SLOVENSKÁ TECHNICKÁ UNIVERZITA V BRATISLAVE
FAKULTA ELEKTROTECHNIKY A INFORMATIKY

DEŠIFROVANIE V QC-LDPC MCELIECEOVOM KRYPTOSYSTÉME

TÍMOVÝ PROJEKT

2018 **Forks**

SLOVENSKÁ TECHNICKÁ UNIVERZITA V BRATISLAVE
FAKULTA ELEKTROTECHNIKY A INFORMATIKY

DEŠIFROVANIE V QC-LDPC MCELIECEOVOM KRYPTOSYSTÉME

TÍMOVÝ PROJEKT

Študijný program:	Aplikovaná informatika
Číslo študijného odboru:	2511
Názov študijného odboru:	9.2.9 Aplikovaná informatika
Školiace pracovisko:	Ústav informatiky a matematiky
Vedúci záverečnej práce:	Ing. Viliam Hromada, PhD., Mgr. Tomáš Fabšič, PhD.

Bratislava 2018 **Forks**

Poďakovanie

Chceli by sme sa poďakovať vedúcim tímového projektu Mgr. Tomášovi Fabšičovi, PhD. a Ing. Viliamovi Hromadovi, PhD. za...

Obsah

Úvod

1 Ponuka

Riešiteľský tím v zložení: Bc. Nikoleta Furičková, Bc. Juraj Karásek, Bc. Matej Ohradzanský, Bc. Peter Radvan a Bc. Lukáš Štrba na tomto mieste predkladá záväznú ponuku na riešenie problému s pracovným názvom: *Dešifrovanie v QC-LDPC McElieceovom kryptosystéme*. Projekt budeme riešiť pod vedením Mgr. Tomáša Fabšiča, PhD. a Ing. Viliama Hromadu, PhD. v rámci predmetu **Tímový projekt**.

V časti Riešiteľský kolektív stručne predstavíme členov tímu. Zameriame sa na ich schopnosti a skúsenosti, ktoré súvisia s problematikou tímového projektu. Nasledovať bude časť, v ktorej vyjadríme našu dôveru v post-kvantovú kryptografiu a jej využitia v *blízkej* budúcnosti. Zadanie projektu a úlohy, ktoré z neho plynú budú opísané v časti Anotácia tímového projektu. Ponuku ukončíme diskusiou o tom, ako je už pri päť členom tíme zložité, dohodnúť si termín týždenných konzultácií so zadávateľmi tímového projektu.

1.1 Riešiteľský kolektív

Tím pozostáva z piatych študentom aplikovanej informatiky na Fakulte elektroniky a informatiky Slovenskej technickej univerzity. Členovia tímu sú spolužiaci už 4. rokom a panujú medzi nimi priateľské vzťahy.

1.1.1 Bc. Nikoleta Furičková
1.1.2 Bc. Juraj Karásek
1.1.3 Bc. Matej Ohradzanský
1.1.4 Bc. Peter Radvan
1.1.5 Bc. Lukáš Štrba

1.2 Motivácia

1.3 Anotácia tímového projektu

Pokrok vo vývoji kvantového počítača má vážne dôsledky aj pre kryptografiu. Je známe, že dostatočne vykonné kvantové počítače budú vedieť efektívne riešiť problém faktorizácie čísla na prvočísla a problém diskrétneho logaritmu. Na náročnosti riešenia týchto problémov je založená bezpečnosť v súčasnosti používaných asymetrických kryptosystémov (napríklad RSA). To znamená, že v prípade existencie dostatočne výkonného kvantového počítača by súčasné asymetrické kryptosystémy už neboli bezpečné. Niektoré odhady hovoria, že takto vykonné kvantové počítače by mohli existovať už o 10 rokov. Je preto dôležité, pracovať na vývoji nových asymetrických kryptosystémov, ktoré budú odolné voči útokom kvantového počítača, a ktoré by mohli nahradiť súčasné asymetrické kryptosystémy. Na dôležitosť tejto témy upozornil aj americký inštitút pre štandardy a technológiu *NIST* v správe Report on Post-Quantum Cryptography. NIST zároveň vyhlásil súťaž Post-Quantum Cryptography Standardization Process s cieľom navrhnúť nové kryptografické štandardy odolné voči kvantovým počítačom. Do súťaže prišlo vyše 60 návrhov kryptosystémov. Tieto návrhy budú v najbližších rokoch verejne analyzované vedeckou komunitou s cieľom vybrať najlepších kandidátov.

Viacero návrhov zaslaných do súťaže je založených na QC-LDPC McElieceovom kryptosystéme. Jedná sa o variant McElieceovho kryptosystému, v ktorom sa využívajú QC-LDPC kódy. Pri šifrovaní sa správa prevedie na kódové slovo QC-LDPC kódu a ku kódovému slovu sa pridá chyba. Pri dešifrovaní je potrebné túto chybu odstrániť. Chybu je možné odstrániť použitím tajného kľúča, ktorý obsahuje matice H a Q. Na odstránenie chyby je možné použiť dve metódy: buď sa použije dekódovací algoritmus pre QC-LDPC kódy, ktorý využíva maticu H, alebo sa použije dekódovací algoritmus pre QC-MDPC kódy, ktorý používa maticu H*Q. Cieľom práce je porovnať efektívnosť týchto dvoch metód. Úlohy, ktoré z toho vyplývajú sú nasledovné:

- naštudujte princípy fungovania QC-LDPC McElieceovho kryptosystému
- oboznámte sa s implementáciou QC-LDPC McElieceovho kryptosystému v knižnici BitPunch (implementácia je v jazyku C)
- porovnajte efektívnosť dvoch vyššie spomenutých metód na odstránenie chyby zo správy zašifrovanej QC-LDPC McElieceovym kryptosystémom

1.4 Rozvrh

Z diskusie členov riešiteľského kolektívu so zadávateľmi tímového projektu vyplynulo, že je jediný možný termín pravidelných konzultácií je utorok ráno (cca 08:00). S návrhom súhlasili všetci prítomní. Neprítomný Bc. Peter Radvan s časom stretnutia dodatočne súhlasil.

Záver

Dúfame, že sme všetko zvládli.

Zoznam použitej literatúry