění nařízení vlády č. 240/2008 Sb.
- Vyhláška č. 523/2005 Sb., o bezpečnosti informačních a komunikačních systémů a dalších elektronických zařízení nakládajících s utajovanými informacemi a o certifikaci stínicích komor.
- Vyhláška č. 524/2005 Sb., o zajištění kryptografické ochrany utajovaných informací.
- Vyhláška č. 525/2005 Sb., o provádění certifikace při zabezpečování kryptografické ochrany utajovaných informací.
- Vyhláška č. 526/2005 Sb., o stanovení vzorů používaných v oblasti průmyslové bezpečnosti a o seznamech písemností a jejich náležitostech nutných k ověření splnění podmínek pro vydání osvědčení podnikatele a o způsobu podání žádosti podnikatele (vyhláška o průmyslové bezpečnosti), ve znění vyhlášky č. 11/2008 Sb.
- Vyhláška č. 527/2005 Sb., o stanovení vzorů v oblasti personální bezpečnosti a bezpečnostní způsobilosti a o seznamech písemností přikládaných k žádosti o vydání osvědčení fyzické osoby a k žádosti o doklad o bezpečnostní způsobilosti fyzické osoby a o způsobu podání těchto žádostí (vyhláška o personální bezpečnosti).
- Vyhláška č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků, ve znění vyhlášky č. 19/2008 Sb.
- Vyhláška č. 529/2005 Sb., o administrativní bezpečnosti a o registrech utajovaných informací, ve znění vyhlášky č. 55/2008 Sb.

Příloha 1. Právní předpisy

PŘÍLOHA P II: PŘEHLED PRÁVNÍCH PŘEDPISŮ SOUVISEJÍCÍCH S OCHRANOU UTAJOVANÝCH INFORMACÍ

Citlivá činnost – zákony upravující citlivou činnost:

- Zákon č. 38/1994 Sb., o zahraničním obchodu s vojenským materiálem a o doplnění zákona č. 455/1991 Sb., o živnostenském podnikání (živnostenský zákon), ve znění pozdějších předpisů, a zákona č. 140/1961 Sb., trestní zákon, ve znění pozdějších předpisů.
- Zákon č. 18/1997 Sb., o mírovém využívání jaderné energie a ionizujícího záření (atomový zákon) a o změně a doplnění některých zákonů, ve znění pozdějších předpisů.
- Zákon č. 310/2006 Sb., o nakládání s některými věcmi využitelnými k obranným a bezpečnostním účelům na území České republiky a o změně některých dalších zákonů (zákon o nakládání s bezpečnostním materiálem).
- Zákon č. 376/2007 Sb., kterým se mění zákon č. 61/1988 Sb., o hornické činnosti, výbušninách a o státní báňské správě, ve znění pozdějších předpisů, a zákon č. 200/1990 Sb., o přestupcích, ve znění pozdějších předpisů.

Předpisy EU vztahující se k ochraně utajovaných informací.

Předpisy NATO vztahující se k ochraně utajovaných informací.

- Předpisy NATO nejsou určeny k volnému šíření, některé jsou označeny jako utajované informace.
- Bezpečnostní výbor NATO rozhodl, že lze veřejně publikovat níže uvedené předpisy:

- C-M(2002)49 [NU-PD]
- C-M(2002)49-COR3 [NU-PD]
- C-M(2002)49-COR6 [NU-PD]
- C-M(2002)49-COR8 [NU-PD]
- AC-35-D-2000-REV6
- AC-35-D-2003-REV4
- AC-35-D-2005-REV1
- C-M(2002)49-COR7
- AC-35-D-2002-REV3
- AC-35-D-2001-REV2

Příloha 2. Právní předpisy

PŘÍLOHA P III: CERBERIS TECHNICKÉ INFORMACE

Technical specifications

Protocols	Ethernet: Fibre Channel: SONET/SDH: ATM:	10 Mbps, 100Mbps, 1Gbps and 10Gbps FC-1G, FC-2G and FC-4G OC-3, OC-12, OC-48 and OC-192 OC-3, OC-12
Cryptography	AES 256-bit	
Key Management	QKD protocols: BB84 and SARG QKD server with automated key creation and exchange Secret keys exchanged between QKD server and encryption appliances through secure key channel	
Authentication	HMAC-SHA-1 (classical link) Wegmann Carter (QKD link) RSA public key X.509 certificates	
Performance	Key refresh rate: 1 key/min up to 12 encryption appliances Quantum link channel length up to 50km on single mode dark fiber (longuer distance on request)	
Access Control	Identity based identification Rule based	
Audit Trail	Event log, audit log, date and time of secure connexion Configuration changes Interface Status Alarms	
Secure Management	*QKD Server* *Cryptographic appliance*	SNMPv3, Ethernet 10/100 Rj45, touch panel SNMPv1, v2 and v3, Ethernet 10/100 Rj45, browser TLS or IPSec trusted path In-band on local and network interfaces
Indicators	Blue touch panel, 240x180 pixels (QKD server) Two line 20 characters LCD display (encryption appliances) LED indicating status of local interface, network interface, temperature, battery status, system operation and secure status, power	
Physical Security	Tamper proof storage of encryption keys and users passwords Tamper resistant metal case	
Environmental	Operating temperature Non-operating temperature Operating humidity Non-operating humidity	5° to 30° C -10° to 60° C 0 to 80% RH @ 40° C 95% RH @ 40° C

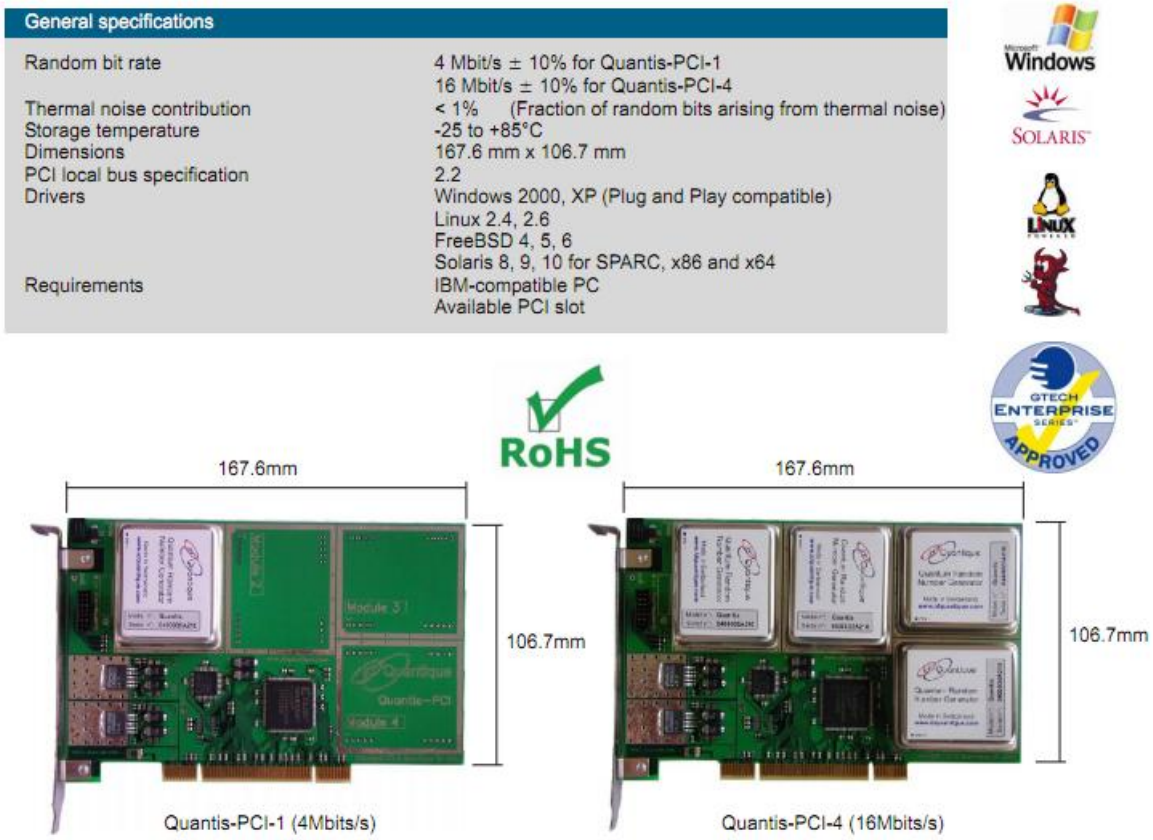
id Quantique SA, ch. de la Marbrerie 3, 1227 Carouge, Switzerland, Tel. +41 (0)22 301 83 71 Fax. +41 (0)22 301 83 79
sales@idquantique.com, www.idquantique.com Cerberis v.2.0 Specifications as of June 2008

id Quantique
A quantum Leap For Cryptography

Příloha 3. Technické parametry zařízení Cerberis

PŘÍLOHA P IV: QUANTUM RANDOM NUMBER GENERATOR

PCI karta



General specifications

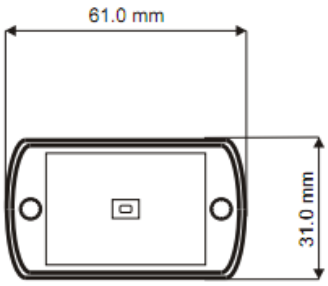
Random bit rate	4 Mbit/s ± 10% for Quantis-PCI-1 16 Mbit/s ± 10% for Quantis-PCI-4
Thermal noise contribution	< 1% (Fraction of random bits arising from thermal noise)
Storage temperature	-25 to +85°C
Dimensions	167.6 mm x 106.7 mm
PCI local bus specification	2.2
Drivers	Windows 2000, XP (Plug and Play compatible) Linux 2.4, 2.6 FreeBSD 4, 5, 6 Solaris 8, 9, 10 for SPARC, x86 and x64
Requirements	IBM-compatible PC Available PCI slot

Příloha 4. Technické parametry QRNG - PCI karta

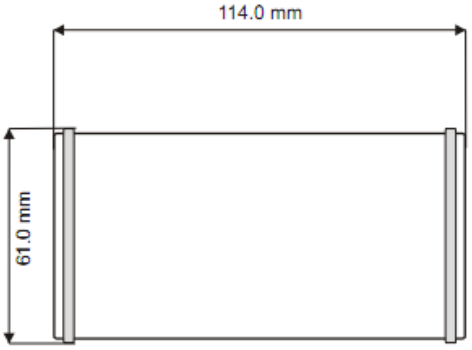
USB zařízení

General specifications	
Random bit rate	4 Mbit/s ± 10%
Thermal noise contribution	< 1% (Fraction of random bits arising from thermal noise)
Storage temperature	-25 to +85°C
Dimensions	61mm x 31mm x 114mm
USB specification	2.0
Drivers	Windows 2000, XP (Plug and Play compatible) Linux 2.4, 2.6
Requirements	IBM-compatible PC Available USB connector
Power	via USB port

Quantis USB Front view



Quantis USB Top view

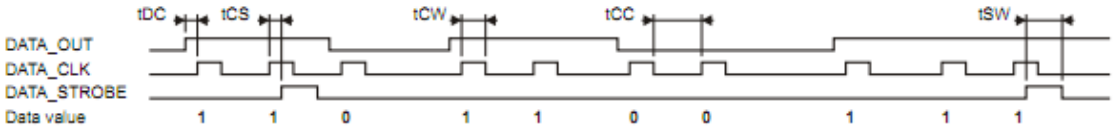


Příloha 5. Technické parametry QRNG – USB zařízení

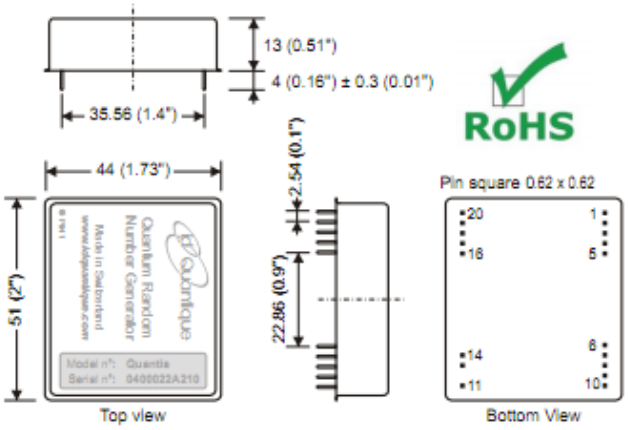
OEM modul

Switching characteristics

tDC	25ns	DATA_OUT before DATA_CLK
tCS	25ns	DATA_CLK before DATA_STROBE
tCW	50ns	DATA_CLK pulse width
tCC	100ns	Minimum time between two DATA_CLK pulses
tSW	75ns	DATA_STROBE pulse width



Outline dimension mm (inches)



RoHS

Pin lay-out

1	GND	20	GND
2	VCC	19	NC (Reserved)
3	SHDN	18	NC (Reserved)
4	Module_Detection	17	NC (Reserved)
5	NC (Reserved)	16	NC (Reserved)
6	DATA_OUT	15	NO PIN
7	DATA_CLK	14	NC
8	DATA_STROBE	13	NC
9	STATUS	12	NO PIN
10	GND	11	GND

NC: No connection - Do not connect.

Ordering information

Quantis - OEM	OEM Module generating a random bit stream of 4 Mbits/s
Quantis - USB	USB device with 1 module generating a random bit stream of 4 Mbits/s
Quantis - PCI-1	PCI card with 1 module generating a random bit stream of 4 Mbits/s
Quantis - PCI-4	PCI card with 4 modules generating a random bit stream of 16 Mbits/s

id Quantique SA, ch. de la Marbrerie 3, 1227 Carouge, Switzerland, Tel. +41 (0)22 301 83 71, Fax +41 (0)22 301 83 79
sales@idquantique.com, www.idquantique.com

Příloha 6. Technické parametry QRNG – OEM modul

PŘÍLOHA P V: MAGIQ QPN™ SECURITY GATEWAY 8505

MagiQ

New York Headquarters:
MagiQ Technologies, Inc.
171 Madison Avenue, Suite 1300
New York, NY 10016-5110
Telephone: (646) 638-1001
Fax: (646) 638-4331
Web: www.magiqtech.com

Somerville MA Labs:
MagiQ Technologies, Inc.
11 Ward Street
Somerville, MA 02143-4215
Telephone: (617) 661-8300
Fax: (617) 354-9844

MAGIQ QPN™ SECURITY GATEWAY 8505

- Full optical layer of QKD with Transmitter & Receiver
- Best of breed optical & electronics components
- Real-time, continuous, symmetrical quantum key regeneration
- Key refresh rate up to 100 keys/second
- True Random Number Generator
- 100 km transmission distance
- 140 km transmission distance with decoy state architecture (DSA)
- Compliant with industry standards BB84, 3DES, AES

QKD SECURITY

- 256 bit AES QKD
- Decoy state available

INTERFACES

- Up to 16 RJ45 interfaces
- FC single mode fiber interfaces
- Management: 10/100 Ethernet

PHYSICAL

- Tamper-evident chassis
- Footprint: 7" H x 19" W x 24" D
- Rack mountable in standard 19" rack
- Power: 115-230 VAC, 50-60 Hz, -48 VDC
- Weight: 40 lbs.

ENVIRONMENTAL

- Operating Temperature: 10° to 35° C (50° to 95° F)
- Operating Humidity: Up to 95% non-condensing

REGULATORY

Emissions:

- FCC Class A
- BSMI Class A
- CISPR Class A
- VCCI Class A

Safety:

- UL
- CSA
- CE
- VDE
- IEC 60950 (UL)
- CSA-C22.2 No.60950-00
- EN 60950 for the participating European nations
- EN 60950 for all country deviations
- Class 1 laser safety

ABOUT MAGIQ TECHNOLOGIES, INC.

MagiQ Technologies (www.magiqtech.com) is the quantum information processing (QIP) company. Through its unique blend of science, business and engineering expertise, the Company is the first to commercialize the advancements in quantum information to benefit forward-looking organizations seeking competitive advantage through technology. Founded in 1999, MagiQ is a privately-held company headquartered in New York City with research & development laboratories in Somerville, Mass.

Příloha 7. Technické parametry MagiQ QPN™ Security gateway 8505