Kryptosystém McEliece

Diplomová práce

Bc. Vojtěch Myslivec

vedoucí: prof. Ing. Róbert Lórencz, CSc.

Fakulta informačních technologií
České vysoké učení technické v Praze

9. června 2016

Obsah

Obsah

Postkvantová kryptografie

Postkvantová kryptografie

- Kvantové počítače – Shorův algoritmus 1994.

Postkvantová kryptografie

- Kvantové počítače – Shorův algoritmus 1994.
- *RSA*, *ECDSA*, ...

Postkvantová kryptografie

- Kvantové počítače – Shorův algoritmus 1994.
- *RSA*, *ECDSA*, ...
- Kandidáti pro postkvantovou kryptografii [3, 4].
  - Symetrická kryptografie – *AES*
  - *Lattice-based* (svaz)
  - *Hash-based*
  - *Code-based*

Postkvantová kryptografie

- Kvantové počítače – Shorův algoritmus 1994.
- *RSA*, *ECDSA*, ...
- Kandidáti pro postkvantovou kryptografii [3, 4].
  - Symetrická kryptografie – *AES*
  - *Lattice-based* (svaz)
  - *Hash-based*
  - *Code-based* – McEliece

Obsah

Kryptosystém McEliece

- *Robert McEliece* 1978 [1].
- Systém pro asymetrické šifrování.

Kryptosystém McEliece

- *Robert McEliece* 1978 [1].
- Systém pro asymetrické šifrování.
- Využívá lineární kód pro opravu chyb.
  - Náhodný chybový vektor jako součást šifry.
  - Dekódovat neznámý lineární kód je NP-těžká úloha [2].

Kryptosystém McEliece

- *Robert McEliece* 1978 [1].
- Systém pro asymetrické šifrování.
- Využívá lineární kód pro opravu chyb.
  - Náhodný chybový vektor jako součást šifry.
  - Dekódovat neznámý lineární kód je NP-těžká úloha [2].
- Velké klíče (stovky kilobitů až jednotky megabitů).

Generování klíčů

Generování klíčů

Generování klíčů

1. *Lineární kód* $\mathcal{K}$ (n, k) opravující t chyb, s $k \times n$ generující maticí G.
2. Náhodná $k \times k$ regulární matice S.
3. Náhodná $n \times n$ permutační matice P.
4. Vypočítáme $k \times n$ matici $\hat{G} = SGP$.

Generování klíčů

1. *Lineární kód* $\mathcal{K}$ (n, k) opravující t chyb, s $k \times n$ generující maticí G.
2. Náhodná $k \times k$ regulární matice S.
3. Náhodná $n \times n$ permutační matice P.
4. Vypočítáme $k \times n$ matici $\hat{G} = SGP$.

Vygenerované klíče

Veřejné parametry

Čísla k, n, t

Veřejný klíč

Matice $\hat{G}$ $(\hat{G} = SGP)$

Soukromý klíč

Matice S, P a kód $\mathcal{K}$ generovaný G.

Algoritmy

Šifrování

Algoritmus E:

Máme zprávu m délky k, veřejný klíč $\hat{G}$ a parametr t.

1. Vygenerujeme chybový vektor z délky n s *Hammingovou vahou* t.
2. Šifrový text $c = m\hat{G} + z$.

Algoritmy

Šifrování

Algoritmus E**:**

Máme zprávu m délky k, veřejný klíč $\hat{G}$ a parametr t.

1. Vygenerujeme chybový vektor z délky n s *Hammingovou vahou* t.
2. Šifrový text $c = m\hat{G} + z$.

Dešifrování

Algoritmus D**:**

1. Vypočítáme $\hat{c} = cP^{-1}$.
2. Dekódujeme $\hat{m}$ z $\hat{c}$ pomocí použitého kódu.
   $Dek(\hat{c}) = \hat{m}$
3. Vypočítat původní zprávu $m = \hat{m}S^{-1}$.

Obsah

Binární Goppa kódy

- *Valery Goppa* 1970 [5].
- Nová kategorie *lineárních kódů* – AG kódy $\sim$ Goppa kódy.

Binární Goppa kódy

- *Valery Goppa* 1970 [5].
- Nová kategorie *lineárních kódů* – AG kódy $\sim$ Goppa kódy.
- Neexistují útoky na strukturu kódu.

Binární Goppa kódy

- *Valery Goppa* 1970 [5].
- Nová kategorie *lineárních kódů* – AG kódy $\sim$ Goppa kódy.
- Neexistují útoky na strukturu kódu.
- Základ pro *code-based* kryptografii.

Binární Goppa kódy

Sestrojení binárního (ireducibilního) Goppa kódu

Kód Γ s parametry (n, k) opravující t chyb.

Binární Goppa kódy

Sestrojení binárního (ireducibilního) Goppa kódu

Kód Γ s parametry (n, k) opravující t chyb.

- **Goppův polynom** g
  (Ireducibilní) polynom stupně t z okruhu polynomů nad konečným tělesem $\mathbb{F} = GF(2^m)$

$$g \in \mathbb{F}[x] \quad deg(g) = t$$

Binární Goppa kódy

Sestrojení binárního (ireducibilního) Goppa kódu

Kód Γ s parametry (n, k) opravující t chyb.

- **Goppův polynom** g
  (Ireducibilní) polynom stupně t z okruhu polynomů nad konečným tělesem $\mathbb{F} = GF(2^m)$

$$g \in \mathbb{F}[x] \quad deg(g) = t$$

- **Podpora** L
  Posloupnost n různých prvků z tělesa $\mathbb{F}$, které nejsou kořenem g

$$L = (L_1, \ldots, L_n) \quad \forall i, j : L_i \in \mathbb{F} \wedge L_i \neq L_j \wedge g(L_i) \neq \mathbf{0}$$

Binární Goppa kódy

Sestrojení binárního (ireducibilního) Goppa kódu

Kód Γ s parametry (n, k) opravující t chyb.

- **Goppův polynom** g
  (Ireducibilní) polynom stupně t z okruhu polynomů nad konečným tělesem $\mathbb{F} = GF(2^m)$

$$g \in \mathbb{F}[x] \quad deg(g) = t$$

- **Podpora** L
  Posloupnost n různých prvků z tělesa $\mathbb{F}$, které nejsou kořenem g

$$L = (L_1, \ldots, L_n) \quad \forall i, j : L_i \in \mathbb{F} \wedge L_i \neq L_j \wedge g(L_i) \neq \mathbf{0}$$

- **Kontrolní matice** H
  pokračování ...

Binární Goppa kódy

Sestrojení binárního (ireducibilního) Goppa kódu

- **Kontrolní matice H**

$$H = VD$$

Sestrojení binárního (ireducibilního) Goppa kódu

- **Kontrolní matice H**

$$H = VD$$

$$V = \begin{pmatrix} 1 & 1 & \dots & 1 \\ L_1 & L_2 & \dots & L_n \\ \vdots & \vdots & \ddots & \vdots \\ L_1^{t-1} & L_2^{t-1} & \dots & L_n^{t-1} \end{pmatrix}$$

Sestrojení binárního (ireducibilního) Goppa kódu

- **Kontrolní matice H**

$$H = VD$$

$$V = \begin{pmatrix} 1 & 1 & \dots & 1 \\ L_1 & L_2 & \dots & L_n \\ \vdots & \vdots & \ddots & \vdots \\ L_1^{t-1} & L_2^{t-1} & \dots & L_n^{t-1} \end{pmatrix}$$

$$D = \begin{pmatrix} g(L_1)^{-1} & & & \\ & g(L_2)^{-1} & & \\ & & \ddots & \\ & & & g(L_n)^{-1} \end{pmatrix}$$

Binární Goppa kódy

Dekódování

Binární Goppa kódy

Dekódování

Pattersonův algoritmus [6]

Binární Goppa kódy

Dekódování

Pattersonův algoritmus [6]

- Opravuje až t chyb.
- Kritická místa:
  - Výpočet odmocniny.
  - Hledání kořenů.

Binární Goppa kódy

Dekódování

Pattersonův algoritmus [6]

- Opravuje až t chyb.
- Kritická místa:
  - Výpočet odmocniny.
  - Hledání kořenů.
- Detaily v práci.

Obsah

Implementace

- Software *Wolfram Mathematica*.
- Implementace rozdělena do samosataných *balíků*.
- Implementováno:
  - Funkce pro operace v konečných tělesech (včetně rozšířených).
  - Goppa kódy
  - McEliece

Ukázka

Obsah

Shrnutí

Práce se zabývá:

Shrnutí

Práce se zabývá:

- Popisem kryptosystému, včetně varianty pro digitální podpis.

Shrnutí

Práce se zabývá:

- Popisem kryptosystému, včetně varianty pro digitální podpis.
- Goppa kódy.

Shrnutí

Práce se zabývá:

- Popisem kryptosystému, včetně varianty pro digitální podpis.
- Goppa kódy.
- Rozborem existujících kryptoanalýz a útoků.

Shrnutí

Práce se zabývá:

- Popisem kryptosystému, včetně varianty pro digitální podpis.
- Goppa kódy.
- Rozborem existujících kryptoanalýz a útoků.
- Moderními variantami a metodami na zkrácení klíčů.

Shrnutí

Práce se zabývá:

- Popisem kryptosystému, včetně varianty pro digitální podpis.
- Goppa kódy.
- Rozborem existujících kryptoanalýz a útoků.
- Moderními variantami a metodami na zkrácení klíčů.
- Implementací a měřením asymptotických složitostí.

Otázky

Prostor pro otázky.

Otázky

Prostor pro otázky.

Otázky oponenta:

Otázky

Prostor pro otázky.

Otázky oponenta:

1. Má vůbec smysl hledat úsporu prostoru u soukromého klíče, i s ohledem na vaše tvrzení, že kapacity disků jsou téměř neomezené a limit je primárně v přenosu veřejného klíče?

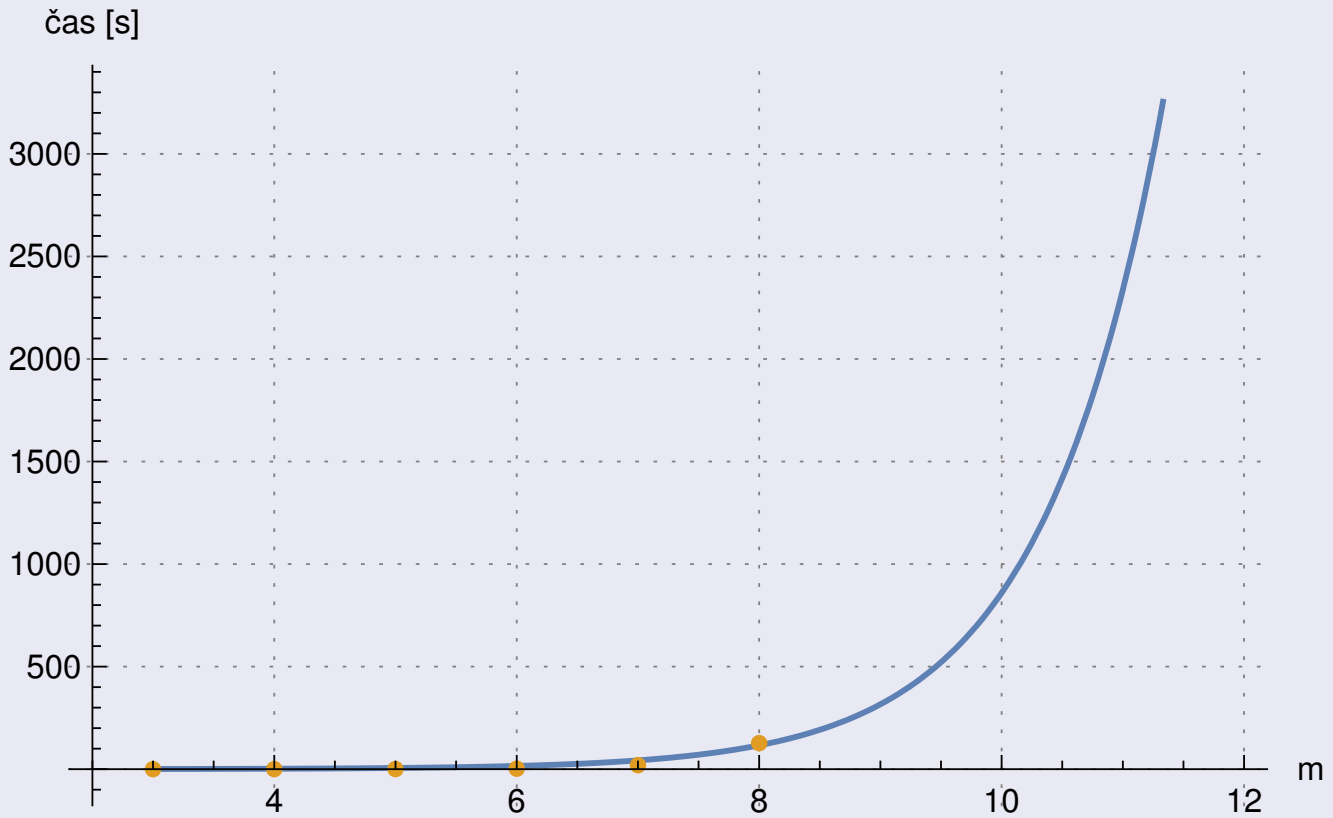
Otázky

Prostor pro otázky.

Otázky oponenta:

1. Má vůbec smysl hledat úsporu prostoru u soukromého klíče, i s ohledem na vaše tvrzení, že kapacity disků jsou téměř neomezené a limit je primárně v přenosu veřejného klíče?
2. Zkoušel jste změřit dobu generování klíčů, šifrování a dešifrování pro bezpečné parametry, tedy např. $m = 12$, $t = 41$?

2. rozumné parametry



Obrázek: Extrapolace doby trvání generování klíčů v závislosti na m.

Reference

[1] Robert J. McEliece. A Public-Key Cryptosystem Based on Algebraic Coding Theory v *JPL Deep Space Network Progress Report*, strany 114-116. 1978. Dostupné online `http://ipnpr.jpl.nasa.gov/progress_report2/42-44/44N.PDF`

[2] Elwyn R. Berlekamp, Robert J. McEliece, Henk C. A. van Tilborg. On the Inherent Intractibility v *IEEE Transactions of Information Theory*, vol. IT-24, No. 3, strany 384-386. IEEE, květen 1978.

[3] Daniel J. Bernstein, Johannes Buchmann, Erik Dahmen. *Post-Quantum Cryptography*. ISBN 978-3-540-88701-0. Springer Berlin Heidelberg, 2009.

[4] J. M. Schanck, W. Whyte, Z. Zhang. Criteria for selection of public-key cryptographic algorithms for quantum-safe hybrid cryptography (Internet-draft). IETF, 2016. Dostupné online `https://datatracker.ietf.org/doc/draft-whyte-select-pkc-qsh/`

[5] Valery D. Goppa. A New Class of Linear Correcting Codes v *Problemy*