

Zápisnica č. 4

Dátum: 9.10.2018

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 problematikou dekódovania prijatých správ v kryptosystéme QC-MDPC McEliece. Na príklade sme si ukázali ako toto dekódovanie prebieha prostredníctvom algoritmu *Bit Flipping* a zároveň ako reprezentovať jeho realizáciu prostredníctvom bipartitných Tannerových grafov.
- Podľa slov vedúcich TP je ponuka v dobrom stave.

Úlohy:

- Zopakovanie si vysvetleného a opätovné prečítanie článkov.
- Postupné študovanie knižnice BitPunch.

Poznámka:

Zapisovateľ: Bc. Lukáš Štrba

Overovateľ: Bc. Peter Radvan