**SLOVENSKÁ TECHNICKÁ UNIVERZITA V BRATISLAVE**
**FAKULTA ELEKTROTECHNIKY A INFORMATIKY**

Evidenčné číslo: 007

# DEŠIFROVANIE V QC-LDPC MCELIECEOVOM KRYPTOSYSTÉME

## TÍMOVÝ PROJEKT

**2018** **Forks**

**SLOVENSKÁ TECHNICKÁ UNIVERZITA V BRATISLAVE**
**FAKULTA ELEKTROTECHNIKY A INFORMATIKY**

Evidenčné číslo: 007

# 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 Ing. Viliamovi Hromadovi, PhD. a Mgr. Tomášovi Fabšičovi, PhD. za...

# Obsah

**Úvod** **1**

**1 Ponuka** **2**

**Záver** **3**

**Zoznam použitej literatúry** **4**

# Úvod

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.

# 1 Ponuka

...

# Záver

Dúfame, že sme všetko zvládli.

# Zoznam použitej literatúry