ČVUT

FIT

Asymetrický šifrovací algoritmus McEliece

Vojtěch Myslivec
autor

vedoucí práce
prof. Ing. Róbert Lórencz, CSc.

McEliece

- Asymetrický šifrovací algoritmus
- Kandidát pro poskvantovou dobu
- Založen na lineárním kódování
- Úmyslné zanesení chyby jako součást šifry

Robert McEliece

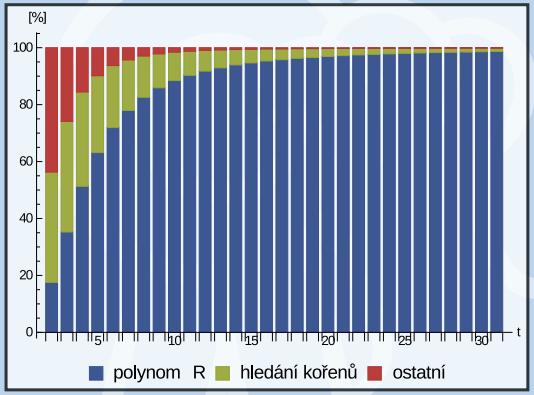
Implementace

- V programu Wolfram Mathematica
- Implementovány knihovny pro:
  - Rozšířená konečná tělesa
  - Binární Goppa kódy

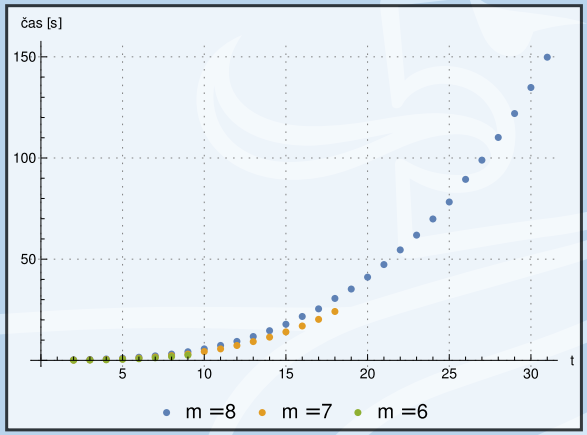
$$c = m\hat{G} + z = (1\ 0\ 0\ 0)\begin{pmatrix} 1&0&0&0&1&1&0&0&0&0&1&1&0&1&1&1 \\ 0&1&0&0&1&1&1&0&1&1&0&0&1&0&1&1 \\ 0&1&1&1&1&1&0&1&0&1&0&1&0&0&1&1 \\ 0&1&0&0&1&1&0&1&0&0&1&0&1&1&0&0 \end{pmatrix} + (0\ 0\ 0\ 0\ 1\ 1\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 1)$$

Měření

- Měření časových závislostí výpočtů
- Izolace kritických částí



Poměr kritických částí při dešifrování



Závislost doby dešifrování na parametru *m*

Řešerše

- Výhody a nevýhody
  - \+ Rychlost, odolnost, ...
  - – Velikost klíče, prostorová složitost, ...
- Kryptoanalýza
  - Slabiny
  - Útoky
  - Bezpečné parametry
- Moderní varianty a konverze

https://github.com/VojtechMyslivec/mceliece-mathematica/ **vojtech@xmyslivec.cz**