ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE
FAKULTA INFORMAČNÍCH TECHNOLOGIÍ

ZADÁNÍ DIPLOMOVÉ PRÁCE

Název:	Asymetrický šifrovací algoritmus McEliece
Student:	Bc. Vojtěch Myslivec
Vedoucí:	prof. Ing. Róbert Lórencz, CSc.
Studijní program:	Informatika
Studijní obor:	Počítačová bezpečnost
Katedra:	Katedra počítačových systémů
Platnost zadání:	Do konce letního semestru 2016/17

Pokyny pro vypracování

Prostudujte asymetrický šifrovací algoritmus McEliece založený na binárních Goppa kódech. Proveďte rešerši existujících kryptoanalýz algoritmu McEliece a jeho variant. Zvažte metody zabývající se zkrácením velikosti klíčů. Implementujte šifrovací a dešifrovací algoritmy a změřte jejich výpočetní časovou a prostorovou náročnost v závislosti na velikosti klíče.

Seznam odborné literatury

Dodá vedoucí práce.

L.S.

prof. Ing. Róbert Lórencz, CSc.
vedoucí katedry

prof. Ing. Pavel Tvrdík, CSc.
děkan

V Praze dne 2. února 2016

České vysoké učení technické v Praze
Fakulta informačních technologií
Katedra počítačových systémů

Diplomová práce

Asymetrický šifrovací algoritmus McEliece

Bc. Vojtěch Myslivec

Vedoucí práce: prof. Ing. Róbert Lórencz, CSc.

20. března 2016

Prohlášení

Prohlašuji, že jsem předloženou práci vypracoval(a) samostatně a že jsem uvedl(a) veškeré použité informační zdroje v souladu s Metodickým pokynem o etické přípravě vysokoškolských závěrečných prací.

Beru na vědomí, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., autorského zákona, ve znění pozdějších předpisů. V souladu s ust. § 46 odst. 6 tohoto zákona tímto uděluji nevýhradní oprávnění (licenci) k užití této mojí práce, a to včetně všech počítačových programů, jež jsou její součástí či přílohou, a veškeré jejich dokumentace (dále souhrnně jen „Dílo“), a to všem osobám, které si přejí Dílo užít. Tyto osoby jsou oprávněny Dílo užít jakýmkoli způsobem, který nesnižuje hodnotu Díla, a za jakýmkoli účelem (včetně užití k výdělečným účelům). Toto oprávnění je časově, teritoriálně i množstevně neomezené. Každá osoba, která využije výše uvedenou licenci, se však zavazuje udělit ke každému dílu, které vznikne (byť jen zčásti) na základě Díla, úpravou Díla, spojením Díla s jiným dílem, zařazením Díla do díla souborného či zpracováním Díla (včetně překladu), licenci alespoň ve výše uvedeném rozsahu a zároveň zpřístupnit zdrojový kód takového díla alespoň srovnatelným způsobem a ve srovnatelném rozsahu, jako je zpřístupněn zdrojový kód Díla.

V Praze dne 20. března 2016 .....

Odkaz na tuto práci

Myslivec, Vojtěch. *Asymetrický šifrovací algoritmus McEliece.* Diplomová práce. Praha: České vysoké učení technické v Praze, Fakulta informačních technologií, 2016.

Abstrakt

V několika větách shrňte obsah a přínos této práce v češtině. Po přečtení abstraktu by se čtenář měl mít čtenář dost informací pro rozhodnutí, zda chce Vaši práci číst.

Klíčová slova McEliece, asymetrická kryptografie, postkvantová kryptografie, binární Goppa kódy, konečná tělesa, polynomy, Wolfram Mathematica

Abstract

Sem doplňte ekvivalent abstraktu Vaší práce v angličtině.

Keywords McEliece, public-key cryptography, post-quantum cryptography, binary Goppa codes, finite fields, polynomy, Wolfram Mathematica

Obsah

Seznam obrázků

Úvod

Tato práce se zabývá asymetrickým kryptosystémem *McEliece*. Mezi největší přednosti tohoto systému patří jeho odolnost vůči kvantovým počítačům a je tak jedním z vhodných kandidátů pro asymetrickou kryptografii pro postkvantovou dobu.

V prvních kapitolách této práce jsou popsány nezbytné primitivy z oblasti matematiky a teorie kódování, které jsou potřeba pro pochopení a použití kryptosystému McEliece. Jedná se především o počítání s *konečnými tělesy* a *polynomy* (kapitola 1) a binární *Goppa* kódy (kapitola 2).

Kryptosystému *McEliece* se věnuje kapitola 3. Kromě základního popisu generování klíčů a algoritmů pro šifrování a dešifrování je probráno i *Niederreiterovo* schéma – „úprava“ kryptosystému *McEliece* pro získání *digitálního podpisu*. Jsou ukázány slabiny, nevýhody i možné útoky na kryptosystém McEliece a též zmíněna praktická varianta systému odolná vůči těmto aspektům.

V poslední části práce je probrána implementace kryptosystému *McEliece* v softwaru *Wolfram Mathematica* včetně změřených časových složitostí (kapitola 4),.

Kapitola 1

Obecná algebra

V kapitole jsou probrány definice a algoritmy nutné pro práci s *konečnými tělesy* a *polynomy* nad konečným tělesem. V práci se předpokládá základních znalostí z oblasti *algebry*. Pro tato témata je doporučena literatura [4, 5, 6, 7, 2] (kde lze též najít většinu důkazů následujících vět).

1.1 Základní termíny

Pro ujasnění je uvedena definice tělesa:

Definice 1 (Těleso) *Nechť M je neprázdná množina $a + a \cdot$ binární operace*[1]*. Struktura $T = (M, +, \cdot)$ se nazývá těleso, pokud platí*

1. *$(M, +)$ je* komutativní grupa *(nazývána* aditivní*)*
2. *$(M \setminus \{0\}, \cdot)$*[2] *je* grupa *(nazývána* multiplikativní*)*
3. *Platí (levý i pravý)* distributivní zákon*:*

$$\forall a, b, c \in M : \big(a(b + c) = ab + ac\big) \wedge \big((b + c)a = ba + ca\big)$$

Těleso, které má konečný počet prvků, se nazývá *konečné těleso*.

Věta 1 *Nechť T je* konečné těleso*, pak jeho počet prvků (*řád*) je p^n, kde p je prvočíslo a $n \in \mathbb{N} \wedge n \geq 1$.*

Číslo p se nazývá *charakteristika*. Navíc platí, že *všechna konečná tělesa* se stejným počtem prvků jsou navzájem *izomorfní*. *Konečné těleso* řádu p^n je tedy dále označováno jako $GF(p^n)$ (z anglického *Gallois field*, dle francouzského matematika *Évariste Galois*).

[1] Pro zjednodušení zápisu je $\cdot$ často vynecháváno.
[2] Prvek *0* je *nulový* (*neutrální*) prvek *aditivní grupy*.

1.2 Reprezentace prvků

Jak bude ukázáno dále, je vhodné prvky tělesa $GF(p^n)$ reprezentovat jako *polynomy* s koeficienty z množiny $\mathbb{Z}_p = \{0, 1, \ldots, p-1\}$, tedy prvek $a \in GF(p^n)$ lze zapsat:

$$A(x) = \sum_{i=0}^{n-1} a_i x^i, a_i \in \mathbb{Z}_p$$

O takovém polynomu říkáme, že je to *polynom nad tělesem $GF(p)$ (řádu maximálně $n-1$)*. Na prvek a je též možné se dívat jako na vektor či n-tici koeficientů a_i:

$$A(x) \cong a \cong (a_{n-1}a_{n-2}\ldots a_0) \cong a_{n-1}a_{n-2}\ldots a_0$$

V této práci se mezi těmito reprezentacemi prvků nadále volně přechází, jak bude v daném kontextu potřeba potřeba[3].

1.3 Operace v tělese $GF(p^n)$

V následujících sekcích jsou probrány operace potřebné pro počítání s tělesy $GF(p^n)$. Konkrétní zvolené algoritmy a jejich implementace je detailně popsána v kapitole 4.

1.3.1 Sčítání

Sčítání v tělese $GF(p^n)$ je definováno stejně jako sčítání polynomů, s tím, že sčítání jednotlivých koeficientů je prováděno *modulo p* (v tělese $GF(p)$:

$$A(x) + B(x) = \sum a_i x^i + \sum b_i x^i = \sum |a_i + b_i|_p \, x^i$$

1.3.2 Násobení

Násobení v tělese $GF(p^n)$ nelze provádět „po složkách“, jako je tomu u sčítání. U takto definované operace by většina prvků neměla (multiplikativní) *inverzi* a nejednalo by se tak o *těleso*.

Při násobení prvků se opět využije jejich reprezentace pomocí polynomů. Výsledkem násobení pak je:

$$A(x) \cdot B(x) = \sum_{i=0}^{n-1} a_i x^i \cdot \sum_{i=0}^{n-1} b_i x^i = \sum_{i=0}^{2n-2} \left| \sum_{j+k=i} a_j \cdot b_k \right|_p x^i$$

Jak je naznačeno, násobení i sčítání koeficientů se provádí *modulo p* (v tělese $GF(p)$.

[3] V některých materiálech se používá i obráceného zápisu ($a_0 a_1 \ldots a_p - 1$).

Kvůli uzavřenosti násobení v tělese je nutné zavést operaci $A(x) \mod P(x)$, neboli zbytek po dělení polynomu $A(x)$ polynomem $P(x)$. Dále je třeba pro určení tělesa $GF(p^n)$ určit *ireducibilní* polynom, který bude použitý při operaci násobení.

Definice 2 *Polynom $P(x)$ nad tělesem $GF(p)$ je* ireducibilní *právě tehdy, když pro každé dva polynomy $A(x)$ a $B(x)$ nad $GF(p)$ platí:*

$$A(x) \cdot B(x) = P(x) \Rightarrow (deg(A(x)) = 0) \vee (deg(B(x)) = 0)$$

Neboli pro *ireducibilní* polynom platí, že neexistuje rozklad na polynomy nad $GF(p)$ stupně alespoň 1.

Příklad: Polynom $x^3 + x + 1$ je nad tělesem $GF(2)$ *ireducibilní*, protože neexistuje jeho rozklad na polynomy stupně alespoň 1.
Polynom $x^2 + 1$ není nad tělesem $GF(2)$ *ireducibilní*, protože:

$$(x+1) \cdot (x+1) = x^2 + |1+1|_2 \, x + 1 = x^2 + 1$$

Nyní je možné zavést operaci násobení dvou prvků tělesa jako násobení dvou polynomů *modulo zadaný ireducibilní* polynom:

$$A(x) \cdot B(x) = \sum a_i x^i \cdot \sum b_i x^i = \sum \left| \sum_{j+k=i} a_j \cdot b_k \right|_p x^i \mod P(x)$$

Poznámka Pokud by zvolený $P(x)$ nebyl *ireducibilní*, jednalo by se o *okruh*, nikoliv o *těleso*, protože by neexistovala *multiplikativní inverze* pro některé prvky a navíc by i existovaly tzv. *dělitelé nuly*.

1.3.3 Umocňování

Pro rozšíření operací o opakované násobení je vhodné zavést operaci umocňování.

Definice 3 *Pro prvek a tělesa T a číslo $n \in \mathbb{N}$ je operace umocňování definována následovně:*

$$\begin{aligned} a^0 &= 1 \\ a^n &= \underbrace{a \cdot a \cdot \ldots \cdot a}_{n\text{-krát}} \\ a^{-n} &= \left(a^{-1}\right)^n \end{aligned}$$

Pro efektivní výpočet mocniny prvku je vhodné použít algoritmus *Square-and-Multiply*, kde se dílčí operace „square“ a „multiply“ provádí operací $\cdot$ v daném tělese $GF(p^n)$.

1.3.4 Inverze

Inverzi v *grupě* lze obecně definovat následovně:

Definice 4 (Inverze) *Nechť a je prvkem a $\mathbb{O}$ neutrálním prvkem* grupy $G = (M, \circ)$. *Prvek $\bar{a}$ je* inverzí *prvku a, pokud platí následující rovnice:*

$$a \circ \bar{a} = \mathbb{O}$$

1.3.4.1 Aditivní inverze

Inverze v *aditivní grupě* je značena znaménkem minus „$-$“ a je z definice velmi triviální:

$$|A(x) + (-A(x))|_p = 0 \Rightarrow -A(x) = \sum |-a_i|_p \, x^i$$

Neboli je to aditivní inverze jednotlivých koeficientů *modulo* p (v tělese $GF(p)$).

1.3.4.2 Multiplikativní inverze

Inverze v *multiplikativní grupě* je značena záporným exponentem „$^{-1}$“ či symbolem dělení.

$$\left|A(x) \cdot A(x)^{-1}\right|_p = \left|\frac{A(x)}{A(x)}\right|_p = 1$$

Tuto *multiplikativní inverzi* je třeba počítat *rozšířeným Euklidovým algoritmem pro polynomy* (*EEA*), či případně jinými algoritmy, jako je např. *algoritmus Itoh-Teechai-Tsujii* (*ITT*) [7, 3].

Rozšířený Euklidův algoritmus pro polynomy, stejně jako v modulární aritmetice (neboli pro tělesa $GF(p)$), stojí na nalezení *Bézoutovy rovnosti*. Pro výpočet *EEA* je třeba výpočtu dělení polynomů se zbytkem[4].

[4] Někdy uváděno jako dlouhé dělení.

Kapitola 2

Lineární kódy

2.1 Kódování

2.2 Lineární kódy

2.2.1 Hammingovy kódy

2.3 Goppa kódy

Ireducibilní binární Goppa kódy

Kapitola 3

Kryptosystém McEliece

3.1 Asymetrické šifrování McEliece

3.2 Niederreiterovo schéma

3.3 Bezpečnost algoritmů

3.3.1 Typy útoků

3.3.2 Slabiny systému

3.3.3 Existující útoky

3.3.4 Praktická varianta

CCA2-odolná varianta

Kapitola 4

Implementace

Závěr

Literatura

[1]

[2]

[3]

[4]

[5]

[6]

[7]

[8]

Příloha A

Seznam použitých zkratek

GF Gallois field

Příloha **B**

Obsah přiloženého CD

- `readme.txt` ..... stručný popis obsahu CD
- `exe` ..... adresář se spustitelnou formou implementace
- `src`
  - `impl` ..... zdrojové kódy implementace
  - `thesis` ..... zdrojová forma práce ve formátu LaTeX
- `text` ..... text práce
  - `thesis.pdf` ..... text práce ve formátu PDF
  - `thesis.ps` ..... text práce ve formátu PS