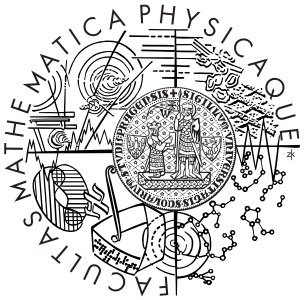
Univerzita Karlova v Praze

Matematicko-fyzikální fakulta

DIPLOMOVÁ PRÁCE



Aleš Fuchs

Aplikace Gröbnerových bází v kryptografii

Katedra algebry

Vedoucí diplomové práce: Mgr. Jan Šťovíček Ph.D.

Studijní program: Matematika

Studijní obor: Matematické metody informační bezpečnosti

Praha 2011

Rád bych poděkoval svému vedoucímu Mgr. Janu Šťovíčkovi Ph.D. za vedení diplomové práce a také za jeho trpělivost při mé dočasné apatii. Rovněž patří můj dík rodině a přítelkyni za podporu při studiu a zajištění potřebného zázemí. Děkuji také svým kamarádům za občasná rozptýlení, která mi přišla v průběhu sepisování vhod.

Prohlašuji, že jsem tuto diplomovou práci vypracoval samostatně a výhradně s použitím citovaných pramenů, literatury a dalších odborných zdrojů.

Beru na vědomí, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., autorského zákona v platném znění, zejména skutečnost, že Univerzita Karlova v Praze má právo na uzavření licenční smlouvy o užití této práce jako školního díla podle §60 odst. 1 autorského zákona.

V Praze dne 15. srpna 2011 Aleš Fuchs

Název práce: Aplikace Gröbnerových bází v kryptografii

Autor: Aleš Fuchs

Katedra: Katedra algebry

Vedoucí diplomové práce: Mgr. Jan Šťovíček Ph.D., Katedra algebry

Abstrakt: V této práci studujeme přípustná uspořádání a postupy redukce polynomu množinou jiných polynomů v prostředí polynomiálních okruhů nad konečnými tělesy. Zde hrají významnou roli Gröbnerovy báze nějakého ideálu, které díky svým vlastnostem umožňují řešit problém náležení do daného ideálu. Zkoumáme také vlastnosti takzvaných redukovaných Gröbnerových bází, které jsou pro daný ideál jednoznačně určené a v jistém ohledu minimální. Dále se zabýváme rozšířením této teorie do prostředí volných algeber nad konečnými tělesy, kde proměnné nekomutují. Na rozdíl od prvního případu zde Gröbnerovy báze mohou být nekonečné i pro konečně generované oboustranné ideály. V poslední kapitole uvádíme asymetrický kryptosystém Polly Cracker založený právě na problému náležení do ideálu jak v komutativní, tak v nekomutativní teorii. Zkoumáme známé metody kryptoanalýzy aplikované na tyto systémy a v několika případech i opatření, která útokům předchází. Souhrn opatření aplikujeme v poslední části věnované návrhům bezpečných konstrukcí Polly Crackeru.

Klíčová slova: nekomutativní Gröbnerovy báze, Polly Cracker, bezpečnost, kryptoanalýza

Title: Applications of Gröbner bases in cryptography

Author: Aleš Fuchs

Department: Department of Algebra

Supervisor: Mgr. Jan Šťovíček Ph.D., Department of Algebra

Abstract: In the present paper we study admissible orders and techniques of multivariate polynomial division in the setting of polynomial rings over finite fields. The Gröbner bases of some ideal play a key role here, as they allow to solve the ideal membership problem thanks to their properties. We also explore features of so called reduced Gröbner bases, which are unique for a particular ideal and in some way also minimal. Further we will discuss the main facts about Gröbner bases also in the setting of free algebras over finite fields, where the variables are non-commuting. Contrary to the first case, Gröbner bases can be infinite here, even for some finitely generated two-sided ideals. In the last chapter we introduce an asymmetric cryptosystem Polly Cracker, based on the ideal membership problem in both commutative and noncommutative theory. We analyze some known cryptanalytic methods applied to these systems and in several cases also precautions dealing with them. Finally we summarize these precautions and introduce a blueprint of Polly Cracker reliable construction.

Keywords: noncommutative Gröbner bases, Polly Cracker, security, cryptanalysis

Obsah

1. Úvod

1.1 Asymetrická kryptografie

Soudobá kryptografie je rozdělená do dvou oblastí, *symetrické* a *asymetrické*. Asymetrická kryptografie využívá na rozdíl od prvního oboru různé klíče pro šifrování a dešifrování. Jeden z těchto klíčů je veřejný a jeden soukromý, který zná pouze osoba, která instanci systému vytvořila.

Pokud zprávu šifruje vlastník soukromého klíče, nazýváme protokol *elektronický podpis*. Šifrový text může kdokoli dešifrovat a schopnost šifrování dokazuje, že zpráva pochází opravdu od osoby, která zná soukromý klíč.

Pokud otevřený text šifruje někdo pomocí veřejného klíče, může být zpráva opět dešifrována pouze osobou, která zná klíč soukromý. Takový protokol umožňuje šifrovanou komunikaci po veřejné lince, kterou je možné odposlouchávat, bez nutnosti výměny soukromého klíče mezi komunikujícími stranami, což je nutné při použití metod symetrické kryptografie. S rozvojem elektronické komunikace se tento způsob šifrování velmi dobře ujal.

Asymetrický způsob šifrování má kořeny na konci 19. století, kdy V. S. Jevons poprvé v [Jev] popsal možné použití tzv. *jednocestných funkcí* v kryptografii. Jednosměrná funkce f má tu vlastnost, že ke každému x lze snadno získat hodnotu $y = f(x)$, a přitom výpočet inverzní funkce $f^{-1}(y)$ je sice možný, ale výpočetně mnohem náročnější. V kryptografii jsou k účelům šifrování ze zřejmých důvodů použitelné hlavně bijektivní jednocestné funkce, naopak nebijektivní jednocestné funkce mají dobré využití v oblasti hashovacích funkcí. Dobře známou jednocestnou funkcí je násobení, kdy součin dvou dostatečně velkých prvočísel lze jen obtížně zpětně rozložit. Podobně funguje i

umocňování nad konečným tělesem, které je v asymetrické kryptografii velmi hojně používáno, a pro inverzní funkci se ujal název *diskrétní logaritmus*. Obecně lze nalézt nejvíce jednocestných funkcí v oblasti algebry a teorie čísel.

Poprvé však byla aplikace tohoto přístupu publikována až v roce 1976, kdy W. Diffie a M. Hellman navrhli postup výměny společného soukromého klíče pomocí asymetrické kryptografie. Pointa byla ve využití problému diskrétního logaritmu a kryptosystémy, které z něj vzešly, jako například RSA, ElGamal a DSA, se používají dodnes. V Diffie-Hellmanově článku [DiHe] byl použit termín *Trapdoor jednocestné funkce* neboli *jednocestné funkce se zadními vrátky*, který označuje jednocestnou funkci, pro kterou je snadné najít inverzní funkci, pokud je známa nějaká dodatečná informace (zadní vrátka).

Třídu asymetrických kryptosystémů můžeme dále rozdělit na *deterministické* a *probabilistické*. Deterministický přístup zaručuje, že při stejné sadě klíčů bude otevřený text vždy zašifrován do stejné zprávy. V tomto odvětví můžeme nalézt většinu dnes známých asymetrických systémů. Nevýhodou zde je, že pokud je prostor otevřených textů, nebo množina předpokládaných otevřených textů dostatečně malá, nechá si útočník zašifrovat všechny otevřené texty, a tím získá jakousi kódovou knihu, kterou může použít k dešifrování libovolné zprávy. Tomuto útoku můžeme předejít takzvaným přidáním soli, tedy náhodného paddingu, který lze v otevřeném textu lehce rozpoznat a odstranit. Šifrový text tak bude pokaždé jiný, a tudíž nemá útočník šanci. Použití paddingu přesouvá deterministický kryptosystém do skupiny probabilistických. První návrh ryze probabilistického kryptosystému zveřejnili S. Goldwasser a S. Micali v [GoMi] v roce 1982.

Později v roce 1993 byl M. Fellowsem a N. Koblitzem v článku [FeKo] předveden probabilistický kryptosystém *Polly Cracker* založený na teorii Grö-

bnerových bází. Jejich návrh byl ale podroben důkladné kryptoanalýze a kvůli několika objeveným slabinám začal být postupně veřejností vnímán jako nepoužitelný. V roce 2004 se k této látce opět vrátil T. Rai a ve své disertační práci navrhl obecnější instanci Polly Crackeru, který - jak doufal - bude vůči všem dosud známým útokům odolný.

V diplomové práci nejprve ukážeme potřebné výsledky a algoritmy z teorie Gröbnerových bází, a poté předvedeme původní návrh Polly Crackeru společně s útoky, které odhalily trhliny v jeho bezpečnosti. Poté prověříme účinnost těchto útoků v nekomutativní teorii a uvedeme případná bezpečnostní opatření, jež shrneme ve finálním návrhu.

2. Komutativní Gröbnerovy báze

Teorii Gröbnerových bází pro polynomiální okruhy vyvinul Bruno Buchberger v roce 1965 v [Buch]. Pojmenoval je podle vedoucího své disertační práce, Wolfganga Gröbnera. Poskytují efektivní nástroj k řešení základních problémů komutativní algebry a za poslední čtyři desetiletí se jim s exponenciálním vývojem výpočetní síly dostalo velké pozornosti. K některým problémům, které Gröbnerovy báze teoreticky řeší, však stále neexistují efektivní nástroje, především kvůli velkým paměťovým nárokům na jejich výpočet.

V této kapitole uvedeme základní vlastnosti Gröbnerových bází a vysvětlíme jejich důležitost při redukci polynomu množinou polynomů. Kapitolu pojmeme jako přehled výsledků a úvod do problematiky, kterou podrobněji rozvedeme v následující části. Pro podrobnější výklad problematiky a důkazy ke zde uvedeným výsledkům odkážeme čtenáře například na publikace [AdLo] nebo [BeWe].

2.1 Uspořádání termů

Definice 2.1.1 (Term)**.** Buď $\mathbb{F}$ těleso a $R = \mathbb{F}[x_1, x_2, \ldots, x_n]$ buď množina všech komutativních polynomů s koeficienty z $\mathbb{F}$. Prvky R jsou tedy konečné součty monočlenů ve tvaru $a \cdot x_1^{\beta_1} x_2^{\beta_2} \cdots x_n^{\beta_n}$, kde $a \in \mathbb{F}$ a $\beta_i \in \mathbb{N}$ pro $i = 1, 2, \ldots, n$. (Poznamenejme, že $\mathbb{N}$ zde značí množinu nezáporných celých čísel, $\{0, 1, 2, \ldots\}$.) R je komutativní okruh vzhledem k běžným operacím sčítání a násobení polynomů. R je také $\mathbb{F}$-vektorový prostor s bází $T^n = \{x_1^{\beta_1} \cdots x_n^{\beta_n} \mid \beta_i \in \mathbb{N}, i = 1, 2, \ldots, n\}$. Prvky množiny T^n nazýváme *termy*. Budeme používat

zápis $\mathbf{x}^{\boldsymbol{\beta}}$ značící term $x_1^{\beta_1} x_2^{\beta_2} \cdots x_n^{\beta_n}$.

Stupeň polynomu budeme značit $deg(\mathbf{x}^{\boldsymbol{\beta}}) = \sum_{i=1}^{n} \beta_i$.

Definice 2.1.2 (Přípustné uspořádání termů)**.** Uspořádání $<$ na množině T^n nazveme *přípustné*, pokud

(i) pro všechny termy $\mathbf{x}^{\boldsymbol{\alpha}}, \mathbf{x}^{\boldsymbol{\beta}} \in T^n$ platí právě jedna z relací $\mathbf{x}^{\boldsymbol{\alpha}} < \mathbf{x}^{\boldsymbol{\beta}}$, $\mathbf{x}^{\boldsymbol{\alpha}} = \mathbf{x}^{\boldsymbol{\beta}}$ nebo $\mathbf{x}^{\boldsymbol{\alpha}} > \mathbf{x}^{\boldsymbol{\beta}}$, tedy $<$ je *lineární uspořádání*,

(ii) $1 < \mathbf{x}^{\boldsymbol{\beta}}$ pro všechny $\mathbf{x}^{\boldsymbol{\beta}} \neq 1$ a

(iii) jestliže $\mathbf{x}^{\boldsymbol{\alpha}} < \mathbf{x}^{\boldsymbol{\beta}}$, pak $\mathbf{x}^{\boldsymbol{\alpha}}\mathbf{x}^{\boldsymbol{\gamma}} < \mathbf{x}^{\boldsymbol{\beta}}\mathbf{x}^{\boldsymbol{\gamma}}$ pro všechny $\mathbf{x}^{\boldsymbol{\gamma}} \in T^n$.

Toto uspořádání budeme také v textu označovat jako přípustné na množině $R = \mathbb{F}[x_1, x_2, \ldots, x_n]$.

Poznámka 2.1.3. Přípustné uspořádání můžeme zavést také na množině monočlenů $M = \{a \cdot \mathbf{x}^{\boldsymbol{\alpha}} \mid a \in \mathbb{F}, \mathbf{x}^{\boldsymbol{\alpha}} \in T^n\}$ stejně jako na množině termů s tím, že koeficienty nemají na uspořádání žádný vliv.

Pozorování 2.1.4. Mějme $\mathbf{x}^{\boldsymbol{\alpha}}, \mathbf{x}^{\boldsymbol{\beta}} \in T^n$. Pokud $\mathbf{x}^{\boldsymbol{\alpha}}$ dělí $\mathbf{x}^{\boldsymbol{\beta}}$, pak $\mathbf{x}^{\boldsymbol{\alpha}} \leq \mathbf{x}^{\boldsymbol{\beta}}$.

Pozorování 2.1.5. Pro přípustné uspořádání navíc platí, že je *dobré*. To znamená, že každá ostře klesající posloupnost prvků je konečná. Pokud by existovala nekonečná posloupnost $\mathbf{x}^{\boldsymbol{\alpha}_1} > \mathbf{x}^{\boldsymbol{\alpha}_2} > \cdots$, byl by ideál generovaný těmito termy podle Hilbertovy věty o bázi konečně generovaný. Pak by ale muselo existovat j takové, že $\mathbf{x}^{\boldsymbol{\alpha}_j}$ by bylo lineární kombinací termů $\mathbf{x}^{\boldsymbol{\alpha}_1}, \ldots, \mathbf{x}^{\boldsymbol{\alpha}_{j-1}}$, což by vedlo ke sporu, vzhledem k předešlému pozorování.

Nyní uvedeme tři nejčastěji používaná přípustná uspořádání.

Definice 2.1.6 (Lex - lexikografické uspořádání)**.** Uspořádejme libovolně proměnné $x_1, x_2, \ldots, x_n$, například $x_1 > x_2 > \cdots > x_n$. Pro n-tice $\boldsymbol{\alpha} =$

$(\alpha_1, \alpha_2, \ldots, \alpha_n)$, $\boldsymbol{\beta} = (\beta_1, \beta_2, \ldots, \beta_n) \in \mathbb{N}^n$, definujme $\mathbf{x}^{\boldsymbol{\alpha}} < \mathbf{x}^{\boldsymbol{\beta}}$, právě když pro první souřadnice zleva, které se liší, platí $\alpha_i < \beta_i$.

Definice 2.1.7 (DegLex - graduovaně lexikografické uspořádání)**.** Uspořádejme libovolně proměnné $x_1, x_2, \ldots, x_n$, například $x_1 > x_2 > \cdots > x_n$. Pro n-tice $\boldsymbol{\alpha} = (\alpha_1, \alpha_2, \ldots, \alpha_n)$, $\boldsymbol{\beta} = (\beta_1, \beta_2, \ldots, \beta_n) \in \mathbb{N}^n$, definujme $\mathbf{x}^{\boldsymbol{\alpha}} < \mathbf{x}^{\boldsymbol{\beta}}$, právě když

(i) $deg(\mathbf{x}^{\boldsymbol{\alpha}}) < deg(\mathbf{x}^{\boldsymbol{\beta}})$ nebo

(ii) $deg(\mathbf{x}^{\boldsymbol{\alpha}}) = deg(\mathbf{x}^{\boldsymbol{\beta}})$ a zároveň $\mathbf{x}^{\boldsymbol{\alpha}} < \mathbf{x}^{\boldsymbol{\beta}}$ v Lex uspořádání.

Definice 2.1.8 (WeightLex - váhovaně lexikografické uspořádání)**.** Uspořádejme libovolně proměnné $x_1, x_2, \ldots, x_n$, například $x_1 > x_2 > \cdots > x_n$. Dále mějme tzv. *váhový vektor* $w = (w_1, w_2, \ldots, w_n)$ nezáporných reálných čísel. Pro n-tice $\boldsymbol{\alpha} = (\alpha_1, \alpha_2, \ldots, \alpha_n)$, $\boldsymbol{\beta} = (\beta_1, \beta_2, \ldots, \beta_n) \in \mathbb{N}^n$, definujme $\mathbf{x}^{\boldsymbol{\alpha}} < \mathbf{x}^{\boldsymbol{\beta}}$, právě když

(i) $\sum_{i=1}^{n} \alpha_i \cdot w_i < \sum_{i=1}^{n} \beta_i \cdot w_i$ nebo

(ii) $\sum_{i=1}^{n} \alpha_i \cdot w_i = \sum_{i=1}^{n} \beta_i \cdot w_i$ a zároveň $\mathbf{x}^{\boldsymbol{\alpha}} < \mathbf{x}^{\boldsymbol{\beta}}$ v Lex uspořádání.

Definice 2.1.9 (Ideál generovaný množinou)**.** Připomeňme že $I \subseteq R$ nazýváme *ideál*, pokud je uzavřený vzhledem ke sčítání a pokud $f \cdot g \in I$ pro všechny $f \in I$, a všechny $g \in R$. Mějme $A \subseteq R$, potom *ideálem generovaným množinou* A rozumíme nejmenší ideál okruhu R, který množinu A obsahuje, a značíme jej $\langle A \rangle$. V takovém případě nazýváme A *generující množinou* $\langle A \rangle$. Pokud je A konečná množina $A = \{f_1, f_2, \ldots, f_s\}$, pak $\langle A \rangle = \langle f_1, f_2, \ldots, f_s \rangle = \left\{ \sum_{i=1}^{s} u_i f_i \mid u_i \in R, i = 1, 2, \ldots, s \right\}$.

Definice 2.1.10. Buď $<$ přípustné uspořádání na $R = \mathbb{F}[x_1, x_2, \ldots, x_n]$. Mějme množinu $A \subseteq R$ a polynom $f = c_1\mathbf{x}^{\boldsymbol{\alpha}_1} + c_2\mathbf{x}^{\boldsymbol{\alpha}_2} + \cdots + c_r\mathbf{x}^{\boldsymbol{\alpha}_r} \in R$, kde

$c_i \neq 0$ pro všechna $i = 1, 2, \ldots r$ a kde $\mathbf{x}^{\boldsymbol{\alpha}_1} > \mathbf{x}^{\boldsymbol{\alpha}_2} > \cdots > \mathbf{x}^{\boldsymbol{\alpha}_r}$. Definujeme:

- *vedoucí term* polynomu f jako $lt(f) = \mathbf{x}^{\boldsymbol{\alpha}_1}$,
- *vedoucí koeficient* polynomu f jako $lc(f) = c_1$,
- *vedoucí monočlen* polynomu f jako $lm(f) = c_1\mathbf{x}^{\boldsymbol{\alpha}_1} = lc(f) \cdot lt(f)$,
- *ideál vedoucích monočlenů* množiny A jako $Lm(A) = \langle lm(f) \mid f \in A \rangle$,
- množinu termů z polynomu f s nenulovým koeficientem budeme značit $supp(f)$, $supp(A) = \{supp(f) \mid f \in A\}$.

Poznámka 2.1.11. Uvědomme si, že pro různá přípustná uspořádání se mohou vedoucí termy lišit.

2.2 Redukce polynomů

V této podkapitole se zaměříme na algoritmus redukce polynomu množinou polynomů, který je přirozeným rozšířením algoritmu dělení polynomu polynomem. Při redukci Gröbnerovou bází získáme nástroj k řešení problému náležení do ideálu.

Definice 2.2.1. Mějme polynomy $f, g, h \in R = \mathbb{F}[x_1, x_2, \ldots, x_n]$, kde $g \neq 0$. Řekneme, že polynom f *se redukuje na* h *modulo* g *v jednom kroku*, právě když $lm(g)$ dělí nějaký nenulový člen m polynomu f a $h = f - \dfrac{m}{lm(g)}g$, kde h již neobsahuje žádný člen se stejným termem jako m. V takové situaci budeme psát $f \xrightarrow{g} h$.

Nyní mějme polynom f a $A = \{f_1, f_2, \ldots, f_s\}$ množinu nenulových polynomů z R. Řekneme, že f *se redukuje na* h *modulo* A, právě když existuje posloupnost indexů $i_1, i_2, \ldots, i_t \in \{1, \ldots, s\}$ a posloupnost polynomů

$h_1, h_2, \ldots, h_{t-1}$ z R takových, že $f \xrightarrow{f_{i_1}} h_1 \xrightarrow{f_{i_2}} \cdots \xrightarrow{f_{i_{t-1}}} h_{t-1} \xrightarrow{f_{i_t}} h$. V tomto případě budeme psát $f \xrightarrow{A}_+ h$.

Definice 2.2.2. Řekneme, že polynom h je *redukovaný* vzhledem k množině nenulových polynomů $A = \{f_1, f_2, \ldots, f_s\}$, pokud ho již nelze množinou A dále redukovat.

Jestliže $f \xrightarrow{A}_+ h$ a h je redukovaný vzhledem k A, nazveme h *zbytkem* f *po redukci množinou* A a značíme $f \xrightarrow{A} h$.

Samotný algoritmus pro redukci polynomu f množinou polynomů $A = \{f_1, f_2, \ldots, f_s\}$ zde uvádět nebudeme. Řekněme jen, že množina A musí být (libovolně) uspořádaná a v každé iteraci i určíme největší polynom, jakým lze průběžný polynom h_{i-1} redukovat a redukci provedeme. Pokud již redukovat nelze, algoritmus ukončíme.

Vyvstává zde však problém, kdy při různých uspořádáních množiny A může algoritmus vrátit různý výsledek.

2.3 Komutativní Gröbnerovy báze

Definice 2.3.1. Buď I ideál okruhu $R = \mathbb{F}[x_1, x_2, \ldots, x_n]$. Množinu nenulových polynomů $G = \{g_1, \ldots, g_t\} \subseteq I$ nazveme *Gröbnerova báze ideálu* I, právě když pro každý nenulový polynom $f \in I$ existuje $i \in \{1, \ldots, t\}$ takové, že $lt(g_i)|lt(f)$. Jinými slovy, G je Gröbnerova báze ideálu I, právě když $Lm(G) = Lm(I)$.

Poznámka 2.3.2. Z definice vyplývá, že každá Gröbnerova báze nějakého ideálu je zároveň jeho množinou generátorů.

Věta 2.3.3. *Buď I ideál okruhu $R = \mathbb{F}[x_1, x_2, \ldots, x_n]$ a $G = \{g_1, \ldots, g_t\} \subseteq I$ množina nenulových polynomů. Následující tvrzení jsou ekvivalentní:*

(i) G *je Gröbnerova báze ideálu* I*.*

(ii) $f \in I$*, právě když* $f \xrightarrow{G} 0$*.*

(iii) $f \in I$*, právě když* $f = \sum_{i=1}^{t} h_i g_i$*, kde* $lt(f) = \max_{1 \leq i \leq t}(lt(h_i) \cdot lt(g_i))$*.*

(iv) Pro každý polynom $f \in R$ *je jeho zbytek vzhledem ke* G *jednoznačný.*

Definice 2.3.4. Zbytek polynomu f vzhledem ke Gröbnerově bázi G definujeme jako *normální formu* f a značíme ji $N_G(f)$.

Poznámka 2.3.5. Věta 2.3.3 nám dává možnost rozhodnout problém náležení do ideálu. K řešení nám stačí už jen najít Gröbnerovu bázi daného ideálu. Pokud bude normální forma redukovaného polynomu nulová, je jisté, že polynom do ideálu náleží.

Kdyby G nebyla Gröbnerova báze ideálu I, redukce polynomu $f \in I$ množinou G by ve většině případů neodhalila lineární kombinaci z bodu (iii).

V další části této podkapitoly se budeme zabývat hledáním Gröbnerovy báze pro nějaký ideál okruhu R.

Definice 2.3.6. Nechť f, g jsou dva nenulové polynomy okruhu $R = \mathbb{F}[x_1, x_2, \ldots, x_n]$. Buď $L = nsn(lt(f), lt(g))$. Polynom $S(f,g) = \frac{L}{lm(f)} f - \frac{L}{lm(g)} g$ nazýváme *S-polynom* f a g.

Příklad 2.3.7. Uvažme polynomy $f = x^2y + 2$, $g = 3xy^2 + 6x^2$ a uspořádání DegLex s proměnnými uspořádanými $x > y$. Potom $L = nsn(x^2y, xy^2) = x^2y^2$ a tudíž $S(f,g) = (x^2y^2 + 2) - (x^2y^2 + 2x^2) = -2x^2 + 2$.

Věta 2.3.8 (Buchbergerova)**.** *Buď* $G = \{g_1, \ldots, g_t\}$ *množina nenulových polynomů z* $R = \mathbb{F}[x_1, x_2, \ldots, x_n]$*. Pak* G *je Gröbnerova báze ideálu* $I = \langle g_1, \ldots, g_t \rangle$*, právě když pro každé* $i \neq j$ *platí* $S(f,g) \xrightarrow{G} 0$*.*

Využitím Buchbergerovy věty se dostáváme k Buchbergerově algoritmu, který pro množinu polynomů $\{f_1, f_2, \ldots, f_r\}$ generujících ideál I nalezne Gröbnerovu bázi tohoto ideálu.

Algoritmus 2.3.9 (Buchbergerův)**.**
VSTUP: $A = \{f_1, f_2, \ldots, f_r\} \subset \mathbb{F}[x_1, x_2, \ldots, x_n]$, kde $f_i \neq 0$.
VÝSTUP: $G = \{g_1, g_2, \ldots, g_t\}$, Gröbnerova báze ideálu $\langle f_1, f_2, \ldots, f_r \rangle$.

$G := A$;
$H := \{\{f_i, f_j\} \mid f_i, f_j \in G, f_i \neq f_j\}$;
WHILE $(H \mathrel{!}= \emptyset)$ DO
  Zvol libovolnou dvojici $\{f, g\} \in H$;
  $H := H \setminus \{f, g\}$;
  $S(f, g) \xrightarrow{G} h$; ($h$ je redukované vzhledem ke G)
  IF $(h \mathrel{!}= 0)$ THEN
    $H := H \cup \{\{u, h\} \mid u \in G\}$;
    $G := G \cup \{h\}$;
  END IF
END WHILE

Poznámka 2.3.10. Z Hilbertovy věty o bázi vyplývá, že Gröbnerova báze na výstupu Buchbergerova algoritmu je vždy konečná. Přesto ještě nemáme takovou Gröbnerovu bázi, jakou bychom potřebovali. Algoritmus není zcela deterministický, a tudíž může vypočítat pokaždé jiný výstup. Některé ideály mohou mít dokonce nekonečně mnoho Gröbnerových bází. Je tedy potřeba zavést ještě jeden termín.

Definice 2.3.11. O množině $G = \{g_1, g_2, \ldots, g_t\}$ řekneme, že je to *redukovaná Gröbnerova báze*, pokud se jedná o Gröbnerovu bázi, pro každé $i = 1, \ldots, t$ platí $lc(g_i) = 1$ a g_i je redukovaný vzhledem ke $G \setminus \{g_i\}$.

Poznámka 2.3.12. Redukovanou Gröbnerovu bázi dostaneme z libovolné Gröbnerovy báze G tím, že pro každé $g \in G$ provedeme následující:

(i) Pokud $g \xrightarrow{G\setminus\{g\}} 0$, pak g vyjmeme z G.

(ii) Pokud $g \xrightarrow{G\setminus\{g\}} g'$, pak g' nahradíme za g.

Tento postup můžeme zařadit na konec Buchbergerova algoritmu, ačkoli efektivnější je redukovat již průběžnou množinu generátorů.

Očividně se při použití redukované Gröbnerovy báze zefektivní také řešení problému náležení do ideálu.

Poslední nespornou výhodu redukované Gröbnerovy báze uvedeme v následující větě.

Věta 2.3.13. *Mějme okruh $R = \mathbb{F}[x_1, x_2, \ldots, x_n]$ a na něm přípustné uspořádání. Potom každý nenulový ideál $I \subset R$ má jednoznačnou redukovanou Gröbnerovu bázi vzhledem k tomuto uspořádání.*

Důkaz. Lze nalézt v [AdLo] [1.8.7]. ⊠

3. Nekomutativní Gröbnerovy báze

V roce 1986 přišel T. Mora [Mo86] se zobecněním Gröbnerových bází pro nekomutativní polynomiální okruhy. Výsledky této teorie se od předchozí kapitoly příliš neliší. Hlavní změnou je zde možnost existence nekonečných Gröbnerových bází. To bylo důvodem zkoumání jejich využití v kryptografii. Pokud by se ukázalo, že lze zaručit neexistence konečné Gröbnerovy báze pro nějaký ideál společně s dostatečnou obtížností hledání jakékoli nekonečné Gröbnerovy báze takového ideálu, dal by se tento fakt využít k hledání jednocestných funkcí.

Většina výsledků v následující kapitole platí pro obecnější třídy nekomutativních algeber nad libovolným tělesem, ale my budeme uvažovat $R = F\langle x_1, \ldots, x_n \rangle$ jako volnou algebru nad tělesem $\mathbb{F}$ v n nekomutujících proměnných. Další poznatky z této oblasti lze nalézt například v [Gre], nebo [Mo94]. Experimentální výsledky a optimalizace zde uvedených algoritmů jsou popsány v [Kel].

3.1 Uspořádání termů

Nejprve připomeneme význam volné algebry nad tělesem a zavedeme několik základních pojmů.

Definice 3.1.1. Mějme těleso $\mathbb{F}$ a n nekomutujících proměnných $x_1, x_2, \ldots, x_n$. *Termem*, popřípadě *slovem* rozumíme konečný součin proměnných $t = x_{\beta_1} x_{\beta_2} \cdots x_{\beta_s}$, kde $1 \leq \beta_i \leq n$. Každé slovo t je tedy definováno *délkou* $l(t) = s$, kde $0 \leq s < \infty$, a posloupností indexů $\{\beta_i\}_{i=1}^{s}$. Term délky 0 definujeme jako

1. Množinu všech termů označíme $\mathcal{B}$.

Volnou algebrou $R = \mathbb{F}\langle x_1, \ldots, x_n\rangle$ myslíme volný $\mathbb{F}$-modul s $\mathbb{F}$-bází bází $\mathcal{B}$, s jednotkovým prvkem 1 a jako násobení na množině $\mathcal{B}$ zavedeme *konkatenaci*, neboli *zřetězení*.

Každý prvek z R tedy můžeme zapsat jako $\sum_i \alpha_i \cdot t_i$, kde $\alpha_i \in \mathbb{F}$, $t_i \in \mathcal{B}$ a pouze konečně mnoho $\alpha_i \neq 0$. Řekneme, že term s *dělí* term t, pokud existují $u, v \in \mathcal{B}$ takové, že $t = usv$.

Přípustná uspořádání v nekomutativním případě se chovají podobně jako ta v komutativním případě. Je zde ale nutné vyhnout se nekonečným ostře klesajícím posloupnostem termů. Například při použití lexikografického uspořádání pro proměnné uspořádané $x_1 > x_2 > \cdots > x_n$ existuje nekonečná posloupnost $x_1 > x_2x_1 > x_2x_2x_1 > x_2x_2x_2x_1 > \cdots$. Lexikografické uspořádání není v nekomutativním případě dobré.

Definice 3.1.2 (Přípustné uspořádání termů)**.** Uspořádání $<$ na množině $\mathcal{B}$ nazveme *přípustné*, pokud pro všechny termy $t_1, t_2, t_3, t_4 \in \mathcal{B}$ splňuje následující:

(i) Platí právě jedna z relací $t_1 < t_2$, $t_1 = t_2$ nebo $t_1 > t_2$, tedy $<$ je *lineární uspořádání*.

(ii) $1 < t_1$ pro všechny $t_1 \neq 1$.

(iii) Pokud $t_1 < t_2$, pak $t_4t_1t_3 < t_4t_2t_3$.

(iv) Neexistuje nekonečná ostře klesající posloupnost $t_1 > t_2 > \cdots$ termů $t_i \in \mathcal{B}$, tedy $<$ je *dobré uspořádání*.

Toto uspořádání budeme také v textu označovat jako přípustné na množině $R = \mathbb{F}\langle x_1, x_2, \ldots, x_n\rangle$.

Pozorování 3.1.3. Pokud pro termy $t_1, t_2, t_3 \in \mathcal{B}$ platí $t_1 = t_2 t_3$, $t_1 \neq 1$ a $t_2 \neq 1$, pak $t_1 > t_2$ a $t_1 > t_3$.

Nyní uvedeme příklad dvou používaných přípustných uspořádání.

Definice 3.1.4 (LenLex - délkově lexikografické uspořádání)**.** Uspořádejme libovolně proměnné $x_1, x_2, \ldots, x_n$, například $x_1 > x_2 > \cdots > x_n$. Pro slova $t_1 = x_{\alpha_1} \cdots x_{\alpha_r}, t_2 = x_{\beta_1} \cdots x_{\beta_s} \in \mathcal{B}$ definujme $t_1 < t_2$, právě když

(i) $l(t_1) = r < s = l(t_2)$ nebo

(ii) $r = s$ a zároveň existuje $1 \leq i \leq r$, kde $x_{\alpha_j} = x_{\beta_j}$ pro $j < i$ a $x_{\alpha_i} < x_{\beta_i}$.

Definice 3.1.5 (WeightLex - váhovaně lexikografické uspořádání)**.** Uspořádejme libovolně proměnné $x_1, x_2, \ldots, x_n$, například $x_1 > x_2 > \cdots > x_n$. Dále mějme tzv. *váhový vektor* $w = (w_1, w_2, \ldots, w_n)$ nezáporných reálných čísel. Pro slova $t_1 = x_{\alpha_1} \cdots x_{\alpha_r}, t_2 = x_{\beta_1} \cdots x_{\beta_s} \in \mathcal{B}$ definujme $t_1 < t_2$, právě když

(i) $\sum_{i=1}^{r} w_{\alpha_i} < \sum_{i=1}^{s} w_{\beta_i}$ nebo

(ii) $\sum_{i=1}^{r} w_{\alpha_i} = \sum_{i=1}^{s} w_{\beta_i}$ a zároveň $t_1 < t_2$ v LenLex uspořádání.

Poznámka 3.1.6. Uspořádání LenLex je jen speciálním případem WeightLex při použití váhového vektoru $w = (1, \ldots, 1)$.

Definice 3.1.7. Buď $<$ přípustné uspořádání na $R = \mathbb{F}\langle x_1, x_2, \ldots, x_n \rangle$. Mějme množinu $A \subseteq R$ a polynom $f = c_1 t_1 + c_2 t_2 + \cdots + c_r t_r \in R$, kde $c_i \neq 0$ pro všechna $i = 1, 2, \ldots r$ a kde $t_1 > t_2 > \cdots > t_r$. Dále definujeme:

- *vedoucí term* polynomu f jako $tip(f) = t_1$,
- *vedoucí koeficient* polynomu f jako $Ctip(f) = c_1$,
- *ocas* polynomu f jako $tail(f) = f - Ctip(f) \cdot tip(f)$,

- *množinu vedoucích termů* množiny A jako $Tip(A) = \{tip(f) \mid f \in A\}$,
- $NonTip(A) = \mathcal{B} \setminus Tip(A)$,
- množinu termů z polynomu f s nenulovým koeficientem budeme značit $supp(f)$, $supp(A) = \{supp(f) \mid f \in A\}$,
- koeficient u termu t_j polynomu f budeme značit $coef_{t_j}(f) = c_j$.

Definice 3.1.8 (Ideál generovaný množinou)**.** Připomeňme že $I \subseteq R$ nazýváme *oboustranný ideál* nebo zjednodušeně *ideál*, pokud je uzavřený vzhledem ke sčítání a pokud $f \cdot g \cdot h \in I$ pro všechny $g \in I$, a všechny $f, h \in R$. Mějme $A \subseteq R$, potom *ideálem generovaným množinou* A rozumíme nejmenší ideál okruhu R, který množinu A obsahuje, a značíme jej $\langle A \rangle$. V takovém případě nazýváme A *generující množinou* $\langle A \rangle$. Pokud je A konečná množina $A = \{f_1, f_2, \ldots, f_s\}$, pak $\langle A \rangle = \langle f_1, f_2, \ldots, f_s \rangle = \left\{ \sum_{i=1}^{s} g_i f_i h_i \mid g_i, h_i \in R, i = 1, 2, \ldots, s \right\}$.

Ideál generovaný pouze prvky z $\mathcal{B}$ budeme nazývat *termový ideál*. Mějme ideál $I \subseteq R$, termový ideál generovaný množinou $Tip(I)$ budeme značit I_{TERM}.

Tvrzení 3.1.9. *Mějme oboustranný ideál I volné algebry $R = \mathbb{F}\langle x_1, \ldots, x_n \rangle$. Množina $NonTip(I)$ je bází množiny zbytkových tříd R/I, neboli platí*

$$R = I \oplus Span(NonTip(I)),$$

jako direktní součet vektorových prostorů.

Důkaz. Tvrzení bylo dokázáno v [Gre] [Theorem 2.1].

Nejprve dokážeme, že $I \cap Span(NonTip(I)) = \emptyset$. Mějme $x \in Span(NonTip(I)) \setminus \{0\}$, pak $tip(x) \in NonTip(I)$. Pokud by $x \in I$, potom by platilo také $tip(x) \in Tip(I)$, což je spor.

Dále nechť $A = \{v \in R \setminus (I \oplus Span(NonTip(I)))\}$. Díky přípustnému uspořádání existuje minimální prvek t množiny $Tip(A)$. Vezměme nějaký vektor $v \in A$, který má $tip(v) = t$.

Pokud $t \in NonTip(I)$, pak vzhledem k minimalitě v platí $tail(v) = v_i + v_n$, kde $v_i \in I$ a $v_n \in Span(NonTip(I))$. Ale protože $t \in Nontip(I)$, musí platit $v = v_i + (v_n + Ctip(v)t) \in I \oplus Span(NonTip(I))$, což je ve sporu s výběrem v.

Nyní uvažme, že $t \in Tip(I)$. Zvolme nějaký vektor $w \in I$ takový, že $tip(w) = t$. Pak $tip(v - Ctip(v)/Ctip(w) \cdot w) < tip(v)$ a z minimality v dostáváme opět $v - Ctip(v)/Ctip(w) \cdot w = v_i + v_n$ pro nějaké $v_i \in I$ a $v_n \in Span(NonTip(I))$. A stejně tak $v = (v_i + Ctip(v)/Ctip(w) \cdot w) + v_n \in I \oplus Span(NonTip(I))$ dává spor.

Tím jsme dokázali, že množina A je prázdná, a tedy platí i tvrzení. ⊠

Poznámka 3.1.10. Tedy každé nenulové $f \in R$ může být jednoznačně zapsáno jako $f = i_f + N_I(f)$, kde $i_f \in I$ a $N_I(f) \in Span(NonTip(I))$.

Definice 3.1.11. $N_I(f)$ z předchozí poznámky nazýváme *normální forma prvku f vzhledem k I*.

3.2 Redukce polynomu

Stejně jako v komutativním případě je i zde redukce polynomu součástí Buchbergerova algoritmu.

Poznámka 3.2.1. Při redukci polynomu $f \in R$ množinou $A = \{f_1, \ldots, f_k\}$ hledáme $t_1, \ldots, t_k \in \mathbb{N}$, $r \in R$, $\alpha_{ij} \in \mathbb{F}$ a $u_{ij}, v_{ij} \in \mathcal{B}$ pro $1 \leq i \leq k$ a $1 \leq j \leq t_i$ takové, že

(i) $f = \sum_{i=1}^{k} \sum_{j=1}^{t_i} \alpha_{ij} u_{ij} f_i v_{ij} + r$,

(ii) $tip(f) \geq max(tip(u_{ij} f_i v_{ij}))$ a

(iii) žádný $tip(f_i)$ nedělí žádný term ze $supp(r)$.

Polynom r je tedy zbytkem po redukci množinou A.

Algoritmus 3.2.2 (Redukce polynomu, nekomutativní verze)**.**
VSTUP: $f \in R$ a uspořádaná množina $A = \{f_1, f_2, \ldots, f_k\} \subset R$, kde $f_i \neq 0$.
VÝSTUP: t_i, u_{ij}, v_{ij} a r splňující podmínky z poznámky 3.2.1.

$t_i := 0$ pro $1 \leq i \leq k$; $r := 0$; $h := f$; $i := 1$;
WHILE $(h \; != 0)$ DO
  WHILE $(i \leq k)$ DO
    IF $(tip(h) == u \cdot tip(f_i) \cdot v)$ pro nějaké $u, v \in \mathcal{B}$ THEN
      $t_i := t_i + 1$;
      $u_{it_i} := \frac{Ctip(h)}{Ctip(f_i)} \cdot u\cdot$;
      $v_{it_i} := v$;
      $h := h - u_{it_i} \cdot f_i \cdot v_{it_i}$;
      IF $(h \; != 0)$ THEN
        $i := 1$; (h se redukoval na menší polynom, zkoušej opět od f_1)
      ELSE
        $i := k + 1$; (h se redukoval na 0, ukonči výpočet)
      END IF
    ELSE
      $i := i + 1$; (f_i nedělí $tip(h)$, zkus f_{i+1})
    END IF
  END WHILE
  IF $(h \; != 0)$ THEN
    $r := r + Ctip(h) \cdot tip(h)$;
    $h := tail(h)$; (žádné f_i nedělí $tip(h)$ zkus další term z h)

$i := 1$; (další term z h opět zkus dělit všemi $tip(f_i)$)

END IF

END WHILE

Pro představu ukážeme jednoduchý příklad nekomutativní redukce.

Příklad 3.2.3. Uvažujme *LenLex* uspořádání $<$ na $R = \mathbb{F}\langle x, y, z\rangle$, s proměnnými uspořádanými $x > y > z$. Mějme polynom $f = yxyxzz$, který budeme redukovat uspořádanou množinou $A = \{f_1 = xyz + xz, f_2 = yxzz - xxz + yzx\}$. Vedoucí termy jsou $tip(f_1) = xyz$, $tip(f_2) = yxzz$ a algoritmus pobíhá následovně.

$tip(h) = yxyxzz$ není dělitelný $tip(f_1)$, ale je dělitelný $tip(f_2)$.

$tip(h) = yx \cdot tip(f_2)$, a tedy $h = h - yx \cdot f_2 = yxxxz - yxyzx$.

$tip(h) = yxxxz$ není dělitelný $tip(f_1)$ ani $tip(f_2)$, tudíž $r = 0 + yxxxz$ a $h = -yxyzx$.

$tip(h) = -h = -y \cdot tip(f_1) \cdot x$, a tedy $h = h + y \cdot f_1 \cdot x = yxzx$.

$tip(h) = yxzx$ již nejde dělit $tip(f_1)$ ani $tip(f_2)$ a $r = r + yxzx$, $h = 0$.

Tímto algoritmus končí a dostáváme $f = -y \cdot f_1 \cdot x + yx \cdot f_2 + (yxxxz + yxzx)$.

Definice 3.2.4. Mějme uspořádanou množinu $A = \{f_1, \ldots, f_s\} \subset R$ a $f \in R$. Skutečnost, že r dostaneme redukcí f množinou A značíme zápisem $f \xrightarrow{A}_+ r$. Pokud je r navíc redukované vzhledem k A používáme značení $f \xrightarrow{A} r$.

Dále řekneme, že $A \subseteq R$ je *tip-redukovaná*, právě když $tip(f_i)$ nedělí $tip(f_j)$ pro různé $f_i, f_j \in A$.

3.3 Nekomutativní Gröbnerovy báze

Definice 3.3.1. Buď I oboustranný ideál nekomutativní volné algebry $R = \mathbb{F}\langle x_1, x_2, \ldots, x_n\rangle$ a $<$ přípustné uspořádání na R. Množinu nenulových polynomů $G \subset I$ nazveme *Gröbnerova báze ideálu I vzhledem k $<$*, právě když

pro každý nenulový polynom $f \in I$ existuje $g \in G$ a $p, q \in \mathcal{B}$ takové, že $p \cdot tip(g) \cdot q = tip(f)$. Jinými slovy, G je Gröbnerova báze ideálu I vzhledem k $<$, právě když $\langle Tip(G)\rangle = \langle Tip(I)\rangle$.

Poznámka 3.3.2. Gröbnerovy báze mají dobré využití při redukci polynomu kvůli podmínce 3.2.1 (ii). Mějme množinu generátorů $A = \{f_1, \ldots, f_r\}$ ideálu I a jeho Gröbnerovu bázi $G = \{g_i\}$. Pro každý polynom $f \in I$ umíme najít vyjádření $f = \sum_{i=1}^{k} \sum_{j=1}^{t_i} \alpha_{ij} u_{ij} g_i v_{ij}$ takové, že platí $tip(f) \geq max(tip(u_{ij} g_i v_{ij}))$. Vyjádření $f = \sum_{i=1}^{k} \sum_{j=1}^{t'_i} \alpha'_{ij} u'_{ij} f_i v'_{ij}$ splňující takovou podmínku ale vždy existovat nemusí.

Poznámka 3.3.3. Pro účely diplomové práce budeme uvažovat pouze konečně generované ideály, viz Kapitola 4. I za těchto podmínek však může být Gröbnerova báze ideálu nekonečná. V takovém případě ale vyvstává otázka, jak redukovat polynom f nekonečnou množinou $A = \{f_1, f_2, \ldots\}$, kde $tip(f_1) \leq tip(f_2) \leq \cdots$.

Pokud bude pro každý $t \in Tip(A)$ existovat jen konečně mnoho f_i takových, že $tip(f_i) = t$, lze tento problém snadno převést na redukci polynomu konečnou podmnožinou množiny A. Stačí si uvědomit, že existuje pouze konečný počet prvků $f_j \in A$, pro které platí $tip(f_j) \leq tip(f)$. Ostatní prvky množiny A není třeba brát v potaz, protože se do procesu redukce nikdy nezapojí, jak je vidět z podmínky 3.2.1 (ii). Navíc platí následující tvrzení, dokázané v [Gre].

Tvrzení 3.3.4. *Buď G Gröbnerova báze oboustranného ideálu $I \subseteq R = \mathbb{F}\langle x_1, x_2, \ldots, x_n\rangle$ vzhledem k nějakému přípustnému uspořádání $<$ a $f \in R$. Mějme konečnou $A = \{g_1, \ldots, g_k\} = \{g \in G \mid tip(g) < tip(f)\}$. Potom výsledek redukce polynomu f množinou A nezávisí na uspořádání prvků v A a platí $f \xrightarrow{A} N_I(f)$.*

Důkaz. Předpokládejme, že $f \xrightarrow{A} r$. Zřejmě žádný prvek z $Tip(G)$ nedělí žádný term polynomu r, tudíž $r \in Span(NonTip(G))$. Polynom f lze zapsat jako $f = \sum_{i=1}^{k} \sum_{j=1}^{t_i} u_{ij} f_i v_{ij} + r$ podle 3.2.1 a zároveň jako $f = i_f + N_I(f)$ podle 3.1.10. Jelikož $\sum_{i=1}^{k} \sum_{j=1}^{t_i} u_{ij} f_i v_{ij}, i_f \in I$ a $r, N_I(f) \in Span(NonTip(G))$, musí platit také $r = N_I(f)$. Nezávislost na uspořádání množiny A plyne z definice Gröbnerovy báze. ⊠

Definice 3.3.5. Nechť $f, g \in R = \mathbb{F}\langle x_1, x_2, \ldots, x_n \rangle$. Mějme termy $b, c \in \mathcal{B}$ takové, že:

(i) $tip(f) \cdot c = b \cdot tip(g)$ a

(ii) $tip(f)$ nedělí b a $tip(g)$ nedělí c.

Potom *překrytím polynomů f a g termy b a c* rozumíme

$$O(f, g, b, c) = \frac{1}{Ctip(f)} \cdot f \cdot c - \frac{1}{Ctip(g)} \cdot b \cdot g.$$

Poznámka 3.3.6. Překrytí je nekomutativní verzí S-polynomu uvedeného v sekci 2.3.6. Pro překrytí platí

$$tip(O(f, g, b, c)) < tip(f) \cdot c = tip(g) \cdot b.$$

Příklad 3.3.7. Uvažujme *LenLex* uspořádání na $<$ na $R = \mathbb{F}\langle x, y, z \rangle$, s proměnnými uspořádanými $x > y > z$. Mějme polynomy $f = xzxx + zyx$ a $g = xxyx + z$ s vedoucími termy $tip(f) = xzxx, tip(g) = xxyx$. Pak existují následující překrytí.

$O(f, g, xzx, xyx) = f \cdot xyx - xzx \cdot g = zyxxyx - xzxz,$

$O(f, g, xz, yx) = f \cdot yx - xz \cdot g = zyxyx - xzz,$

$O(g, f, xxy, zxx) = g \cdot zxx - xxy \cdot f = -xxyzyx + zzxx$ a

$O(f, f, xzx, zxx) = f \cdot zxx - xzx \cdot f = -xzxzyx + zyxzxx.$

Poznámka 3.3.8. Jak lze vidět z předešlého příkladu, pro dvojici polynomů může existovat více možných překrytí. S tím musíme počítat při konstrukci Gröbnerovy báze. V komutativním případě byla jednoznačnost zaručena použitím nejmenšího společného násobku. Navíc se můžeme setkat i s překrytím polynomu se sebou samým.

Následuje nekomutativní verze Buchbergerovy věty, která je konkrétnější formou Diamantového lemma [Berg]. Předvedeme také důkaz uvedený v [Gre], avšak v opravené verzi.

Věta 3.3.9. *Mějme $\mathbb{F}$ těleso, $R = \mathbb{F}\langle x_1, x_2, \ldots, x_n\rangle$ a $<$ přípustné uspořádání na R. Dále mějme tip-redukovanou množinu $G \subset R$ takovou, že pro každé překrytí $g_1, g_2 \in G$ platí $O(g_1, g_2, b, c) \xrightarrow{G} 0$. Potom je G Gröbnerovou bází oboustranného ideálu $\langle G\rangle$.*

Důkaz. Pro spor uvažujme, že vedoucí term nějakého $x \in \langle G\rangle$ není dělitelný žádným prvkem z $Tip(G)$. Tento polynom lze napsat ve formě

$$x = \sum_i \sum_{j=1}^{t_i} \alpha_{ij} \cdot p_{ij} \cdot g_i \cdot q_{ij},$$

pro nějaké $t_i \in \mathbb{N}$, $\alpha_{ij} \in \mathbb{F}$ a $p_{ij}, q_{ij} \in \mathcal{B}$, kde jen konečný počet $\alpha_{ij} \neq 0$. Představme si všechna taková vyjádření $\mathbb{U}$ polynomu x. Pro každé vyjádření $U \in \mathbb{U}$ definujeme $Head(U) = \max Tip(\{p_{ij} \cdot g_i \cdot q_{ij}\})$, největší term vyskytující se v sumě daného vyjádření. Označme $p^* = \min_{U\in\mathbb{U}} Head(U)$. Existence minimálního p^* plyne z vlastnosti přípustného uspořádání 3.1.2 (iv). Z množiny všech vyjádření $\mathbb{U}$ vyberme podmnožinu $\mathbb{U}' = \{U \in \mathbb{U} \mid Head(U) = p^*\}$. Z těchto vyjádření pak vyberme jedno $U^* \in \mathbb{U}'$, které má minimální velikost množiny $\{p_{ij} \cdot tip(g_i) \cdot q_{ij} \mid p_{ij} \cdot tip(g_i) \cdot q_{ij} = p^*\}$.

Jelikož není $tip(x)$ dělitelný žádným prvkem z $Tip(G)$, musí platit $tip(x) < p^*$, a tudíž se term p^* musí v sumě vyskytovat alespoň dvakrát, aby se koeficienty navzájem vynulovaly. Pro nějaké dva různé výskyty definujme i_1, i_2, j_1, j_2

takové, že

$$p^* = p_{i_1 j_1} \cdot tip(g_{i_1}) \cdot q_{i_1 j_1} = p_{i_2 j_2} \cdot tip(g_{i_2}) \cdot q_{i_2 j_2}$$

a pro zjednodušení označme

$$p = p_{i_1 j_1},\ g = g_{i_1},\ q = q_{i_1 j_1},\ p' = p_{i_2 j_2},\ g' = g'_{i_2} \text{ a } q' = q_{i_2 j_2}.$$

U těchto dvou výskytů můžou nastat následující situace:

Případ 1: $l(p) = l(p')$.

V takovém případě $tip(g)$ dělí $tip(g')$ nebo naopak, což je spor s tip-redukovaností G.

Případ 2: $l(p) \neq l(p')$, bez újmy na obecnosti předpokládejme $l(p) < l(p')$.

Pak buď $l(q) < l(q')$, nebo $l(q) \geq l(q')$.

Případ 2.1: $l(p) < l(p')$ a zároveň $l(q) < l(q')$.

Pak $tip(g)$ obsahuje $tip(g')$ jako podslovo a tudíž $tip(g')$ dělí $tip(g)$, což je opět spor s tip-redukovaností G.

Případ 2.2: zbývá pouze $l(p) < l(p')$ a zároveň $l(q) > l(q')$.

Situaci ještě rozdělíme:

Případ 2.2.1: $l(p') \geq l(p \cdot tip(g))$.

V takovém případě se $tip(g)$ a $tip(g')$ v p^* pozičně vůbec nepřekrývají. Tudíž existuje term m takový, že $p^* = p \cdot tip(g) \cdot m \cdot tip(g') \cdot q'$, a tedy $q = m \cdot tip(g') \cdot q'$ a $p' = p \cdot tip(g) \cdot m$. Označme si

$$Ctip(g) = \alpha,\ tail(g) = \sum_i \alpha_i p_i,$$
$$Ctip(g') = \beta \text{ a } tail(g') = \sum_i \beta_i p'_i.$$

Potom platí

$$\begin{aligned} p \cdot g \cdot q &= p \cdot g \cdot m \cdot tip(g') \cdot q' \\ &= p \cdot g \cdot m \cdot (g'/\beta) \cdot q' \ - \ p \cdot g \cdot m \cdot (tail(g')/\beta) \cdot q' \\ &= (\alpha/\beta) \cdot p \cdot tip(g) \cdot m \cdot g' \cdot q' \ + \ \sum_i (\alpha_i/\beta) \cdot p \cdot p_i \cdot m \cdot g' \cdot q' \end{aligned}$$

$$
\begin{aligned}
& - \sum_i (\beta_i/\beta) \cdot p \cdot g \cdot m \cdot p_i \cdot q' \\
= \; & (\alpha/\beta) \cdot p' \cdot g' \cdot q' \; + \; \sum_i (\alpha_i/\beta) \cdot p \cdot p_i \cdot m \cdot g' \cdot q' \\
& - \sum_i (\beta_i/\beta) \cdot p \cdot g \cdot m \cdot p_i \cdot q'.
\end{aligned}
$$

A tedy můžeme $p \cdot g \cdot q$ vyjádřit jako součet $p' \cdot g' \cdot q'$ a nějakých dalších termů menších než p^*. Tím získáme vyjádření polynomu x s menším počtem výskytů termu p^*, což dává spor s výběrem minimálního vyjádření U^*.

Případ 2.2.2: $l(p') < l(p \cdot tip(g))$.

Nyní existuje poziční překrytí $tip(g)$ a $tip(g')$ v p^*, řekněme $tip(g) \cdot s = r \cdot tip(g')$. Potom platí

$$p \cdot r = p',\ q = s \cdot q' \text{ a } p^* = p \cdot tip(g) \cdot s \cdot q'$$

a dostáváme

$$
\begin{aligned}
p \cdot g \cdot q \; = \; & p \cdot g \cdot q \; - \; (Ctip(g)/Ctip(g')) \cdot p' \cdot g' \cdot q' \\
& + (Ctip(g)/Ctip(g')) \cdot p' \cdot g' \cdot q' \\
= \; & Ctip(g) \cdot p \cdot (1/Ctip(g)) \cdot g \cdot s \cdot q' \\
& - Ctip(g) \cdot p \cdot (1/Ctip(g')) \cdot r \cdot g' \cdot q' \\
& + (Ctip(g)/Ctip(g')) \cdot p' \cdot g' \cdot q' \\
= \; & Ctip(g) \cdot p \cdot O(g, g', r, s) \cdot q' \; + \; (Ctip(g)/Ctip(g')) \cdot p' \cdot g' \cdot q'
\end{aligned}
$$

Podle předpokladu $O(g, g', r, s) \xrightarrow{G} 0$ a tedy musí platit

$$tip(x) \neq tip(p \cdot O(g, g', r, s) \cdot q').$$

Stejně jako v minulém případě lze snížit počet výskytů p^* ve vyjádření polynomu x, čímž opět dostáváme spor s minimalitou U^*. ⊠

Následuje nekomutativní verze Buchbergerova algoritmu, který stejně jako v minulé kapitole generuje Gröbnerovu bázi.

Algoritmus 3.3.10 (Buchbergerův, nekomutativní verze)**.**

VSTUP: Množina $A = \{f_1, f_2, \ldots, f_r\}$, kde $f_i \neq 0$ a
$\langle A \rangle = I \subset R = \mathbb{F}\langle x_1, x_2, \ldots, x_n \rangle$.

VÝSTUP: $G = \{g_1, g_2, \ldots\}$, Gröbnerova báze ideálu I.

$G := A$;
$H := \{\{f_i, f_j\} \mid f_i, f_j \in G, f_i \neq f_j\}$;
WHILE $(H \; != \emptyset)$ DO
  Zvol libovolnou dvojici $\{h_1, h_2\} \in H$;
  $H := H \setminus \{h_1, h_2\}$;
  FOR všechny překrytí $O(h_1, h_2, b, c)$ DO
    $O(h_1, h_2, b, c) \xrightarrow{G} r$; ($r$ je redukované vzhledem ke G)
    IF $(r \; != 0)$ THEN
      $H := H \cup \{\{u, r\} \mid u \in G\}$;
      $G := G \cup \{r\}$;
    END IF
  END FOR
END WHILE

Poznámka 3.3.11. U nekomutativní verze nelze brát termín „algoritmus“ doslova, protože Gröbnerova báze může obsahovat nekonečně mnoho prvků, a tedy Buchbergerův algoritmus nemusí skončit po konečně mnoha krocích. V praxi je nutné proces po určitém počtu kroků ukončit vynuceně, a tím získat pouze takzvanou *částečnou Gröbnerovu bázi*. Ve zbytku podkapitoly ukážeme postačující podmínku existence konečné Gröbnerovy báze.

B. J. Keller zkoumal v [Kel] pomocí výpočetního systému Opal různé metody optimalizací Buchbergerova algoritmu pro nekomutativní algebry. Jed-

ním z kritérií, která testoval, bylo určení přípustného uspořádání. Ačkoli z experimentů nevzešel žádný univerzální vítěz, uspořádání LenLex bylo označeno jako souhrnně nejlepší.

Mezi optimalizace patří přístup k vybírání dvojic $\{h_1, h_2\} \in H$, kdy některým dvojicím se může podle dané heuristiky dát přednost, ale výběr žádné dvojice se nesmí odsouvat donekonečna. V tomto ohledu se jeví jako nejlepší strategie výběr takové dvojice, která má nejmenší společný násobek vzhledem k LenLex uspořádání.

Dále se dá výpočet zrychlit redukcí průběžné generující množiny. Je vhodné redukovat množinu G a následně upravit i množinu dvojic H při každém přidání nového zbytku r.

Ve zbytku podkapitoly se budeme věnovat podmínce existence konečné Gröbnerovy báze. Následující tvrzení bylo dokázáno v [Gre] [Proposition 2.5]

Tvrzení 3.3.12. *Buď $<$ přípustné uspořádání na R. Dále buď $I \subsetneq R$ termový ideál, potom existuje jednoznačně určená minimální množina termů generujících I.*

Důkaz. Nechť A je množina všech nejednotkových termů z ideálu I a definujme

$$M = \{r \in A \mid \forall s \in A, (s \text{ dělí } r) \Rightarrow (s = r)\}.$$

Díky přípustnému uspořádání v A neexistuje nekonečná ostře klesající posloupnost termů, a tudíž M není prázdná.

Mějme C nějakou množinu termů generujících I. Pro každý prvek $c \in C$ existuje nějaký prvek $m \in M$, který ho dělí, protože m bude na konci nějaké ostře klesající posloupnosti navzájem se dělících prvků, která začíná termem c. Tudíž $C \subset \langle M \rangle$, a tedy i $I \subset \langle M \rangle$ a M generuje I.

Také platí, že pro každé $m \in M$ existuje nějaké $c \in C$, které ho dělí. Z definice M pak plyne, že $m = c$, a tudíž $M \subset C$. Tím jsme dokázali, že M je jedinečná minimální množina termů generujících I. ⊠

Poznámka 3.3.13. Množina M z předchozího důkazu je nezávislá na výběru přípustného uspořádání $<$ a může být nekonečná. Mějme Gröbnerovu bázi G, pak $Tip(G)$ musí obsahovat minimální množinu termů generující $\langle Tip(I)\rangle$.

Tvrzení 3.3.14. *Nechť $<$ je přípustné uspořádání na R a $I \subseteq R$ ideál takový, že $dim_{\mathbb{F}}(R/I)$ je konečná. Potom existuje konečná množina termů generující I_{TERM}.*

Důkaz. Toto tvrzení bylo dokázáno v [Gre] [Proposition 2.10].

Jak je uvedeno v 3.1.9, R/I a $Span(NonTip(I))$ jsou izomorfní jako vektorové prostory. Jelikož je $NonTip(I)$ bází $Span(NonTip(I))$, musí být konečná. Protože je R konečně generovaná, jako $\mathbb{F}$-algebra, je $\mathcal{B}$ konečně generovaná jako pologrupa. Označme si $A = \{b_1, \ldots, b_k\}$ množinu generující $\mathcal{B}$.

Mějme t prvek minimální množiny M termů generujících I_{TERM}, která podle 3.3.12 vždy existuje. Potom t lze zapsat ve tvaru $t = b_{i_1} b_{i_2} \cdots b_{i_l}$, kde $1 \leq i_l \leq k$.

Předpokládejme, že $(b_{i_2} b_{i_3} \cdots b_{i_l}) \in Tip(I)$. Protože $(b_{i_2} b_{i_3} \cdots b_{i_l}) | t$ plyne z konstrukce minimální množiny termů generujících I_{TERM} v 3.3.12, že $(b_{i_2} b_{i_3} \cdots b_{i_l}) = t$. Dostáváme tedy spor s minimalitou a musí platit $(b_{i_2} b_{i_3} \cdots b_{i_l}) \in NonTip(I)$. Term t nyní můžeme vyjádřit jako $b_{i_1} c$, kde $c \in NonTip(I)$. Tudíž je termů $t \in M$ jen konečně mnoho a množina $M \cap Tip(I)$ generuje ideál I_{TERM}, což dokazuje naše tvrzení. ⊠

Důsledek 3.3.15. Pokud má okruh zbytkových tříd R/I konečnou dimenzi nad $\mathbb{F}$, potom Gröbnerova báze ideálu I je konečná a po konečně mnoha krocích ji lze vypočítat Buchbergerovým algoritmem 3.3.10.

3.4 Nekomutativní redukované Gröbnerovy báze

Definice 3.4.1. Buď $<$ přípustné uspořádání na R a $I \subseteq R$ oboustranný ideál. Označme A minimální množinu termů generujících I_{TERM}. Potom množinu $G = \{t - N_I(t) \mid t \in A\}$ nazýváme *redukovaná Gröbnerova báze ideálu I vzhledem $k <$.*

Poznámka 3.4.2. Díky tvrzení 3.3.12 je zaručena jednoznačnost množiny A, a tedy má v nekomutativním případě redukovaná Gröbnerova báze stejný význam jako v komutativním případě:

(i) G je Gröbnerova báze ze ideálu I vzhledem k $<$.

(ii) Vedoucí koeficient každého prvku G je roven jedné.

(iii) Pro $g \in G$ platí $tail(g) \in Span(NonTip(I))$.

(iv) $Tip(G)$ je minimální množinou termů generujících I_{TERM}.

Poznámka 3.4.3. Definice 3.4.1 je konstrukční, a tedy nám dává postup, jak vypočítat redukovanou Gröbnerovu bázi ideálu I vzhledem k $<$. K tomu, abychom ji získali v konečně mnoha krocích, musí být splněny následující podmínky:

(i) K nalezení minimální množiny termů A generujících I_{TERM} potřebujeme, aby byla konečná. Předpis pro minimální množinu generátorů jsme předvedli v důkazu tvrzení 3.3.12.

(ii) Pro zjištění normální formy termu z A potřebujeme konečnou podmnožinu nějaké Gröbnerovy báze G', která ho bude redukovat. Pokud pro takovou G' platí, že pro každý term $t \in Tip(G')$ existuje jen konečně

mnoho polynomů $g_i \in G'$ takových, že $tip(g_i) = t$. Pak se redukce vždy provede v konečně mnoha krocích, vzhledem k poznámce 3.3.3.

4. Kryptosystém Polly Cracker

V roce 1993 představili M. Fellows a N. Koblitz [FeKo] asymetrický algebraický kryptosystém, který využívá kombinatorický problém k nalezení jednocestných funkcí se zadními vrátky, které pak ustanoví veřejným klíčem. Později bylo toto schéma zobecněno aplikací problému náležení do ideálu. Vznikl kryptosystém Polly Cracker, který může být upraven do podoby libovolného NP-problému tak, že jeho prolomení je stejně obtížné jako vyřešení dané instance. Například v [Kob] lze nalézt konstrukce Polly Crackeru na bázi problému 3-obarvení grafu a problému perfektního kódu na grafu. Stěžejním prvkem jsou zde právě Gröbnerovy báze, které se k řešení problému náležení do ideálu používají. Tento systém se však nikdy nedočkal náklonnosti veřejnosti, protože se ukázalo, že je těžké nalézt praktické provedení, pro které by neexistoval útok obcházející teoretickou bezpečnost. Aby předešel známým útokům, sestrojil T. Rai roku 2004 verzi Polly Crackeru [Rai] založenou na nekomutativních volných algebrách nad nějakým tělesem. V této kapitole předvedeme obě verze kryptosystému společně s jejich kryptoanalýzou a návrhem bezpečného řešení.

4.1 Komutativní Polly Cracker

Buď $\mathbb{F}$ těleso a I ideál nad $R = \mathbb{F}[x_1, \ldots, x_n]$. Mějme $G = \{g_1, \ldots, g_t\}$ Gröbnerovu bázi ideálu I. Množina G bude představovat soukromý klíč.

Za veřejný klíč vybereme množinu polynomů $Q = \{q_j\}_{j=1}^{s} \subseteq I$ takovou, že vypočítaní Gröbnerovy báze ideálu $\langle Q \rangle$ je neproveditelné (v polynomiálním čase). Prvky množiny Q mohou být voleny jako lineární kombinace prvků

z Gröbnerovy báze.

Prostor otevřených textů M je množina polynomů z R, které jsou redukované vzhledem ke G.

Při posílání zprávy $m \in M$ ji zašifrujeme tím, že k ní přičteme lineární kombinaci $r = \sum_{j=1}^{s} u_j \cdot q_j$ prvků z veřejného klíče, kde u_j jsou náhodně volené polynomy. Tím získáme šifrový text $c = m+r$. Šifrování je tedy probabilistický proces.

Dešifrování je provedeno pomocí redukce šifrované zprávy c Gröbnerovou bází G. Protože $r \in I$, platí $r \xrightarrow{G} 0$, a tedy $c \xrightarrow{G} m$. Přitom dělení šifrované zprávy množinou, která není Gröbnerova báze, může dát pro každou takovou množinu jiný výsledek. Na druhou stranu nám ke správnému dešifrování stačí získat libovolnou Gröbnerovu bázi, tudíž je nutné, aby vypočítání jakékoli Gröbnerovy báze ideálu I bylo pro útočníka nemožné.

Definice 4.1.1. Ve zkratce se tedy Polly Cracker sestává z těchto prvků:
Soukromý klíč: Gröbnerova báze $G = \{g_1, \ldots, g_t\}$ ideálu $I \in R = \mathbb{F}[x_1, \ldots, x_n]$.
Veřejný klíč: Množina vhodně zvolených polynomů $Q = \{q_j\}_{j=1}^{s} \subseteq I$.
Prostor otevřených textů: Množina polynomů $M \subset R$ taková, že pro všechny $m \in M$ platí $m \xrightarrow{G} m$.
Šifrování: $c = m + r$, kde $m \in M$ a $r = \sum_{j=1}^{s} u_j \cdot q_j$.
Dešifrování: Redukce soukromým klíčem, $c \xrightarrow{G} m$.

4.2 Kryptoanalýza komutativního Polly Crackeru

Při odhadu bezpečnosti jde o to určit, zda útočník je či není schopen vypočítat z šifrového textu a veřejného klíče otevřený text nebo soukromý klíč v dostatečně krátké době. Vzhledem k tomu, že se rychlost provedení takového útoku zpravidla vyjadřuje asymptotickým vztahem vůči parametrům systému, jako například maximálnímu stupni polynomů z veřejného klíče, je Polly Cracker chápán jako prolomený, pokud lze útok úspěšně provést v polynomiálním čase vzhledem k tomuto parametru.

Teoreticky je tento kryptosystém bezpečný, protože je ekvivalentní NP-těžkému problému náležení do ideálu, viz [Huỳ]. Přechod k praxi však ukázal, že při špatném nastavení parametrů může dojít k odkrytí informací o soukromém klíči. Stejně tak se může stát, že po neopatrném zašifrování je útočník schopen vyčíst, které monočleny patří do zprávy m a které do šifrovacího polynomu r.

Pro efektivní implementaci se počítá buď s hustými polynomy, kde se ukládají všechny koeficienty včetně nulových v určitém pořadí, nebo s řídkými polynomy, které jsou reprezentovány výčtem všech nenulových monočlenů.

Pro stručnost zde předvedeme pouze dva základní útoky použité proti Polly Crackeru. Výčet dalších technik uvedeme v podkapitole 4.4.

Útok 4.2.1 (Lineární-algebraický)**.** V případě husté reprezentace přišel D. Naccache et al. v poměrně ofenzivním článku [Nac] s návrhem *lineárního-algebraického útoku*. Vytvořil systém rovnic $c = m + \sum_{j=1}^{s} u_j \cdot q_j$, kde m a u_j jsou proměnné a při husté reprezentaci s nimi zacházíme jako s vektory koeficientů u daných termů, tudíž šifrování vnímáme jako zobrazení mezi vekto-

rovými prostory. V takovém případě je možné pomocí metod lineární algebry rovnici vyřešit v polynomiálním čase vzhledem k dimenzi vektorových prostorů, a tedy zjistit podobu otevřeného textu. Poznamenejme, že k sestrojení lineárních rovnic je potřeba znalost $supp(u_j)$. Útočník po úspěšném pokusu neodhalí nic o soukromém klíči a při příštím útoku musí vše provést znovu.

Útok 4.2.2 (Inteligentní lineární-algebraický)**.** Pokud budeme pracovat s řídkými polynomy, není metoda útoku 4.2.1 účinná. Avšak H. W. Lenstra ml. navrhl v [Kob] takzvaný *inteligentní lineární-algebraický útok*, kde využívá možnosti, že po zašifrování rozpozná některé termy polynomů u_j. Při použití řídkých polynomů je totiž málo pravděpodobné, že v sumě $\sum_{j=1}^{s} u_j \cdot q_j$ se některé termy objeví vícekrát a jejich koeficienty se sečtou, nebo dokonce vynulují. Útočník tak může takové termy odhadnout rovnou z polynomu c. Postupně pak může dokázat odvodit všechny termy ze $supp(u_j)$ a díky tomu sestrojí soustavu lineárních rovnic, kde proměnné jsou opět koeficienty jednotlivých termů ze $supp(u_j)$ a $supp(c)$. Tento útok má stejný dopad jako původní lineární-algebraický útok. Konkrétní příklad uvedeme po rozboru dopadu útoku na nekomutativní Polly Cracker ve 4.4.6.

Opatření 4.2.3. Při konstrukci kryptosystému lze sestrojit veřejný klíč tak, aby byla pravděpodobnost, že se některé termy při šifrování sečtou nebo vyruší, co nejvyšší. Stejně tak by na tento aspekt musel myslet i ten, kdo zprávu šifruje.

Objevují se ale další komplikace. Složitě provázaná množina polynomů q_j by mohla až příliš zvětšit veřejný klíč. Útočník by také mohl vztahy mezi polynomy odhalit a využít je k rychlejšímu řešení soustavy.

V článku [Nac] byla popsána ještě jedna vlastnost komutativního Polly

Crackeru. Odkrývá fakt, že problém náležení do ideálu v tomto systému není vždy stejně složitý jako nalezení Gröbnerovy báze.

Definice 4.2.4. Pro $f, f' \in R$ mějme vyjádření $nsn(lt(f), lt(f')) = \psi \cdot lt(f) = \psi' \cdot lt(f')$. Pro tyto dva polynomy definujeme

$$deg(f, f') = max\{deg(\psi \cdot f), deg(\psi' \cdot f')\}.$$

Věta 4.2.5. *Mějme přípustné uspořádání $<$ na polynomiálním okruhu $R = \mathbb{F}[x_1, \ldots, x_n]$. Dále mějme $A = \{f_1^0, \ldots, f_s^0\} \subset R$ a označme $I = \langle A \rangle$. Nechť pro polynom $h \in I$ existuje konstanta $D \in \mathbb{N}$ a vyjádření $h = \sum_{i=1}^{s} p_i f_i^0$ pro nějaké $p_i \in R$ takové, že $deg(p_i f_i^0) \leq D$ pro každé i.*

Definujme posloupnost množin $\{T^j(A)\}_j$ rekurentně,

$$T^0(A) = A \text{ a}$$
$$T^k(A) = T^{k-1}(A) \cup \{S(f, f') \mid f, f' \in T^{k-1}(A), deg(f, f') \leq D\}.$$

Pak existuje $N \in \mathbb{N}$ a polynom $f \in T^N(A)$ takový, že $lt(f)$ dělí $lt(h)$.

Důkaz. Větu dokázal A. Dickenstein et al. v článku [Dic].

Pro spor předpokládejme, že pro každé $k \geq 0$ a každé $f \in T^k(A)$ platí, že $lt(f)$ nedělí $lt(h)$. Nyní zvažme všechna vyjádření polynomu h

$$\mathbb{U} = \{\{t_i f_i\} \mid t_i \in \mathcal{B},\ k \in \mathbb{N} \text{ a } f_i \in T^k(A) \text{ (ne nutně různé) t.ž. } h = \sum_i t_i f_i\}.$$

Pro každé vyjádření $U_j \in \mathbb{U}$ definujeme

- $Head(U_j) = \max_{(t_i f_i) \in U_j}\{lt(t_i f_i)\}$,
- $J(U_j) = \{i \mid lt(t_i f_i) = Head(U_j)\}$,
- $\tau(U_j) = |J(U_j)|$ a
- $deg(U_j) = \max_{i \in J(U_j)}\{deg(t_i f_i)\}$.

Z $\mathbb{U}$ vybereme minimální vyjádření U^* podle těchto kritérií:

(i) $deg(U^*) = \min_{U_j \in \mathbb{U}}\{deg(U_j)\}$. Z předpokladů plyne, že $deg(U^*) \leq D$.

(ii) $Head(U^*) = \min\{Head(U_j) \mid U_j \in \mathbb{U},\ deg(U_j) = deg(U^*)\}$. Takové minimum existuje díky faktu z pozorování 2.1.5.

(iii) $\tau(U^*) = \min\{\tau(U_j) \mid U_j \in \mathbb{U},\ deg(U_j) = deg(U^*)$ a $Head(U_j) = Head(U^*)\}$.

Protože žádné $lt(f)$ nedělí $lt(h)$, musí být $\tau(U^*) \geq 2$, aby se koeficienty vedoucích termů navzájem vynulovaly, jinak by platilo $lt(h) = Head(U^*)$. Vezměme tedy dva indexy $i, j \in J(U^*)$, pak $nsd(t_i, t_j) = \theta$ a pro nějaké $\psi, \psi' \in \mathcal{B}$ platí $t_i = \psi\theta$ a $t_j = \psi'\theta$, a tedy

$$nsn(lt(f_i), lt(f_j)) = \psi \cdot lt(f_i) = \psi' \cdot lt(f_j) \text{ a}$$
$$\theta \cdot S(f_i, f_j) = \tfrac{1}{lc(f_i)} t_i f_i - \tfrac{1}{lc(f_j)} t_j f_j,$$

přímo z definice S-polynomu 2.3.6. Všimněme si, že $deg(\psi f_i) \leq deg(t_i f_i) \leq deg(U^*)$ a $deg(\psi' f_j) \leq deg(t_j f_j) \leq deg(U^*)$. Protože $f_i, f_j \in T^k(A)$ pro nějaké $k \geq 0$, náleží $S(f_i, f_j)$ do $T^{k+1}(A)$. Z vlastnosti S-polynomu dostáváme

$$lt(\theta \cdot S(f_i, f_j)) < lt(t_i f_i) = lt(t_j f_j).$$

Protože lze polynom $t_i f_i$ vyjádřit jako rozdíl $\frac{lc(f_i)}{lc(f_j)} t_j f_j$ a jiného polynomu s menším vedoucím termem, existuje také vyjádření U^{**} polynomu h, s vlastnostmi $deg(U^{**}) \leq deg(U^*)$, $Head(U^{**}) = Head(U^*)$ a $\tau(U^{**}) < \tau(U^*)$, což je spor s výběrem U^*. ⊠

Útok 4.2.6 (Redukce částečnou Gröbnerovou bází)**.** Posloupnost $\{T^j(A)\}_j$ z předešlé věty lze implementovat úpravou komutativního Buchbergerova algoritmu 2.3.9, když zpracujeme pouze každou dvojici $\{f, g\} \in H$, pro kterou platí $deg(f, g) \leq D$, a S-polynom této dvojice nezredukujeme množinou G.

Útok založený na větě 4.2.5 probíhá následovně. Útočník nezná konstantu D^* reprezentující maximální stupeň termu v minimálním vyjádření šifrovacího polynomu $r = \sum_{j=1}^{s} u_j \cdot q_j$ z definice 4.1.1. Proto si určí nějakou vhodně nízkou konstantu D_1 a v průběhu upraveného Buchbergerova algoritmu si nezpracované dvojice z H pamatuje. Pokud je $D_1 < D^*$, pak není zaručeno, že vedoucí term nějakého polynomu z výsledné množiny $T_1^{k_1}(A)$ dělí $lt(r)$, a tedy je možné, že šifrový text $c = m + r$ je redukovaný vzhledem k $T_1^{k_1}(A)$. V takovém případě určí útočník konstantu $D_2 > D_1$ a výpočet nechá pokračovat se stejným nastavením proměnných, jako na konci předchozího výpočtu, tedy $T_2^0(A) = T_1^{k_1}(A)$. Zvyšování konstanty opakuje, dokud se mu nepodaří pro nějaké D_j zredukovat šifrový text množinou $T_j^{k_j}(A)$ na polynom c'. Předpokládáme, že pokud $c' = m$, útočník pozná že jde o otevřený text. Jestliže $c' \neq m$, existuje pro něj opět nějaké D^* a útočník celý postup opakuje, dokud nedostane otevřený text m.

Osoba, která šifrovací polynom r konstruuje, nemůže určit jak velká je konstanta D^*. Má totiž stejné informace jako kterýkoli útočník. Může pouze simulovat stejný útok, což je pro běžnou šifrující stranu příliš náročný úkon. Tudíž můžeme říci, že osoba, která šifruje, si nemůže být jista bezpečností šifrového textu.

Na druhou stranu, pokud se útočník dostane k první úspěšné redukci $c \xrightarrow{G} c' \neq m$, nemusí redukovat šifrový text polynomem f_i z minimálního vyjádření U^*, a nový polynom c' může mít minimální vyjádření s daleko vyšší konstantou D^*. I kdyby si útočník předpočítal množinu $T^\omega(A)$ pro nějaké obrovské ω, nemusí být úspěšná redukce snazší, než výpočet úplné Gröbnerovy báze z veřejného klíče.

Další metody napadení Polly Crackeru při speciálním nastavení jeho pa-

rametrů byly popsány například v [EGS] a [HoSt]. Některé dokonce odhalují soukromý klíč. Lze je nalézt v [GeSt].

Kvůli zmíněným vadám na bezpečnosti Polly Crackeru se časem utvrdil negativní postoj kryptologické veřejnosti k vytváření systémů na principu Gröbnerových bází. Naprostá většina publikací se zabývá kryptoanalýzou.

Jsou zde však i pokusy o vylepšení stávajících návrhů, jako třeba Polly Two uveřejněný v [Ly], který odlišně pracuje s veřejným klíčem a slibuje efektivnost a odolnost vůči všem do té doby známým útokům. Výzva o prolomení jednoho šifrového textu byla pokořena v [Ste] pomocí heuristické kombinace několika druhů útoků. Již se objevily i další teoretické útoky.

Nedávno vyšel článek [CCT] zabývající se Polly Crackerem na bázi takzvaných mřížkových ideálů generovaných dvojčleny, kde se k dešifrovaní používá přesun do jiné soukromé mřížky, která není izometrická s veřejnou mřížkou. Výpočet v soukromé mřížce je snazší a zadními vrátky je v tomto případě automorfizmus z veřejné do soukromé mřížky.

Jiným směrem se vydal T. S. Rai [Rai], který se pokusil sestrojit Polly Cracker na nekomutativní volné algebře nad tělesem. Ten předvedeme v následující podkapitole.

Dále byl v [AcKr] navržen obecný kryptosystém na pravých modulech nad volnými monoidovými okruhy, který je zobecněním všech dosud zmíněných variant Polly Crackeru a dokonce i známých schémat asymetrické kryptografie, jako RSA a ElGamal. Tímto přístupem se v našem textu ale zabývat nebudeme.

4.3 Nekomutativní Polly Cracker

Tento kryptografický systém má se svým komutativním předchůdcem mnoho společného. V otázce bezpečnosti má ale jisté výhody díky obtížnějšímu výpočtu Gröbnerovy báze z veřejného klíče. Na druhou stranu je bezpečné nastavení parametrů stále nevyřešený problém a zdá se, že zaručení nekonečnosti Gröbnerovy báze je dalším aspektem, který tuto úlohu ztěžuje.

Mějme nekomutativní volnou algebru $R = \mathbb{F}\langle x_1, x_2, \ldots, x_n\rangle$ a na ní přípustné uspořádání $<$. Dále mějme oboustranný ideál $I \subset R$ s konečnou redukovanou Gröbnerovou bází $G = \{g_1, \ldots, g_t\}$. Cílem při vytváření instance nekomutativního Polly Crackeru je určit veřejný klíč $Q = \{q_1, \ldots, q_s\} \subset I$ tak, aby výpočet Gröbnerovy báze ideálu $\langle Q\rangle$ byl výpočetně nedosažitelný. V tomto případě se využívá konstrukcí, které by měly zajistit, aby měl ideál $\langle Q\rangle$ Gröbnerovu bázi nekonečnou. Dodnes navrhnuté konstrukce jsou ale postavené na hypotéze, jejíž platnost stále není prokázaná.

Definice 4.3.1 (Nekomutativní Polly Cracker)**.**
Soukromý klíč: Konečná redukovaná Gröbnerova báze $G = \{g_1, \ldots, g_t\}$ oboustranného ideálu $I \subset R = \mathbb{F}\langle x_1, \ldots, x_n\rangle$.
Veřejný klíč: Množina polynomů $Q = \{q_r \mid q_r = \sum_{i=1}^{t}\sum_{j=1}^{d_{ir}} f_{rij} g_i h_{rij}\}_{r=1}^{s}$ taková, že výpočet Gröbnerovy báze $\langle Q\rangle \subsetneq I$ je reálně neproveditelný. f_{rij} a h_{rij} zde značí vhodně vybrané monočleny.
Prostor otevřených textů: Množina polynomů $M \subseteq Span(NonTip(I))$.
Šifrování: $c = m + p$, kde $m \in M$ a $p = \sum_{i=1}^{s}\sum_{j=1}^{k_i} F_{ij} q_i H_{ij}$ pro náhodně vybrané monočleny F_{ij} a H_{ij}.
Dešifrování: Redukce soukromým klíčem, $c \xrightarrow{G} m$.

Tato definice byla prvním návrhem nekomutativní verze Polly Crackeru, který v [Rai] zveřejnil T. Rai. Ve stejné práci také navrhl, jak vybrat jednotlivé

komponenty tak, aby byly odolné vůči známým útokům na komutativní Polly Cracker. Jeho myšlenku dál rozvedl A. Helde v [Hel]. Oba postupy uvedeme v podkapitole 4.5.

4.4 Kryptoanalýza nekomutativního Polly Crackeru

Útok 4.4.1 (Lineární-algebraický)**.** Rai ve své disertační práci [Rai] tvrdí, že nekomutativní systém je oproti komutativnímu Polly Crackeru více imunní vůči základnímu lineárnímu-algebraickému útoku 4.2.1.

Uvažme šifrování $c = m + \sum_{i=1}^{s} \sum_{j=1}^{k_i} F_{ij} q_i H_{ij}$ pro nějaké monočleny F_{ij} a H_{ij}. V této rovnici neznáme F_{ij}, H_{ij} a členy polynomu m, a pokud vytvoříme soustavu rovnic k jednotlivým termům šifrového textu, budou zde figurovat jako proměnné pouze koeficienty příslušných monočlenů, stejně jako v komutativním případě. Nyní tedy pro každý term τ ze $supp(c)$ platí

$$coef_\tau(c) = coef_\tau(m) + \sum_r \delta_r \cdot \beta_r \cdot \lambda_r,$$

kde $\delta_r \cdot \beta_r \cdot \lambda_r$ značí součin koeficientů pro term τ, který se objevuje v některém ze součinů $F_{ij} q_i H_{ij}$. Protože se v součinech může term τ objevit vícekrát, píšeme na pravé straně sumu. Pokud $t \notin supp(M)$, pak zřejmě $coef_{t_l}(m) = 0$. Naopak, pokud se koeficienty na pravé straně vynulují, nepromítne se daný term do šifrového textu a nevznikne pro něj rovnice. Koeficienty β_r monočlenů z polynomů q_i jsou veřejně známé, a tudíž jsou rovnice ve vygenerované soustavě kvadratické.

Poznámka 4.4.2. Protože ale pracujeme nad komutativním tělesem, je možné stejnou soustavu rovnic dostat, pokud budeme šifrovat pomocí monočlenů

$$F'_{ij} = coef(H_{ij}) \cdot F_{ij},\ H'_{ij} = \tfrac{1}{coef(H_{ij})} H_{ij},$$

kde všechny $\lambda_r = coef(H'_{ij}) = 1$. Tak získáme soustavu lineárních rovnic a řešení má tedy stejnou složitost jako v případě Polly Crackeru nad polynomiálním okruhem.

Opatření 4.4.3. Soustavu lze vyřešit pouze pokud je počet proměnných menší než počet rovnic. Proto je při konstrukci systému rozumné pro takový útok počet proměnných dostatečně zvýšit, například zvýšením konstant k_i, avšak ne na úkor zvýšení počtu rovnic v soustavě, tedy na úkor zvýšení počtu termů v šifrovém textu. Na druhou stranu, vysokému počtu termů v šifrovém textu lze předejít výběrem monočlenů F_{ij} a H_{ij} takových, že jejich termy nejsou pro měnící se i, j příliš daleko od sebe. Pokud útočník neví, nebo nedokáže odvodit, jaké termy monočlenů F_{ij} a H_{ij} byly použité při šifrování, není ani schopen sestavit soustavu rovnic.

Útok 4.4.4 (Inteligentní lineární-algebraický)**.** Co se týče inteligentního lineárního-algebraického útoku 4.2.2, jde zde stejně jako v komutativním případě o vyčtení termů použitých ke konstrukci šifrového textu při počítání s řídkými polynomy.

Polynomy s nekomutujícími proměnnými zaručují o něco vyšší bezpečnost. Mějme term polynomiálního okruhu $r \in R = \mathbb{F}[x_1, \ldots, x_n]$ a při známém $s \in R$ chceme zjistit, jestli s dělí r a podobu t z rozkladu $st = r$. Pokud dělitelnost platí, je t určen jednoznačně.

Pro term volné algebry $r' \in R' = \mathbb{F}\langle x_1, \ldots, x_n \rangle$ a známé $s' \in R'$ je ale situace komplikovanější. Pokud s' dělí r', pak hledáme dva termy $u, v \in R'$ takové, že $r' = us'v$ a s' se navíc může v r' vyskytovat jako podslovo hned několikrát. Pravděpodobnost více výskytů se zvyšuje s větším rozdílem délek $len(r')$ a $len(s')$, naopak s vetším počtem proměnných se snižuje. Z pohledu útočníka je tedy problém určení rozkladu, který byl v součinu fakticky použit,

složitější.

Opatření 4.4.5. Proti nekomutativní verzi útoku platí stejná opatření jako v komutativním případě. Můžeme mu předejít, pokud se dostatečný počet termů v sumě $\sum_{i=1}^{s}\sum_{j=1}^{k_i} F_{ij}q_iH_{ij}$ objeví vícekrát, což při generování soustavy rovnic sníží jejich počet, ale zachová stejný počet proměnných. Lze nahlédnout, že tomuto požadavku vyhovuje konstrukce, při které jsou polynomy q_i stejné, až na koeficienty. Navíc se vyplatí mít stejné až na koeficienty i monočleny F_{ij} a H_{ij} pro každé i. Jejich termy nejsou veřejně známe, a i pokud je útočník odvodí, dostane soustavu rovnic, kde každý koeficient nějakého termu šifrového textu je součtem alespoň s proměnných. Konkrétní návrh systému odolnému vůči těmto útokům uvedeme v podkapitole 4.5.

Příklad 4.4.6. Pro ilustraci sestrojíme jednoduchý příklad veřejného klíče s šifrováním zprávy a pokusíme se o předvedení inteligentního lineárního-algebraického útoku.

Buď $<$ přípustné uspořádání $LenLex$ na $R = \mathbb{F}\langle x, y\rangle$ a bez ohledu na soukromý klíč mějme veřejný klíč

$$q_i = \sum_{l=1}^{3} \beta_{il}t_l = \beta_{i1}xyyx + \beta_{i2}yxx + \beta_{i3}y, \text{ pro } i = 1, 2.$$

Řekněme, že chceme šifrovat zprávu

$$m = \sum_{i=1}^{4} \mu_i r_i = \mu_1 xxxyxyy + \mu_2 xyxxxx + \mu_3 xyyxy + \mu_4 yxxy.$$

A pro šifrování zvolíme náhodně

$$\begin{aligned} F_{11} &= \delta_{11}xxy & H_{11} &= \lambda_{11}x, \\ F_{12} &= \delta_{12}x & H_{12} &= \lambda_{12}xx, \\ F_{21} &= \delta_{21}yx & H_{21} &= \lambda_{21}yx, \\ F_{22} &= \delta_{22} & H_{22} &= \lambda_{22}y. \end{aligned}$$

Pro zkrácení zápisu označíme součin koeficientů novou proměnnou

$$\rho_{lij} = \delta_{ij}\beta_{il}\lambda_{ij}, \text{ pro } i,j = 1,2 \text{ a } l = 1,2,3.$$

Šifrový text tedy bude vypadat následovně

$$\begin{aligned} c &= m + \sum_{i=1}^{2}\sum_{j=1}^{2} F_{ij}q_iH_{ij} \\ &= \rho_{111}xxyxyyyx + \rho_{121}yxxyyyxy + \mu_1xxxyxyy + \\ &\quad (\rho_{112}+\rho_{211})xxyyxxx + \rho_{221}yxyxxyx + (\rho_{212}+\mu_2)xyxxxx + \\ &\quad \rho_{311}xxyyx + (\rho_{122}+\mu_3)xyyxy + \rho_{321}yxyyx + \rho_{312}xyxx + \\ &\quad (\rho_{222}+\mu_4)yxxy + \rho_{322}yy, \end{aligned}$$

přičemž útočník vidí jen výsledné součty koeficientů $c = \sum_{i=1}^{12}\epsilon_i s_i$. Předpokládejme, že náhodné zvolení koeficientů nezpůsobilo žádné vynulování ve výsledném součtu, to je také velice pravděpodobné.

Nyní se postavme do role útočníka a pokusme se zprávu dešifrovat. Předně si všimněme vedoucího monočlenu $\epsilon_1 s_1$, který - pokud nedošlo k vynulování termů větších než s_1 - musí být součtem nějakých násobků vedoucích monočlenů $F_{ij}(\beta_{i1}t_1)H_{ij}$. Vidíme, že $t_1 = xyyx$ skutečně dělí $s_1 = xxyxyyxx$, a to jediným možným způsobem. Zároveň můžeme vzhledem k poznámce 4.4.2 uvažovat všechny monočleny H_{ij} monické, což nám dává $F'_{i1} = \varphi_{i1}xxy$, $H'_{i1} = x$. Nyní je potřeba pomocí koeficientů zjistit, jaké q_i tyto monočleny ve skutečnosti násobily.

Pokud označíme $\varphi_{11} = \epsilon_1/\beta_{11}$, vidíme, že koeficient $\varphi_{11}\beta_{12} = \rho_{211}$ se u termu $xxy\cdot t_2\cdot x$ v c nevyskytuje, ale koeficient $\varphi_{11}\beta_{13} = \rho_{311}$ u termu $xxy\cdot t_3\cdot x$ ano. Pro φ_{21}, ale nenajdeme žádný výskyt, a tudíž pravděpodobně vznikl term s_1 pouze násobením $F'_{11}q_1H'_{11}$. To nám umožňuje od šifrového textu tři monočleny odečíst a dvou se tak zbavíme úplně.

Kdybychom museli zvážit možnost, že $\epsilon_1 s_1$ je skutečně součtem více násobků $F'_{ij}(\beta_{il}t_l)H'_{ij}$, museli bychom do systému rovnic přidat novou, která by

tento vztah vyjadřovala.

Další v pořadí je monočlen $\epsilon_2 s_2$, také dělitelný termem t_1. Zde se stejným postupem dostaneme k monočlenům $F'_{i2} = \varphi_{i2} yx, H'_{i2} = xx$ a při naprosté shodě výskytu koeficientů můžeme předpokládat, že $\epsilon_2 s_2 = F'_{22} q_2 H'_{22}$. Odečtením nám tak ubudou další tři monočleny.

Třetí monočlen $\epsilon_3 s_3$ není dělitelný t_1 ani t_2. Buďto by musel vzniknout jako zbytek po vynulování vyšších monočlenů, což je dosti nepravděpodobné, nebo se může jednat o monočlen otevřeného textu. Zkusíme tedy $\mu_1 r_1 = \epsilon_3 s_3$.

Podobným postupem se můžeme dostat až k odkrytí celého otevřeného textu. Jak je vidět, každá úvaha vytváří další možnosti a pokud se jednou cestou nedostaneme ke kýženému výsledku, můžeme zvolit další nejpravděpodobnější variantu. Vysokou roli zde hraje jakási heuristika, ohodnocující jednotlivé cesty, proto tedy *inteligentní útok*. Pokud se v průběhu útoku rozhodneme počítat s tím, že některé monočleny vznikly součtem více monočlenů při šifrování, zbude nám navíc na konci soustava rovnic, kterou je ještě třeba řešit, což dává význam označení *lineární-algebraický útok*.

Kdybychom zavedli opatření 4.4.5 a při šifrování se rozhodli, že monočleny F_{ij} a H_{ij} budou mít s měnícím se i stále stejné termy a pouze různé koeficienty, dostali bychom ve výsledku každý koeficient ϵ_l z c jako součet minimálně tolika koeficientů, kolik je polynomů ve veřejném klíči. Žádný koeficient by tak nebylo možné odhadnout přímo z šifrového textu.

Útok 4.4.7 (Na soukromý klíč)**.** Další hrozbu představuje získání soukromého klíče přímo výpočtem z veřejného klíče. Takové odhalení by mělo za následek trvalé zlomení systému a přístup ke všem otevřeným textům, které jím byly zašifrovány.

Opatření 4.4.8. Proti útoku na veřejný klíč lze systém chránit tím, že na-

stavíme parametry d_{ir} různé a dostatečně vysoké.

Naopak, pokud ke konstrukci veřejného klíče použijeme monické polynomy f_{rij}, h_{rij}, tedy polynomy s vedoucími koeficienty rovnými jedné, a pokud bude útočník znát jejich formu, lze tento útok provést snáze. Vzniká totiž větší pravděpodobnost, že z termů výsledných polynomů $q_r = \sum_{i=1}^{t} \sum_{j=1}^{d_{ir}} f_{rij} g_i h_{rij}$, které se v sumě objeví pouze jednou lze přímo odvodit koeficienty soukromého klíče.

V některých případech může stačit jen nalezení částečné Gröbnerovy báze ideálu $\langle q_i \rangle$, která vznikne předčasným ukončením Buchbergerova algoritmu 3.3.10. Po redukci šifrového textu jakoukoli dosažitelnou částečnou Gröbnerovou bází by útočník neměl získat otevřený text.

V podkapitole věnující se kryptoanalýze komutativního Polly Crackeru jsme uvedli větu 4.2.5, která dokazovala, že problém náležení do ideálu nemusí být vždy stejně obtížný, jako vypočítání Gröbnerovy báze. Věta zahrnovala návrh konstrukce částečné Gröbnerovy báze, která obsahuje alespoň jeden polynom, jehož vedoucí term dělí vedoucí term polynomu, u kterého problém náležení do ideálu řešíme.

V nekomutativním prostředí je nutné znění věty 4.2.5 upravit. Bohužel se nám nepodařilo její platnost prokázat ani vyvrátit, a tudíž ji zde uvedeme pouze jako hypotézu.

Definice 4.4.9. Nechť pro $f, f' \in R$ existuje překrytí $O(f, f', b, c)$, pak definujeme $deg(f, f', b, c) = max\{l(f \cdot c), l(b \cdot f')\}$.

Hypotéza 4.4.10. Mějme přípustné uspořádání $<$ na volné algebře $R = \mathbb{F}\langle x_1, \ldots, x_n \rangle$. Dále mějme $A = \{f_1^0, \ldots, f_s^0\} \subset R$ a označme $I = \langle A \rangle$. Nechť pro polynom $h \in I$ existuje konstanta $D \in \mathbb{N}$ a vyjádření $h = \sum_{i=1}^{s} p_i f_i^0 q_i$ pro nějaké $p_i, q_i \in R$ takové, že $deg(p_i f_i^0 q_i) \leq D$ pro každé i.

Definujme posloupnost množin $\{T^j(A)\}_j$ rekurentně, $T^0(A) = A$ a $T^k(A) = T^{k-1}(A) \cup \{O(f, f', b, c) \mid f, f' \in T^{k-1}(A), b, c \in \mathcal{B}, deg(f, f', b, c) \leq D\}$. Pak existuje $N \in \mathbb{N}$ a polynom $f \in T^N(A)$ takový, že $tip(f)$ dělí $tip(h)$.

Pozorování 4.4.11. Hlavní změnou oproti komutativnímu případu je zde použití překrytí dvou polynomů namísto S-polynomu při generování systému množin $T^i(A)$. Zatímco S-polynom je díky nejmenšímu společnému násobku určen jednoznačně pro každou dvojici polynomů, překrytí může mezi dvěma polynomy existovat více.

Navíc by bylo vhodné uvážit i jiné verze předešlé hypotézy. Do množiny $T^i(A)$ bychom mohli zařadit kromě překrytí i oboustranné překrytí pro dvojici dělících se polynomů. Tedy, pokud bychom měli $tip(f) = b \cdot tip(f') \cdot c$ pro nějaké $f, f' \in T^{k-1}(A)$ a $b, c \in \mathcal{B}$, kde $max\{l(f), l(bf'c)\} < D$, zařadili bychom do množiny $T^k(A)$ i polynom $f - bf'c$.

Hlavní úskalí při sledování důkazu věty 4.2.5 představoval fakt, že pro minimální vyjádření U^* polynomu h může pro každou dvojici indexů $i, j \in J(U^*)$ platit $tip(p_i f_i q_i) = tip(p_j f_j q_j)$ aniž by pro polynomy f_i a f_j existovalo nějaké překrytí, například v případě $l(p_i) \geq l(p_j f_j)$. Pak bychom nemohli dojít ke sporu pomocí získání ještě menšího vyjádření polynomu h.

Útok 4.4.12 (Redukce částečnou Gröbnerovou bází)**.** Pokud by se podařilo prokázat platnost hypotézy 4.4.10, znamenalo by to, že s mírnou úpravou Buchbergerova algoritmu 3.3.10, by bylo možné pokusit se dešifrovat posílanou zprávu pomocí částečné Gröbnerovy báze, stejně jako v útoku 4.2.6. My však doufáme, že v nekomutativním případě útok tak snadný nebude a Polly Cracker z definice 4.3.1 bude oproti původnímu návrhu i v tomto ohledu zaručovat o něco vyšší míru zabezpečení.

Pokud by měl útočník kromě znalosti veřejného klíče a prostoru otevřených textů také k dispozici dešifrovací černou skříňku, mohl by ji využít k odhalení soukromého klíče. Dešifrovací černou skříňkou myslíme nástroj, který pro šifrový text vrátí příslušný otevřený text, ale nelze zjistit, jak výpočet probíhá a co k němu černá skříňka používá. Následující metoda útoku byla navrhnuta v [Bul].

Útok 4.4.13 (Chosen-cyphertext)**.** Mějme instanci nekomutativního Polly Crackeru, kde soukromým klíčem je konečná redukovaná Gröbnerova báze $G = \{g_1, \ldots, g_t\}$. Pokud jsou všechny $tip(g_i)$ veřejně známé, nebo je lze vypočítat z veřejného klíče, stačí útočníkovi sestrojit falešné šifrové texty

$$C_i = \sum_{i=1}^{s} \sum_{j=1}^{k_i} F_{ij} q_i H_{ij} + tip(g_i).$$

Poté je nechá dešifrovat černou skříňkou. Platí $C_i \xrightarrow{G}_+ tip(g_i)$, a protože je G redukovaná Gröbnerova báze, platí také $tip(g_i) \xrightarrow{G} \frac{tail(g_i)}{Ctip(g_i)}$, kde navíc $Ctip(g_i) = 1$. Získá tedy množinu $G' = \{g'_i \mid g'_i = tip(g_i) + tail(g_i)\} = G$.

Útok 4.4.14 (Modifikace útoku chosen-cyphertext)**.** Jak je uvedeno v [RaBu], není nutné znát $Tip(G)$, pokud je známé přípustné uspořádání použité v kryptosystému. Můžeme totiž určit term $T = max(Tip(Q)) \in \langle Tip(G) \rangle$. Při dešifrování všech termů $p \leq T$ dostaneme množinu $G' = \{g'_p = p - N_{\langle G \rangle}(p)\} \subseteq \langle G \rangle$. Protože ale $Tip(G) \subseteq Tip(G')$, platí $\langle G \rangle = \langle G' \rangle$ a G' je také Gröbnerovou bází množiny $\langle G \rangle$.

Opatření 4.4.15. Ačkoli je dopad tohoto útoku pro kryptosystém fatální, opatření proti němu je celkem jednoduché, jak bylo také poznamenáno v [RaBu]. Jediné co je nutné upravit, je prostor otevřených textů. Zmenšeme M tak, aby $NonTip(G) \setminus M \neq \emptyset$ a pro každé $i = 1, \ldots, t$ existoval term $b_i \in NonTip(G) \setminus M$ takový, že $b_i \in supp(g_i)$ a že $u \cdot b_i \cdot v \notin M$ pro žádné

$u, v \in \mathcal{B}$. Pokud by se po dešifrování ukázalo, že otevřený text nebyl prvkem M, dešifrovací černá skříňka by místo výsledku vrátila chybovou hlášku.

Praktické provedení tohoto opatření by ale opět muselo být promyšlené tak, aby se z množiny M nedaly získat žádné informace o G.

4.5 Návrhy bezpečných konstrukcí

Jak jsme slíbili, v této podkapitole předvedeme návrhy nekomutativního Polly Crackeru, které mají šanci obstát před stále se rozvíjející kryptoanalýzou. Nejdříve ale uvedeme pár poznatků, které k těmto návrhům vedou.

Studiem konečně generovaných oboustranných ideálu s nekonečnou Gröbnerovou bází se zabývali například E. Green, T. Mora a V. Ufnarovski v [GMU]. V minulosti se v oblasti algebry důkazům neexistence konečné Gröbnerovy báze pro nějaký ideál ale nevěnovalo příliš pozornosti. Spíše se toto odvětví zabývalo podmínkami existence konečné Gröbnerovy báze pro nějaký ideál. Ve spojitosti s kryptografií začal hledat T. Rai různé vzory množin generátorů ideálů s nekonečnou Gröbnerovou bází. Využil přitom *Opal*, výpočetní systém vytvořený pro počítání nekomutativních Gröbnerových bází, napsaný v jazyku C++. Jeho výsledky naleznete v [Rai] stejně jako zhodnocení bezpečnosti jejich využití při konstrukci Polly Crackeru.

Ukázalo se, že vhodným soukromým klíčem pro efektivní generování veřejného klíče a pro dešifrování je jednoprvková množina, tedy polynom, pro jehož vedoucí term neexistuje žádné překrytí se sebou samým.

Ve své práci T. Rai také vznesl hypotézu, která sice nemá pevné algebraické podklady, ale je postavena na pozorování nedostatků do té doby objevených ideálů s nekonečnou Gröbnerovou bází.

Hypotéza 4.5.1. Buď $R = \mathbb{F}\langle x, \ldots, x_n \rangle$ nekomutativní volná algebra nad

tělesem, kde $n \geq 2$. Dále buď $A = \{f_1, \ldots, f_r\}$ konečná podmnožina R, jejíž všechny prvky mají stejný vedoucí term T délky $l(T) = \alpha > 4$. Nechť počet všech termů ze $supp(A)$ délky $(\alpha - 1)$ je roven N a předpokládejme:

(i) $N \approx 2r$,

(ii) $N \approx \frac{1}{3}n^{\alpha-1}$ a

(iii) $N < \frac{1}{2}n^{\alpha-1}$.

Potom je velmi pravděpodobné, že redukovaná Gröbnerova báze ideálu $\langle A \rangle$ je nekonečná.

Poznámka 4.5.2. Dodáme jen, že $n^{\alpha-1}$ je počet všech termů délky $(\alpha - 1)$, tudíž zhruba jedna třetina všech takových termů se objevuje někde v polynomech f_i. Navíc je jejich počet dvakrát větší než počet samotných polynomů f_i a mohou se vyskytovat i ve více polynomech. To nám zaručuje (alespoň hypoteticky) vysokou pravděpodobnost toho, že po vytvoření tip-redukované množiny A' z množiny A budou vedoucí termy zhruba délky $(\alpha - 1)$. Počet překrytí v množině A' tedy bude pravděpodobně také vysoký. Podmínka (iii) nám má na druhou stranu zaručit, že takových termů nebude příliš mnoho na to, aby se překrytí zredukovala na nulu.

Příklad 4.5.3. Mějme přípustné uspořádání $LenLex$ na $R = \mathbb{F}_{389}\langle x, y \rangle$, kde $x > y$. Dále mějme množinu $A = \{f_1, f_2, f_3\}$, kde všechny tři polynomy jsou tvaru

$$\begin{aligned} f_i \ &= xxxxy + a_{i1}xxyyx + a_{i2}xyxyy + a_{i3}yyyxx + \\ &\quad a_{i4}xyxx + a_{i5}xyxy + a_{i6}yxxy + a_{i7}yxyx + a_{i8}yxyy + a_{i9}yyxx + h_i, \end{aligned}$$

kde $a_{ij} \in \mathbb{F}_{389}$ a h_i jsou polynomy se stejnými termy délky nejvýše 3, ale různými koeficienty z $\mathbb{F}_{389}$.

V našem případě je $n = 2, T = xxxxy, \alpha = l(T) = 5, r = 3$ a $N = 6$. Množina A vyhovuje podmínkám hypotézy 4.5.1, neboť $N = 2r, N \approx \frac{1}{3}n^{\alpha-1} = 5$ a $N < \frac{1}{2}n^{\alpha-1} = 8$. Pokud označíme A' množinu vzniklou tip-redukcí množiny A, dostaneme $Tip(A') = \{xxxxy, xxyyx, xyxyy\}$.

Na základě předchozí hypotézy a účinných opatření proti známým útokům navrhl A. Helde ve své disertační práci [Hel] instanci nekomutativního Polly Crackeru. Ten je speciálním případem systému z definice 4.3.1.

Definice 4.5.4 (Heldeho návrh bezpečného systému)**.**
Soukromý klíč: Náhodný polynom $g \in R = \mathbb{F}\langle x_1, \ldots, x_n\rangle$, jehož vedoucí term nemá žádné překrytí se sebou samým.

Veřejný klíč: Množina polynomů $Q = \{q_r\}_{r=1}^{s}$ splňující podmínky hypotézy 4.5.1. Polynomy q_r mají všechny stejné termy, liší se pouze v koeficientech.

Prostor otevřených textů: Množina polynomů $M \subsetneq Span(NonTip(\langle g\rangle))$ vybraná tak, aby alespoň jeden term polynomu g ležel ve $Span(NonTip(\langle g\rangle)) \setminus M$.

Šifrování: Vyberme náhodně množinu termů $\{u_j\}_{j=1}^{2k}$ tak, že $u_{2i-1} \cdot u_{2i} \neq u_{2j-1} \cdot u_{2j}$ pro všechny $1 \leq i \neq j \leq k$. Dále zajistíme, aby $tip(q_i) = T \leq max_{1\leq j\leq k}(u_{2j-1} \cdot u_{2j})$.

Nyní pro každé $1 \leq i \leq s$ vybereme náhodně množinu koeficientů $\{a_{ij}\}_{j=1}^{2k}$ a nastavíme $\{F_{ij}, H_{ij}\}_{j=1}^{k} = \{a_{i(2j-1)}u_{2j-1}, a_{i(2j)}u_{2j}\}_{j=1}^{k}$.

Šifrový text je $c = m + p$, kde $m \in M$ a $p = \sum_{i=1}^{s}\sum_{j=1}^{k} F_{ij}q_iH_{ij}$. Je důležité, aby p obsahoval dostatečný počet termů z množiny M.

Dešifrování: Redukce soukromým klíčem, $c \xrightarrow{g} m$. Pokud po redukci obdržíme prvek ze $Span(NonTip(\langle g \rangle)) \setminus M$, vrátí systém chybovou hlášku.

Poznámka 4.5.5. Ačkoli je tento kryptosystém navrhnut tak, aby vyhovoval bezpečnostním požadavkům v podkapitole 4.4, je zde stále několik bodů, které potřebují prošetřit. Pro hypotézu 4.5.1 dosud není prokazatelně zaručena dostatečná pravděpodobnost existence nekonečné redukované Gröbnerovy báze ideálu $\langle Q \rangle$. Metoda šifrování, kdy $T \leq max_{1 \leq j \leq k}(u_{2j-1} \cdot u_{2j})$, je také založena pouze na experimentálním pozorování.

5. Závěr

Práce popisuje základní poznatky z teorie Gröbnerových bází v prostředí polynomiálních okruhů. Redukce polynomu množinou jiných polynomů je proces, u nějž nelze vždy očekávat stejný výsledek, vzhledem k uspořádání dané množiny. Gröbnerovy báze ale mají tu vlastnost, že vždy ke stejnému výsledku spějí, a navíc umožňují řešit NP-těžký problém náležení do ideálu, který samy generují. Pro libovolný ideál polynomiálního okruhu existuje konečná Gröbnerova báze a navíc ke každému ideálu existuje jednoznačně určená minimální takzvaná redukovaná Gröbnerova báze.

Složitost problému nalezení Gröbnerovy báze se kryptografové snažili využít k sestrojení jednocestných funkcí použitých v kryptosystému Polly Cracker. Ukázalo se ale, že v některých případech lze zprávu dešifrovat i bez nalezení úplné Gröbnerovy báze ideálu, a byla navrhnuta řada různorodých útoků, které bezpečnost schématu prolomily.

Zatímco se veřejnost stavěla k šancím na úspěch Polly Crackeru negativně, pokoušeli se někteří přijít s návrhem podobného systému, který by však byl díky vlastnostem jiného prostředí imunní vůči známým útokům. Jedním z pokusů byla adaptace totožného schématu na bázi nekomutativní teorie volných algeber nad tělesy, ve které na rozdíl od komutativního případu existují ideály s nekonečnou redukovanou Gröbnerovou bází. Tento fakt prakticky znemožňuje výpočet celé Gröbnerovy báze a snižuje pravděpodobnost, že výpočet částečné Gröbnerovy báze bude stačit pro úspěšné dešifrování.

V podkapitole 4.4 jsme prošetřili účinnost známých útoků na nekomutativní verzi Polly Crackeru a předvedli jsme případná opatření, která by systém měla před útoky chránit. V poslední části 4.5 byla tato opatření shrnuta společně s doporučenou metodou pro hledání ideálů s nekonečnou redu-

kovanou Gröbnerovou bází a ve výsledku tak dala vzniknout finálnímu návrhu instance Polly Crackeru, který by mohl být předmětem dalšího zkoumání.

Literatura

[AcKr] *Ackermann P. a Kreuzer M.:* **Gröbner Basis Cryptosystems,** Universität Dortmund, Německo, 2005.

[AdLo] *Adams W. a Loustaunau P.:* **An Introduction to Gröbner Bases,** Amer. Math. Soc., Providence, 1994.

[Berg] *Bergman G.:* **The diamond lemma for ring theory,** Adv. Math. 29, 1978, str. 178-218

[BeWe] *Becker T. a Weispfenning V.:* **Gröbner Basis: A Computational Approach to Commutative Algebra,** Springer-Verlag, New York, 1993.

[Buch] *Buchberger B.:* **Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal,** Disertační práce, University of Innsbruck, Německo, 1965.

[Bul] *Bulygin S.:* **Chosen-ciphertext attack on noncommutative Polly Cracker,** http://arxiv.org/abs/cs/0508015, 2008.

[CCT] *Caboara M., Caruso F. a Traverso C.:* **Lattice Polly Cracker cryptosystems,** Journal of Symbolic Computation 46, 2011, str. 534 - 549.

[CLOs] *Cox D., Little J. a O'Shea D.:* **Ideals, varieties and algorithms: an introduction to computational algebraic geometry and commutative algebra, 2nd ed,** Springer, 1997.

[Dic] *Dickenstein A., Fitchas N., Giusti M. a Sessa C.:* **The membership problem for unmixed polynomial ideals is solvable in single exponential time,** Discrete Applied Mathematics 33, 1991, str. 73 - 94.

[DiHe] *Diffie W. a Hellman M.:* **New Directions in Cryptography,** IEEE Trans. Info. Theory 22, 1976, str. 644 - 654.

[EGS] *Endsuleit R., Geiselmann W. a Steinwandt R.:* **Attacking a polynomial-based cryptosystem: Polly Cracker,** Int. Jour. Information Security 1, 2002, str. 143 - 148.

[FeKo] *Fellows M. a Koblitz N.:* **Combinatorial cryptosystems galore!,** Contemporary Math. 168, 1994, str. 51 - 61.

[GMU] *Green E., Mora T., Ufnarovski V.:* **The non-commutative Gröbner freaks,** Progress in Comp. Sci. and App. Logic, 15, Basel, 1998.

[Gre] *Green E.:* **Noncommutative Gröbner bases, and projective resolutions,** Basel, 1999.

[GeSt] *Geiselmann W. a Steinwandt R.:* **Cryptanalysis of Polly Cracker,** IEEE Trans. Information Theory 48, 2002, str. 2990 - 2991.

[GoMi] *Goldwasser S. a Micali S.:* **Probabilistic encryption** & **how to play mental poker keeping secret all partial information,** Proc. 14th annual ACM symp. on Theory of computing, 1982, str. 365 - 377.

[HoSt] *Hofheinz D., a Steinwandt R.:* **A "Differential" Attack on Polly Cracker,** IEEE Int. Symp. Information Theory, 2002, str. 211.

[Hel] *Helde A.:* **Noncommutative Gröbner bases in Polly Cracker cryptosystems,** Disertační práce, NTNU, Norsko, 2009.

[Huỳ] *Huỳnh D.:* **A superexpoential lower bound for Gröner bases and Church-Rosser commutative Thue systems,** Inform Control 68, 196–206, 1986.

[Kel] *Keller B.:* **Algorithms and Orders for Finding Noncommutative Gröbner Bases,** Disertační práce, VPI & SU, USA, 1997.

[Kob] *Koblitz N.:* **Algebraic aspects of cryptography,** Springer, New York, 1998.

[Ly] *Le Van Ly:* **Polly Two — A Public Key Cryptosystem based on Polly Cracker,** Disertační práce, Bochum, 2002.

[Jev] *Jevons W. S.:* **The Principles of Science: A Treatise on Logic and Scientific Method,** Macmillan & Co., London, 1874, str. 141.

[Mo86] *Mora T.:* **Groebner Bases for Non-Commutative Polynomial Rings,** Springer-Verlag, London, Velká Británie, 1986.

[Mo94] *Mora T.:* **An introduction to commutative and non-commutative Gröbner bases,** Theoretical Computer Science 134, 1994, str. 131 - 173.

[Nac] *Barkee b., Deh Cac Can, Ecks J., Moriarty T., Ree R.F:* **Why you cannot even hope to use Gröbner bases in public-key cryptography? An open letter to a scientist who failed and a challenge to those who have not yet failed,** Journal of Symbolic Computations (18), 1994.

[RaBu] *Rai T. S. a Bulygin S.:* **Noncommutative Polly Cracker-type cryptosystems and chosen-ciphertext security,** http://eprint.iacr.org/2005/344, 2008.

[Rai] *Rai T. S.:* **Infinite Gröbner Bases And Noncommutative Polly Cracker Cryptosystems,** Disertační práce, Virginia Polytechnic Institute and State University, 2004.

[Ste] *Steinwandt R.:* **A ciphertext-only attack on Polly Two,** Journal Applicable Algebra in Engineering, Communication and Computing 21, Springer, 2010.