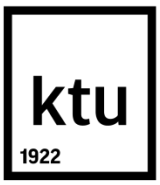

KAUNAS UNIVERSITY OF TECHNOLOGY
FACULTY OF MATHEMATICS AND NATURAL SCIENCES

Albertas Dvirnas

ANALYSIS OF THE GROWTH OF ALGEBRAS AND THEIR APPLICABILITY IN CRYPTOGRAPHY

Master thesis

Supervisor
prof. Eligijus Sakalauskas

KAUNAS, 2015

KAUNAS UNIVERSITY OF TECHNOLOGY

FACULTY OF MATHEMATICS AND NATURAL SCIENCES

ANALYSIS OF THE GROWTH OF ALGEBRAS AND THEIR APPLICABILITY IN CRYPTOGRAPHY

Master thesis

Applied Mathematics (code 621G12001)

Supervisor
prof. Eligijus Sakalauskas

Referee
dr. Vidas Regelskis

Student
Albertas Dvirnas

KAUNAS, 2015

KAUNO TECHNOLOGIJOS UNIVERSITETAS

MATEMATIKOS IR GAMTOS MOKSLŲ FAKULTETAS

Albertas Dvirnas

Taikomoji matematika (kodas 621G12001)

Baigiamojo projekto „Algebrų augimo ir jų pritaikomumo kriptografijoje analizė" (Analysis of the growth of algebras and their applicability in cryptography)

AKADEMINIO SĄŽININGUMO DEKLARACIJA

2015 m. 06 mėn. 01 d.

Kaunas

Patvirtinu, kad mano, **Alberto Dvirno,** baigiamasis darbas tema „Algebrų augimo ir jų pritaikomumo kriptografijoje analizė" (Analysis of the growth of algebras and their applicability in cryptography) yra parašytas visiškai savarankiškai, o visi pateikti duomenys ar tyrimų rezultatai yra teisingi ir gauti sąžiningai. Šiame darbe nei viena darbo dalis nėra plagijuota nuo jokių spausdintinių ar internetinių šaltinių, visos kitų šaltinių tiesioginės ir netiesioginės citatos nurodytos literatūros nuorodose. Įstatymu nenumatytų piniginių sumų už šį darbą niekam nesu mokėjęs.

Aš suprantu, kad išaiškėjus nesąžiningumo faktui, man bus taikomos nuobaudos, remiantis Kauno technologijos universitete galiojančia tvarka.

_____ _____

(studento vardas ir pavardė, įrašyti ranka) (parašas)

Contents

Santrauka **6**

1 Overview **8**

2 Objectives **10**

3 Mathematical preliminaries **11**

3.1 Notation conventions and basic definitions 11

3.2 Finitely presented algebras 12

3.3 Monomial ordering 13

4 Properties of finitely presented algebras **15**

4.1 Canonical form 15

4.1.1 Braid groups 15

4.1.2 Weyl algebra 16

4.1.3 Other finitely presented algebras 16

4.2 Gröbner basis 17

4.3 Growth of algebras 20

4.4 Gelfand-Kirillov's dimension 20

4.5 Center 23

4.6 Centralizer 25

5 Cryptographic preliminaries **27**

5.1 Computational problems 27

5.2 Shpilrain-Ushakov's Key Exchange Protocol 28

6 Application to Key exchange protocol **30**

6.1 New ideas 30

6.2 Practical considerations 33

6.3 Shpilrain-Ushakov assumptions 34

6.4 Direct attack 35

6.5 Decomposition problem 35

6.6 Other security concerns 35

7 Generalizations **36**

8 Computational algebra packages **37**

8.1 Sage 37

8.2 Magma 38

8.3 GAP 39

9 Conclusions **41**

Acknowledgments **42**

References **43**

Dvirnas, A. Algebrų augimo ir jų pritaikomumo kriptografijoje analizė. Magistro baigiamasis darbas / vadovas prof. Eligijus Sakalauskas; Kauno technologijos universitetas, Matematikos ir gamtos mokslų fakultetas, Taikomosios matematikos katedra. Kaunas, 2015. 44 psl.

Santrauka

Pagrindinė magistrinio darbo užduotis buvo įsisavinti Veilio algebrų savybes ir išsiaiškinti, ar jas galima pritaikyti kriptografiniam Shpilrain-Ushakov rakto apsikeitimo protokolui. Vėliau darbo užduotis buvo praplėsta į bandymą išsiaiškinti ir pritaikyti ir kitokias, lėtai augančias algebras.

Pagrindinis nagrinėtas objektas magistriniame darbe buvo laisvoji asociatyvi algebra, ir jos dvipusiai idealai, generuojami baigtinės aibės generatorių. Tokias algebras mes pavadinome baigtinai pateiktomis algebromis.

Kiekvienai iš nagrinėtų algebrų, pasinaudodami Gröbnerio bazių teorija, suradome kanonines formas. Šios reikalingos skaičiuojant laisvosios algebros elemento reikšmę moduliu idealui.

Žinodami kanoninių formų išraiškas, taip pat radome ir algebrų augimo greitį. Radome, kad vienų nagrinėtų algebrų greitis yra tiesinis, o Veilio algebrų (Apibrėžimas 4.5) - kvadratinis. Naudodami formalią terminologiją, pirmąsias algebras vadinome algebromis su Gelfando-Kirilovo dimensija vienas, o antrąsias - su algebromis su Gelfando-Kirilovo dimensija du.

Vėliau literatūroje radome teoremą, teigiančią, jog Gelfando-Kirilovo dimensija gali būti nulis, vienas, du, arba bet koks realus skaičius, didesnis už du.

Algebros, kurių Gelfando-Kirilovo dimensija yra nulis turi baigtinį elementų skaičių. Tačiau mus domina begalinių algebrų taikymai. Komutatyvių algebrų Gelfando-Kirilovo dimensija yra vienas. Tačiau mes norime nagrinėti nekomutatyvių begalinių algebrų taikymus, tad šių algebrų nenagrinėjame. Algebros, kurių Gelfando-Kirilovo dimensija daugiau nei du - augančios greičiau nei kvadratiškai, todėl šiose algebrose mažiau praktiška atlikti skaičiavimus, tad šių algebrų taip pat nenagrinėjame. Todėl liko dviejų tipų augimo algebros, t.y. nekomutatyvios algebros, kurių Gelfando-Kirilovo dimensija yra vienas, bei algebros, kurių Gelfando-Kirilovo dimensija yra du. Šias algebras nagrinėjome su tikslu taikyti nekomutatyvioje kriptografijoje.

Įrodėme svarbią tokio tipo algebroms savybę, teigiančią, jog, turint baigtinai pateiktą algebrą A virš teigiamos charakteristikos lauko k, komutatyvus žiedas $k[x]$ yra algebros elemento x centralizatoriaus poaibis. Be to, ši savybė galioja, ir kai komutatyvus žiedas skaičiuojamas virš algebros centro.

Centralizatoriaus savybę panaudojome apibendrindami Shpilrain-Ushakov rakto apsikeitimo protokolą lėtai augančioms algebroms. Deja, pastebėjome, kad protokolą apibendrindami tokiu būdu dalinai prarandame centralizatoriaus paslėptumą, kadangi dalį centralizatoriaus šiose algebrose yra lengviau apskaičiuoti, nei kasų grupėse, kurių taikymu buvo paremtas originalus Shpilrain-Ushakov rakto apsikeitimo protokolas.

Galiausiai, pateikėme protokolo realizacijos pavyzdžių ir pabandėme paaiškinti, kokie turėtų būti saugumo parametrai ir kokios problemos kiltų bandant pilnai realizuoti mūsų pasiūlytą protokolą. Be to, pateikėme keletą pasiūlymų apibendrinimams. Šioje vietoje nesustojome, ir su darbo vadovu toliau ieškosime šių algebrų inovatyvių pritaikymų kituose raktų apsikeitimo protokoluose.

1 Overview

In this thesis we will be considering the free associative algebras $k\langle X\rangle$, where X is an alfabet, usually consisting of two elements, i.e. $X = \{x, y\}$. It forms a non-commutative polynomial ring under the usual addition and multiplication operations, and a vector space under the usual addition and multiplication by a scalar operations, and therefore, it forms an algebra.

In particular, we will consider infinite algebras (algebras with infinite number of elements) with relations, i.e. we'll choose an ideal I for the algebra $k\langle X\rangle$, and then consider the quotient algebra $k\langle X\rangle/I$.

To understand these better and work with them, we need a way to write a result of a multiplication of two elements of an algebra in a unique way, i.e. we need a normal form. If we have a normal form, then we can give an answer to a question whether two elements of a free associative algebra are the same modulo the ideal.

Additionally, we need to know the growth of the algebra, so that we know how many monomials can we have in the normal form of a product of two elements from the free associative algebra. This, for some special forms of the ideal, can be achieved by using the non-commutative Gröbner basis [9]. We will develop this theory in subsection 4.2.

Calculating Gröbner basis for arbitrary ideals is not an easy task and often the Gröbner basis itself is not finite, so we will need to make use of the tools of computational algebra systems. These we will develop in section 8.

Having found a finite Gröbner basis of an ideal of a free associative algebra, we will be able to find a normal form for an arbitrary element of the algebra, as well as the growth rate of the algebra. This then can be used in various calculations that we'll consider.

We will consider Shpilrain-Ushakov's key exchange protocol [4] and adapt it to the new algebras that we have mastered. We will consider algebras of different growth rates, but we will rule out the commutative case and the free associative algebra case immediately as they fail to satisfy the security or efficiency conditions of the proposed key exchange protocol. Most of our interest will be on the Weyl algebras and what will be called an "almost commutative case", i.e. algebras of linear growth.

The growth of algebras we will be considering will be either linear or quadratic. In the former case, when the order is $4n$ or $6n$, and n^2 in the latter case. Because the growth of these algebras is small, we will be able to compute the products of two elements efficiently.

From the theory Gelfand-Kirillov dimension we will learn that we can't get a much better

result, since, for example, growth rate $\log(n)$ would mean that such an algebra would actually contain finite number of elements. Matrix representations can be found for such algebras [2]. We could make use of matrix theory based attacks can be implemented in the cryptographic protocols based on these algebras.

Finally, we will give some suggestions for the generalizations of the protocol we were considering and what else could be done in this field.

2 Objectives

The work on the master thesis started with the initial goal of understanding the structure of the Weyl algebras and finding an implementation of them in Shpilrain-Ushakov's key exchange protocol. Other objectives and ideas were developed while solving this task, and we summarize the main objectives in the following list.

- Understand the structure of the Weyl algebras and find an implementation of them in Shpilrain-Ushakov's key exchange protocol;
- Make use of computer algebra systems for implementations of finitely presented algebras;
- Understand the structure of slowly growing algebras;
- Generalize the implementation of the key exchange protocol to other algebras of slow growth.

3 Mathematical preliminaries

In this section we present the mathematical preliminaries and the background material for the main observations, which will come in the following sections.

3.1 Notation conventions and basic definitions

X - **alphabet** with letters $x_1, \ldots, x_n, \ldots$. If there's only two letters in the alphabet, we usually denote them by $x_1 = x$ and $x_2 = y$.

X^* - the set of words (monomials) $w = x_{i_1} x_{i_2} \ldots x_{i_k}$, where $x_{i_1}, \ldots x_{i_k} \in X$, $k \geq 0$, $\omega = 1$ - the empty word, and $deg(w) = k$ - the degree of a word.

$k[X]$ - the commutative polynomial ring with variables from alphabet X over field k.

$k\langle X \rangle$ the non-commutative polynomial ring with variables from X over field k.

(F) - ideal generated by the set of polynomials F over a given polynomial ring.

$LM(f)$ - the leading monomial of a polynomial $f \in k\langle X \rangle$ without the coefficient.

$LT(f)$ - the leading term of a polynomial $f \in k\langle X \rangle$, i.e. the leading monomial with the coefficient.

$char(k)$ - the characteristic of the field k.

$\mathbb{Z}_p$ - field of characteristic p, consisting of congruent classes of integers modulo p, i.e. $\mathbb{Z}_p = \{0, 1, \ldots, p-1\}$.

For any two elements $x, y \in A$, where A is any algebra, a **Lie bracket** is defined as

$$[x, y] := xy - yx \tag{3.1}$$

The **center** of an algebra A is the set $Z(A)$, defined as

$$Z(A) := \{v \in A \mid [w, v] = 0 \; \forall \; w \in A\} \tag{3.2}$$

The **centralizer** of an element $v \in A$ is the set $C(v)$, defined as

$$C(v) := \{w \in A \mid [w, v] = 0\} \tag{3.3}$$

We will sometimes use a different notation $C_v(A)$ to mean the centralizer of v in the algebra A.

We assume the reader to be familiar with most notions from courses in linear and abstract algebra. Therefore the notions of vector space, group, ring, algebra, field, ideal should be well

understood. Introduction to these topics can be found in [7].

Notation of a non-commutative polynomial ring might be unfamiliar, so we expand on that.

Let X be an alphabet of noncommuting indeterminates over a field k. Then we can form a noncommutative polynomial ring, also called a "free k-ring", generated by X, and denoted by

$$R = k\langle X\rangle$$

The elements of this ring are polynomials in X with coefficients from k. R becomes a free algebra if it has a structure of a vector space over k as well.

Example 3.1. Let $X = \{x, y\}$, $k = \mathbb{Z}$, then $k\langle x, y\rangle$ is a free algebra over k with the multiplication on the monomials $x_1^i y_1^j \dots x_n^i y_n^j$ and $x^{l_1} y^{k_1} \dots x^{l_m} y^{k_m}$ defined as a concatenation, i.e.

$$\left(x^{i_1} y^{j_1} \dots x^{i_n} y^{j_n}\right) \cdot \left(x^{l_1} y^{k_1} \dots x^{l_m} y^{k_m}\right) = x^{i_1} y^{j_1} \dots x^{i_n} y^{j_n} x^{l_1} y^{k_1} \dots x^{l_m} y^{k_m}.$$

Now, let

$$w = 3x + 4y + 5xyxy,\ v = 2x - 3y + 6xyx$$

be two polynomials in x, y with coefficients from $\mathbb{Z}$.

Then we can easily multiply w and v:

$$\begin{aligned} w \cdot v &= (3x + 4y + 5xyxy) \cdot (2x - 3y + 6xyx) \\ &= 6x^2 - 9xy + 18x^2yx + 8yx - 12y^2 + 24yxyx + 10xyxyx - 15xyxy^2 + 30xyxyxyx \end{aligned}$$

In what follows, we will be interested in algebras as quotients of the form $k\langle X\rangle/I$, where $I = (F)$ - finitely generated ideal of $k\langle X\rangle$, F - set of polynomials in $k\langle X\rangle$, generating I.

This leads us to the definition of the finitely presented algebras.

3.2 Finitely presented algebras

Definition 3.2. Let k be a field, X - alfabet, $k\langle X\rangle$ - corresponding free algebra. Then if $A = k\langle X\rangle/(F)$ with a finite number of polynomials in F, then A is called a **finitely presented algebra**.

A simplest example might be the one of the commutative ring, when the only relation is $xy = yx$:

Example 3.3. Let $X = \{x, y\}$, $F = \{xy - yx\}$. Then $k\langle x, y\rangle/(xy - yx) = k[x, y]$.

Example 3.4. A special class of algebras,

$$A^n = k\langle x, y\rangle/(x^2, xyx, \ldots, xy^n x)$$

an example of Golod-Shafarevich algebras [8], are finitely presented, but if we consider algebra

$$A = \lim_{n\to\infty} A^n = k\langle x, y\rangle/(x^2, xyx, \ldots, xy^n x, \ldots)$$

called the limit algebra of A^n, we see that it is not finitely presented.

Sometimes we will use another notation for the finitely presented algebras, writing in a way comparable to the generators-relations notation used to write a presentation of a group:

$$A = k\langle\ x, y \mid f_1 = 0, f_2 = 0, \ldots, f_n = 0\ \rangle$$

In general, it might not be an easy task in finitely presented algebras to find out if two elements of the free algebra are equal modulo the ideal. It turns out that this question can be answered using the theory of non-commutative Gröbner basis, which we will consider in a later section.

If we have an alphabet $X = \{x, y\}$ of two non-commuting indeterminates, then two monomials xy and yx are different. But at first we don't know whether $xy > yx$. It is then important to be able to say which monomial is "bigger", i.e. we have to choose an ordering.

3.3 Monomial ordering

There can be many orderings. Here we will restrict ourselves to introducing one of them, called "deglex".

We impose a total order (antisymmetric, transitive and total binary relation) on alphabet $X = \{x_1, x_2, \ldots\}$ by setting $x_i \prec x_j$ if and only if $i < j$.

Definition 3.5. The total order on X can be extended to a total order on X^*, called the **deglex** (degree lexicographical) order in such a way: If $u, w \in X^*$ then $u \prec w$ if and only if either:

(i) $\deg(u) < \deg(w)$, or

(ii) $\deg(u) = \deg(w)$ where $u = vx_iu'$ and $w = vx_jw'$ for some $v, u', w' \in X^*$ and $x_i, x_j \in X$ with $x_i < x_j$.

When applying (ii) we first find the common left subword v of the highest degree, and then compare the next two letters x_i and x_j using the total order on X.

Example 3.6. Let $X = \{x, y\}$ with $x \prec y$. We list the words in X^* of degree ≤ 3, sorted in deglex:

$$1 \prec x \prec y \prec xy^2 \prec xy \prec yx \prec y^2 \prec x^3 \prec x^2y \prec xyx \prec xy^2 \prec yx^2 \prec yxy \prec y^2x \prec y^3.$$

We can further extend the ordering to the free associative algebra $k\langle X\rangle$. Firstly we say that $LT(f) \prec LT(g)$ if either $LM(g) \prec LM(f)$ or $lc(f) < lc(g)$, where lc means the leading coefficient in front of leading monomial.

Example 3.7. Consider $\mathbb{Z}_7\langle x, y\rangle$, $x \prec y$, and $f = 3xy$, $g = 2xy$.

Then $LM(f) = xy$, $LM(g) = xy$, and $lc(f) = 3 > 2 = lc(g)$, hence $LT(g) \prec LT(f)$.

Then we consider what happens if the leading coefficients are the same as well, by following this rule:

If $f, g \in k\langle X\rangle$, then $f \prec g$ if $LT(f) \prec LT(g)$ or, if $LT(f) = LT(g)$, then consider recursively whether $LT(f - LT(f)) \prec LT(g - LT(g))$.

Example 3.8. Consider $k\langle x, y\rangle$, $x \prec y$, and $f = x + y + xy^2$, $g = xy^2 + y^3$.

Then $LT(f) = xy^2$, $LT(g) = y^3$, and $xy^2 \prec y^3$, hence $f \prec g$.

Example 3.9. Consider $k\langle x, y\rangle$, $x \prec y$, and $f = 2y + xy^2 + y^3$, $g = 2xy^2 + y^3$.

Then $LT(f) = y^3$, $LT(g) = y^3$, and $LT(f) = LT(g)$, but $LT(2y + 2xy^2) = xy^2 \prec 2xy^2 = LT(2xy^2)$, hence $f \prec g$.

4 Properties of finitely presented algebras

In some specific cases for finitely presented groups or algebras, it is known how to compute canonical forms for words, as well as centers and centralizers. We give a brief description of these.

4.1 Canonical form

Definition 4.1. Let's consider an arbitrary element f of a free algebra (group), F - set of relations. If we can find a way how to write this element modulo the relations F, which would give an unique presentation for each element of the quotient algebra (group), we call it the **canonical form** of an element f.

Note that there might be many different canonical forms, each giving the required result.

Here we give some examples of canonical forms and other properties of specific groups and algebras.

4.1.1 Braid groups

Example 4.2. Consider for $n \geq 2$, the braid group B_n, defined by the Artin presentation by generators and relations:

$$\left\langle \sigma_1, \ldots, \sigma_{n-1} \;\middle|\; \begin{array}{c} \sigma_i\sigma_j = \sigma_j\sigma_i \text{ for } |i-j| \geq 2 \\ \sigma_i\sigma_{i+1}\sigma_i = \sigma_{i+1}\sigma_i\sigma_{i+1} \text{ for } |i-j| = 1 \end{array} \right\rangle. \tag{4.4}$$

An important example of a positive braid (braid which has only generators in positive degrees) is the *fundamental braid* $\Delta_n \in B_n$:

$$\Delta_n = (\sigma_1 \cdots \sigma_{n-1})(\sigma_1 \cdots \sigma_{n-2}) \cdots \sigma_1 \tag{4.5}$$

Then we have a theorem (Theorem 1.2 in [23]), which gives a unique presentation for an arbitrary braid word:

Theorem 4.3. *For every braid $w \in B_n$, there is a unique presentation given by:*

$$w = \Delta_n^r P_1 P_2 \cdots P_k \tag{4.6}$$

where $r \in \mathbb{Z}$ is maximal, P_i are permutation braids, $P_k \neq \varepsilon$ and $P_1 P_2 \cdots P_k$ is a left-weighted decomposition.

This presentation is called Garside normal form. The complexity of transforming any word

$w \in B_n$ into a canonical form is $O(|w|^2 n \log n)$, where $|w|$ is the length of a word in $w \in B_n$ [23].

Example 4.4. For a positive integer n, consider a monoid $M = \langle a_1, \ldots, a_n \rangle$, defined by relations

$$a_j a_i a_k = a_j a_k a_i = a_k a_j a_i, i \leq j$$

and called the Chinese monoid of rank n. Then every element of M has a unique presentation of the form $x = b_1 b_2 \ldots b_n$, where all elements b_i, $i = \overline{1,n}$ can be written in terms of the generators a_j, $j = \overline{1,n}$.

$$b_1 = a_1^{k_{11}},\ b_2 = (a_2 a_1)^{k_{21}} a_2^{k_{22}} \ldots b_n = (a_n a_1)^{k_{n1}} (a_n a_2)^{k_{n2}} \ldots (a_n a_{n-1})^{k_{n(n-1)}} a_n^{k_{nn}}$$

4.1.2 Weyl algebra

Definition 4.5. If $R = k\langle x, y \rangle$, and $F = \{yx - xy - 1\}$, then the finitely presented algebra $A_1(k) = R/(F)$ is called the first Weyl algebra over k.

Theorem 4.6. *We have that the first Weyl algebra $A_1(k)$ satisfies these properties* [24]:

1. $[y, x^n] = nx^{n-1}$, $n = 1, 2, \ldots$;
2. $[y^n, x] = ny^{n-1}$, $n = 1, 2, \ldots$;
3. $Z(A_1(k)) = k[x^p, y^p]$, *i.e. the center of the algebra is a free k-ring, generated by x^p, y^p*;
4. *Canonical form of an element of an algebra $A_1(k)$ is*

$$W = \sum_{i,j=0}^{\infty} a_{ij} x^i y^j, \quad a_{ij} \in k; \tag{4.7}$$

Having a canonical form, we have an unique presentation for an element of an algebra, and we can calculate efficiently. For example, it's not too difficult to check if $W = 2xy^7 + x^2$ is in the centralizer of x:

Example 4.7. Consider $a = x$, $W = 2xy^7 + x^2$, $k = \mathbb{Z}_7 = \{0, 1, \ldots, 6\}$. Then

$$[a, W] = [x, 2xy^7 + x^2] = [x, 2xy^7] + [x, x^2] = x2xy^7 - 2xy^7 x = 2x[x, y^7] = -2x \cdot 7y^6 = 0,$$

therefore $W \in C_x$.

4.1.3 Other finitely presented algebras

Example 4.8. Example of an algebra with monomial relations $A_2 = k\langle x, y \rangle / (y^2,\ xyx,\ yxy)$ [11]:

We can write an arbitrary element w of the k-algebra A_2, as an infinite sum

$$w = \sum_{i=0}^{\infty} \left(a_{i1}x^i + a_{i2}x^i y + a_{i3}yx^{i+1} + a_{i4}yx^{i+2}y \right) \tag{4.8}$$

with a finite number of non-zero coefficients. Here $a_{ij} \in k$ are the coefficients from the base field k. We call this form a canonical form of an element. Any other element of an algebra which is not of this form can be rewritten in such a form using the relations of the algebra.

Indeed, $x^2y^2 + yxyx + yx^2y \to x^2 \cdot 0 + 0 \cdot 0 + yx^2y = 0$, since $y^2 \to 0,\ yx \to 0,\ xy \to 0$. So element $x^2y^2 + yxyx + yx^2y$ can be rewritten in a canonical form as yx^2y.

However, we haven't explained in this example how we actually came up with the normal form that we presented. In this particular example it was enough to find it by considering monomials xx, xy, yx, yy and the reduction that we have to do using the relations. However, if we had some more complicated relations than just monomial relations, as we'll see in 4.2, we need to do some additional work before finding the canonical form.

4.2 Gröbner basis

It is of interest to us because of multiple of reasons. One of them is that it helps to find a canonical form of an element for a finitely presented algebra. It is also applied in quite a few cryptographic protocols [20]. Finally, it is even used to study the growth of algebra. However, this subject is very wide nowadays and beyond the scope of this thesis, even in the commutative case, so we try here to give a brief exposition by considering an example, and relate the reader to literature for more details, for example book by Graaf [9], or [17].

We are interested to see how fast a specific algebra grows, because we'll need it in computational applications later on. The slower the growth of algebra, the better in terms of speed, but there is a trade-of between how many useful properties of faster growing algebras can we retain.

Given a finitely presented algebra, if a Gröbner basis exists, then we have a canonical form, growth, and eventually an application in cryptography.

Definition 4.9. Consider G to be a set of generators for the ideal I in the free associative algebra $k\langle X\rangle$. Then G is a **Gröbner basis** for I if for every nonzero element $f \in I$ there is a generator $g \in G$ such that $LM(g)$ is a subword of $LM(f)$.

Having a set of generators satisfying this property is useful because, according to Theorem 5.3 in [17], there is an algorithm, by which we can compute the unique normal form of $f \in k\langle X\rangle$

modulo I, $NF_I(f)$.

Furthermore, making use of what is called a Diamond lemma, it can be shown how to compute actual Gröbner basis G for the ideal I (Theorem 6.5 in [17]).

In the next example we will explain what the main steps in calculating the Gröbner basis for a specific ideal are.

Example 4.10. We will be considering the algebra

$$A_2 = k\langle x, y\rangle/(y^2, x^2y + xyx + yx^2) \tag{4.9}$$

Let $I = (y^2, x^2y + xyx + yx^2)$ be the ideal in $k\langle x, y\rangle$. We will find it's Gröbner basis for deglex ordering $y \prec x$.

Firstly, we will find the possible overlaps of the leading terms of the generators. The leading terms are y^2, x^2y, and there are two overlaps, i.e. $y^3 = y^2 \cdot y = y \cdot y^2$ and $x^2y^2 = x^2y \cdot y = x^2 \cdot y^2$.

More generally, in this example we have $I = (g_1, g_2)$, and $u_1LT(g_1) = u_1vu_2 = LT(g_1)u_2$, where $u_1 = u_2 = y$, and $w_1LT(g_1) = w_1ww_2 = LT(g_2)w_2$ with $w_1 = x^2$, $w_2 = y$.

Then we calculate the so-called S-polynomials:

$$u_1g_1 - g_1u_2 = y \cdot y^2 - y^2 \cdot y = 0$$

and

$$\begin{aligned} w_1g_1 - g_2w_2 &= x^2y^2 - (x^2y + xyx + yx^2)y \\ &= -xyxy - yx^2y \\ &\to -xyxy + y(xyx + yx^2) \\ &= -xyxy + yxyx \\ &\to -xyxy + yxyx \\ &\to xyxy - yxyx \end{aligned}$$

The new polynomial has leading term $xyxy$, which creates three new pairs: $xyxy^2 = xyxy \cdot y = xyx \cdot y^2$, $x^2yxy = x \cdot xyxy = x^2y \cdot xy$, $xyxyxy = xyxy \cdot xy = xy \cdot xyxy$. Then the S-polynomials are:

$$xyxy(y^2) - (xyxy - yxyx)y = yxyxy \to y^2xyx \to 0,$$

$$\begin{aligned} &(x^2y + xyx + yx^2)xy - x(xyxy - yxyx) \\ &= xyx^2y + yx^3y + xyxyx \\ &\to -xyxyx - yx^2yx - yxyx^2 + yxyx^2 \\ &\to -yxyx^2 + yxyx^2 \\ &= 0 \end{aligned}$$

and

$$\begin{aligned} & xy(xyxy - yxyx) - (xyxy - yxyx)xy \\ & = yxyx^2y \\ & \to -yxyxyx \\ & \to 0 \end{aligned}$$

Therefore, all the new S-polynomials have been reduced to zero, and the Gröbner basis for the ideal I is

$$G = \{y^2, x^2y + xyx + yx^2, xyxy - yxyx\}$$

Furthermore, when we have calculated the Gröbner basis, we can attempt to describe the normal words, i.e. how would a normal form of an element $f \in k\langle X\rangle$ modulo I would look like.

In general, a monomial might begin with one of the combinations xx, xy, yx, yy.

The last one, $yy = y^2$, clearly can not occur in the normal word, since y^2 is a leading monomial of on of the generators in G.

First one, xx can not be followed by y (since we have a leading monomial x^2y), therefore it has to be followed by x, which then has to be followed by another x, giving a normal monomial x^n of length n.

Second one, xy, has to be followed by x, then x again, since $xyxy$ is not allowed, and it has to be followed by x again since x^2y is not allowed, giving xyx^{n-2} of length n.

For yx, we have yx^{n-1} and $yxyx^{n-3}$.

Therefore, the normal form for $f \in k\langle X\rangle/I$ can be written as

$$f = \sum_{i=0}^{\infty} a_{i1}x^i + a_{i2}xyx^i + a_{i3}yx^i + a_{i4}yxyx^i$$

However, we are not always lucky to get a finite Gröbner basis. The next example is of an ideal in $k\langle x, y\rangle$ which does not have a finite Gröner basis.

Example 4.11. Consider algebra

$$A = k\langle x, y\rangle/(xyx, yxy, x^2y + yx^2)$$

with deglex ordering $y \prec x$.

The leading monomials are clearly xyx, yxy and x^2y.

We first find that the only two overlaps giving a non-zero S-polynomials are $xyx \cdot xy =$

$xyx^2y = xy \cdot x^2y$ and $x^2y \cdot x = x^2yx = x \cdot xyx$. It gives us the non-zero S-polynomials

$$xy(x^2y + yx^2) - xyx^2y = xy^2x^2$$

and

$$x^2yx - (x^2y + yx^2)x \to yx^3$$

These polynomials gives us another overlap $xy^2 \cdot x^2y$, producing a non-zero S-polynomial,

$$xy^2(x^2y + yx^2) - xy^2x^2y = xy^3x^2$$

Then, by induction, we can find S-polynomials xy^nx^2, $n \geq 2$. In this case, the Gröbner basis for the ideal I is

$$G = \{xyx, yxy, x^2y + yx^2, yx^3, xy^2x^2, \ldots, xy^nx^2, \ldots\}$$

4.3 Growth of algebras

When we multiply two elements of an algebra, we are interested in how big the number of monomials in the normal form of the resulting element is.

Example 4.12. If we consider $k[x, y]$, then, taking $(x + y)$ to various degrees, we have

$$(x + y)^2 = x^2 + xy + yx + y^2 = x^2 + 2xy + y^2$$

$$(x + y)^3 = x^3 + 3x^2y + 3xy^2 + y^3$$

And continuing this, we see that the growth of this commutative algebra in two variables is linear, $n + 1$.

Example 4.13. It turns out that free associative algebra in two variables $k\langle x, y\rangle$ is of quadratic growth, since, for example

$$(x + y)^2 = x^2 + xy + yx + y^2$$

and the number of monomials grows as n^2.

4.4 Gelfand-Kirillov's dimension

We can't just take random elements of an algebra and look at their powers in general case. There is a nice too, called the Gelfand-Kirillov's dimension, which can be used to understand the growth

of an algebra [22].

Given a field k and a finitely generated k-algebra A, **Gelfand-Kirillov (GK) dimension** of A is defined to be

$$GK\dim(A) := \lim_{n\to\infty} \frac{\log(\dim V^n)}{\log n} \tag{4.10}$$

where V, a finite-dimensional subspace of A, generates k-algebra A.

It turns out, that the only possible numbers for Gelfand-Kirillov dimension are 0, 1, 2, or any real number greater than two [22]. Algebras with dimension 0 are finite dimensional algebras. Algebra of dimension 2 is, for example, the first Weyl algebra.

Finitely generated algebras of Gelfand-Kirillov dimension one satisfy a polynomial idenity [10], and are called polynomial identity algebras (PI-algebras). There's a book written on this topic [21].

Furthermore, it is known that if k is algebraically closed field and A is an integral domain (no zero divisors), then A is in fact commutative [26]. Therefore, in order to consider non-commutative algebras, we'll have to allow for zero divisors to exist. This motivates the introduction of monomial relations that the use for the algebras we are considering.

Example 4.14. Here we will consider the algebra A_2 (Example 4.8) in two indeterminates x and y, and three relations, $y^2 = xyx = yxy = 0$ over a field k. Clearly, this algebra is non-commutative, since

$$[x, y] = xy - yx \neq 0 \tag{4.11}$$

Also, from the three relations of the algebra it follows that y, xy and yx are zero divisors.

Furthermore, we can easily find a growth function for this algebra. Consider a subspace

$$V = k + kx + ky \tag{4.12}$$

Then $A = \bigcup_{n=0}^{\infty} V^n$, where $V^0 = k$.

When $n \geq 3$, there are $4n - 3$ monomials that appear in V^n, in particular

$$1,\ y,\ xy, \ldots,\ x^{n-1}y,\ yx,\ \ldots,$$
$$yx^{n-1},\ yx^2y, \ldots,\ yx^{n-2}y$$

Therefore, $\dim V^n = 4n - 3$, and

$$GK\dim(A) = \lim_{n\to\infty} \frac{\log(4n-3)}{\log n} = 1 \tag{4.13}$$

Example 4.15. Algebra $A_3 = k\langle\, x, y \mid y^2, x^2y + xyx + yx^2\rangle$ (from Example 4.10) is of slow growth.

This algebra was already considered when giving an example of the Gröbner basis. Take $V_3 = k + kx + ky$, then the only monomials in V_3^n are clearly

$$1,\ x, \ldots, x^n,\ y, \ldots,\ yx^{n-1},\ xy, \ldots,\ xyx^{n-2},\ yxy, \ldots,\ yxyx^{n-3}$$

therefore, $\dim V_3^n = 4n - 2$. Then

$$GK\dim A_3 = \lim_{n\to\infty} \frac{\log(4n-2)}{\log n} = \lim_{n\to\infty} \frac{4n}{4n-2} = 1$$

Example 4.16. In addition, we have found the following algebras to be of slow growth:

$$A_4 = k\langle\, x, y \mid y^2 = xyxy = yxyx = x^2yx^2 = xyx^2 = 0\,\rangle \tag{4.14}$$

$$A_5 = k\langle\, x, y \mid y^3 = xyx = y^2xy = yxy = yxy^2 = y^2x = 0\,\rangle \tag{4.15}$$

$$A_6 = k\langle\, x, y \mid yxy = xyx = y^2x = xy^2 = 0\,\rangle \tag{4.16}$$

These algebras have have monomial ideals, hence calculation of the Gröbner basis for them does not introduce any new relations. Therefore it is easy to find the generating monomials in the case of each of these algebras.

Consider the algebra A_4 and it's subspace $V_4 = k + kx + ky$. The only monomials which appear when we calculate V_4^n, when $n \geq 5$, are

$$1,\ x, \ldots, x^n,\ y,\ xy, \ldots,\ x^{n-1}y,\ yx, \ldots,\ yx^{n-1},\ yxy, \ldots,\ yx^{n-2}y,\ x^2yx,$$
$$\ldots,\ x^{n-2}yx,\ yx^2yx, \ldots,\ yx^{n-3}yx,$$

therefore, $\dim V_4^n = 6n - 9$. Then

$$GK\dim A_4 = \lim_{n\to\infty} \frac{\log(6n-9)}{\log n} = \lim_{n\to\infty} \frac{6n}{6n-9} = 1$$

Consider the algebra A_5 and it's subspace $V_5 = k + kx + ky$. Only monomials in V_5^n, when $n \geq 4$, are

$$1,\ x, \ldots, x^n,\ y,\ xy, \ldots,\ x^{n-1}y,\ yx, \ldots,\ yx^{n-1},\ yx^2y, \ldots,\ yx^{n-2}y,\ yx^2y^2, \ldots,\ yx^{i-3}y^2$$

therefore, $\dim V_5^n = 5n - 7$. Then

$$GK\dim A_5 = \lim_{n\to\infty} \frac{\log(5n-7)}{\log n} = \lim_{n\to\infty} \frac{5n}{5n-7} = 1$$

Consider the algebra A_6 and it's subspace $V_6 = k + kx + ky$. The only monomials, that appear in V_3^n, when $n \geq 4$, are

$$1,\ x, \ldots, x^n,\ y, \ldots,\ y^n,\ xy, \ldots,\ x^{n-1}y,\ yx, \ldots,\ yx^{n-1},\ yx^2y, \ldots,\ yx^{n-2}y$$

therefore, $\dim V_6^n = 5n - 4$. Then

$$GK\dim A_6 = \lim_{n\to\infty} \frac{\log(5n-4)}{\log n} = \lim_{n\to\infty} \frac{5n}{5n-4} = 1$$

Hence, algebras $A_4,\ A_5,\ A_6$ are indeed of the slow growth.

4.5 Center

In this section we present as well a few important properties of the center and the centralizer in specific finitely presented algebras.

Theorem 4.17. *The center of algebra $A_2 = k\langle x, y\rangle/(y^2,\ xyx,\ yxy)$, i.e. the elements that commute with all elements of an algebra, is*

$$Z(A_2) = \{b_0 + \sum_{i=1}^{\infty} b_i y x^{i+1} y |\ b_i \in k\} \tag{4.17}$$

Proof. Consider how the center acts on an arbitrary element of $w \in A_2$. First, we note that w can be written as

$$w = \sum_{i=0}^{\infty} \left(a_{i1}x^i + a_{i2}x^i y + a_{i3} y x^{i+1} + a_{i4} y x^{i+2} y\right) \tag{4.18}$$

and all the monomials of w commute with $yx^{i+2}y$ when $i \neq 0$:

$$\left[x^i, yx^{i+2}y\right] = x^i y x^{i+2} y - y x^{i+2} y x^i = 0$$

because we have a relation $xyx = 0$.

$$\left[x^i y, yx^{i+2}y\right] = x^i y^2 x^{i+2} y - yx^{i+2} yx^i y = 0$$

because $y^2 = 0$ and $xyx = 0$

$$\left[yx^{i+1}, yx^{i+2}y\right] = yx^{i+1} yx^{i+2} y - yx^{i+2} yx^{i+1} = 0$$

because $xyx = 0$.

Then, calculating the commutator, we have

$$\left[w, b_0 + \sum_{i=1}^{\infty} b_i yx^{i+1}y\right] = [w, b_0] + \left[w, \sum_{i=1}^{\infty} b_i yx^{i+1}y\right] =$$
$$= 0 + w\sum_{i=1}^{\infty} b_i yx^{i+1}y - (\sum_{i=1}^{\infty} b_i yx^{i+1}y)w = 0$$

Therefore, we have a subset relation to one direction:

$$\{b_0 + \sum_{i=1}^{\infty} b_i yx^{i+1}y \mid b_i \in k\} \subseteq Z(A_2) \tag{4.19}$$

Conversly, consider what elements commute with the generators x and y. From

$$[w, x] = 0 \tag{4.20}$$

we have that

$$a_{i2}(x^i yx - x^{i+1}y) = 0$$

from which it follows that $a_{i2} = 0$ and

$$a_{i3} yx^{i+2} = 0$$

from which it follows that $a_{i3} = 0$ for all i.

From

$$[w, y] = 0 \tag{4.21}$$

we have that

$$a_{i1}(yx^i y) = 0$$

from which it follows that $a_{i1} = 0,\ i \neq 0$.

But since $Z(A_2)$ must commute with all elements, it has to commute both with x and y. Therefore we must have each a_{i1}, a_{i2}, a_{i3} except possibly a_{01} be zero. Hence

$$Z(A_2) \subseteq \{b_0 + \sum_{i=1}^{\infty} b_i y x^{i+1} y |\ b_i \in k\} \tag{4.22}$$

and therefore

$$Z(A_2) = \{b_0 + \sum_{i=1}^{\infty} b_i y x^{i+1} y |\ b_i \in k\} \tag{4.23}$$

□

We could perform similar calculation to find the center for the other finitely presented algebras. We already presented the center of the first Weyl algebra in the section about canonical forms.

In general, it might not be easy to find normal forms. We might firstly want to have a normal form for an element and then we would have to check if any of the monomials commutes with all other monomials. If one of them does then the center will be bigger than the field k.

4.6 Centralizer

In order to apply the algebra of Gelfand-Kirillov one or two (in case of Weyl algebra) to Shpilrain-Ushakov protocol, we need to find a subalgebra which would commute with a particular element $v \in A$. For this we prove a simple property:

Theorem 4.18. *For A - a finitely presented algebra over field k, with $v \in A$, we have*

$$k[v] \subseteq C(v)$$

Proof.

$$[v, k[v]] = v \sum_{k=0}^{\infty} a_k v^k - \sum_{k=0}^{\infty} a_k v^k v =$$
$$= \sum_{k=0}^{\infty} a_k v^{k+1} - \sum_{k=0}^{\infty} a_k v^{k+1} = 0,$$

therefore, $k[v] \subseteq C(v)$.

□

The same property holds even if we change the field k with the center of an algebra $Z(A)$. Therefore, in the cases where we know what the center of an algebra is, we can calculate much bigger parts of centralizer, if not all of it. (At the point of writing this we are not aware of result with inequality to the other direction for the centralizer).

Here we give an example for a particular algebra, depicting a calculation with a part of it's centralizer.

Example 4.19. Let $k = \mathbb{Z}_7$, and $X = x^2y + xy$. Then $W = 2 + X + 2X^2 \in C_X$. Indeed,

$$\begin{aligned}[W, X] &= [2 + X + 2X^2, x^2y + xy] \\ &= [2 + (x^2y + xy) + 2(x^2y + xy)(x^2y + xy), x^2y + xy] \\ &= 0\end{aligned}$$

Therefore, we have found a nice way how to calculate the centralizer in the finitely presented algebras. Since those algebras are of slow growth additionaly, taking X to various powers does not introduce too many monomials, therefore we can try to apply this in a cryptographic protocol.

5 Cryptographic preliminaries

In this thesis we are considering one of the tools from cryptography, the key exchange problem. This problem deals with ways of how to exchange keys or information between two parties so that no one else can obtain a copy of it.

Alice and **Bob** will be the main participants in the exchange, with the ultimate goal for both Alice and Bob to share the same common secret key, so that no-one else would know it.

The secret private key can then used in transmitting messages between the two parties in the public/private key cipher algorithms, where the encryption key is public, and the decryption key is the one that only Alice and Bob knows.

While searching for efficient and secure cryptographic protocols, a few authors came up with key establishment protocols based on hard problems from combinatorial theory, such as conjugacy search problem [12], subgroup membership search problem [14], homomorphism search problem [13] or decomposition search problem [15].

5.1 Computational problems

The main computational problem considered in this thesis is the decomposition problem:

Definition 5.1. Decomposition problem: given two elements ω, ω_1 of the platform group G, and two subgroups $A, B \subseteq G$, find elements $a \in A$ and $b \in B$ such that $\omega_1 = a\omega b$.

In 2005, Shpilrain and Ushakov continued the research in decomposition problem by publishing a paper presenting a key establishement protocol based on the non-commutative groups [4].

They suggested improvements on the straightforward arrangement of a key establishement protocol, which assumes that $ab = ba$ for all $a \in A, b \in B$ [15]. Firstly, they suggested choosing subgroups A and B as subgroups of a **centralizers** of a certain element $a_1, b_2 \in G$, i.e. $A \subseteq C_G(a_1)$, $B \subseteq C_G(b_2)$.

Having privately chosen a_1, Alice publishes A, and similarly, having privately chosen b_2, Bob publishes B. Alice then chooses an element $a_2 \in B$ and sends $w_1 = a_1 w a_2$ to Bob, and Bob chooses $b_1 \in A$ and sends $w_2 = b_1 w b_2$ to Alice.

Then, while observing this exchange, the adversary must find a_1, a_2 such that $w_1 = a_1 w a_2$, where $a_2 \in A$, but does not explicitly know what set to choose a_1 from. Therefore, the adversary would have to calculate something like centralizer $C_G(B)$, since then $a_1 \in C_G(B)$, usually a hard

problem.

5.2 Shpilrain-Ushakov's Key Exchange Protocol

Here we present a formal description of Shpilrain-Ushakov's key exchange protocol. Firstly, Alice and Bob agree on a public elements $w \in G$.

1. Alice picks an element $a_1 \in G$, which is of length l, and chooses a subgroup of $C_G(a_1)$, then publishing it's generators $A = \{\alpha_1, \ldots, \alpha_k\}$.

2. Bob picks an element $b_2 \in G$, which is of length l, and chooses a subgroup $C_G(b_2)$, then publishing its generators $B = \{\beta_1, \ldots, \beta_m\}$.

3. Alice picks a random a_2 from $span(\beta_1, \ldots, \beta_m)$, and sends the normal form $P_A = N(a_1 w a_2)$ to Bob.

4. Bob picks a random b_1 from $span(\alpha_1, \ldots, \alpha_k)$ and sends normal form $P_B = N(b_1 w b_2)$ to Alice.

5. Alice calculates $K_A = a_1 P_B a_2$

6. Bob calculates $K_B = b_1 P_A b_2$

   Since $a_1 b_1 = b_1 a_1$ and $a_2 b_2 = b_2 a_2$, we have the secret shared key $K = K_A = K_B$.

For their original protocol, Shpilrain-Ushakov suggested using braid group B_n as a platform group, with $n = 64$ and $l = 1024$, and using an algorithm to calculate centralizers from the article [16].

Then it is stated that the platform group should satisfy 6 properties in order for the protocol to be efficient and secure:

1. G has to be a non-commutative group, having exponential growth, i.e. the number of elements of length n in G has to be exponential in n,

2. Calculation of the normal forms for elements of G should be efficient,

3. Should be computationally easy to multiply and invert on normal forms,

4. Should be computationally easy to generate pairs $a, \{a_1, \ldots, a_k\}$, s.t. $aa_i = a_i a$ for all $i = 1 \ldots k$

5. It should not be easy to compute

$$C(g_1, \ldots g_n) = C(g_1) \cap \ldots \cap C(g_k) \tag{5.24}$$

6. Even if $K = C(g_1, \ldots, g_n)$ has been found, should be difficult to find $x \in K$, $y \in K_1$ such that $xwy = w'$, where K_1 is a subgroup fixed by a generating set.

There has been a lot of interest in this protocol, and very recently a linear decomposition attack was proposed for such a protocol with a group as a platform in [25]. This shows that there is still research being done for this protocol and it is not yet known what is the best platform, therefore with our ideas we are trying to understand better this prospective field.

6 Application to Key exchange protocol

6.1 New ideas

So far, we have mainly considered the algebras A_1 (Definition 4.5), A_2 (Example 4.8), A_3 (Example 4.10), and A_4, A_5, A_6 (Example 4.16).

Since in each of these algebras we have a canonical form of an element, and since we have proved a centralizer property, we are ready in this section to make a generalization of the Shpilrain-Ushakov's key exchange protocol to these finitely presented algebras. We will use these algebras as platform algebras for Shpilrain-Ushakov's protocol.

In analogy with Shpilrain-Ushakov's suggestion, we would choose $C = k[a_1] \subseteq C_{a_1}(A)$ and $D = k[b_2] \subseteq C_{b_2}(A)$. Alice will choose an element a_1 from the algebra A, and choose an element $v \in k[a_1] \subseteq C_{a_1}(A)$ to send to Bob. Bob would choose an element out of $k[v]$. This can of course be generalized by choosing to send more generators from the centralizer, or using the center of the algebra instead of the field k to choose the constants.

Outline

Choose random $u \in A$.

1. Alice chooses $a_1 \in A$ (private), and sends random $v \in k\,[a_1]$ to Bob;
2. Bob chooses $b_2 \in A$ (private), and sends random $w \in k\,[b_2]$ to Alice;
3. Alice chooses $a_2 \in k\,[w]$, Bob chooses $b_1 \in k\,[v]$;
4. Alce sends $a_1 u a_2$ to Bob;
5. Bob sends $b_1 u b_2$ to Alice;
6. Alice computes $K_A = a_1 b_1 u b_2 a_2$
7. Bob computes $K_B = b_1 a_1 u a_2 b_2$

Notice that Alice and Bob chooses their first elements a_1, b_2 at random (preferably not too large, there's a trade-off between efficiency-security here). But the second elements, a_2, b_1 are chosen so that a_2 commutes with b_2 and a_1 commutes with b_1, since $b_1 \in C(a_1)$ and $a_2 \in C(b_2)$.

Finally,

$$K_A = a_1 b_1 u b_2 a_2 = b_1 a_1 u a_2 b_2 = K_B \tag{6.25}$$

and we conclude that Alice and Bob has a shared private key.

We start of by considering the first Weyl algebra, of which the properties we developed in the previous section.

Example 6.1. Consider $A_1 = k\langle x, y\rangle/(yx - xy - 1)$ with $char(k) = 3$:

Choose a random $u = \mathrm{y} + 2x^2 + 2 \in A_1$

1. Alice chooses a private $a_1 = (2x + 2)\,\mathrm{y} + x^2 + x \in A$, and sends a random $v = 2 + 2a_1 + a_1^2 = (x^2 + 2x + 1)\,\mathrm{y}^2 + (x^3 + 2x^2 + 2)\,\mathrm{y} + x^4 + 2x^3 + x^2 + 2x + 1 \in k[a_1]$ to Bob;

2. Bob chooses a private $b_2 = 2\mathrm{y} + 2x + 2 \in A$, and sends a random $w = 2 + 2b_2 + b_2^2 = \mathrm{y}^2 + 2x\mathrm{y} + x^2 + 2 \in k[b_2]$ to Alice;

3. Alice chooses $a_2 = 1 + w + w^2 = \mathrm{y}^4 + x\mathrm{y}^3 + x^3\mathrm{y} + x^4 \in k[w]$;

4. Bob chooses $b_1 = v + 2v^2 = (2x^4 + 2x^3 + 2x + 2)\,\mathrm{y}^4 + (x^5 + x^4 + x^3 + x^2 + x + 1)\,\mathrm{y}^3 + (x^2 + 2x + 1)\,\mathrm{y}^2 + (x^7 + x^6 + x^4 + 2x^3 + 2x^2 + 2)\,\mathrm{y} + 2x^8 + 2x^7 + 2x^6 + 2x^5 + x^3 + x^2 + 2x \in k[v]$;

5. Alice sends
$$\begin{aligned} a_1 u a_2 = {} & (2x+2)\,\mathrm{y}^6 + \left(x^3 + x^2 + x + 1\right)\mathrm{y}^5 + \left(x^3 + 1\right)\mathrm{y}^4 + \left(2x^5 + x^4 + x^3 + 2x + 1\right)\mathrm{y}^3 \\ & + \left(x^6 + x^5 + x^4 + x^3\right)\mathrm{y}^2 + \left(x^6 + x^3\right)\mathrm{y} + 2x^8 + 2x^7 + 2x^6 + 2x^4 + x^3 \end{aligned}$$
to Bob;

6. Bob sends
$$\begin{aligned} b_1 u b_2 = {} & \left(x^4 + x^3 + x + 1\right)\mathrm{y}^6 + \left(2x^6 + 2x^5 + x^3 + 2x^2 + 2\right)\mathrm{y}^5 + \left(x^6 + 2x^5 + 2x^3 + x^2 + x\right)\mathrm{y}^4 \\ & + \left(x^8 + x^7 + 2x^6 + x^5 + x^3\right)\mathrm{y}^3 + \left(x^9 + x^8 + 2x^6 + 2x^3 + x^2 + 1\right)\mathrm{y}^2 \\ & + \left(2x^9 + x^8 + 2x^5 + x^4 + 2x^3 + x^2 + 2\right)\mathrm{y} + 2x^{11} + x^{10} + 2x^8 + x^7 + x^6 + x^5 + 2x + 1 \end{aligned}$$
to Alice;

7. Alice calculates
$$\begin{aligned} K_A = {} & a_1 b_1 u b_2 a_2 \\ = {} & \left(2x^5 + x^4 + 2x^3 + 2x^2 + x + 2\right)\mathrm{y}^{11} + \left(x^7 + 2x^6 + x^5 + x^4 + 2x^3 + x^2\right)\mathrm{y}^{10} \\ & + \left(2x^6 + 2x^5 + x^4 + x^3 + 2x^2 + x + 2\right)\mathrm{y}^9 + \left(x^9 + x^8 + 2x^6 + 2x^5 + x^4 + 2x^3 + 2x^2 + 2\right)\mathrm{y}^8 \\ & + \left(x^9 + 2x^8 + x^7 + x^6 + x^4 + x + 2\right)\mathrm{y}^7 + \left(x^{11} + 2x^9 + x^8 + 2x^7 + x^5 + 2x^4 + 2x^2 + 2x\right)\mathrm{y}^6 \\ & + \left(x^{11} + 2x^{10} + x^9 + x^8 + 2x^7 + 2x^4 + x^2 + x + 2\right)\mathrm{y}^5 \\ & + \left(2x^{13} + x^{12} + 2x^{11} + 2x^{10} + x^9 + 2x^8 + 2x^7 + 2x^4 + x^3 + 2x^2 + x\right)\mathrm{y}^4 \\ & + \left(x^{12} + x^{11} + 2x^{10} + 2x^9 + 2x^7 + x^5 + 2x^4 + x + 2\right)\mathrm{y}^3 \\ & + \left(2x^{15} + 2x^{14} + x^{12} + x^{11} + 2x^{10} + x^8 + 2x^7 + x^6 + x^5 + x^4 + 2x^3\right)\mathrm{y}^2 \\ & + \left(2x^{15} + x^{14} + 2x^{13} + 2x^{12} + x^{10} + x^7 + 2x^6 + 2x^5 + x^4\right)\mathrm{y} \\ & + 2x^{17} + x^{15} + 2x^{14} + x^{13} + x^{11} + x^{10} + 2x^9 + 2x^8 + x^4 + 2x^3 \end{aligned}$$

8. Bob calculates

$$
\begin{aligned}
K_B &= b_1 a_1 u a_2 b_2 \\
&= \left(2x^5 + x^4 + 2x^3 + 2x^2 + x + 2\right) \mathrm{y}^{11} + \left(x^7 + 2x^6 + x^5 + x^4 + 2x^3 + x^2\right) \mathrm{y}^{10} \\
&\quad + \left(2x^6 + 2x^5 + x^4 + x^3 + 2x^2 + x + 2\right) \mathrm{y}^9 + \left(x^9 + x^8 + 2x^6 + 2x^5 + x^4 + 2x^3 + 2x^2 + 2\right) \mathrm{y}^8 \\
&\quad + \left(x^9 + 2x^8 + x^7 + x^6 + x^4 + x + 2\right) \mathrm{y}^7 + \left(x^{11} + 2x^9 + x^8 + 2x^7 + x^5 + 2x^4 + 2x^2 + 2x\right) \mathrm{y}^6 \\
&\quad + \left(x^{11} + 2x^{10} + x^9 + x^8 + 2x^7 + 2x^4 + x^2 + x + 2\right) \mathrm{y}^5 \\
&\quad + \left(2x^{13} + x^{12} + 2x^{11} + 2x^{10} + x^9 + 2x^8 + 2x^7 + 2x^4 + x^3 + 2x^2 + x\right) \mathrm{y}^4 \\
&\quad + \left(x^{12} + x^{11} + 2x^{10} + 2x^9 + 2x^7 + x^5 + 2x^4 + x + 2\right) \mathrm{y}^3 \\
&\quad + \left(2x^{15} + 2x^{14} + x^{12} + x^{11} + 2x^{10} + x^8 + 2x^7 + x^6 + x^5 + x^4 + 2x^3\right) \mathrm{y}^2 \\
&\quad + \left(2x^{15} + x^{14} + 2x^{13} + 2x^{12} + x^{10} + x^7 + 2x^6 + 2x^5 + x^4\right) \mathrm{y} \\
&\quad + 2x^{17} + x^{15} + 2x^{14} + x^{13} + x^{11} + x^{10} + 2x^9 + 2x^8 + x^4 + 2x^3 \,;
\end{aligned}
$$

We see that the keys match, i.e. $K_A = K_B$

Example 6.2. For the other algebra A_2, we will consider a simple example of this protocol with a small characteristic $char(k) = 3$.

Choose $u = 2x^2 + xy$. Then:

1. Alice chooses $a_1 = x^2y + x^2 \in A$ (private), and sends random $v = x^4y + x^4 + 2x^2y + 2x^2 + 2 \in k\,[a_1]$ to Bob;

2. Bob chooses $b_2 = yx^2y + x^2y + 2x \in A$ (private), and sends random $w = x^3y + yx^2y + x^2y + 2x^2 + 2x + 1 \in k\,[b_2]$ to Alice;

3. Alice chooses $a_2 = x^5y + 2x^4y + 2x^4 + 2yx^2y + x^3 + 2x^2y + x + 2 \in k\,[w]$, Bob chooses $b_1 = 2x^8y + 2x^8 + 2x^6y + 2x^6 + x^4y + x^4 + x^2y + x^2 \in k\,[v]$;

4. Alce sends $a_1 u a_2 = 2x^9y + x^8y + x^8 + 2x^7 + x^6y + 2x^5 + x^4 + 2x^3y$ to Bob;

5. Bob sends $b_1 u b_2 = x^{12}y + 2x^{11} + x^{10}y + 2x^9 + 2x^8y + x^7 + 2x^6y + x^5$ to Alice;

6. Alice computes $K_A = a_1 b_1 u b_2 a_2 = 22x^{18}y + x^{17}y + x^{17} + 2x^{16}y + 2x^{16} + 2x^{15}y + x^{15} + x^{14} + x^{11}y + x^{10}y + 2x^{10} + 2x^9y + 2x^9 + x^8y + x^8 + 2x^7$

7. Bob computes $K_B = b_1 a_1 u a_2 b_2 = 22x^{18}y + x^{17}y + x^{17} + 2x^{16}y + 2x^{16} + 2x^{15}y + x^{15} + x^{14} + x^{11}y + x^{10}y + 2x^{10} + 2x^9y + 2x^9 + x^8y + x^8 + 2x^7$

Since $K_A = K_B$, the shared key was calculated succesfuly.

6.2 Practical considerations

We are working with infinite algebras and taking elements to quite high degrees in these algebras. There is always a possibility of making the calculations very inefficient if we allow Alice and Bob to choose very big elements of an algebra in the beginning. This signals that it will be very difficult to make the protocol both practical and secure. It is also an exotic new direction of research where a lot of more research has to be done to develop an efficient and implementable protocol. Therefore we don't claim the implementation to be provably secure, rather we want to familiarise ourselves and other readers with the possible security parameters, security concerns, attacks, and continue research in this field.

We will consider here the algebra $A_6 = k\langle x, y\rangle/(y^2, xyx, yxy)$ from one of the previous examples, with the canonical form

$$w = \sum_{i=0}^{\infty} \left(a_{i1}x^i + a_{i2}x^i y + a_{i3}yx^{i+1} + a_{i4}yx^{i+2}y\right)$$

We try to fix a small prime p, for example $p = 97$. Then we take the coefficients from the finite field, i.e.

$$a_{ik} \in \mathbb{Z}_p = \{0, 1, \ldots, p-1\}$$

Then we fix $n = 5$, and consider the set of all truncated sums of a canonical form of an element of A,

$$W_n = \left\{ \sum_{i=0}^{n-1} \left(a_{i1}x^i + a_{i2}x^i y + a_{i3}yx^{i+1} + a_{i4}yx^{i+2}y\right) \mid a_{ik} \in \mathbb{Z}_p \right\} \tag{6.26}$$

The size of W_n depends on the prime p and the truncation parameter n. It is a simple calculation to find this number. We find $|W| = p^{4n}$.

Therefore, there are p^{4n} elements in our keyspace, from which we choose the public element u, and Alice chooses the element a_1, while Bob chooses the element b_2.

For practical considerations, we would like $|W|$ to be at least 2^{128}. With the parameters we already have chosen, $p = 97$, $n = 5$, this requirement is satisfied. In this case, the length of original words will have at most 20 monomials.

Next is the choice of public elements v and w. Here actually in our protocol we much simplified the Shpilrain-Ushakov's protocol in order to be able to explain by simple examples what is happening in the each step of calculation. We improve on our first protocol by choosing $v_1, \ldots, v_l$ and $w_1, \ldots, w_m$. If we know the center of an algebra, we can increase the key-space for these public

elements.

In this step it is not initially necessary to have 2^{128} elements in the key-space, as we actually need. The security concern is how easy is to solve $v = \alpha_0 + \alpha_1 a_1 + \ldots + \alpha_n a_1^n$ for a_1, when $\alpha_0, \ldots, \alpha_n$ are unknown aswell. The attempts to solve these kind of nonlinear multivariate equations are beyond the scope of this thesis and are left for the future considerations. We could assume $n = 4$ for efficient calculations for now.

Next step is to choose an a_2 from $span(w_1, \ldots, w_m)$. It should be enough to take $m = 20$, or less, if we considered the span over center, rathen than the field.

Then in the final steps we can not make any more parameter choices.

Finally, we present one of the modified protocol's outline for the algebra A_2:

Outline

Choose random $u \in W_n$, a set of truncated elements of algebra over the field $\mathbb{Z}_{97}$, with $n = 4$.

1. Alice chooses $a_1 \in W_n$ (private), and sends random elements $v_1, \ldots, v_{20} \in k\,[a_1]$ to Bob;
2. Bob chooses $b_2 \in W_n$ (private), and sends random elements $w_1, \ldots, w_{20} \in k\,[b_2]$ to Alice;
3. Alice chooses $a_2 \in span(w_1, \ldots, w_{20})$, Bob chooses $b_1 \in span(v_1, \ldots, v_{20})$;
4. Alce sends $a_1 u a_2$ to Bob;
5. Bob sends $b_1 u b_2$ to Alice;
6. Alice computes $K_A = a_1 b_1 u b_2 a_2$
7. Bob computes $K_B = b_1 a_1 u a_2 b_2$

6.3 Shpilrain-Ushakov assumptions

1. The group (in this case algebra) is of exponential growth in terms of length f elements of length n in A, and depends on the characteristic of the field k.
2. Calculating normal forms is efficient thanks to the Gröbner basis method which helped to find normal forms;
3. It's easy to multiply as we have only linear (linearly growing algebras) or quadratic (Weyl algebra) growth;

4. Easy to generate pairs $a, \{a_1, \ldots, a_k\}$ with $aa_i = a_i a$ as we can use the centralizer property;

5. We can find parts of the centralizer, but the set itself is infinite;

6. The last property, solving the decomposition problem, should be analized further, but we chose the parameters in such a way that there wouldn't be a possibility of the exaustion of the key space.

6.4 Direct attack

We could attempt a direct attack of the protocol by attacking the decomposition problem, i.e. finding such a_1 and a_2, such that $w_1 = a_1 w a_2$, where a_1 and a_2 are chosen according to Shpilrain-Ushakov's theme. Since we also have $w_2 = b_1 w b_2$, we also know that a_1 and b_1, so as a_2 and b_2 are from the same centralizers.

6.5 Decomposition problem

We at least know that we should choose key-space big enough for a_2 and b_1 so that brute-force was not possible by writing down the equations.

6.6 Other security concerns

The algebra of that we are considering is infinite dimensional, therefore it is not possible to create a faithful representation into finite dimensional matrices over the base field k, unless we consider representations into matrices over a polynomial ring. Then a matrix representation attack of this protocol would involve system of nonlinear equations - therefore a similar attack to the possible attack in the calculation of the public elements v and w that we identified.

It is of further interest to find out what are the drawbacks of this protocol against other attacks when we're applying these algebras. On our side is that there is a lot of slowly growing algebras. The downside is that there still might be a lot of things that can go wrong. For example we didn't take into the account what happens because of the nilpotency of some elements in the algebras of linear growth.

7 Generalizations

In this section we informally present the possible generalizations of the protocol and what other directions we have been trying or will try to take.

One interesesting idea to choose is to hide the characteristic of the field, or use a different characteristic when we are calculating the initial elements a_1 and b_2. This can be done since we have a big pool space for these first elements, and choosing a characteristic from a certain range would make it more difficult for the adversary to break the protocol. The downside of this is that we will have intentionally to choose larger key space initially, to satisfy the lowest possible value of p, the characteristic of the field. But since the number of elements is p^{4n}, we have quite a lot of freedom in this.

Since we have an algebra in this case, we could consider additions and multiplications for particular monomials and also take into account the nilpotent elements to make more efficient calculations.

It would also be interesting if we managed to find a different method for calculating the elements of the centralizer than the one presented here.

Another generalization would be to consider modules instead of algebras, or even consider categorical generalization as in [27].

It is left to the future considerations of this project to find the best algebra for implementations of a succesfull protocol.

Finally, we would also like to attempt applying these kind of finitely presented algebras we were considering here, in different key exchange protocols.

8 Computational algebra packages

In this work we have used three computational algebra packages to work with finitely presented algebras: Sage, Magma and GAP.

8.1 Sage

We included a package "ore_algebra" in the standart distribution of SAGE to work with the Weyl algebras [18]. Then it is easy to define the first Weyl algebra over a field of positive characteristic p, $\mathbb{Z}_p$.

```
# Field
ZP.<x> = GF(p)[]
# Weyl algebra
A.<Dx> = OreAlgebra(ZP)
```

Having defined the algebra, we can perform various calculations in the terminal of sage. We only have to note that we have defined `y:=Dx`.

Then we can use SAGE to do all the calculations in the example 6.1.

```
# A and B agree on a random element A_1(k)
w = 2*x^2+Dx+2

# A chooses private element of A_1(k)
A1 = x^2+2*x*Dx+x+2*Dx

# A chooses an element which belongs to a centralizer of A1
CA1 = 2+2*A1+A1^2

# B chooses private element of A_1(k)
B2 = Dx+2*x+Dx+2

# B chooses an element which belongs to a centralizer of B2
BA1 = 2+2*B2+B2^2
```

```
# A chooses an element commuting with BA1
A2 = 1+BA1+BA1^2

# B chooses an element commuting with CA1
B1 = CA1+2*CA1^2

# Calculate public element PA, PB
PA = A1*w*A2
PB = B1*w*B2

# Private keys, KA should equal KB
KA = A1*PB*A2
KB = B1*PA*B2
```

Moreover, we can choose a random element of a desired length in the Weyl algebra in order to generalise the example we calculated to a more general case.

```
# define a random element from the first Weyl Algebra
# m -  order of x, y
def weyl_element():
D = 0
for i in range(m):
for j in range(m):
D = D + GF(p).random_element()*x^(i)*Dx^(j)
return D
```

8.2 Magma

We used Magma online calculator [19] to perform calculations on more general finitely presented algebras.

There is a nice way in Magma how to define a finitely presented algebra:

```
k := GF(3);
A<x,y> := FPAlgebra<k, x, y | y^2, x*y*x*y, y*x*y*x, x^2*y*x^2 ,x*y*x^2>;
```

Then we can calculate an example of how the key exchange protocol works in the algebra

$$A = k\langle x, y\rangle/(y^2, xyxy, yxyx, x^2yx^2, xyx^2)$$

```
// choose a random element of an algebra A
u:=2*x^2+x*y+y^4;
 u;
//Alice choose a1
a1:=x^2+x^2*y+y*2;
//Bob choose b2
b2:=2*x+2*x^2*y+y;
// Alice, element from a1 centralizer
v:= 2+2*a1+a1^2+a1^3;
// Bob, element from  b2 centralizer
w:=1+b2+2*b2^2;
// Alice, element from w centralizer
a2:=2+w+2*w^2;
// Bob, element from v centralizer
b1:=1+2*v^2;
// Pa
a1*u*a2;
// Pb
b1*u*b2;
// Shared key
Ka:=b1*a1*u*a2*b2;
Kb:=a1*b1*u*b2*a2;
```

8.3 GAP

Even though Magma is very convenient computer algebra system to use for calculations with finitely presented algebras, it's online calculator has limitations of how big the calculations you can make compared to the full version of Magma. The full version of GAP, on the other hand, is freely available.

It is somehow trickier how to define a finitely presented algebra in GAP. Rather, we can do

so for ideals over free associative algebra that have a finite Gröbner basis. To this goal we are using "GBNP" package.

The definition of a free associative algebra over field F is not too complicated:

```
F:= GF(17);;
A:= FreeAssociativeAlgebraWithOne(F,"a","b");
g:= GeneratorsOfAlgebraWithOne(A);
```

Then we can define a set of generators for the ideal and transform it to a different presentation.

```
KI_GP := [g[1]^2-g[1]*g[2]];
KI:=GP2NP(KI_GP);;
```

Finally, there is a function `SGröbner`, which allows us to calculate the Gröbner basis of the ideal.

```
GB := SGrobner([KI]);
```

Then, if the Gröbner basis is finite, we can calculate a normal form for an element $f \in k\langle X\rangle$, for example $f = x^2y^2 \in k\langle x, y\rangle$, when $I = (x^2 - xy)$:

```
f:= [ [[2,2]],[1]];;
p:=StrongNormalFormNP(f,GB);
```

If there is doubt whether the Gröbner basis is finite, it is possible to calculate the truncated Gröbner basis as well, assigning weights to the generators and then producing the Gröbner basis up to a sum weight n:

```
G := SGrobnerTrunc(KI,n,weights);;
```

9 Conclusions

In this thesis, we studied the properties of various finitely presented algebras and proved a few of their properties related to the growth and centralizer.

We generalized the Shpilrain-Ushakov's protocol to the setting where we can use slowly growing finitely presented algebras as a platform.

We explained what properties do the finitely presented algebras have to satisfy if we want to use them as a platform for the protocol.

We made computer realizations for specific finitely presented algebras in three different computer algebra systems.

It remains to be seen how secure the protocol is against various innovative attacks and what is the trade-off between the slowness of growth in the algebra and the security parameters.

Acknowledgments

I thank my advisor, Eligijus Sakalauskas, for his support and time devoted to helping me understand the ideas developed in the thesis, I thank Victor Ufnarovski, who helped me to motivate myself to finally understand the meaning of Gröbner basis, to Vytautas Jakutis, who was my fellow student working on Weyl algebras, to Alexei Michalkovich, who helped to distinguish right ideas from wrong ideas in the seminars, to the late Gediminas Simonas Dosinas, who first introduced me to a theory of Weyl Algebras in the summer two years ago.

References

[1] Lam, T. Y. *A First Course in Noncommutative RingsSpringer-Verlag*. New York, 1991.

[2] Roiter, Andrei, *Representations of finite-dimensional algebras*, Vol. 73.,Springer Science and Business Media, 1997.

[3] Guccione, Jorge A.; Juan J. Guccione; Christian Valqui. *On the centralizers in the Weyl algebra*. arXiv preprint arXiv:0912.5202, 2009.

[4] Shpilrain, Vladimir; Alexander Ushakov. *A new key exchange protocol based on the decomposition problem*. arXiv preprint math/0512140, 2005.

[5] Etingof, Pavel I., et al. *Introduction to representation theory*. Vol. 59. American Mathematical Soc., 2011.

[6] Zhang, Jiangfeng; Jianghua Zhang. *On the representation of derivative algebras in characteristic* $p > 0$. Illinois Journal of Mathematics 46.1, 2002. 45-61.

[7] Thomas Hungerford. *Abstract Algebra: An Introduction*. Cengage Learning. ISBN 1-285-41497-7, 2012.

[8] Piontkovski, Dmitri. *A remark on Golod–Shafarevich algebras*. arXiv preprint arXiv:1412.8601, 2014.

[9] W. A. de Graaf. *Lie Algebras: Theory and Algorithms* . North-Holland Mathematical Library, 56. North-Holland Publishing Co., Amsterdam, 2000.

[10] Small, Lance.*W. Rings satisfying a polynomial identity*. No. 5. Fachbereich Mathematik, Universität Essen, 1980.

[11] Sharifi, Yaghoub. *Centralizers in associative algebras*. Diss. Science: Department of Mathematics, 2013.

[12] I. Anshel; M. Anshel; D. Goldfeld. *An algebraic method for public-key cryptog- raphy*. Math. Res. Lett. 6 , 1999. 287.

[13] Grigoriev, Dima; Ilia Ponomarenko. *Homomorphic public-key cryptosystems and encrypting boolean circuits*. Applicable Algebra in Engineering, Communication and Computing 17.3-4, 2006. 239-255.

[14] Shpilrain, Vladimir; Gabriel Zapata. *Using the subgroup membership search problem in public key cryptography*. Contemporary Mathematics 418, 2006. 169.

[15] J. C. Cha; K. H. Ko; S. J. Lee; J. W. Han; J. H. Cheon. *An E±cient Im- plementation of Braid Groups*. ASIACRYPT 2001, Lecture Notes in Comput. Sci. 2248, 2001. 144

[16] N. Franco; J. Gonzalez-Meneses.*Computation of Centralizers in Braid groups and Garside groups*. Rev. Mat. Iberoamericana 19 (2), 2003. 367

[17] Murray Bremner. *Notes from a mini-course "Free associative algebras, noncommutative Gröbner bases, and universal associative envelopes for nonassociative structures*. [viewed on 2015-05-30]. Accesible online <http://arxiv.org/abs/1303.0920>.

[18] Manuel Kauers; Maximilian Jaroschek; Fredrik Johansson. *Ore Polynomials in Sage*, ArXiv 1306.4263, 2013.

[19] Magma Calculator. [viewed on 2015-05-30]. Accesible online: <http://magma.maths.usyd.edu.au/calc/>.

[20] Ali, Rashid; Martin Kreuzer. *Weyl Gröbner basis cryptosystems*. 2011.

[21] Drensky, Vesselin; Edward Formanek. *Polynomial identity rings*. Springer, 2004.

[22] Krause, Günter R.; Thomas H. Lenagan. *Growth of algebras and Gelfand-Kirillov dimension*. Vol. 22. American Mathematical Soc., 2000.

[23] Garber, David. *Braid group cryptography*. Braids: Introductory Lectures on Braids, Configurations and Their Applications 19, 2010. 329.

[24] Tsuchimoto, Yoshifumi. *Preliminaries on Dixmier conjecture*. Mem. Fac. Sci. Kochi Univ. Ser. A Math 24, 2003. 43-59.

[25] Myasnikov, Alexei; Vitaliĭ Romankov. *A linear decomposition attack*, Groups Complexity Cryptology 7.1, 2015, 81-94.

[26] Bell, Jason P. *Centralizers in domains of finite Gelfand–Kirillov dimension*. Bulletin of the London Mathematical Society, 2009.

[27] Inassaridze, Nick, Tamaz Kandelaki, Manuel Landra. *Categorical interpretations of some key agreement protocols*. Journal of Mathematical Sciences 195.4, 2013, 439-444.