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**

1 Ponuka **2**

1.1 Riešiteľský kolektív 2

1.2 Anotácia tímového projektu 4

1.3 Motivácia 5

1.4 Organizácia projektu 5

2 Teoretická časť **6**

3 Praktická časť **7**

Záver **8**

Zoznam použitej literatúry **9**

Prílohy **I**

A Štruktúra elektronického nosiča **II**

B Používateľská príručka **III**

Zoznam obrázkov a tabuliek

Zoznam skratiek a značiek

GF - Galois Field

RSA - Rivest–Shamir–Adleman

Zoznam algoritmov

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. Zadanie a úlohy, ktoré z neho plynú budú opísané v časti Anotácia tímového projektu. Nasledovať bude časť, v ktorej vyjadríme našu dôveru v post-kvantovú kryptografiu a jej využitia v *blízkej* budúcnosti. Ponuku ukončíme popisom organizácie projektu.

1.1 Riešiteľský kolektív

Tím pozostáva z piatich študentov aplikovanej informatiky na Fakulte elektroniky a informatiky Slovenskej Technickej Univerzity. Členovia tímu sú spolužiaci už 4 roky a panujú medzi nimi priateľské vzťahy. Pracovný názov nášho kolektívu je *Forks*.

Bc. Nikoleta Furičková
Pozícia v tíme: Analytička

Je absolventkou bakalárskeho štúdia na Fakulte elektrotechniky a informatiky Slovenskej Technickej Univerzity v Bratislave, v študijnom programe Aplikovaná informatika, odbor Bezpečnosť informačných systémov. Bakalárske štúdium ukončila vypracovaním bakalárskej práce s názvom: *Invertovateľnosť blokovo cyklických matíc*. Bakalársku prácu robila pod vedením Mgr. Tomáša Fabšiča, PhD., pričom získala cenné skúsenosti a poznatky, ktoré sa dajú dobre využiť pri riešení tímového projektu.

Bc. Juraj Karásek
Pozícia v tíme: Developer

Je absolventom bakalárskeho štúdia na Fakulte elektrotechniky a informatiky Slovenskej Technickej Univerzity v Bratislave, v študijnom programe Aplikovaná informatika, odbor

Bezpečnosť informačných systémov. Bakalárske štúdium ukončil vypracovaním bakalárskej práce s názvom: *Porovnanie vybraných mechanizmov distribuovaného konsenzu z hľadiska IT bezpečnosti.*

Bc. Matej Ohradzanský
Pozícia v tíme: Developer

Je absolventom bakalárskeho štúdia na Fakulte elektrotechniky a informatiky Slovenskej Technickej Univerzity v Bratislave, v študijnom programe Aplikovaná informatika, odbor Bezpečnosť informačných systémov. Bakalárske štúdium ukončil vypracovaním bakalárskej práce s názvom: *Lúštenie substitučných šifrier.* Bakalársku prácu robil pod vedením prof. Ing. Pavla Zajaca, PhD. a v apríli tohto roku sa zúčastnil SVOČ-ky (*Študentská vedecká a odborná činnosť*), pričom sa umiestnil na prvom mieste vo svojej kategórii.

Bc. Peter Radvan
Pozícia v tíme: Web Developer

Je absolventom bakalárskeho štúdia na Fakulte elektrotechniky a informatiky Slovenskej Technickej Univerzity v Bratislave, v študijnom programe Aplikovaná informatika, odbor Bezpečnosť informačných systémov. Bakalárske štúdium ukončil s vyznamenaním. Pod vedením Ing. Viliama Hromadu, PhD. vypracoval bakalársku prácu s názvom: *ABC kryptosystém*, pri tvorbe ktorej získal množstvo vedomostí z oblasti post-kvantovej kryptografie, ktoré predstavujú značný náskok v analytickej časti projektu.

Bc. Lukáš Štrba
Pozícia v tíme: Analytik a vedúci riešiteľského kolektívu?

Je absolventom bakalárskeho štúdia na Fakulte elektrotechniky a informatiky Slovenskej Technickej Univerzity v Bratislave, v študijnom programe Aplikovaná informatika, odbor Bezpečnosť informačných systémov. Bakalárske štúdium ukončil s vyznamenaním. Pod vedením Ing. Viliama Hromadu, PhD. vypracoval bakalársku prácu s názvom: *Kubický ABC kryptosystém*, pri tvorbe ktorej získal množstvo vedomostí z oblasti post-kvantovej kryptografie. Tieto poznatky sú stále aktuálne a predstavujú dobrý základ potrebný na úspešné vypracovanie projektu.

1.2 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 výkonné 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:

- naštudovanie si princípov fungovania QC-LDPC McElieceovho kryptosystému
- oboznámenie sa s implementáciou QC-LDPC McElieceovho kryptosystému v knižnici BitPunch (implementácia je v jazyku C)
- porovnanie efektívnosti dvoch vyššie spomenutých metód na odstránenie chyby zo správy zašifrovanej QC-LDPC McElieceovym kryptosystémom

1.3 Motivácia

Pre projekt sme sa rozhodli preto, že si uvedomujeme hrozbu, ktorú by predstavovalo zostrojenie dostatočne silného kvantového počítača pre dnešný svet. Dôkazom aktuálnosti tejto problematiky je aj fakt, že existujú viaceré medzinárodné projekty organizované napr. *NATO* alebo *VEGA*, do ktorých je zapojený aj Ústav informatiky a matematiky FEI STU. Skúmanie rôznych post-kvantových kryptosystémov je nesmierne dôležité a sme radi, že sa toho môžeme zúčastniť. Získané vedomosti môžu predstavovať cenný zdroj nových informácií pre členov tímu, ktorí sa už podrobnejšie stretli s post-kvantovou kryptografiou a zároveň dobrý základ pre členov, ktorí sú noví a vedomosti iba zbierajú. Veríme, že naše výsledky z tímového projektu pomôžu k napredovaniu výskúmu v tejto oblasti.

1.4 Organizácia projektu

Z diskusie členov riešiteľského kolektívu so zadávateľmi tímového projektu vyplynulo, že 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. Z pravidelných stretnutí sa priebežne tvoria zápisnice, ktoré sú spolu s ostatnými materiálmi a informáciami dostupné na stránke projektu. Súčasťou vypracovania projektu je aj odovzdanie dokumentácie, v ktorej bude opísaný matematický model QC-LDPC McElieceovho kryptosystému, ako aj nami zistené výsledky meraní. Na vypracovanie analytickej časti projektu neuvažujeme nad žiadnymi špeciálnymi hardvérovými požiadavkami, ale v prípade spúšťania väčšieho množstva výpočtov uvažujeme nad využitím klastra STU v Bratislave.

2 Teoretická časť

3 Praktická časť

Záver

Dúfame, že sme všetko zvládli.

Zoznam použitej literatúry

Prílohy

A Štruktúra elektronického nosiča II
B Používateľská príručka III

A Štruktúra elektronického nosiča

\
\Tímový projekt.pdf
\Zdrojové súbory - *upravená knižnica BitPunch*

B Používateľská príručka

Elektronický nosič obsahuje dokumentáciu k Tímovému projektu a upravenú verziu knižnice BitPunch.

Používateľ musí mať nainštalovaný kompilátor jazyka C. Na kompilovanie knižnice *BitPunch* je možné použiť priložený *makefile*:

- *Kompilovanie knižnice* v príkazovom riadku: v priečinku *../BitPunch/lib* zadať príkaz **make**
- *Spustenie implementácie*: v priečinku *../BitPunch/lib/dist/test* spustiť novovytvorený binárny súbor pomocou príkazu **./BitPunch**