KAUNO TECHNOLOGIJOS UNIVERSITETAS

MATEMATIKOS IR GAMTOS MOKSLŲ FAKULTETAS

TAIKOMOSIOS MATEMATIKOS KATEDRA

Vytautas Jakutis

VEILIO GRIOBNERIO BAZIŲ KRIPTOSISTEMŲ KRIPTANALIZĖ

Magistro darbas

Vadovas
prof. dr. E. Sakalauskas

KAUNAS, 2014

KAUNO TECHNOLOGIJOS UNIVERSITETAS

MATEMATIKOS IR GAMTOS MOKSLŲ FAKULTETAS

TAIKOMOSIOS MATEMATIKOS KATEDRA

TVIRTINU
Katedros vedėjas
doc. dr. N. Listopadskis

2014 06 02

VEILIO GRIOBNERIO BAZIŲ KRIPTOSISTEMŲ KRIPTANALIZĖ

Taikomosios matematikos magistro baigiamasis darbas

Vadovas
(parašas) prof. dr. E. Sakalauskas
2014 06 01

Recenzentas
(parašas) doc. dr. A. Aleksa
2014 06 01

Atliko
FMMM 2 gr. stud.
(parašas) V. Jakutis
2014 05 30

KAUNAS, 2014

KVALIFIKACINĖ KOMISIJA

Pirmininkas: Juozas Augutis, profesorius (VDU)

Sekretorius: Eimutis Valakevičius, profesorius (KTU)

Nariai: Jonas Valantinas, profesorius (KTU)

Vytautas Janilionis, docentas (KTU)

Vidmantas Pekarskas, profesorius (KTU)

Zenonas Navickas, profesorius (KTU)

Arūnas Barauskas, dr., direktoriaus pavaduotojas (UAB „Danet Baltic“)

Jakutis V. Veilio Griobnerio bazių kriptosistemų kriptanalizė: Taikomosios matematikos magistro darbas / vadovas prof. dr. E. Sakalauskas; Taikomosios matematikos katedra, Matematikos ir gamtos mokslų fakultetas, Kauno technologijos universitetas. – Kaunas, 2014. – 24 p.

SANTRAUKA

2011 m. paskelbta Veilio Griobnerio bazių kriptosistema yra naujas nekomutatyvus Griobnerio bazių kriptosistemų variantas, kurio kriptanalizė dar nebuvo atlikta. Darbe pateikiamas kriptanalizės metodas taiko Veilio algebrų reprezentaciją, sudaro matricines lygtis ir įvertina jų skaičių. Veilio algebros indeksui esant n lygčių skaičius yra $O(const^n)$.

Jakutis V. Cryptanalysis of Weyl Gröbner Basis Cryptosystems : Master's work in applied mathematics / supervisor dr. prof. E. Sakalauskas; Department of Applied mathematics, Faculty of Mathematics and Natural Sciences, Kaunas University of Technology. – Kaunas, 2014. – 24 p.

SUMMARY

Weyl Gröbner Basis Cryptosystem, published in 2011, is a new noncommutative Gröbner basis cryptosystem variant with no cryptanalysis yet performed. The method, presented in this Master's work, applies Weyl algebra representation, constructs matrix equations and estimates their count. Weyl algebra index being n the equation count is $O(const^n)$.

TURINYS

ALGORITMŲ SĄRAŠAS

1. ĮVADAS

Šio darbo tikslas yra pateikti Veilio Griobnerio bazių kriptosistemos (ALI; KREUZER, 2012) (WGBC) užšifravimo operacijos lygtį matricine forma ir panagrinėti išskleistų lygčių skaičius.

Šiomis dienomis, 20 metų po polinominio laiko (angl. polynomial time, SIPSER, 2006) faktorizavimo algoritmas kvantiniams kompiuteriams (SHOR, 1997) paskelbimo, kvantinių kompiuterių grėsmė yra labai karšta tema kriptografijos pasaulyje. Yra didžiulis poreikis kurti kvantines kriptosistemas, kurios išliktų saugios, kai kvantiniai kompiuteriai būtų įgyvendinti. Tokios kriptosistemos yra vadinamos post-kvantinėmis. Pirmaujančių kriptosistemų tipai (BERNSTEIN; BUCHMANN, 2009) yra santraukos funkcijomis paremti parašai, kodais paremtos kriptosistemos, gardelėmis paremtos kriptosistemos ir kelių kintamųjų kriptosistemos. Veilio Griobnerio bazių kriptosistema (WGBC) (ALI, 2011) yra nauja algebrinė kelių kintamųjų viešojo rakto kriptosistema, paremta Veilio algebrų idealų Griobnerio bazių skaičiavimo sudėtingumu. Ji priklauso Griobnerio bazių kriptosistemų tipui, kuris apibrėžtas (ACKERMANN; KREUZER, 2006).

Darbe siekiamu tikslu atrasti būdą WGBC kriptosistemos užšifravimo operaciją užrašyti matricine forma tikimasi atrasti supaprastintą uždavinio variantą, kurio sudėtingumas būtų mažesnis. Bus glaustai pateikiamos abstrakčios algebros ir Griobnerio bazių teorijos bei viena Veilio algebros reprezentacija.

2. TEORIJOS APŽVALGA

2.1. ALGEBRINĖS STRUKTŪROS

2.1.1. Grupių teorija

Struktūra, kurią sudaro aibė G ir operacija $\cdot : G \times G \to G$, yra vadinama *monoidu* G, jeigu ji tenkina šias savybes:

- $\forall g, h, i \in G : g \cdot (h \cdot i) = (g \cdot h) \cdot i$;
- $\exists e \in G : \forall g \in G : e \cdot g = g \cdot e = g$, čia e - vadinamas *neutraliuoju* elementu.

Funkcija $f : G \to G'$ yra vadinama *monoidų G ir G' homomorfizmu f*, jeigu G ir G' yra monoidai ir $\forall g, h \in G : f(g \cdot h) = f(g) \cdot f(h)$ ir $f(e_G) = e_{G'}$. Visų monoidų G ir G' homomorfizmų aibę žymėsime $\mathrm{Hom}(M, M')$.

Monoidas G yra vadinamas *Abelio grupe G*, jeigu jis tenkina šias savybes:

- $\forall g \in G : \exists g^{-1} \in G : g \cdot g^{-1} = g^{-1} \cdot g = e$;
- $\forall g, h \in G : g \cdot h = g \cdot h$.

2.1.2. Žiedų teorija

Struktūra, kurią sudaro aibė R, operacija $\cdot : R \times R \to R$, vadinama daugyba, ir operacija $+ : R \times R \to R$, vadinama sudėtimi, yra vadinama *žiedu R*, jeigu ji tenkina šias savybes:

- struktūra iš R ir $+$ yra Abelio grupė, kurios neutralusis elementas vadinamas nuliu ir žymimas $\mathbf{0}$;
- struktūra iš R ir $\cdot$ yra monoidas, kurio neutralusis elementas vadinamas vienetu ir žymimas $\mathbf{1}$;
- $\forall r \in R : \mathbf{0} \cdot r = r \cdot \mathbf{0} = \mathbf{0}$;
- $\forall r, s, t \in R : r \cdot (s + t) = r \cdot s + r \cdot t$ ir $(s + t) \cdot r = s \cdot r + t \cdot r$.

Tarkime turime žiedus R ir R'. Funkcija $f : R \to R'$ yra vadinama *žiedų R ir R' homomorfizmu f*, jeigu ji tenkina šias savybes:

- f yra monoidų homomorfizmas, čia monoidai yra R ir R' ir jų operacijos yra atitinkamų žiedų sudėties operacija;
- f yra monoidų homomorfizmas, čia monoidai yra R ir R' ir jų operacijos yra atitinkamų žiedų daugybos operacija.

Visų žiedų R ir R' homomorfizmų aibę žymėsime $\mathrm{Hom}(R, R')$.

Žiedo R *charakteristika*, žymima $\mathrm{char}(R)$, vadinsime mažiausią natūralųjį skaičių n, tokį, kad $\underbrace{\mathbf{1} + \cdots + \mathbf{1}}_{n\text{kartų}} = \mathbf{0}$. Jeigu toks n neegzistuoja, tai charakteristika bus 0.

Abelio grupė I yra vadinama *žiedo R kairiniu idealu I*, jeigu ji tenkina šias savybes:

- $I \subseteq R$;
- Abelio grupės I operacija yra žiedo R sudėtis;
- $\forall r \in R : \forall g \in I : r \cdot g \in I$.

Abelio grupė I yra vadinama *žiedo R dešininiu idealu I*, jeigu ji tenkina šias savybes:

- $I \subseteq R$;
- Abelio grupės I operacija yra žiedo R sudėtis;
- $\forall r \in R : \forall g \in I : g \cdot r \in I$.

Abelio grupė I yra vadinama *žiedo R idealu I*, jeigu ji yra žiedo R kairinis idealas I ir žiedo R dešininis idealas I.

Žiedo R idealą I vadinsime sugeneruotu aibės X (žymėsime $I = (X)$), jeigu I yra mažiausias R idealas, kuriam $X \subseteq I$.

Žiedas R yra vadinamas *komutatyviu žiedu R*, jeigu $\forall r, s \in R : r \cdot s = s \cdot r$.

Žiedas R yra vadinamas *lauku R*, jeigu struktūra iš $R \backslash \{0\}$ ir $\cdot$ yra Abelio grupė.

2.1.3. Modulių teorija

Struktūra, kurią sudaro Abelio grupė M (kurios operacija žymima $+$), žiedas R ir operacija $f : R \times M \to M$, vadinama skaliarine daugyba, yra vadinamas *kairiniu moduliu M virš R* (arba tiesiog moduliu), jeigu $\forall r, s \in R : \forall m, n \in M : f(r + s, m) = f(r, m) + f(s, m)$ ir $f(r \cdot s, m) = f(r, s \cdot m)$ ir $f(r, m+n) = f(r, m) + f(r, n)$. Skaliarinės daugybos operaciją rašysime sutrumpintai, pvz. jeigu $r \in R$ ir $m \in M$, tai $f(r, m)$ rašysime tiesiog rm.

Tarkime turime modulius M ir M' virš R. Funkcija $f : M \to M'$ yra vadinama *modulių M ir M' homomorfizmu f virš R*, jeigu ji tenkina šias savybes:

- f yra monoidų M ir M' homomorfizmas, čia monoidų operacijos yra atitinkamų modulių sudėties operacija;
- $\forall r \in R : \forall m \in M : f(rm) = rf(m)$.

Visų modulių M ir M' homomorfizmų virš R aibę žymėsime $\mathrm{Hom}_R(M, M')$.

Modulis M virš R yra vadinamas *vektorine erdve M virš R*, jeigu R yra laukas ir skaliarinei daugybai f galioja teiginys $\forall u \in M : \mathbf{1}u = u$.

Poaibis $S \subseteq M$ yra vadinamas *modulio M virš R generatorių aibe*, jeigu visi $m \in M$ gali būti užrašomi per kokius nors $s_1, \ldots, s_n \in S$ ir $r_1, \ldots, r_n \in R$: $m = r_1 s_1 + \cdots + r_n s_n$.

Tarkime turime modulį M virš R. Poaibis $S \subseteq M$ yra vadinamas *tiesiškai priklausomu virš R*, jeigu egzistuoja tokie skirtingi $s_1, \ldots, s_n \in S$ ir tokie $r_1, \ldots, r_n \in R$, kurie nevisi yra lygūs $\mathbf{0}$, kad $r_1 s_1 + \cdots + r_n s_n = 0$. Jeigu S nėra tiesiškai priklausomas virš R, tai jis vadinamas *tiesiškai nepriklausomu virš R*.

Poaibis $S \subseteq M$ yra vadinamas *modulio M baze virš R*, jeigu S yra M generatorių aibė ir S yra tiesiškai nepriklausomas virš R.

Modulis M virš R yra vadinamas *laisvuoju moduliu M virš R*, jeigu jis turi bazę.

Tarkime turime laisvąjį modulį A virš R, jo bazę S ir formalių simbolių aibę $X = \{x_i\}_{i=1}^{n}$. Jeigu visi S elementai yra X konkatenacijos (įskaitant tuščią konkatenaciją ϵ) - jeigu visiems $s \neq \epsilon \in S$ egzistuoja tokia aibė $\{i_j | 1 \leq j \text{ ir } 1 \leq i_j \leq n\}$, kad $s = x_{i_1} x_{i_2} \dots$ - tai X elementus vadinsime sudaromosiomis, laisvąjį modulį A virš R vadinsime *laisvuoju moduliu M virš R su sudaromosiomis X* ir žymėsime $A = R\langle X \rangle = R\langle x_1, \dots, x_n \rangle$.

Konkatenacijoje šalia parašytas vienodas sudaromąsias sutrumpintai laipsnine forma, pvz. $x_1 x_1 = x_1^2$ arba $x_1 x_1 x_3 = x_1^2 x_2^0 x_3$. Laisvųjų modulių elementus vadinsime *daugianariais*. Atskiras daugianario išraiškos $r_1 m_1 + \dots + r_n m_n$ dalis vadinsime taip:

- r_i - *koeficientai*;
- m_i - *nariai*;
- koeficientas ir narys užrašytas kartu $r_i m_i$ - *vienanaris*.

Tarkime turime laisvąjį modulį $M = R\langle X \rangle$ ir poaibį $F \subseteq M$. Laisvasis modulis $\overline{M}$, kurio elementų išraiškos po kiekvienos operacijos yra pertvarkomos taikant lygtis $\forall f \in F : f = e$ taip, kad sutvarkyta (vadinama *standartine*) forma naudotų nurodytą bazę, yra vadinamas *laisvuoju moduliu $\overline{M}$ virš R su sudaromosiomis X ir apribojimais F* ir žymimas $\overline{M} = R\langle X \rangle / (F)$.

2.1.4. Algebrų teorija

Struktūra, kurią sudaro žiedas A, žiedas R ir operacija $f : R \times A \to A$, vadinama skaliarine daugyba, yra vadinamas *kairine algebra A virš R* (arba tiesiog algebra), jeigu $\forall r, s \in R : \forall a, b \in A :$ $f(r + s, a) = f(r, a) + f(s, a)$ ir $f(r \cdot s, a) = f(r, s \cdot a)$ ir $f(r, a + b) = f(r, a) + f(r, b)$. Skaliarinės daugybos operaciją rašysime sutrumpintai, pvz. jeigu $r \in R$ ir $a \in A$, tai $f(r, a)$ rašysime tiesiog ra.

Algebra A virš R yra vadinama *laisvąja algebra A virš R*, jeigu modulis A virš R yra laisvasis ir žiedo A operacija $\cdot : A \times A \to A$ yra distributyvi daugyba bazės elementus konkatenuojant - turint A bazę S, visiems $a \in A$, išreikštiems per $\{a_i\}_{i=0}^{n} \subseteq S$, ir visiems $b \in A$, išreikštiems per $\{b_i\}_{i=0}^{m} \subseteq S$, daugyba yra $a \cdot b = (r_1 a_1 + \dots + r_n a_n) \cdot (s_1 b_1 + \dots + s_m b_m) = (r_1 a_1 b_1 + \dots + r_n a_n b_1) + \dots + (r_1 a_1 b_m + \dots + r_n a_n b_m)$, čia $\{r_i\}_{i=0}^{n} \subseteq R$, $\{s_i\}_{i=0}^{m} \subseteq R$ ir $\{a_i b_j | 1 \leq i \leq n \text{ ir } 1 \leq j \leq m\} \subseteq S$.

Tarkime turime laisvąją algebrą $A = R\langle X \rangle$ ir poaibį $F \subseteq A$ ($\forall f \in F : f \neq \mathbf{0}$). Laisvoji algebra $\overline{A}$, kurios elementų aibė yra sudaryta A elementų išraiškas perrašius naudojant lygtis $\forall f \in F : f = \mathbf{0}$, yra vadinamas *laisvąja algebra $\overline{A}$ virš R su sudaromosiomis X ir apribojimais F* ir žymimas $\overline{M} = R\langle X \rangle / (F)$.

Laisvoji algebra $A_n(R) = R\langle x_1, \dots, x_n, \partial_1, \dots, \partial_n \rangle / (\{[x_i, x_j], [\partial_i, \partial_j], [x_i, \partial_j] - \partial_{ij} | i, j \in \{1, \dots, n\}\})$, kur $n \in \mathbb{N}$, $[a, b] = ab - ba$ ir $\partial_{ij} = \mathbf{1}$, kai $i = j$, $\mathbf{0}$ - kitu atveju, yra vadinama *n-tąja Veilio algebra*. n yra vadinamas Veilio algebros indeksu. $A_n(R)$ bazė yra sudaryta iš tokios formos

elementų: $x_1^{i_1} \cdots x_n^{i_n} \partial_1^{i_{n+1}} \cdots \partial_n^{i_{2n}}$. Vektorių i vadinsime *laipsnių vektoriumi*. Vektoriaus i elementų sumą vadinsime *daugianario laipsniu*.

Pavyzdžiui, 1-oji Veilio algebra $A_1(R)$ yra $R\langle x_1, \partial_1 \rangle / (x_1\partial_1 - \partial_1 x_1 - \mathbf{1})$.

Laisvąją algebrą $R\langle x_1, \dots, x_n \rangle / (\{x_i x_j - x_j x_i | i, j \in \{1, \dots, n\}\})$ žymėsime $R[x_1, \dots, x_n]$ (arba tiesiog $R[X]$) ir kartais vadinsime *daugianarių žiedu*. $R[X]$ bazė yra sudaryta iš tokios formos elementų: $x_1^{i_1} \cdots x_n^{i_n} = X^i$. Vektorių i vadinsime *laipsnių vektoriumi*. Vektoriaus i elementų sumą vadinsime *daugianario laipsniu*.

Tarkime turime algebras A ir A' virš R. Funkcija $f : A \to A'$ yra vadinama *algebrų A ir A' homomorfizmu f virš R*, jeigu ji tenkina šias savybes:

- f yra žiedų A ir A' homomorfizmas;
- $\forall r \in R : \forall a \in A : f(ra) = rf(a)$.

Visų algebrų A ir A' homomorfizmų virš R aibę žymėsime $\mathrm{Hom}_R(A, A')$.

Algebra $\mathrm{Hom}_R(M, M')$ virš R yra vadinama modulių M ir M' homomorfizmų virš R algebra $\mathrm{Hom}_R(M, M')$, jeigu ji tenkina šias savybes:

- sudėtis yra $(f, g) \to (m \to f(m) + g(m))$;
- daugyba yra $(f, g) \to (m \to f(g(m)))$;
- skaliarinė daugyba yra $(r, f) \to (m \to rm)$.

2.1.5. Reprezentacijų teorija

Algebrų A ir $\mathrm{Hom}_R(M, M)$ homomorfizmas $\rho : A \to \mathrm{Hom}_R(M, M)$ virš R yra vadinamas A *reprezentacija į M*, jeigu R yra komutatyvus žiedas.

Reprezentacija ρ vadinama *tikra reprezentacija* (angl. faithful reprezentation), jeigu funkcija ρ yra injektyvi.

2.2. GRIOBNERIO BAZĖS

Šiame skyriuje k žymėsime kokį nors žiedą ir $k[X]$ - ne daugianarių žiedą, o tokią laisvąją algebrą virš k su sudaromosiomis X ir tokiais apribojimais, kad $k[X]$ bazę galime išreikšti kaip $U = \{X^\alpha | \alpha \in \mathbb{Z}_{\geq 0}^n\}$.

Sakysime, kad tvarka σ *gerai sutvarko* (DASGUPTA, 2014, p. 22) aibę A, jeigu:

a) σ visiškai sutvarko (angl. total order) aibę A;
b) kiekvienas netuščias poaibis $B \subseteq A$ turi didžiausią elementą $a \in A$.

Tarkime turime aibę $\mathbb{Z}_{\geq 0} = \{z | z \in \mathbb{Z} \text{ ir } z \geq 0\}$ ir $k[X]$ bazę $U = \{X^\alpha | \alpha \in \mathbb{Z}_{\geq 0}^n\}$. *Narių tvarka σ* yra tvarka, tenkinanti savybes:

a) tvarka σ gerai sutvarko aibę U;
b) $\forall \alpha, \beta, \sigma \in \mathbb{Z}^n_{\geq 0} : X^\alpha >_\sigma X^\beta \quad X^{\alpha+\sigma} >_\sigma X^{\beta+\sigma}$.

Tarkime turime funkciją $\log$, kuri grąžina duoto nario laipsnių vektorių α, ir funkciją $\deg(\alpha) = \alpha_1 + \cdots + \alpha_n$.

Sakome, kad daugianaris f dalija daugianarį g, jeigu visi vektoriaus $\log(g) - \log(f)$ elementai yra neneigiami.

Sakome, kad daugianaris f yra daugianario g dalybos iš daugianario h rezultatas, jeigu $\log(f) = \log(g) - \log(h)$.

Sakome, kad narių tvarka $\sigma = DegRevLex$, jeigu visiems nariams u_1 ir u_2 galioja teiginys: $u_1 >_{DegRevLex} u_2$ tada ir tik tada, kai $\deg(\log(u_1)) > \deg(\log(u_2))$ arba $\deg(\log(u_1)) = \deg(\log(u_2))$ ir laipsnių vektoriaus $\log(u_1) - \log(u_2)$ paskutinė nenulinė koordinatė yra neigiama.

Tarkime $k[X] = \{f | f = \sum_{\alpha \in \mathbb{Z}^n_{\geq 0}} a_\alpha X^\alpha$ ir $f \neq \mathbf{0}\}$. Tada apibrėžiame tokias funkcijas:

- daugialaipsnis : $k[X] \to \mathbb{Z}^n_{\geq 0}$ grąžina daugianario f didžiausio (pagal narių tvarką σ) nario laipsnių vektorių α, su kuriuo $a_\alpha \neq \mathbf{0}$;
- PK : $k[X] \to k$ yra $\text{PK}(f) = a_{\text{daugialaipsnis}(f)}$ (pirmasis koeficientas);
- PN : $k[X] \to U$ yra $\text{PN}(f) = X^{\text{daugialaipsnis}(f)}$ (pirmasis narys);
- PV : $k[X] \to k[X]$ yra $\text{PV}(f) = \text{PK}(f) \cdot \text{PN}(f)$ (pirmasis vienanaris).

Tarkime turime poaibį $F = \{f_1, \ldots, f_s\} \subset k[X]$. Kiekvienas $f \in k[X]$ gali būti užrašytas tokia forma:

$$f = a_1 f_1 + \cdots + a_s f_s + r, \tag{2.1}$$

kur $a_i, r \in k[X]$, ir r yra lygus $\mathbf{0}$ arba r yra daugianaris, kurio nė vienio nario su nenuliniu koeficientu nedalija nė vienas iš aibės $\{\text{PV}(f_1), \ldots, \text{PV}(f_s)\}$ elementų. Tokia daugianario f išraiška yra vadinama *normaliąja forma*. r yra vadinamas *liekana*. Normaliosios formos ieškojimas dar yra vadinamas *dalyba* arba *redukcija*.

Taip pat, jeigu f normaliosios formos liekana r sutampa su f, sakysime, kad f yra neredukuojamas pagal F.

1 algoritmas. Normalioji forma

1: **procedūra** NF($f_1, \dots, f_s, f$)
2: **visiems** i nuo 1 iki s **kartoti**
3: $a_i \leftarrow \mathbf{0}$
4: $r \leftarrow \mathbf{0}$
5: $p \leftarrow f$
6: **kol** $p \neq \mathbf{0}$ **kartoti**
7: $i \leftarrow 1$
8: dalybaįvyko $\leftarrow$ ne
9: **kol** $i \leq s$ & dalybaįvyko $=$ ne **kartoti**
10: **jei** PV(f_i) dalija p **tada**
11: $a_i \leftarrow a_i + \text{PV}(p)/\text{PV}(f_i)$
12: $p \leftarrow p - (\text{PV}(p)/\text{PV}(f_i))f_i$
13: dalybaįvyko $\leftarrow$ taip
14: **kitu atveju**
15: $i \leftarrow i + 1$
16: **jei** dalybaįvyko $=$ ne **tada**
17: $r \leftarrow r + \text{PV}(p)$
18: $p \leftarrow p - \text{PV}(p)$
19: **grąžinti** $a_1, \dots, a_s, r$

Pastebėkime, kad duoto daugianario f skirtingų normaliųjų formų pagal aibę F gali būti ir daugiau nei viena. Tačiau egzistuoja ir tokia ypatinga aibė, vadinama Griobnerio baze, kuri generuoja tokį patį idealą, kaip ir F, tačiau duoda tik unikalias normaliąsias formas. Daugianarių aibę G vadinsime *Griobnerio baze* tada ir tik tada kai visų idealo, kurį generuoja G, daugianarių normaliųjų formų liekana r yra 0. Iš visos daugybės ekvivalenčių Griobnerio bazės apibrėžimų, pastarasis yra vienas paprasčiausių.

Griobnerio bazė G vadinama *redukuota Griobnerio baze*, jei ji tenkina šias savybes:

a) $\forall g \in G : PK(g) = \mathbf{1}$;
b) visiems $g \in G$: nė vienas g narys nepriklauso idealui, kurį generuoja $G \backslash \{g\}$ pirmųjų vienanarių aibė.

Naudinga žinoti Hilberto bazės teoremą - visiems $k[X]$ (čia k yra Noether žiedas - kurio visi netušti idealų poaibiai turi didžiausią idealą) idealams egzistuoja baigtinė generuojančių daugianarių aibė, jeigu visi žiedo k idealai turi baigtinę generuojančių elementų aibę. Taip pat kiekvienas $k[X]$ idealas turi po unikalią redukuotą Griobnerio bazę.

Tarkime turime Griobnerio bazę G, kuri generuoja tą patį idealą, kaip ir F. Pats pirmasis funkcijos GriobnerioBazė : $F \to G$ skaičiavimo algoritmas yra *Buchbergerio algoritmas* (BUCHBERGER, 1965). Galima manyti, kad Buchbergerio algoritmas apibendrina kelių kintamųjų netiesinį Euklido algoritmą DBD skaičiavimui, Gauso eliminavimo algoritmą ir net Simplekso algoritmą.

2.3. KELIŲ KINTAMŲJŲ VIEŠOJO RAKTO KRIPTOGRAFIJA

Funkcija $f : X \to Y$ yra vadinama *vienkrypte* (ROBSHAW, 2011a), jeigu visiems $x \in X$ funkcijos $f(x)$ skaičiavimo algoritmo sudėtingumo klasė yra priskiriama įveikiamoms (pvz. P), tačiau praktiškai visiems $y \in Y$ bent vieno x, tokio, kad $f(x) = y$, suradimo (f skaičiavimo atvirkštine kryptimi) algoritmo sudėtingumo klasė yra priskiriama neįveikiamoms (pvz. EXPTIME).

Vienkryptė funkcija f, kurios skaičiavimo atvirkštine kryptimi algoritmo sudėtingumo klasė tampa priskiriama įveikiamoms pridėjus kokią nors papildomą informaciją (liuką), yra vadinama *vienkrypte funkcija su liuku* (ROBSHAW, 2011b).

Viešojo rakto kriptosistema (angl. public-key cryptosystem), dar vadinama asimetrine kriptosistema (angl. asymmetric cryptosystem), yra tokia, kurioje skirtingoms operacijoms naudojami skirtingi raktai ir vienas iš raktų gali būti paviešinamas nepažeidžiant kito rakto slaptumo (KALISKI, 2011).

Tarkime M yra tekstogramų aibė, C - šifrogramų aibė ir k_v - paviešintas raktas. Tada operaciją, kuri naudoja k_v vadinsime *užšifravimo* funkcija ir žymėsime $\mathcal{P} : M \to C$.

Viešojo rakto kriptosistema yra vadinama *saugia*, jeigu užšifravimo funkcija $\mathcal{P}$ yra vienkryptė funkcija su liuku. Liukas šiuo atveju yra nepaviešintas raktas k_p ir $\mathcal{P}$ skaičiavimo atvirkštine kryptimi naudojant k_p funkcija yra vadinama iššifravimo funkcija.

Kelių kintamųjų viešojo rakto kriptosistema yra viešojo rakto kriptosistema, kurioje $\mathcal{P}$ išraiška yra sudaryta iš m daugianarių, kurių skaliarai yra iš baigtinio lauko F, laipsnis yra d ir kuriuos sudaro n kintamųjų, lygčių (GOUBIN; PATARIN; YANG, 2011).

2.3.1. Komutatyvi Griobnerio bazės viešojo rakto kriptosistema (CGBC)

Ši kriptosistema sukurta 2006 m. (ACKERMANN; KREUZER, 2006).

Tarkime turime $k[X]$ idealą I ir narių tvarką σ. Privatusis raktas bus idealo Griobnerio bazė $G = \{g_1, \dots, g_s\}$. Viešasis raktas yra baigtinė aibė $Q = \{p_1, \dots, p_s\}$, čia $p_i \in I$ yra parinkti atsitiktinai, taip, kad idealo, kurį generuoja Q, Griobnerio bazės suradimo uždavinys būtų neįveikiamas. Prieš šifrogramos sudarymą yra sudaroma aibė $H = \{h_1, \dots, h_s\}$, čia $h_i \in k[X]$ yra parinkti atsitiktinai. Žinučių aibė M yra pagal G neredukuojamų daugianarių poaibis. Užšifravimas atliekamas iš tekstogramos $m \in M$ suskaičiuojant šifrogramą $c = \sum_{i=1}^{s} h_i p_i + m$. Iššifruojant tekstograma c bus lygi daugianario c normaliosios formos pagal aibę G liekanai r.

CGBC pasiduoda daugeliui atakų, pavyzdžiui paprastajai tiesinės algebros atakai, protingajai tie-

sinės algebros atakai, dalinei Griobnerio bazės atakai ar pasirinktos šifrogramos atakai.

2.3.2. Polly Cracker kriptosistema (PCC)

PCC, sukurta 1994 m. (FELLOWS; KOBLITZ, 1994), yra istoriškai įdomus atskiras CGBC atvejis. Dabar paaiškinsime, kaip veikia PCC. Tarkime K yra baigtinis laukas su p^e elementų; čia p - pirminis skaičius ir $e \in \mathbb{N}$. Šifravimo schema veikia komutatyviame n kintamųjų daugianarių virš lauko K žiede P. Viešasis raktas $Q = \{p_1, \dots, p_s\}$ yra nustatomas parenkant privatųjį raktą, tašką $(a_1, \dots, a_n) \in K^n$, taip, kad $\forall i = 1, \dots, s : p_i(a_1, \dots, a_n) = 0$; čia $p_i \in P$. Žinutės $m \in K$ šifravimui pasirenkame atsitiktinius daugianarius $h_1, \dots, h_s \in P$ ir suskaičiuojame užšifruotą žinutę $c = h_1p_1 + \cdots + h_sp_s + m$; čia $c \in P$. Tada iššifravimas yra padaromas apskaičiuojant c su privačiuoju raktu.

Įvairių PCC variantų kriptanalizė yra atlikta sėkmingai. Pagrindinė PCC silpnybė yra, kad privatusis raktas yra taškas K^n aibėje ir iššifravimas atliekamas apskaičiuojant daugianarį tame taške.

2.3.3. Apibendrinta Griobnerio bazės viešojo rakto kriptosistema (GBC)

Nors ir CGBC atrodo labai pažeidžiama, Ackermann ir Kreuzer šaltinyjeACKERMANN; KREUZER, 2006 yra apibrėžę abstraktesnę Griobnerio bazių kriptosistemą (GBC), kurių atskiri atvejai yra garsios kriptosistemos RSA, ElGamal, Polly Cracker, Polly 2, nekomutatyvusis Polly Cracker variantas. Tai reiškia, kad sudaryti saugią GBC kriptosistemą yra įmanoma. Taip pat kurti GBC kriptosistemas motyvuoja faktas, kad yra tokių nekomutatyvių daugianarių žiedų virš baigtinių laukų idealų, kurių Griobnerio bazės yra begalinės.

PCC buvo apibendrintas iki komutatyvios Griobnerio bazių kriptosistemos (trumpinsime CGBC), kurioje atraminis sunkus uždavinys - daugianarių sistemos sprendimas - buvo pakeistas sunkiu idealų komutatyviuose daugianarių žieduose Griobnerio bazių apskaičiavimo uždaviniu.

Konkrečiau, CGBC atveju, privatusis raktas yra idealo $I \subset P$ Griobnerio bazė $G = \{g_1, \dots, g_s\}$ kartu su kokia nors narių tvarka σ. Viešasis raktas yra baigtinė seka Q iš I, sukonstruota parenkant atsitiktinius daugianarius $p_1, \dots, p_s$ iš idealo I. Žinutės yra daugianariai, kurie yra redukuoti privačiojo rakto G atžvilgiu. Žinutės m siuntimui yra pasirenkami atsitiktiniai daugianariai $h_1, \dots, h_s$ ir suskaičiuojama užšifruota žinutė $c = h_1p_1 + \cdots + h_sp_s + m$. Originali žinutė m tada gali būti atkurta redukuojant c privačiojo rakto G atžvilgiu. Vėl teoriškai CGBC saugumas remiasi ant sudėtingos Griobnerio bazių skaičiavimo problemos. Tačiau praktiškai tikrai saugios CGBC konkrečios sistemos konstravimas yra netrivialus reikalas.

Be to, CGBC taip pat grasina tos pačios atakos kaip ir PCC. VėliauACKERMANN; KREUZER, 2006 atrado, kad populiarioji RSA kriptosistema, taip pat ir El-Gamal, Polly 2 ir Rai yra atskiri bendrosios Griobnerio bazių kriptosistemos (GBC) atvejai. Todėl GBC atrodo tinkamas karkasas ateities kriptosistemoms.

2.3.4. WGBC kriptosistema

Pateikiame pavyzdį iš originalaus straipsnio. Turime šiuos žymėjimus:

- Lauką F, char$(F) = 13$;
- Veilio algebrą $A_n(F)$, $n = 2$;
- A_n narių tvarką $\sigma = DegRevLex$;
- Privačiojo rakto dydį $s = 2$;
- Privačiojo rakto elementų aibę $\{g_i\}_{i=1}^{s}$, kuri yra redukuota σ-Griobnerio bazė:

$$g_1 = 7x_1^7\partial_1^7 + 2x_1^6\partial_1^6 + 3x_1^3 - \partial_1^3 + 4x_1^2 - 3x_1\partial_1 - 2\partial_1^2 + 5x_1 - 7\partial_1 + 1;$$
$$g_2 = 4x_2^5\partial_2^5 + 3x_2^4\partial_2^4 + 5x_2^4 + \partial_2^4 - 3x_2^3 - 4\partial_2^3 + x_2^2 - x_2\partial_2 + 2\partial_2^2 - 3;$$

- Viešojo rakto dydį $r = 2$;
- Viešojo rakto koeficientus $\{h_{i,j}\}_{1\le i\le r;1\le j\le s} \subset A_n$:

$$h_{1,1} = 4x_1^3x_2^{11}\partial_1^3\partial_2^9 + 5x_1^3x_2^{10}\partial_1^3\partial_2^8 + 5x_1 - 3x_2 + 2\partial_1 - 6\partial_2 + 3;$$
$$h_{1,2} = 6x_1^{10}x_2^6\partial_1^{10}\partial_2^4 - 6x_1^9x_2^6\partial_1^9\partial_2^4 - 3x_1 + 4x_2 - 5\partial_1 + 2\partial_2 + 4;$$
$$h_{2,1} = 5x_1^2x_2^{14}\partial_1^6\partial_1^{16} - 4x_1^2x_2^{13}\partial_1^6\partial_2^{15} - 7x_1 + 2x_2 + 4;$$
$$h_{2,2} = x_1^9x_2^9\partial_1^{13}\partial_2^{11} + 7x_1^8x_2^9\partial_1^{12}\partial_2^{11} + 6\partial_1 - 3\partial_2 + 1;$$

- Viešojo rakto elementus $\{p_i = \sum_{j=1}^{s} h_{i,j}g_j\}_{i=1}^{r}$;
- Tekstogramos elementų vektorinę erdvę V virš lauko F, V bazė yra $M = \{x_1^{\alpha_1}x_2^{\alpha_2}\partial_1^{\beta_1}\partial_2^{\beta_2} | \alpha_1, \alpha_2, \beta_1, \beta_2 \in \mathbb{Z}_{\ge 0} \wedge \alpha_1 + \alpha_2 \le 11 \wedge \beta_1 + \beta_2 \le 7\}$;
- Tekstogramos elementą $m \in V$:

$$m = 42x_1x_2^2\partial_1^3\partial_2^4 + 7x_1\partial_1;$$

- Entropijos elementus $\{l_i\}_{i=1}^{r} \subset A_n$:

$$l_1 = -5x_1^{10}x_2^{16}\partial_1^{12}\partial_2^{19} - 2x_1^8x_2^{18}\partial_1^{10}\partial_2^{21};$$
$$l_2 = 4x_1^{11}x_2^{13}\partial_1^9\partial_2^{12} - 6x_1^9x_2^{15}\partial_1^7\partial_2^{14}.$$

2.3.4.1. Šifravimo ir iššifravimo operacijos

Žemiau pateikiame ApCoCoA sistemoje (APCOCOA TEAM, 2013) vykdomą programinį kodą:

```
P := 13;
N := 2;
An ::= ZZ/(P)[x[1..N],y[1..N]];
Use An;
G := [
  Weyl.WStandardForm([
    [7x[1]^7, y[1]^7],
```

```
    [2x[1]^6, y[1]^6],
    [3x[1]^3],
    [-1y[1]^3],
    [4x[1]^2, y[1]^2],
    [1x[1]^2],
    [-3x[1], y[1]],
    [-2y[1]^2],
    [5x[1]],
    [-7y[1]],
    [1]
  ]), Weyl.WStandardForm([
    [4x[2]^5, y[2]^5],
    [3x[2]^4, y[2]^4],
    [5x[2]^4],
    [1y[2]^4],
    [-3x[2]^3],
    [-4y[2]^3],
    [1x[2]^2],
    [-1x[2], y[2]],
    [2y[2]^2],
    [-3]
  ])
];
H := [
    [
        -- H11
        Weyl.WStandardForm([
            [4x[1]^3, x[2]^11, y[1]^3, y[2]^9],
            [5x[1]^3, x[2]^10, y[1]^3, y[2]^8],
            [5x[1]],
            [-3x[2]],
            [2y[1]],
            [-6y[2]],
            [3]
        ]),
        -- H12
        Weyl.WStandardForm([
            [6x[1]^10, x[2]^6, y[1]^10, y[2]^4],
            [-6x[1]^9, x[2]^6, y[1]^9, y[2]^4],
            [-3x[1]],
            [4x[2]],
            [-5y[1]],
            [2y[2]],
            [4]
        ])
    ],
    [
        -- H21
        Weyl.WStandardForm([
            [5x[1]^2, x[2]^14, y[1]^6, y[1]^16],
            [-4x[1]^2, x[2]^13, y[1]^6, y[2]^15],
            [-7x[1]],
            [2x[2]],
            [4]
        ]),
        -- H22
        Weyl.WStandardForm([
            [1x[1]^9, x[2]^9, y[1]^13, y[2]^11],
            [7x[1]^8, x[2]^9, y[1]^12, y[2]^11],
            [6y[1]],
```

```
            [-3y[2]],
            [1]
        ])
    ]
];
P := [
    Weyl.WMul(H[1][1], G[1]) + Weyl.WMul(H[1][2], G[2]),
    Weyl.WMul(H[2][1], G[1]) + Weyl.WMul(H[2][2], G[2])
];
L := [
    Weyl.WStandardForm([
        [-5x[1]^10, x[2]^16, y[1]^12, y[2]^19],
        [-2x[1]^8, x[2]^18, y[1]^10, y[2]^21]
    ]),
    Weyl.WStandardForm([
        [4x[1]^11, x[2]^13, y[1]^9, y[2]^12],
        [-6x[1]^9, x[2]^15, y[1]^7, y[2]^14]
    ])
];
M := Weyl.WStandardForm([
    [42x[1]^1, x[2]^2, y[1]^3, y[2]^4],
    [7x[1], y[1]]
]);
C := M + Weyl.WMul(L[1], P[1]) + Weyl.WMul(L[2], P[2]);

M;
Len(Support(C));
Weyl.WNR(C, G);
```

Po 3.7s programa davė rezultatą:

```
------------------------------
3x[1]x[2]^2y[1]^3y[2]^4 - 6x[1]y[1]
------------------------------
1982
------------------------------
3x[1]x[2]^2y[1]^3y[2]^4 - 6x[1]y[1]
------------------------------
```

Matome, kad originali tekstograma sutampa su iššifruota tekstograma, o šifrogramos daugianaris turi 1982 nenulinius koeficientus.

3. TEORINIAI METODAI IR REZULTATAI

3.1. VEILIO ALGEBROS MATRICINĖ REPREZENTACIJA

Fiksuokime kokį nors pirminį skaičių p. Imkime lauką F (char$(F) = p$), Veilio algebrą $A_n(F)$, ir $S_n = F[t_1, \dots, t_{2n}]$. Veilio algebros sudaromąsias alternatyviai žymėkime $\{\gamma_i\}_{i=1}^{2n}$. Turime tikrą Veilio algebros A_n reprezentaciją $\Phi : A_n \to M_{p^n}(S_n)$ (TSUCHIMOTO, 2008) į matricų algebrą $M_{p^n}(S_n)$, kuri sudaromąsias reprezentuos taip:

$$\Phi(\gamma_i) = \mu_i + t_i = M_i + t_i \mathbb{1}_{p^n}, \tag{3.1}$$

čia μ_i - sudaromąją atitinkantis vektorinės erdvės $F[x_1, x_2, \dots x_n]/(x_1^p, \dots, x_n^p)$ operatorius, M_i - μ_i atitinkanti matrica.

Prisiminkime, kad $\begin{cases} \mu_i = \text{daugyba iš } x_i \\ \mu_{i+n} = \frac{\partial}{\partial x_i} \end{cases}$.

Pavyzdžiui, jeigu $n = 1$, $p = 3$, tai μ_i bus $F[x_1]/(x_1^3)$ operatoriai. Baziniais erdvės elementais pasirinkę $e_1 = 1, e_2 = x_1, e_3 = x_1^2$, operatoriui μ_1 priskirkime jį atitinkančią matricą:

$$\begin{cases} \mu_1 e_1 = x_1 \cdot 1 = 0 \cdot 1 + 1 \cdot x_1 + 0 \cdot x_1^2 \\ \mu_1 e_2 = x_1 \cdot x_1 = 0 \cdot 1 + 0 \cdot x_1 + 1 \cdot x_1^2 \\ \mu_1 e_3 = x_1 \cdot x_1^2 = 0 \cdot 1 + 0 \cdot x_1 + 0 \cdot x_1^2 \end{cases} \Rightarrow M_1 = \begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}. \tag{3.2}$$

Tada $\Phi(x_1) = \Phi(\gamma_1) = M_1 + t_1 \cdot 1_3 = \begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} + \begin{pmatrix} t_1 & 0 & 0 \\ 0 & t_1 & 0 \\ 0 & 0 & t_1 \end{pmatrix} = \begin{pmatrix} t_1 & 0 & 0 \\ 1 & t_1 & 0 \\ 0 & 1 & t_1 \end{pmatrix}$. Analogiškai rasime, kad $\Phi(\partial_1) = \begin{pmatrix} t_2 & 1 & 0 \\ 0 & t_2 & 2 \\ 0 & 0 & t_2 \end{pmatrix}$. Paskaičiuokime sudėtingesnio $A_n(F)$ elemento reprezentaciją:

$$\Phi(x_1\partial_1 + x_1 + \mathbf{1}) = \Phi(x_1)\Phi(\partial_1) + \Phi(x_1) + \Phi(\mathbf{1}) =$$
$$= \begin{pmatrix} t_1 & 0 & 0 \\ 1 & t_1 & 0 \\ 0 & 1 & t_1 \end{pmatrix} \begin{pmatrix} t_2 & 1 & 0 \\ 0 & t_2 & 2 \\ 0 & 0 & t_2 \end{pmatrix} + \begin{pmatrix} t_1 & 0 & 0 \\ 1 & t_1 & 0 \\ 0 & 1 & t_1 \end{pmatrix} + \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} =$$
$$= \begin{pmatrix} t_1t_2 & t_1 & 0 \\ t_2 & 1 + t_1t_2 & 2t_1 \\ 0 & t_2 & 2 + t_1t_2 \end{pmatrix} + \begin{pmatrix} t_1 & 0 & 0 \\ 1 & t_1 & 0 \\ 0 & 1 & t_1 \end{pmatrix} + \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} =$$
$$= \begin{pmatrix} t_1t_2 + t_1 + 1 & t_1 & 0 \\ t_2 + 1 & 2 + t_1t_2 + t_1 & 2t_1 \\ 0 & t_2 + 1 & 3 + t_1t_2 + t_1 \end{pmatrix}.$$

3.2. LYGČIŲ SUDARYMAS

Sudarysime WGBC užšifravimo operacijos $c = m + \sum_{i=1}^{r} l_i p_i$ lygties matricinę formą naudodami anksčiau aprašytą Veilio algebros reprezentaciją Φ.

Tarkime turime labai paprastą atvejį - viešai žinomus $p = 3, n = 1, r = 1, V$(tekstogramos elementų vektorinė erdvė, žr. skyrių „Griobnerio bazės Veilio algebroje“) bazę $M = \{x_1\partial_1, x_1^2\partial_1, x_1\partial_1^2, x_1^2\partial_1^2\}$, $p_1 = \partial_1$ ir $c = 2x_1\partial_1$. Kadangi l_1 gali būti imamas iš visos $A_n(F)$, tai kaskart sudarydami lygtį turime nuspręsti ir apriboti l_1 narių laipsnių vektorius - paprastumui imkime, kad l_1 narių aibė sutampa su M.

Taigi, turime tokią Veilio algebros lygtį:

$$\begin{aligned}
c &= m + l_1 p_1;\\
2x_1\partial_1 &= m + l_1\partial_1;\\
2x_1\partial_1 &= m_1 x_1\partial_1 + m_2 x_1 x_1\partial_1 + m_3 x_1\partial_1\partial_1 + m_4 x_1 x_1\partial_1\partial_1 +\\
&\quad + (l_{11} x_1\partial_1 + l_{12} x_1 x_1\partial_1 + l_{13} x_1\partial_1\partial_1 + l_{14} x_1 x_1\partial_1\partial_1)\partial_1;
\end{aligned}$$

Matricų algebros lygtis, naudojant reprezentaciją Φ, atrodytų taip:

$$\begin{aligned}
\Phi(c) &= \Phi(m) + \Phi(l_1)\Phi(p_1);\\
2\Phi(x_1)\Phi(\partial_1) &= m_1\Phi(x_1)\Phi(\partial_1) + m_2\Phi(x_1)\Phi(x_1)\Phi(\partial_1) +\\
&\quad + m_3\Phi(x_1)\Phi(\partial_1)\Phi(\partial_1) + m_4\Phi(x_1)\Phi(x_1)\Phi(\partial_1)\Phi(\partial_1) +\\
&\quad + (l_{11}\Phi(x_1)\Phi(\partial_1) + l_{12}\Phi(x_1)\Phi(x_1)\Phi(\partial_1) +\\
&\quad + l_{13}\Phi(x_1)\Phi(\partial_1)\Phi(\partial_1) + l_{14}\Phi(x_1)\Phi(x_1)\Phi(\partial_1)\Phi(\partial_1))\Phi(\partial_1);\\
2\Phi(x_1)\Phi(\partial_1) &= m_1\Phi(x_1)\Phi(\partial_1) + m_2\Phi(x_1)\Phi(x_1)\Phi(\partial_1) +\\
&\quad + m_3\Phi(x_1)\Phi(\partial_1)\Phi(\partial_1) + m_4\Phi(x_1)\Phi(x_1)\Phi(\partial_1)\Phi(\partial_1) +\\
&\quad + l_{11}\Phi(x_1)\Phi(\partial_1)\Phi(\partial_1) + l_{12}\Phi(x_1)\Phi(x_1)\Phi(\partial_1)\Phi(\partial_1) +\\
&\quad + l_{13}\Phi(x_1)\Phi(\partial_1)\Phi(\partial_1)\Phi(\partial_1) + l_{14}\Phi(x_1)\Phi(x_1)\Phi(\partial_1)\Phi(\partial_1)\Phi(\partial_1);\\
\mathbf{0} &= (m_1 - 2)\Phi(x_1)\Phi(\partial_1) + m_2\Phi(x_1)\Phi(x_1)\Phi(\partial_1) +\\
&\quad + (m_3 + l_{11})\Phi(x_1)\Phi(\partial_1)\Phi(\partial_1) + (m_4 + l_{12})\Phi(x_1)\Phi(x_1)\Phi(\partial_1)\Phi(\partial_1) +\\
&\quad + l_{13}\Phi(x_1)\Phi(\partial_1)\Phi(\partial_1)\Phi(\partial_1) + l_{14}\Phi(x_1)\Phi(x_1)\Phi(\partial_1)\Phi(\partial_1)\Phi(\partial_1).
\end{aligned}$$

Reprezentuokime lygties narius:

$$\Phi(x_1)\Phi(\partial_1) = \begin{pmatrix} t_1t_2 & t_1 & 0 \\ t_2 & 1+t_1t_2 & 2t_1 \\ 0 & t_2 & 2+t_1t_2 \end{pmatrix};$$

$$\Phi(x_1)\Phi(x_1)\Phi(\partial_1) = \begin{pmatrix} t_1 & 0 & 0 \\ 1 & t_1 & 0 \\ 0 & 1 & t_1 \end{pmatrix} \begin{pmatrix} t_1t_2 & t_1 & 0 \\ t_2 & 1+t_1t_2 & 2t_1 \\ 0 & t_2 & 2+t_1t_2 \end{pmatrix} =$$

$$= \begin{pmatrix} t_1^2t_2 & t_1^2 & 0 \\ 2t_1t_2 & 2t_1+t_1^2t_2 & 2t_1^2 \\ t_2 & 1+2t_1t_2 & 4t_1+t_1^2t_2 \end{pmatrix};$$

$$\Phi(x_1)\Phi(\partial_1)\Phi(\partial_1) = \begin{pmatrix} t_1t_2 & t_1 & 0 \\ t_2 & 1+t_1t_2 & 2t_1 \\ 0 & t_2 & 2+t_1t_2 \end{pmatrix} \begin{pmatrix} t_2 & 1 & 0 \\ 0 & t_2 & 2 \\ 0 & 0 & t_2 \end{pmatrix} =$$

$$= \begin{pmatrix} t_1t_2^2 & 2t_1t_2 & 2t_1 \\ t_2^2 & 2t_2+t_1^2t_2 & 2+4t_1t_2 \\ 0 & t_2^2 & 4t_2+t_1t_2^2 \end{pmatrix};$$

$$\Phi(x_1)\Phi(x_1)\Phi(\partial_1)\Phi(\partial_1) = \begin{pmatrix} t_1 & 0 & 0 \\ 1 & t_1 & 0 \\ 0 & 1 & t_1 \end{pmatrix} \begin{pmatrix} t_1t_2^2 & 2t_1t_2 & 2t_1 \\ t_2^2 & 2t_2+t_1^2t_2 & 2+4t_1t_2 \\ 0 & t_2^2 & 4t_2+t_1t_2^2 \end{pmatrix} =$$

$$= \begin{pmatrix} t_1^2t_2^2 & 2t_1^2t_2 & 2t_1^2 \\ 2t_1t_2^2 & 4t_1t_2+t_1^3t_2 & 4t_1+4t_1^2t_2 \\ t_2^2 & 2t_2+t_1^2t_2+t_1t_2^2 & 2+8t_1t_2+t_1^2t_2^2 \end{pmatrix};$$

$$\Phi(x_1)\Phi(\partial_1)\Phi(\partial_1)\Phi(\partial_1) = \begin{pmatrix} t_1t_2^2 & 2t_1t_2 & 2t_1 \\ t_2^2 & 2t_2+t_1^2t_2 & 2+4t_1t_2 \\ 0 & t_2^2 & 4t_2+t_1t_2^2 \end{pmatrix} \begin{pmatrix} t_2 & 1 & 0 \\ 0 & t_2 & 2 \\ 0 & 0 & t_2 \end{pmatrix} =$$

$$= \begin{pmatrix} t_1t_2^3 & 3t_1t_2^2 & 6t_1t_2 \\ t_2^3 & 3t_2^2+t_1^2t_2^2 & 4t_2+2t_1^2t_2+2t_2^2+t_1^2t_2^2 \\ 0 & t_2^3 & 6t_2^2+t_1t_2^3 \end{pmatrix};$$

$$\Phi(x_1)\Phi(x_1)\Phi(\partial_1)\Phi(\partial_1)\Phi(\partial_1) = \begin{pmatrix} t_1^2t_2^2 & 2t_1^2t_2 & 2t_1^2 \\ 2t_1t_2^2 & 4t_1t_2+t_1^3t_2 & 4t_1+4t_1^2t_2 \\ t_2^2 & 2t_2+t_1^2t_2+t_1t_2^2 & 2+8t_1t_2+t_1^2t_2^2 \end{pmatrix} \begin{pmatrix} t_2 & 1 & 0 \\ 0 & t_2 & 2 \\ 0 & 0 & t_2 \end{pmatrix} =$$

$$= \begin{pmatrix} t_1^2t_2^3 & 3t_1^2t_2^2 & 6t_1^2t_2 \\ 2t_1t_2^3 & 6t_1t_2^2+t_1^3t_2^2 & 12t_1t_2+2t_1^3t_2+4t_1^2t_2^2 \\ t_2^3 & 3t_2^2+t_1^2t_2^2+t_1t_2^3 & 6t_2+2t_1^2t_2+10t_1t_2^2+t_1^2t_2^3 \end{pmatrix};$$

Išskleiskime matricinę lygtį paelemenčiui į 9 daugianarių žiedo $F[t_1, \dots, t_{2n}]$ lygtis:

$$\begin{aligned}
\mathbf{0} &= (m_1-2)t_1t_2 + m_2t_1^2t_2 + (m_3+l_{11})t_1t_2^2 + (m_4+l_{12})t_1^2t_2^2 + l_{13}t_1t_2^3 + l_{14}t_1^2t_2^3;\\
\mathbf{0} &= (m_1-2)(t_1) + m_2(t_1^2+t_2) + (m_3+l_{11})(2t_1t_2)+\\
&\quad + (m_4+l_{12})(2t_1^2t_2+t_2^2) + l_{13}(3t_1t_2^2) + l_{14}(3t_1^2t_2^2+t_2^3);\\
\mathbf{0} &= (m_1-2)(t_2) + m_2(2t_1t_2+2) + (m_3+l_{11})(2t_1+t_2^2)+\\
&\quad + (m_4+l_{12})(2t_1^2+2t_1t_2^2+4t_2) + l_{13}(6t_1t_2+t_2^3) + l_{14}(4t_1^2t_2+2t_2^2+2t_1^2t_2+t_1t_2^3+4t_2^3);\\
\mathbf{0} &= (m_1-2)(t_2) + m_2(2t_1t_2) + (m_3+l_{11})(t_2^2)+\\
&\quad + (m_4+l_{12})(2t_1t_2^2) + l_{13}(t_2^3) + l_{14}(2t_1t_2^3);\\
\mathbf{0} &= (m_1-2)(1+t_1t_2) + m_2(2t_1+t_1^2t_2) + (m_3+l_{11})(2t_2+t_1^2t_2)+\\
&\quad + (m_4+l_{12})(4t_1t_2+t_1^3t_2) + l_{13}(3t_2^2+t_1^2t_2^2) + l_{14}(6t_1t_2^2+t_1^3t_2^2);\\
\mathbf{0} &= (m_1-2)(2t_1) + m_2(t_2+2t_1^2) + (m_3+l_{11})(2+4t_1t_2)+\\
&\quad + (m_4+l_{12})(4t_1+t_2^2+4t_1^2t_2) + l_{13}(4t_2+2t_1^2t_2+2t_2^2+t_1^2t_2^2)+\\
&\quad + l_{14}(12t_1t_2+2t_1^3t_2+t_2^3+4t_1^2t_2^2);\\
\mathbf{0} &= (m_1-2)(0) + m_2(t_2) + (m_3+l_{11})(0)+\\
&\quad + (m_4+l_{12})(t_2^2) + l_{13}(0) + l_{14}(t_2^3);\\
\mathbf{0} &= (m_1-2)(t_2) + m_2(1+2t_1t_2) + (m_3+l_{11})(t_2^2)+\\
&\quad + (m_4+l_{12})(2t_2+t_1^2t_2+t_1t_2^2) + l_{13}(t_2^3) + l_{14}(3t_2^2+t_1^2t_2^2+t_1t_2^3);\\
\mathbf{0} &= (m_1-2)(2+t_1t_2) + m_2(4t_1+t_1^2t_2) + (m_3+l_{11})(4t_2+t_1t_2^2)+\\
&\quad + (m_4+l_{12})(2+8t_1t_2+t_1^2t_2^2) + l_{13}(6t_2^2+t_1t_2^3) + l_{14}(6t_2+2t_1^2t_2+10t_1t_2^2+t_1^2t_2^4).
\end{aligned}$$

Surinkime jų koeficientus prie bazinių elementų. Dėl bazės tiesinio nepriklausomumo savybės, visi koeficientai irgi turi būti lygūs 0. Todėl prie kiekvienos lygties dar skliausteliuose prirašysime į kiek

lauko F lygčių kiekviena išsiskleidžia.

$$\mathbf{0} = (m_1 - 2)t_1t_2 + m_2t_1^2t_2 + (m_3 + l_{11})t_1t_2^2 + (m_4 + l_{12})t_1^2t_2^2 + l_{13}t_1t_2^3 + l_{14}t_1^2t_2^3; (6)$$

$$\mathbf{0} = (m_1 - 2)t_1 + m_2t_1^2 + m_2t_2 + 2(m_3 + l_{11})t_1t_2 +$$
$$+ 2(m_4 + l_{12})t_1^2t_2 + (m_4 + l_{12})t_2^2 + 3l_{13}t_1t_2^2 + 3l_{14}t_1^2t_2^2 + l_{14}t_2^3; (9)$$

$$\mathbf{0} = (m_1 - 2 + 4m_4 + 4l_{12})t_2 + (2m_2 + 6l_{13})t_1t_2 + 2m_2 +$$
$$+ 2(m_3 + l_{11})t_1 + (m_3 + l_{11} + 2l_{14})t_2^2 + 2(m_4 + l_{12})t_1^2 +$$
$$+ 2(m_4 + l_{12})t_1t_2^2 + (l_{13} + 4l_{14})t_2^3 + 6l_{14}t_1^2t_2 + l_{14}t_1t_2^3; (10)$$

$$\mathbf{0} = (m_1 - 2)t_2 + 2m_2t_1t_2 + (m_3 + l_{11})t_2^2 +$$
$$+ 2(m_4 + l_{12})t_1t_2^2 + l_{13}t_2^3 + 2l_{14}t_1t_2^3; (6)$$

$$\mathbf{0} = (m_1 - 2) + (m_1 - 2 + 4m_4 + 4l_{12})t_1t_2 + 2m_2t_1 +$$
$$+ (m_2 + m_3 + l_{11})t_1^2t_2 + 2(m_3 + l_{11})t_2 +$$
$$+ (m_4 + l_{12})t_1^3t_2 + 3l_{13}t_2^2 + l_{13}t_1^2t_2^2 + 6l_{14}t_1t_2^2 + l_{14}t_1^3t_2^2; (10)$$

$$\mathbf{0} = (2m_1 - 4 + 4m_4 + 4l_{12})t_1 + (m_2 + 4l_{13})t_2 + 2m_2t_1^2 +$$
$$+ 2(m_3 + l_{11}) + (4m_3 + 4l_{11} + 12l_{14})t_1t_2 +$$
$$+ (m_4 + l_{12} + 2l_{13})t_2^2 + (4m_4 + 4l_{12} + 2l_{13})t_1^2t_2 +$$
$$+ (l_{13} + 4l_{14})t_1^2t_2^2 + 2l_{14}t_1^3t_2 + l_{14}t_2^3; (10)$$

$$\mathbf{0} = m_2t_2 + (m_4 + l_{12})t_2^2 + l_{14}t_2^3; (3)$$

$$\mathbf{0} = (m_1 - 2 + 2m_4 + 2l_{12})t_2 + m_2 + 2m_2t_1t_2 + (m_3 + l_{11} + 3l_{14})t_2^2 +$$
$$+ (m_4 + l_{12})t_1^2t_2 + (m_4 + l_{12})t_1t_2^2 + l_{13}t_2^3 + l_{14}t_1^2t_2^2 + l_{14}t_1t_2^3; (9)$$

$$\mathbf{0} = (2m_1 - 4 + 2m_4 + 2l_{12}) + (m_1 - 2 + 8m_4 + 8l_{12})t_1t_2 + 4m_2t_1 +$$
$$+ m_2t_1^2t_2 + (4m_3 + 4l_{11} + 6l_{14})t_2 + (m_3 + l_{11} + 10l_{14})t_1t_2^2 +$$
$$+ (m_4 + l_{12})t_1^2t_2^2 + 6l_{13}t_2^2 + l_{13}t_1t_2^3 + 2l_{14}t_1^2t_2 + l_{14}t_1^2t_2^4. (11)$$

Iš viso turime 74 lauko F lygtis.

Iš šio paprasto pavyzdžio tik pamatėme procesą, kaip sudaromos lygtys.

3.3. LYGČIŲ SKAIČIAVIMAS

Akivaizdu, kad daugianarių žiedo $F[t_1, \dots, t_{2n}]$ lygčių visada bus lygiai p^{2n}, jeigu Veilio algebra yra n-toji ir lauko F charakteristika yra p.

Suskaičiuokime, kiek bus lauko F lygčių.

Pirma, akivaizdu, kad nei tikslaus šių lygčių skaičiaus, nei jo viršutinės ribos nepriklauso vien nuo kriptosistemos parametrų, todėl jo vienareikšmiškai pateikti negalime - sudaromųjų $t_1, \dots, t_{2n}$ laipsniai gali būti betkokie - tai yra laipsniai ir lygčių skaičius priklauso nuo l_i, p_i ir m laipsnių. Todėl skaičiuosime

asimptotinę priklausomybę.

Jeigu turime $A_1(F)$ elementą a, kurio didžiausią laipsnį x turintis narys b, tai iš visų b reprezentacijos matricos elemento narių didžiausią laipsnį žymėkime x. Tai reiškia, kad b reprezentacijos elementai turės daugiausiai po $\frac{(x+1)(1+x+1)}{2} = O(x^2)$ nenulinių $F[t_1, t_2]$ narių. Tada viso a reprezentacijos elementai turės taip pat daugiausiai po $O(x^2)$ narių.

Jeigu $h_{i,j}$ bazės didžiausias laipsnis yra y, o g_i - x, tai $p_i = \sum_{j=1}^{s} h_{i,j}g_j$ didžiausias laipsnis bus tiesiog $y+x$. Jeigu l_i bazės didžiausias laipsnis yra z, V bazės - w, o p_i - $y+x$, tai $c = m+\sum_{i=1}^{r} l_i p_i$ ($m \in V$) didžiausias laipsnis bus $z+w+y+x$. Taigi c reprezentacijos turės daugiausiai po $O((z+w+y+x)^2)$ nenulinių $F[t_1, t_2]$ narių. Todėl ir lauko F lygčių skaičius bus daugiausiai $O((z+w+y+x)^2)$.

Pastebėkime, kad nei nuo viešojo rakto dydžio r, nei nuo privačiojo rakto dydžio s lauko F lygčių skaičius nepriklauso.

Akivaizdu, kadangi daugianarių žiedo lygčių skaičius yra $O(\text{const}^n)$, tai ir lauko F lygčių skaičiaus priklausomybė nuo n bus $O(\text{const}^n)$.

4. IŠVADOS

1. Išnagrinėta nauja nekomutatyvi Veilio Griobnerio bazių asimetrinė kriptografinė sistema.
2. Pateiktas kriptanalizės metodas paremtas Veilio algebros reprezentacijų teorija.
3. Gautos priklausomybės tarp parametrų reikšmės ir kriptanalizės lygčių skaičiaus.
4. Lygčių skaičiaus nuo Veilio algebros indekso asimptotinė priklausomybė yra $O(\text{const}^n)$.
5. Lygčių skaičiaus nuo viešojo rakto, privačiojo rakto ir entropijos daugianarių bazių galių asimptotinė priklausomybė yra $O(n^{\text{const}})$.

5. PADĖKOS

Padėka skiriama kassavaitinio kriptografijos ir algebros seminaro organizatoriui ir darbo vadovui prof. Eligijui Sakalauskui ir seminaro kolegai magistrantui Albertui Dvirnui.

LITERATŪRA

1 ALI, R.; KREUZER, M. Weyl Gröbner basis cryptosystems. In. *Computational and combinatorial group theory and cryptography*. Providence, RI: Amer. Math. Soc., 2012, psl. 1–20. Contemp. Math. Taip pat prieinama per internetą: ⟨http://dx.doi.org/10.1090/conm/582/11554⟩.

2 SIPSER, M. *Introduction to the theory of computation. 2nd. ed.* 2006.

3 SHOR, P. W. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM J. Comput.* 1997, t. 26, nr. 5, psl. 1484–1509. Taip pat prieinama per internetą: ⟨http://dx.doi.org/10.1137/S0097539795293172⟩.

4 BERNSTEIN, D.; BUCHMANN, J. *Post-Quantum Cryptography*. 2009. ISBN 9783540887027.

5 ALI, R. *Weyl Gröobner Basis Cryptosystems* [online]. 2011 [**urlseen** 2013-03-15]. 207 psl. Prieiga per internetą: ⟨http://www.opus-bayern.de/uni-passau/volltexte/2011/2319/pdf/Ali_Rashid.pdf⟩.

6 ACKERMANN, P.; KREUZER, M. Gröbner basis cryptosystems. *Appl. Algebra Eng. Commun. Comput.* 2006, t. 17, nr. 3-4, psl. 173–194. Taip pat prieinama per internetą: ⟨http://dx.doi.org/10.1007/s00200-006-0002-0⟩.

7 LANG, S. *Algebra*. 3 leid. New York: Springer, 2002. 918 psl. Graduate Texts in Mathematics. Taip pat prieinama per internetą: ⟨http://dx.doi.org/10.1007/978-1-4613-0041-0⟩. ISBN 978-1-4612-6551-1.

8 ADKINS, W.; WEINTRAUB, S. *Algebra: An Approach Via Module Theory*. 1992. Algebra: An Approach Via Module Theory. ISBN 9780387978390.

9 LAM, T. *A First Course in Noncommutative Rings*. 2001. Graduate Texts in Mathematics. Taip pat prieinama per internetą: ⟨http://dx.doi.org/10.1007/978-1-4419-8616-0⟩. ISBN 978-0-387-95325-0.

10 COX, D.; LITTLE, J.; O'SHEA, D. *Ideals, Varieties, and Algorithms*. 2007. Undergraduate Texts in Mathematics. Taip pat prieinama per internetą: ⟨http://dx.doi.org/10.1007/978-0-387-35651-8⟩. ISBN 978-0-387-35650-1.

11 DASGUPTA, A. *Set Theory*. 2014. Taip pat prieinama per internetą: ⟨http://dx.doi.org/10.1007/978-1-4614-8854-5⟩. ISBN 978-1-4614-8853-8.

12 BUCHBERGER, B. *Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal*. 1965.

13 ROBSHAW, M. One-Way Function. In TILBORG, H. van; JAJODIA, S. (Hrsg.). *Encyclopedia of Cryptography and Security*. 2011, psl. 887–888. Taip pat prieinama per internetą: ⟨http://dx.doi.org/10.1007/978-1-4419-5906-5_467⟩. ISBN 978-1-4419-5905-8.

14 ROBSHAW, M. Trapdoor One-Way Function. In TILBORG, H. van; JAJODIA, S. (Hrsg.). *Encyclopedia of Cryptography and Security*. 2011, psl. 1317–1318. Taip pat prieinama per internetą: ⟨http://dx.doi.org/10.1007/978-1-4419-5906-5_482⟩. ISBN 978-1-4419-5905-8.

15 KALISKI Burt, J. Asymmetric Cryptosystem. In TILBORG, H. van; JAJODIA, S. (Hrsg.). *Encyclopedia of Cryptography and Security*. 2011, psl. 49–50. Taip pat prieinama per internetą: ⟨http://dx.doi.org/10.1007/978-1-4419-5906-5_394⟩. ISBN 978-1-4419-5905-8.

16 GOUBIN, L.; PATARIN, J.; YANG, B.-Y. Multivariate Cryptography. In TILBORG, H. van; JAJODIA, S. (Hrsg.). *Encyclopedia of Cryptography and Security*. 2011, psl. 824–828. Taip pat prieinama per internetą: ⟨http://dx.doi.org/10.1007/978-1-4419-5906-5_421⟩. ISBN 978-1-4419-5905-8.

17 FELLOWS, M.; KOBLITZ, N. Combinatorial cryptosystems galore! In. *Finite fields: theory, applications, and algorithms (Las Vegas, NV, 1993)*. 1994, psl. 51–61. Contemp. Math. Taip pat prieinama per internetą: ⟨http://dx.doi.org/10.1090/conm/168/01688⟩.

18 APCOCOA TEAM. *ApCoCoA: Applied Computatons in Commutative Algebra (Version 1.9.1)*. 2013. Taip pat prieinama per internetą: ⟨http://www.apcocoa.org⟩.

19 TSUCHIMOTO, Y. *Weyl Algebras Revisited* [online]. 2008 [**urlseen** 2014-05-12]. Topics in Non-Commutative Algebraic Geometry and Congruent Zeta Functions. Prieiga per internetą: ⟨http://www.math.kochi-u.ac.jp/docky/bourdoki/NAS/nas005.pdf⟩.