

## Zápisnica č. 5

**Dátum:** 16.10.2018

**Prítomní:**

- Bc. Nikoleta Furičková , Bc. Juraj Karásek, Bc. Matej Ohradzanský, Bc. Peter Radvan a Bc. Lukáš Štrba
- Mgr. Tomáš Fabšič, PhD. a Ing. Viliam Hromada, PhD.

**Program stretnutia:**

- Na dnešnom stretnutí sme sa zaoberali asymetrickým post-kvantovým QC-LDPC McEliece kryptosystémom. Ukázali sme si teoretický model tvorby súkromného a verejného kľúča ako aj spôsob šifrovania a dešifrovania.
- Zaoberali sme sa dvomi spôsobmi dešifrovania, ktorých efektivitu budeme skúmať v praktickej časti tímového projektu.

**Úlohy:**

- Pokračovať v študovaní vybraných *Bit Flipping* algoritmov.
- Ing. Viliam Hromada, PhD. nám prisľúbil zaslanie zdrojových kódov.

**Poznámka:**

**Zapisovateľ:** Bc. Lukáš Štrba

**Overovateľ:** Bc. Peter Radvan