Universitatea “Alexandru Ioan Cuza” din Iaşi
Facultatea de Informatică

LUCRARE DE LICENŢĂ

Multilinear Maps over Ideal Lattices

propusă de

Student: Ciprian Băetu
Coordonator ştiinţific: Prof. Dr. Ferucio Laurenţiu Ţiplea

Sesiunea: iunie - iulie
2017

Universitatea “Alexandru Ioan Cuza” din Iaşi
Facultatea de Informatică

Multilinear Maps over Ideal Lattices

Student: Ciprian Băetu
Coordonator ştiinţific: Prof. Dr. Ferucio Laurenţiu Ţiplea

Sesiunea: iunie - iulie
2017

DECLARAŢIE PRIVIND ORIGINALITATE ŞI RESPECTAREA DREPTURILOR DE AUTOR

Prin prezenta declar că Lucrarea de licenţă cu titlul ”Multilinear Maps over Ideal Lattices” este scrisă de mine şi nu a mai fost prezentată niciodată la o altă facultate sau instituţie de învăţământ superior din ţară sau străinătate. De asemenea, declar că toate sursele utilizate, inclusiv cele preluate de pe Internet, sunt indicate în lucrare, cu respectarea regulilor de evitare a plagiatului:

- toate fragmentele de text reproduse exact, chiar şi n traducere proprie din altă limb, sunt scrise ntre ghilimele şi deţin referinţa precisă a sursei;
- reformularea în cuvinte proprii a textelor scrise de ctre alţi autori deţine referinţa precisă;
- codul sursă, imaginile etc. preluate din proiecte open-source sau alte surse sunt utilizate cu respectarea drepturilor de autor şi deţin referinţe precise;
- rezumarea ideilor altor autori precizează referinţa precisă la textul original.

Iaşi,
24 iunie 2017

Absolvent,
Băetu Ciprian

____
(semnătura în original)

DECLARAŢIE DE CONSIMŢĂMÂNT

Prin prezenta declar că sunt de acord ca Lucrarea de licenţă cu titlul "Multilinear Maps over Ideal Lattices", codul sursă al programelor şi celelalte conţinuturi (grafice, multimedia, date de test etc.) care însoţesc această lucrare să fie utilizate în cadrul Facultăţii de Informatică.

De asemenea, sunt de acord ca Facultatea de Informatică de la Universitatea Alexandru Ioan Cuza din Iaşi să utilizeze, modifice, reproducă şi să distribuie în scopuri necomerciale programele-calculator, format executabil şi sursă, realizate de mine în cadrul prezentei lucrări de licenţă.

Iaşi,
24 iunie 2017

Absolvent,
Băetu Ciprian

____

(semnătura în original)

Contents

Chapter 1

Introduction

Usually, cryptographic primitives are constructed under the assumption that several problems are intractable, i.e. there exist no polynomial-running time algorithm to solve them. Vercauteren [12] realized an extensive research regarding the intractable problems that are most used in cryptography, such as integer factoring, discrete logarithm, computational Diffie-Hellman, shortest vector problem and many others.

In the last ten years, bilinear maps proved to be very useful in cryptography. Making use of the interesting properties of such maps, cryptographers managed to construct schemes for one-round three-party key exchange [10], identity based encryption [2] and many other applications. After the moment that bilinear maps proved to be undoubtedly useful, researchers have tried to generalize the concept. Thus, multilinear maps were defined and the search for their applications has begun. Boneh and Silverberg [3] showed that symmetric multilinear maps can be used to realize a one-round multi-party key exchange scheme but, after their attempts to construct such maps failed, they drew the conclusion that ”such maps might have to either come from outside the realm of algebraic geometry, or occur as ’unnatural’ computable maps arising from geometry.”

Garg, Gentry and Halevi [7] proposed a construction based on lattices that approximate the multilinear maps in hard-discrete-logarithm groups. Using this candidate, they could construct an application to multipartite Diffie-Hellman key exchange scheme and also the first construction of Attribute-Based Encryption for general circuits [8]. A short period after the aforementioned candidate was proposed, Coron, Lepoint and Tibouchi [6] created a similar construction, based on integers instead of lattices.

However, these construction proved to be susceptible to attacks, and a devastating zeroizing attack for the integer construction is presented thoroughly in [4]. Numerous fixing tentatives of these schemes were designed, but for each of them there was found at least another attack. Therefore currently, new methods of constructing multilinear maps and Graded Encoding Schemes still constitute an open field, very interesting for cryptographers.

1.1 Contribution

This work represents a survey over the bilinear and multilinear maps and their applications. Furthermore, in this paper is presented the concept of Graded Encoding Scheme, a modality of approximating multilinear maps. The core of the paper is represented by the review of the lattice-based construction, designed by Garg, Gentry and Halevi in [7].

1.2 Organization

The paper is divised into 5 sections. First one - introduction bla-bla. In the second section, bla bla bla ... etc etc.

Chapter 2

Multilinear Maps and Graded Encoding Systems

In this chapter, multilinear maps are defined and also, the particular case of bilinear maps is discussed, along with results concerning self-bilinear applications. Thereafter, *Graded Encoding Schemes* are defined, as an approximate to multilinear maps.

Observation: Regarding the multilinear applications and Graded Encoding Systems schemes, and also for the lattice-based candidate designed in [7], the paper encompasses one subsection of efficient procedures, and another one of hardness assumptions. The reader should be aware of this detail and realize the analogy and differences of the mentioned schemes.

2.1 Bilinear Maps

As stated before, bilinear maps are a specific case of multilinear maps. They proved to be a highly useful tool in cryptography, with many applications, such as: tripartite protocol [10], identity based encryption [2] and Attribute-based encryption scheme for monotone boolean formulas [9]. In this section, bilinear maps are only defined, while next section presents a relationship between self-bilinear maps and multilinear maps.

Definition 1. (Bilinear Map [1]). *Given the cyclic groups G and G_t (written additively) of the same order p, a (symmetric) map $e : G \times G \to G_t$ is said to be bilinear if the following properties hold:*

1. ***(Bi-linearity)*** *$e({g_1}^{x_1}, {g_2}^{x_2}) = e(g_1, g_2)^{x_1 x_2}$, for any $x_1, x_2 \in \mathbb{Z}_p$ and any $g_1, g_2 \in G$;*
2. ***(Non-degeneracy)*** *If $g_1, g_2 \in G$ are generators of G, then $e(g_1, g_2)$ is a generator of G_t;*
3. ***(Efficient computability)*** *There exists a polynomially-bounded algorithm to compute $e(g_1, g_2)$, for any $g_1, g_2 \in G$.*

2.2 Cryptographic Multilinear Maps

Definition 2. (Multilinear Maps [11]). *Let $k \geq 2$ be an integer number and $G_1, G_2, ..., G_k, G_T$ be $k+1$ cyclic groups (written additively), of same order p. Then, a $k-$multilinear map is a mapping $e : G_1 \times ... \times G_k \to G_T$, with the following properties:*

1. ***(Linearity)*** *For every $g_1 \in G_1, ..., g_k \in G_k$, every $i \in \{1, 2, .., k\}$ and every $\alpha \in \mathbb{Z}_p$, it holds that:*

$$e(g_1, ..., \alpha \cdot g_i, .., g_k) = \alpha \cdot e(g_1, ..., g_k))$$

2. ***(Non-degeneracy)*** *If $g_1 \in G_1, ..., g_k \in G_k$ are generators of their respective groups, then $e(g_1, ..., g_k)$ is a generator of G_T.*

2.2.1 From Self-Bilinear to Multilinear Maps

Definition 3. *A self-bilinear map is a bilinear map where the domain and target groups are the same.*

Proposition 1. *Let G be a cyclic group of order p and $e : G \times G \to G$ be a self-bilinear map. Therefore, a $k-$multilinear map $e_k : G^k \to G$ can be constructed from e, for any $k \geq 2$.*

Proof. The proof is realized by induction. First, for the base case $k = 2$, it is trivial to observe that e itself is a 2-liniar map. Then, suppose that an $n-$multilinear map $e_n : G^n \to G$ can be constructed starting from e, and it can be easily shown that a $(n + 1)$-multilinear map $e_{n+1} : G^{n+1} \to G$ can be constructed, as follows:

$$e_{n+1}(g_1, .., g_n, g_{n+1}) = e(e_n(g_1, .., g_n), g_{n+1}), \forall g_1, .., g_{n+1} \in G.$$

Indeed, from the fact that e_n is multilinear it follows that, for any $g_1 \in G_1, ..., g_n \in G_n$, any $i \in \{1, .., n\}$ and any $\alpha \in \mathbb{Z}_p$, $e_n(g_1, ..., \alpha \cdot g_i, .., g_n) = \alpha \cdot e_n(g_1, ..., g_n))$. Using the bilinearity of e, it results that e_{n+1} respects the **linearity** condition.
Let $g_1, ..., g_n$ be generators of G. Then, using the fact that e_n is $n-$multilinear, it follows that $e_n(g_1, .., g_n)$ is also a generator of G. Corroborating the last result with the non-degeneracy property of e, it ensues that e_{n+1} respects **non-degeneracy** condition, from which the conclusion that e_{n+1} is a $(n + 1)$-multilinear map can be drawn. □

However, Cheon and Lee [5] proved that self-bilinear maps on prime order groups do not exist, except that the computational Diffie-Hellman problem is easy. That is the main motivation of [1], which analyzes the existence of self-bilinear maps on groups of composite order.

2.2.2 Efficient Procedures

In order to use the cryptographic multilinear applications in a real-world environment, efficient procedures must be designed in order to be evaluated by computers. Therefore, as specified in [7] a cryptographic multilinear map scheme is a 5-uple $\mathcal{MMP}$ = **(InstGen, EncTest, add, neg, map)**, as described below:

(a) **Instance Generation.** A procedure with a "factory" role must exist, in order to instantiate the parameters of the scheme. This procedure is **InstGen**.

- **Input:** λ - the security parameter and $k \geq 2$ - the multilinearity parameter.
- **Output:** (**params**, $g_1, .., g_k$), where **params** = $(G_1, .., G_T, p, e)$. Here $G_1, .., G_k$, G_T represent the groups, $p \in \mathbb{Z}$ is their order, e is the representation of the multilinear map and $g_i \in \{0, 1\}^*$ is the representation of a generator of G_i, for every $i \in \{1, .., k\}$.

(b) **Element Encoding.** A procedure that decides if a sequence of bits represents an encoding of an element in one of the groups must be defined, and it is named **EncTest**.

- **Input: params** - the instance parameters, $i \in \{1, .., k+1\}$ - index of the desired group and $x \in \{0,1\}^*$ - encoding of the tested element.
- **Output:** True, if x is a valid encoding of an element in G_i, False otherwise. *Note:* The extension $G_{k+1} = G_T$ is performed.

(c) **Group addition.** The procedure **add** simply applies the group operation upon two provided elements representations.

- **Input: params** - the instance parameters, $i \in \{1, .., k+1\}$ - index of the desired group, x, y - representations of elements to be added.
- **Output:** the representation of $x + y \in G_i$.

(d) **Group negation.** The procedure **neg** returns the inverse representation of the element provided as parameter.

- **Input: params** - the instance parameters, $i \in \{1, .., k+1\}$ - index of the desired group, x - representation of the element to be negated.
- **Output:** the representation of $-x \in G_i$.

(e) **Map computation.** The procedure **map** returns the representation of the multilinear mapping over the elements given as parameters.

- **Input: params** - the instance parameters, $x_1 \in G_1, .., x_k \in G_k$ - elements in domain groups.
- **Output:** the representation of $e(x_1, .., x_k) \in G_T$.

2.2.3 Hardness Assumptions

Chapter 3

Mathematical Background

Chapter 4

Proposed Encoding Scheme

Chapter 5

Security

Bibliography

[1] Ciprian Băetu, Petru Cehan, and Dan Mărculeţ. *On Bilinear Groups of Composite Order*, pages 389–398. Military Technical Academy Publishing House, 2016.

[2] Dan Boneh and Matt Franklin. *Identity-Based Encryption from the Weil Pairing*, pages 213–229. Springer Berlin Heidelberg, Berlin, Heidelberg, 2001.

[3] Dan Boneh and Alice Silverberg. Applications of multilinear forms to cryptography. *Contemporary Mathematics*, 324:71–90, 2002.

[4] Jung Hee Cheon, Kyoohyung Han, Changmin Lee, Hansol Ryu, and Damien Stehlé. *Cryptanalysis of the Multilinear Map over the Integers*, pages 3–12. Springer Berlin Heidelberg, Berlin, Heidelberg, 2015.

[5] Jung Hee Cheon and Dong Hoon Lee. A note on self-bilinear maps. *Bulletin of the Korean Mathematical Society*, 46(2):303–309, 3 2009.

[6] Jean-Sébastien Coron, Tancrède Lepoint, and Mehdi Tibouchi. *Practical Multilinear Maps over the Integers*, pages 476–493. Springer Berlin Heidelberg, Berlin, Heidelberg, 2013.

[7] Sanjam Garg, Craig Gentry, and Shai Halevi. *Candidate Multilinear Maps from Ideal Lattices*, pages 1–17. Springer Berlin Heidelberg, Berlin, Heidelberg, 2013.

[8] Sanjam Garg, Craig Gentry, Shai Halevi, Amit Sahai, and Brent Waters. *Attribute-Based Encryption for Circuits from Multilinear Maps*, pages 479–499. Springer Berlin Heidelberg, Berlin, Heidelberg, 2013.

[9] Ferucio Laurenţiu Ţiplea and Constantin Cătălin Drăgan. Key-policy attribute-based encryption for boolean circuits from bilinear maps. In *Cryptography and Information Security in the Balkans - First International Conference, BalkanCryptSec 2014, Istanbul, Turkey, October 16-17, 2014, Revised Selected Papers*, pages 175–193, 2014.

[10] Antoine Joux. *A One Round Protocol for Tripartite Diffie–Hellman*, pages 385–393. Springer Berlin Heidelberg, Berlin, Heidelberg, 2000.

[11] Ron Rothblum. On the circular security of bit-encryption. Cryptology ePrint Archive, Report 2012/102, 2012.

[12] Fré Vercauteren. Final report on main computational assumptions in cryptography.