Využití kvantové mechaniky v kryptografii

Autoři (J. Štaffa*, J. Macíček**, P. Pazdziora***)

Instituce, adresy (*Křesťanské gymnázium, **Gymnázium Nový Jičín, ***Masarykovo gymnázium Příbor)

E-mail(jstaffa@janstaffa.cz)

Abstrakt:

Tento příspěvek pojednává o tom, jak ochránit naše data před kvantovými počítači, které dokáží snadno prolomit dnešní kryptografické způsoby. Dokázali jsme přenést informaci prostorem pomocí úpravy polarizace fotonu a změřili jsme pravděpodobnost, že foton dorazí na druhou stranu. Může se tento způsob kryptografie stát alternativou k aktuálním způsobům, jako je RSA?

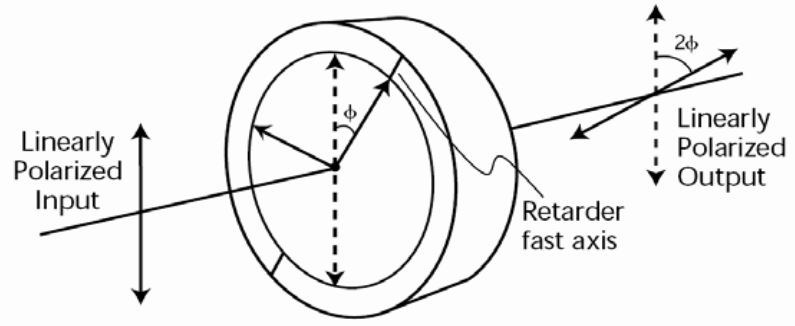
1 Úvod

Aktuální způsoby kryptografie závisí na principu dvou klíčů - klíče osobního a veřejného. Tyto klíče jsou matematicky spojené například pomocí faktorizace obrovských čísel. Toto spojení umožňuje odesílacímu uživateli zprávu zakódovat veřejným klíčem přijímajícího uživatele, pouze ten tuto zprávu dokáže opět rozkódovat svým osobním klíčem. Pro dnešní počítače je prolomení takovéto šifry velice náročné. Pro kvantový počítač je to však mnohem snažší. Jak se to dá řešit? Proti kvantovému počítači použijeme jeho vlastní zbraň - kvantovou fyziku.

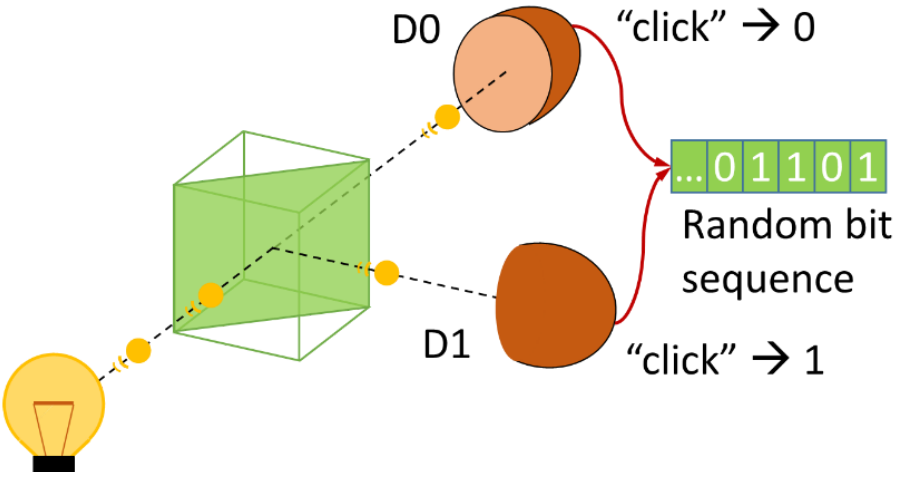
2 Základní principy

Quantum key distribution (QKD) plně závisí na schopnosti generace opravdu náhodných bitů pomocí přirozené náhodnosti kvantové fyziky.

Pokud polarizaci fotonu (směr vlnění) vlnovou destičkou otočíme přesně o ±45˚, tento foton po nárazu na beam splitter - součástku, která propustí foton polarizovaný jedním směrem, ale fotony kolmo polarizované na tento směr odráží - má v perfektním případě šanci přesně 50%, že projde rovně a přesně 50%, že se odrazí. Toto můžeme změřit dvěma detektory, které zaznamenají zásah částice. Podle toho, který detektor zaznamenal zásah můžeme následně vybrat hodnotu tohoto bitu, která bude opravdu náhodná.



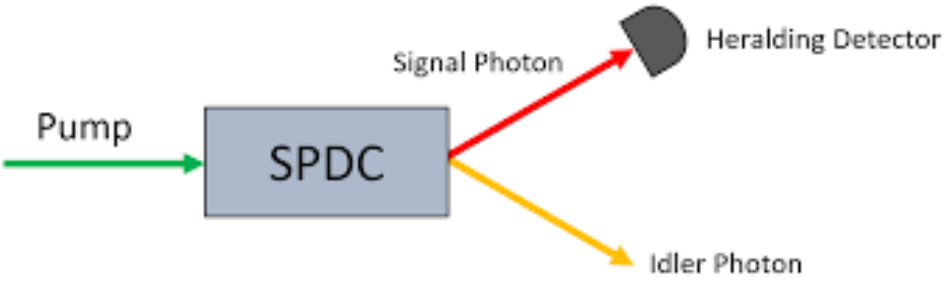
Obrázek 1: Vlnová destička měnící polarizaci světla



Obrázek 2: Generace náhodného bitu pomocí beam splitteru (kostka uprostřed)

Dalším zásadním předpokladem pro QKD je schopnost filtrovat fotony s různou polarizací. K tomu se používá polarizátor - součástka, vypadající jako destička s velmi drobnými výřezy v jednom směru, která propouští fotony pouze tímto směrem. Pokud polarizátor natočíme ve stejném směru, jako je polarizace letícího fotonu, propustí jej vždy, pokud polarizátor natočíme kolmo ke směru polarizace letícího fotonu, kompletně jej zablokuje, pokud jej natočíme pod libovolným jiným úhlem, polarizátor propustí tento foton s nižší pravděpodobností v závislosti na rozdílu tohoto úhlu a kolmého úhlu na směr polarizace fotonu.

Uvolnit velké množství fotonů dokážeme celkem běžně, i domácí lampa uvolní obrovská množství, ale získat konsistentně pouze jeden foton je velice náročné a právě na tom závisí zabezpečení QKD. Pro naše potřeby stačí získat fotonový pár, což je trochu jednodušší. K tomuto procesu se dají použít některé krystaly, například Boritan barnatý, které dokáží oddělit páry fotonů z paprsku světla. Jenže jak můžeme s jistotou vědět, že jsme vytvořili právě jeden foton? Můžeme využít toho, že získáváme vždy pár fotonů a jeden z nich změřit. V perfektním případě, kde není žádná interference, pokud naměříme zásah na jednom detektoru, víme s jistotou, že druhý foton také vyletěl. Zdroj fotonových párů může polarizovat fotony v libovolném směru, ale tento směr se nesmí měnit v průběhu komunikace.



Obrázek 3: Zdroj fotonového páru

3 Protokol BB84

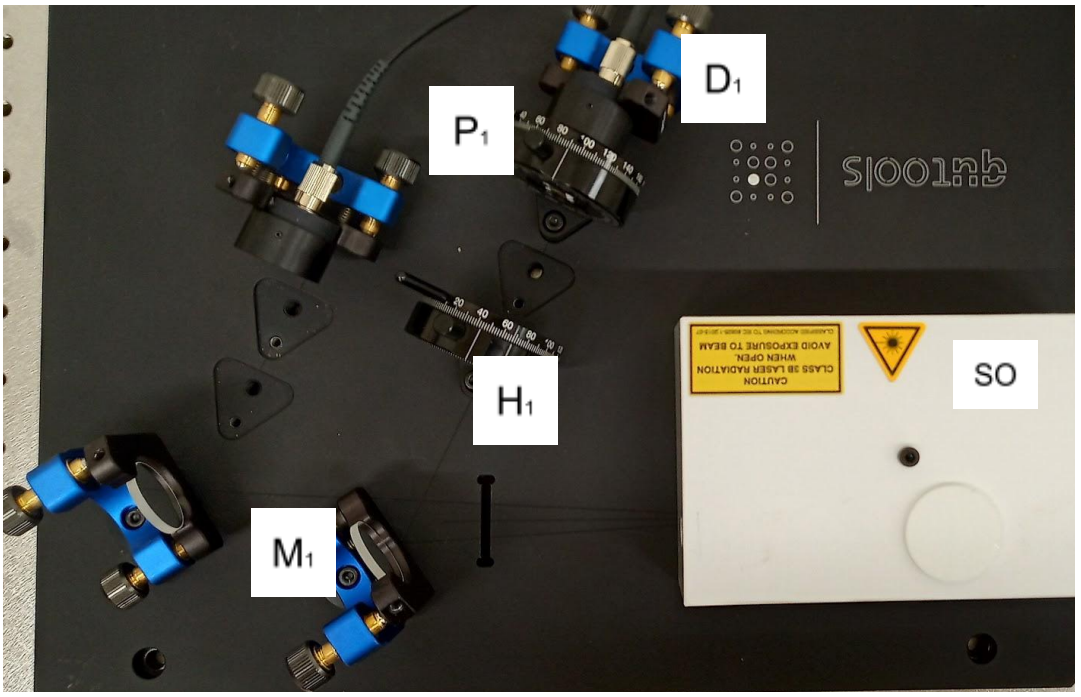
Cílem tohoto protokolu je vytvoření stejného symetrického klíče na obou stranách komunikace a to tak, že jeho prolomení nebude možné ani pro kvantový počítač. Tento klíč může následně být použit k zašifrování zprávy jednou z mnoha šifer například Vernamovou šifrou. Pro maximální zabezpečení musí být vygenerovaný klíč alespoň tak dlouhý, jako je tajná zpráva.

Samotná distribuce klíče je prováděna po jednotlivých bitech výsledného klíče. Pro přenesení každého bitu musí Alice (vysílací strana) náhodně, způsobem zmíněným výše, vygenerovat bit *a* a bázi *b*, která určuje, zda upraví foton do ortogonální či kolmé roviny. Kombinací *a* a *b* získá jednu ze čtyř možných polarizací: Horizontální, Vertikální, nebo ±45˚ ve které vyšle svůj foton získaný ze zdroje fotonových párů. Následně Bob (přijímací strana) také náhodně vybere jednu z bází a příchozí foton na ni změní. Pokud Bob vybere stejnou bázi, jako Alice, vynulují se a získá tedy Alicinu hodnotu *a*. Obě strany si zapamatují jakou bázi použili, Alice si dále zapamatuje svůj bit *a* a Bob si zapamatuje, co v jeho vybrané bázi naměřil. Poté, co je přenesena celá sekvence bitů klíče, obě strany zveřejní všechny své náhodně vybrané báze ve veřejném kanálu a porovnají svojí sekvenci se sekvencí druhé strany. Ze všech zapsaných hodnot vyberou pouze ty, u kterých zvolili stejnou bázi. Pokud se shodli alespoň na předem daném procentu bitů (mělo by jich být alespoň tolik, jako je dlouhá zpráva, kterou chtějí zakódovat). Mohou tuto sekvenci použít jako klíč a zašifrovat zprávu. Tato zpráva už může být poslána veřejným kanálem a je prakticky neprolomitelná.

Co se stane, pokud někdo uprostřed poslouchá? Protokol BB84 toto velice elegantně řeší. Eva (osoba uprostřed) si může také vybrat svou bázi a přečíst bit stejně jako Bob, jenže aby jí to k něčemu bylo, musí něco poslat Bobovi aby mohla být distribuce klíče provedena. Jenže jediné, co Eva dokáže poslat je to, co změřila, což může, ale nemusí být správně - má 50% šanci, že se trefí do stejné báze, jako Alice. Pokud tedy Eva uhodne všechny Aliciny báze, získá stejný klíč, jako Alice a Bob a dokáže tak prolomit šifru? Ano, ale šance, že se to stane je tak astronomicky malá, že to netvoří problém: pro délku klíče *k* je Evina šance $1 : 2^k$ tedy pro klíč o délce 128 je šance, že Eva uhodne klíč 1 : 3.4E38.

4 Výsledky a diskuze

Cílem našeho výzkumu bylo změřit hodnoty počtu zásahů na detektoru při různých konfiguracích polarizátorů a vlnové destičky. Kvůli vysokému množství dat je v tabulce 1 pouze část všech měření - Bobova konfigurace se nemění. V tabulce 2 jsou vždy uvedeny minima a maxima ze všech měření. Maximální hodnota naměřená s rozdílem 0˚ byla 5000 nárazů/s.



Obrázek 4: Použitá aparatura

D1 = detektor nárazů, **P1** = polarizátor, **H1** = vlnová destička, **M1** = zrcadlo, **SO** = zdroj fotonových párů

Alice *a*	Alice *b*	Bob *p*	hodnota (nárazy/s)	pravděpodobnost	∢ P_1 (deg)	∢H_1 (deg)
0	0	0	4900	98%	100˚	5˚
1	0	0	180	4.5%	100˚	50˚
0	1	0	2400	43%	100˚	27.5˚
1	1	0	2400	43%	100˚	-17.5˚

Tabulka 1: Část podrobných výsledků

rozdíl (deg)	rozmezí hodnot (nárazy/s)	pravděpodobnost
0˚	4700 - 5000	94% - 100%
±45˚	2000 - 2700	40% - 54%
90˚	150 - 200	3% - 3.9%

Tabulka 2: Shrnutí naměřených hodnot

Z tabulek lze vyčíst, že čím víc se rozdíl v úhlu polarizace fotonu blíží k 90˚, tím nižší je pravděpodobnost, že foton dorazí k bobovi, což je očekávaný výsledek, neboť jak jsme se již dozvěděli, pokud je směr polarizace kolmý na směr polarizátoru, foton je vždy zablokován.

5 Shrnutí

Quantum key distribution je velmi slibný způsob, jak vyřešit problém zabezpečení dat před kvantovými počítači. Naše výsledky ověřili a potvrdili bezpečnost tohoto způsobu. Dnes však ještě tato technologie není úplně připravená k plošnému používání. Myslíme si však, že je to cesta, po které se budeme jako lidstvo muset vydat.

Poděkování

Děkuji jménem celého našeho vědeckého týmu panu Aurélu Gábrisovi za vědecký podklad pro náš miniprojekt, panu Vojtěchu Svobodovi za pořádání týdne vědy a v neposlední řadě paní vrátné za přívětivost a poskytnutí vhodných podmínek pro práci.

Reference

[1] QNRG. In: *Https://qt.eu* [online]. [cit. 2022-06-21]. Dostupné z: https://qt.eu//app/uploads/2018/11/QNRG.png

[2] Photon spliter. In: *Https://encrypted-tbn0.gstatic.com* [online]. [cit. 2022-06-21]. Dostupné z: https://encrypted-tbn0.gstatic.com/images?q=tbn:ANd9GcRTzNBQSp9Qj-SictHm6fzSUkPSCMPcjKTPsw&usqp=CAU