TESTING POLYGON FOR QUANTUM KEY DISTRIBUTION

Jakub Širjov
Master Degree Programme (2), FEEC BUT
E-mail: xsirjo00@stud.feec.vutbr.cz

Supervised by: Michal Látal
E-mail: xlatal08@stud.feec.vutbr.cz

Abstract: The article explains issues in QKD and their sources. It next describes principle of QKD operation and its individual parts that are required for its function. Part of the article includes simulations from QKDNetsim and NS-3 that show possibilities of the simulation, that were used to create exemplary simulations for future check of QKD traffic on the test polygon.

Keywords: quantum, key, distribution, QKD, photon, simulation, NS-3, QKDNetsim

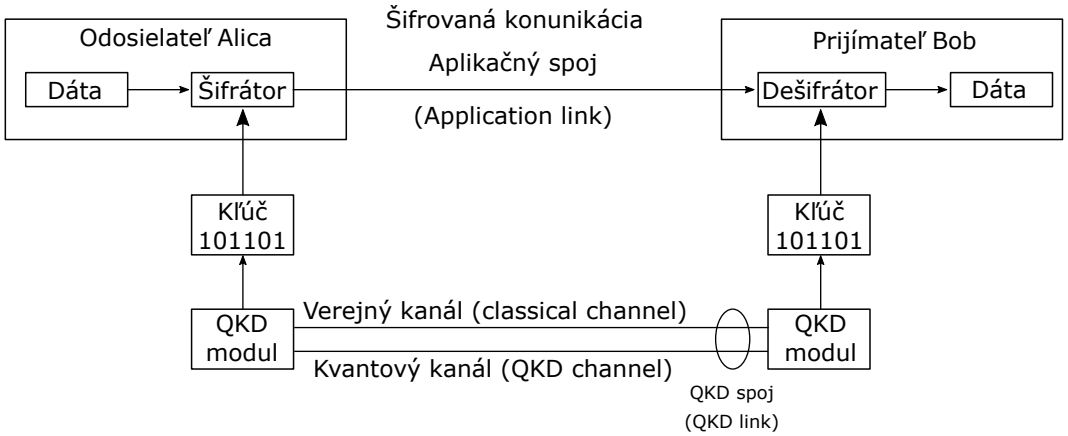
1 ÚVOD DO QKD

V dôsledku neustále prudko narastajúceho výpočtového výkonu sa museli aj šifrovacie metódy zlepšovať, aj keď sú založené na zložitých matematických operáciách a bolo ich už možné rozlúštiť v reálne krátkom čase. Kryptológia sa vyvíjala smermi, ako je šifrovanie chaosom, fraktálnym šifrovaním, kvantovými javmi alebo umelou inteligenciou. Práve kvantové javy sú využívané v kvantovej distribúcii kľúčov (Quantum Key Distribution, skrátene QKD), kde sa využívajú princípy kvantovej mechaniky. Práve QKD je technológia, o ktorej sa dá povedať, že je bezpečná voči útokom s neobmedzeným výpočtovým výkonom [1].

V QKD ako nositeľ informácie je používaná elementárna častica fotón. Technika pre generovanie kľúčov na kvantovej úrovni a ich distribúcia prostredníctvom fotónov sa označuje ako proces kvantovej distribúcie kľúčov. Ako je známe, existujú dve moderné základné metódy pre šifrovanie, a to symetrické a asymetrické. Práve QKD poskytuje prostriedky pre distribúciu symetrických kľúčov [2] [3] [4].

QKD je zobrazený na obr. 1. Alica pošle Bobovi sériu fotónov, kde každý je modulovaný náhodnou hodnotou (qubity). Príkladom je, že Alica pošle Bobovi kartu, kde je náhodne na jednej strane „1“ a na druhej „0“. Ak si Bob prečíta rovnakú stranu ako Alica, tak majú obaja rovnakú hodnotu, ale ak si Bob vyberie druhú stranu, tak si náhodne vyberie „0“ alebo „1“ (náhodou sa môže trafiť do čísla, ktoré Alica posielala, ale na to sa nemožno vždy spoliehať). Keď Alica odošle všetky fotóny a Bob ich všetky prečíta, tak vykonajú takzvanú „Sifting transaction“ ako súčasť „Post processing“, kde si navzájom oznámia len informáciu, ktoré strany karty čítali (nie aké hodnoty prečítali). Zahodia všetky karty, ktoré neboli vybrané správne a zostávajúce karty tvoria sled jednotiek a núl, ktoré sa použijú ako surový kľúč [5]. Pre bežnú implementáciu QKD zahrňuje tri základné komponenty.

- Kvantový kanál (quantum channel) buď optický kábel alebo bezdrôtový prenos slúži pre odoslanie kvantových stavov fotónov (qubity), v ktorých sa prenáša náhodná sekvencia bitov od odosielateľa (Alica) k prijímateľovi (Bob). Tento kanál nemusí byť zabezpečený.
- Overený verejný komunikačný kanál (classical channel) medzi komunikačnými stranami. Jeho dôležitou úlohou je zabezpečiť synchronizáciu a výmenu dát medzi modulmi QKD, a mohli tieto strany uskutočniť „Post processing steps“ a mohli vygenerovať správny a tajný kľúč.



Obr. 1: Základná schéma zostrojenia QKD medzi Alicou a Bobom

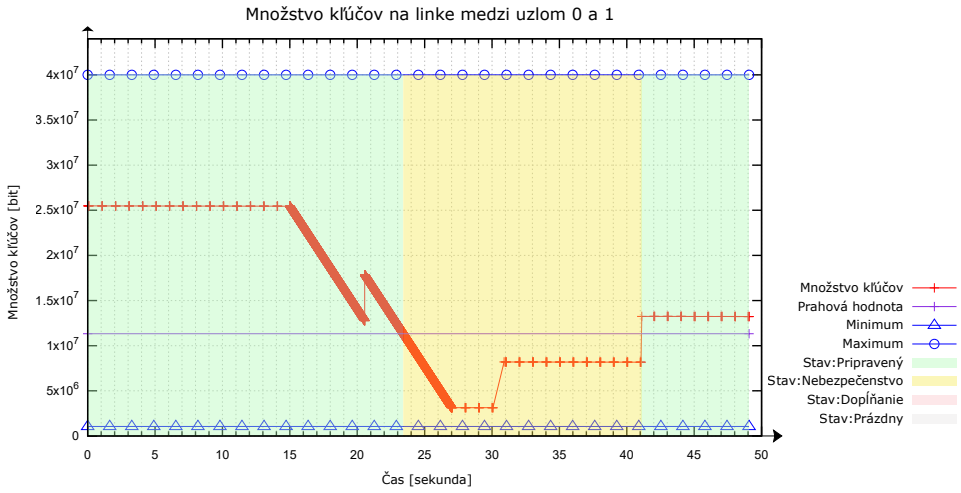
- Protokol pre výmenu kľúčov, ktorý využíva vlastnosti kvantovej mechaniky pre zaistenie bezpečnosti detegovaním odpočúvania alebo chýb a výpočtom množstva informácií, ktoré boli zachytené alebo stratené [6].

2 SIMULÁCIE

QKDNetsim je implementačný model, ktorý obsahuje sieťový modul QKD, kľúče QKD, vyrovnávaciu pamäť QKD, sieťové zariadenie QKD (QKD NetDevice) a „processing applications“. QKDNetsim bol vytvorený na Technickej univerzite v Ostrave [7].

Topológia simulácie sa skladá z 3 uzlov, kde uzol 0 je spojený s uzlom 1 a tento uzol je spojený s uzlom 2. Uzly komunikujú cez P2P spoje. Na tejto topológii boli zobrazené a otestované možnosti tohto simulačného prostredia. QKDNetsim nedokáže simulovať kvantovú úroveň QKD, teda nepoužíva sa na generovanie kľúča, ani pre žiadnu správu kvantového kanálu alebo odpočúvanie na kvantovej/fyzickej úrovni. Jeho činnosť je v prevažnej miere zameraná na použitie tajného kľúča a správu kľúčov na vyšších vrstvách.

Prvá simulácia zobrazuje vplyv rýchlosti tvorenia kľúčov a rýchlosť premávky na vyrovnávaciu pamäť kľúčov. Na začiatku simulácie boli už vo vyrovnávacej pamäti kľúče. Taktiež boli vybrané rôzne časy začiatku tvorby kľúčov tak, aby na grafoch bol viditeľný rozdiel.

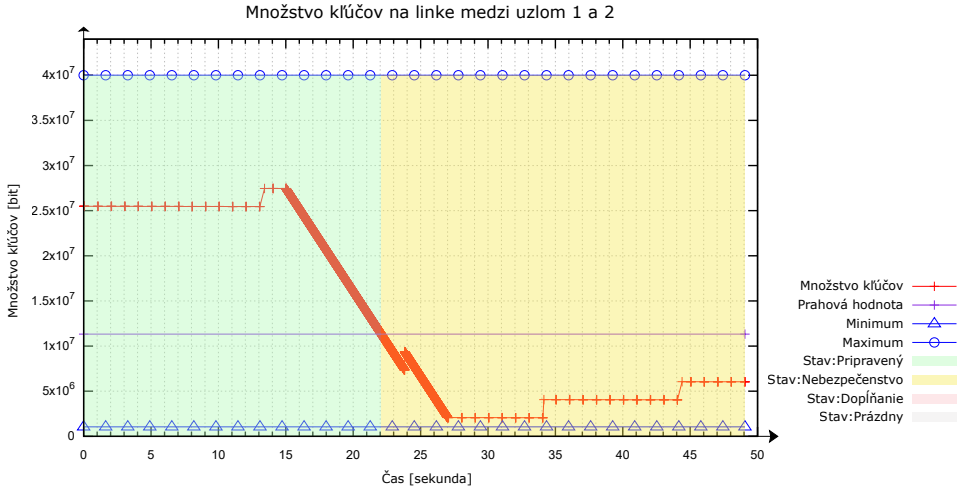


Obr. 2: Priebeh zmeny množstva kľúčov vo vyrovnávacej pamäti medzi nultým a prvým uzlom.

Premávka tvorila celkové množstvo 3 000 000 bitov, jeden paket mal nastavenú veľkosť 60 bitov a ostatné parametre boli nastavené, viď. tab. 1. Z grafov je zjavné, že od definovaného začiatku tvorby kľúčov vždy prebehne 10 sekúnd a až potom sa odošle nastavené množstvo kľúčov a táto situácia sa opakuje.

Tabuľka 1: Prenosové parametre prvej simulácie

Spojenie	QKD spoj 1	QKD spoj 2	Premávka
Začiatok [s]	10	3	15
Koniec [s]	50	50	50
Keyrate [bit/s]	5 072 000	2 007 200	-
Prenosová rýchlosť [Mb/s]	-	-	2



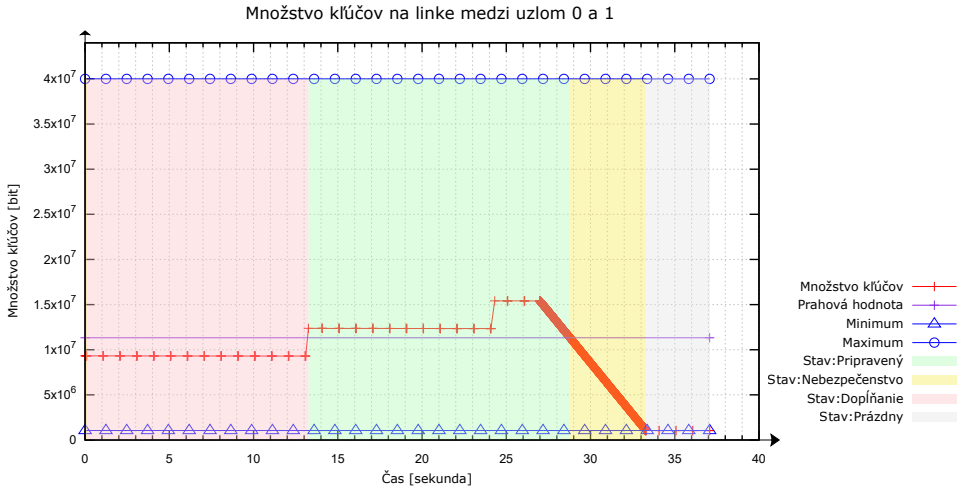
Obr. 3: Priebeh zmeny množstva kľúčov vo vyrovnávacej pamäti medzi prvým a druhým uzlom.

Pri spustení premávky je zjavné znižovanie množstva kľúčov vo vyrovnávacej pamäti. V prípade keď množstvo kľúčov klesne pod prahovú úroveň (treshold), a táto pamäť sa dostane do stavu nebezpečne nízkeho množstva kľúčov (prezentované žltou častou grafu).

V **druhej simulácií** bolo sledované, ako sa bude sieť správať, ak bude nastavená príliš vysoká premávka, nedostatočné generovanie kľúčov a počiatočná hodnota bude nastavená pod prahovou hodnotou, viď obr. 4. Z grafu je zjavné, že v prípade ak v pamäti nie je dostatočné množstvo kľúčov, je na začiatku v stave dopĺňanie a po čase sa dostala do stavu pripravená a po spustení premávky množstvo kľúčov klesne pod minimálnu hodnotu, komunikácia skolabuje a už sa neobnoví. Tieto úrovne je možné nastavovať, ako parametre minimálneho množstva kľúčov (pod touto hodnotou spoj skolabuje), prahová hodnota (pod touto hodnotou je v stave nebezpečenstva), maximálna hodnota (maximálne množstvo uložených kľúčov) a počiatočná hodnota (množstvo kľúčov na začiatku simulácie).

Tabuľka 2: Výstup z konzoly simulačného prostredia QKDNetsim pri simulácií vysokého toku dát, kde nebolo dostatočné množstvo kľúčov, ani dostatočné rýchla regenerácia kľúčov.

Zdrojová IP adresa		10.1.1.1	
Cieľová IP adresa		10.1.2.2	
Odoslané [bit]	4000200	Prijaté [bit]	3112200
Odoslané [paket]	6667	Prijaté [paket]	5187
Pomer [bit]	0.778011	Pomer [paket]	0.778011



Obr. 4: Priebeh zmeny množstva kľúčov medzi nultým a prvým uzlom pri vysokom prenose dát.

3 ZÁVER

V článku bola vysvetlená problematika QKD a tiež princíp jeho fungovania. Následne boli zobrazené simulované vzorové simulácie dvoch scenárov. Vďaka simulátoru QKDNetsim sme schopní správne nastaviť jednotlivé parametre siete tak, aby sieť fungovala aj pri vysokej premávke, pri pevne danej pravidelnosti vytvárania kľúčov. Tieto parametre sú veľmi dôležité, nakoľko pamäť kľúčov by bolo zbytočné mať príliš veľkú, keďže každý kľúč má svoju životnosť. Tento simulátor je vhodný na simuláciu sieťovej vrstvy, kde nás zaujíma iba prenos kľúčov v sieti a nie samotná kvantová vrstva. Je možné si vopred nasimulovať rôzne prenosy a overiť, či by aktuálne nastavenie siete zvládlo daný kvantový prenos. Do budúcna je v pláne sa zaoberať navrhnutím a zostrojením testovacieho polygónu, kde bude možné pripojiť QKD a testovať rôzne druhy prenosov súbežne s prenosom kvantového signálu a sledovať ich vzájomný vplyv.

LITERATÚRA

[1] PETROVSKÝ, Bc. Peter. *Formální analýza kryptografických protokolů*. Brno, 2015. Diplomová práca. VUT Brno. Vedoucí práce Ing. Vlastimil Člupek.

[2] RUSSELL, J. Application of Quantum Key Distribution. *MILCOM 2008 - 2008 IEEE Military Communications Conference* [online]. 2008, **2008**(1), 1-6 [cit. 2020-11-24]. Dostupné z: doi:10.1109/MILCOM.2008.4753169

[3] KOTHARI, Abhishek. Qubit By Qubit. *Medium* [online]. Amerika: medium, 2018 [cit. 2020-11-24]. Dostupné z: https://medium.com/@abhishekkothari/qubit-by-qubit-104139024edc

[4] *Kvantový seriál — díl 9. — Kvantové sítě — Současná situace* [online]. Česko: Quantum Phi, 2020 [cit. 2020-11-24]. Dostupné z: https://qubits.cz/serialy/kvantovy-serial-dil-9-kvantove-site-soucasna-situace/

[5] ELLIOTT, C. Quantum cryptography. *IEEE Security Privacy* [online]. 2004, **2004**(2), 57-61 [cit. 2020-11-24]. Dostupné z: doi:10.1109/MSP.2004.54

[6] JAKUBÍČEK, Michal. *Návrh zabezpečení systému dálkového měření kvality dodávky elektrické energie*. Brno, 2013. Bakalárska práca. VUT Brno. Vedoucí práce Ing. Petr Mlýnek, Ph.D.

[7] *QKDNETSIM* [online]. Česko, Bosnia and Herzegovina: QKDNetSim Team, 2020 [cit. 2020-12-10]. Dostupné z: https://www.qkdnetsim.info/