Multilinear Maps and Possible Applications

Prastudy Fauzi

University of Tartu, Estonia
prastudy.fauzi@gmail.com

Abstract. In this research, we will do a survey on multilinear maps and analyze some parameters in the recent implementations. The student will compare the two implementations, in particular their similarities and improvements made by the more recent work. The student will then analyze some possible applications of multilinear maps for cryptography.

Keywords: multilinear maps, lattice-based cryptography

1 Introduction

Bilinear maps have been well studied in recent years, with many celebrated applications in cryptography, such as non-interactive key exchange and non-interactive zero knowledge. One hopes that multilinear maps will also create breakthroughs in these areas of cryptography. This work will analyze a recent result on a concrete multilinear maps construction [GGH12], and see how it can be applied to existing cryptographic protocols.

The layout of this text is as follows. Section 2 will discuss some preliminaries needed to better understand multilinear maps. Section 3 will discuss the main ideas of the [GGH12] multilinear maps construction, while Section 4 will compare this to the recent [CLT13] construction (We remark that [CLT13] was published during the writing of this text, and thus contains some similar observations about [GGH12]). Section 5 will discuss some possible applications of multilinear maps, and finally we give some concluding remarks in Section 6.

2 Preliminaries

We will give an overview of the mathematical concepts used in the later sections.

2.1 Basic Definitions

Elementary Number Theory. Let n be a positive integer. According to the division algorithm,there are unique values a, b such that $x = an + b, -n/2 < b \leq n/2$.
Define $x \mod n = b$, where $b \in \mathbb{Z}_n$ satisfies the above requirement. Moreover, if we have values $c = (c_1, \cdots, c_k)$, define $[c]_q = (c_1 \mod q, \cdots, c_k \mod q)$

Given two integers $a > 0, b \geq 0$ define $gcd(a, b)$ to be the largest integer d that divides both a and b. If $gcd(a, b) = 1$ we say that a and b are *relatively prime*. Moreover, n integers $a_1, a_2, \cdots a_n$ are pairwise relatively prime if for all $i \neq j$ we have $gcd(a_i, a_j) = 1$.

Theorem 1. *(Chinese Remainder Theorem)*
Consider a system of linear congruences:

$$\begin{cases} x \equiv a_1 & \mod n_1 \\ x \equiv a_2 & \mod n_2 \\ \cdots & \\ x \equiv a_k & \mod n_k \end{cases}$$

If $n_1, n_2, \cdots n_k$ are pairwise relatively prime, then there exists a solution to this system of linear congruences which is unique modulo $n_1 n_2 \cdots n_k$.

Algebraic Structures. A *group* $(G, +)$ is an algebraic structure where:

1. The operation $(+)$ is closed and associative in G,
2. There exists an identity element $0 \in G$ and inverse element $-a$ for each element $a \in G$.

If the operation $(+)$ is also commutative, we say that $(G, +)$ is an *abelian group*. For an integer n and an element $g \in G$, define ng to be the result of:

- $g + g + \cdots + g$ (n times), when $n > 0$,
- $(-g) + (-g) + \cdots + (-g)$ ($-n$ times), when $n < 0$, or
- 0, when $n = 0$.

If every element $a \in G$ can be written as $a = ng$ for some $n \in \mathbb{Z}$, we say that $(G, +)$ is a *cyclic group*. In this case, g is said to be a *generator* of the group, and we can write $G = \langle g \rangle$.
A *ring* $(R, +, \cdot)$ is an algebraic structure that satisfies the following conditions:

1. $(R, +)$ is an abelian group.
2. $(R, \cdot)$ is associative.
3. The distributive laws apply to $(R, +, \cdot)$.

We usually work with rings which are commutative and have an identity element under the operation $(\cdot)$.

Given a ring $(R, +, \cdot)$, a subset I of R is called an *ideal* if it satisfies the following conditions:

1. $(I, +)$ is a subgroup of $(R, +)$.
2. For any two elements $x \in I, r \in R$, $x \cdot r \in I$ and $r \cdot x \in I$.

For example, in the ring $R = \mathbb{Z}$, the ideal $I = 2\mathbb{Z}$ is the set of even integers.

Given $a \in R$ and an ideal I, we can define the *equivalence class*

$$[a] = \{a + x | x \in I\}.$$

Then $[a] = [b] \iff a - b \in I$. The set of all distinct equivalence classes is the *quotient ring* R/I. For example, in the ring $R = \mathbb{Z}$, with ideal $I = 2\mathbb{Z}$, the quotient ring $R/I = \mathbb{Z}/2\mathbb{Z}$ has two equivalence classes $[0] = \{\ldots, -4, -2, 0, 2, 4, \ldots\}$ and $[1] = \{\ldots, -3, -1, 1, 3 \ldots\}$.

A *field* $(F, +, \cdot)$ is a commutative ring which under $(\cdot)$ has an identity element and inverses. $(F, +, \cdot)$ is a field iff $(F, +)$ and $(F - \{0\}, \cdot)$ are both abelian groups and the distributive laws apply. We will mostly use the fields $\mathbb{Z}_q$ (where q is a prime number).

A *polynomial ring* $F[X]$ is a ring formed from a set of polynomials in the variable X, where the coefficients are from a field F. If $f(X) = a_d X^d + \cdots + a_1 X + a_0 \in F[X]$ is an irreducible polynomial, we have the quotient ring $R = F[X]/(f(X))$. Moreover, when F is the field $\mathbb{Z}_q$ we write $R_q = \mathbb{Z}_q[X]/(f(X))$. Additionally, if we have that f has degree d, then $|R_q| = q^d$.

Inner Products. Let V be an n-dimensional vector space over a field F. For $a = (a_1, \ldots, a_n)^\top, b = (b_1, \ldots, b_n)^\top \in V$, define the inner product $\langle a, b \rangle = \sum_{i=1}^{n} a_i b_i$. We will mostly use the polynomial ring $R[x] = \mathbb{Z}_q[x]/(f(x))$, where f is a monic polynomial with degree n. In this case, $a = \sum_{i=0}^{n-1} a_i x^i$, $b = \sum_{i=0}^{n-1} b_i x^i$.

Norms. Let $s = \sum_{i=0}^{d} s_i x^i$ be an element of a polynomial ring R. Define the *Manhattan norm* $\|s\|_1 = \sum_{i=0}^{d} |s_i|$, and the *Euclidean norm* $\|s\|_2 = \sqrt{\sum_{i=0}^{d} s_i^2}$. Unless otherwise stated, we will use $\|s\|$ to mean $\|s\|_2$ for an element $s \in R$.

2.2 Lattices

A *lattice* is a set of points in n-dimensional space with a periodic structure. As such, it is a discrete subgroup of $\mathbb{R}^n$ under addition of vectors in $\mathbb{R}^n$.

Let $b_1, b_2, \cdots, b_k$ be k linearly independent vectors in $\mathbb{R}^n$. Then we can define the lattice generated by these vectors as

$$L(b_1, b_2, \cdots, b_k) = \{\sum a_i b_i | a_i \in \mathbb{Z}\}$$

By this definition, $\{b_1, b_2, \cdots, b_k\}$ form a basis of this lattice, which has dimension k. Every lattice has a basis, but the basis is not unique. For example, if $\{b_1, b_2\}$ is a basis of a lattice L in $\mathbb{R}^2$ then $\{b_1, b_1 + b_2\}$ is also a basis of L. In general, if B is a basis of a lattice L of dimension n, and $U_{n \times n}$ is an integer matrix of determinant 1, then BU is also a basis of L.

A cryptographic construction using lattices can have strong provable security guarantees based on the *worst-case hardness* of lattice problems. This is done by having parameters chosen such that breaking the construction is as hard as solving lattice problems in the worst case [MR08]. One of the most efficient ones are cryptosystems based on learning with errors.

2.3 k-Graded Encoding System

A k-Graded Encoding System is a system that consists of a ring R and a family of sets $S = S_i^{(a)} : 0 \leq i \leq k$ such that [GGH12]:

1. For every index i, $a \neq b \in R$ we have $S_i^{(a)}$ and $S_i^{(b)}$ are disjoint.
2. There is an associative operation $(+)$ such that for all $u_1 \in S_i^{(a)}, u_2 \in S_i^{(b)}$ we have $u_1 + u_2 \in S_i^{(a+b)}$.
3. There is an associative operation $(\times)$ such that for all $u_1 \in S_{i_1}^{(a)}, u_2 \in S_{i_2}^{(b)}$ we have $u_1 \times u_2 \in S_{i_1+i_2}^{(a \cdot b)}$.

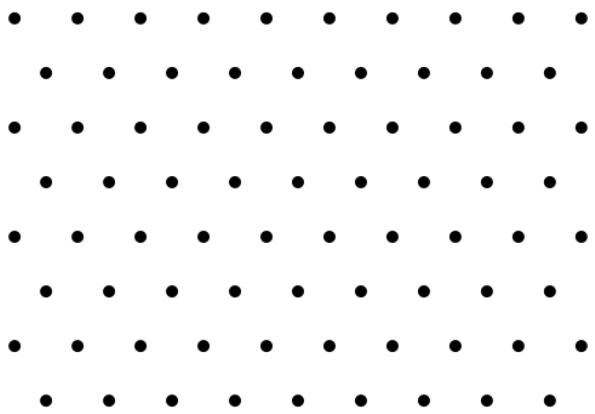

Fig. 1. 2-dimensional lattice with base $\{(1,\, 0),\, (\frac{1}{2},\, \frac{1}{2}\sqrt{3})\}$

2.4 Multilinear Maps

Let $G_1, G_2, \cdots, G_k, G_T$ be cyclic groups of the same order p, Then a k-multilinear map $e : G_1 \times G_2 \times \cdots \times G_k \to G_T$ is a function with the following properties:

1. For elements $g_i \in G_i$, $j \in \{1, 2, \cdots, k\}$ and integer a we have that
$$e(g_1, g_2, \cdots a \cdot g_j \cdots, g_k) = a \cdot e(g_1, g_2, \cdots g_k).$$
2. If the elements $g_i \in G_i$ are all generators of their groups G_i, then $e(g_1, g_2, \cdots g_k)$ is a generator of G_T.

Note that the G_i-s need not be the same. If $G_1 = G_2 = \cdots = G_k = G$, this is called the symmetric case. It has the property that for elements $g_i \in G$ we have $e(g_1, g_2, \cdots g_k) = e(g_{\tau(1)}, g_{\tau(2)}, \cdots g_{\tau(k)})$ for any permutation τ of $\{1, 2, \cdots k\}$.

A multilinear map scheme MMP consists of five procedures [GGH12]:

1. Instance Generation: Given security parameter λ and multilinear parameter κ, output $params = (G_1, G_2, \cdots, G_\kappa, G_T, p, e)$.
2. Element Encoding: Given $params$ (the output of the instance generation), $1 \leq i \leq \kappa + 1$ and $x \in \{0, 1\}^*$, check if the string x is a valid encoding of an element in G_i (or G_T for the case $i = \kappa + 1$).
3. Addition: Given $params, i$ and $x, y \in G_i$, output $x + y \in G_i$.
4. Negation: Given $params, i$ and $x \in G_i$, output $-x \in G_i$.
5. Multilinear Map: Given $params, x_1 \in G_1, \cdots, x_\kappa \in G_\kappa$, outputs $e(x_1, x_2, \cdots x_k) \in G_T$.

2.5 Hardness Assumptions

There are two main hardness assumptions related to multilinear maps, namely the difficulty of the Multilinear Discrete-log and Multilinear Decisional Diffie-Hellman problems [GGH12].

Multilinear Discrete-log (MDL) The MDL problem is hard for a scheme MMP if for all $\kappa > 1, 1 \leq i \leq \kappa$ and all polynomial-time adversaries A,

$$Pr[A(params, i, g_i, \alpha \cdot g_i) = a : (params, g_1, \cdots g_\kappa) \leftarrow InstanceGeneration(1^\lambda, 1^\kappa, \alpha \leftarrow \mathbb{Z}_p)]$$

is negligible in λ. In other words, given values $(params, i, g_i, \alpha \cdot g_i)$ the MDL assumption states that it is difficult to determine the value $\alpha \in \mathbb{Z}_p$.

Multilinear Decisional Diffie-Hellman (MDDH) Given a symmetric scheme MMP, consider the two distributions below:

1. Set $(params, g) \leftarrow InstanceGeneration(1^\lambda, 1^\kappa)$. Choose $\alpha_1, \cdots, \alpha_\kappa \leftarrow \mathbb{Z}_p$ and $\alpha = \prod_{i=1}^{\kappa} \alpha_i$. Output $(params, g, \alpha_1 \cdot g, \cdots \alpha_\kappa \cdot g, \alpha \cdot e(g, g, \cdots, g))$
2. Set $(params, g) \leftarrow InstanceGeneration(1^\lambda, 1^\kappa)$. Choose $\alpha_1, \cdots, \alpha_\kappa, \alpha \leftarrow \mathbb{Z}_p$. Output $(params, g, \alpha_1 \cdot g, \cdots \alpha_\kappa \cdot g, \alpha \cdot e(g, g, \cdots, g))$.

The MDDH problem is hard if for all $\kappa > 1$ there is a negligible probability (in λ) of distinguishing between these two distributions. In other words, given values $(g, \alpha_1 \cdot g, \cdots \alpha_\kappa \cdot g, c \cdot e(g, g, \cdots, g))$, the MDDH assumption states that it is difficult to distinguish between the 2 games where c is a random value $\alpha \in \mathbb{Z}_p$ or c is a product of all the α_is.

3 Multilinear Maps Construction from Ideal Lattices

In this section, we will review the multilinear maps construction of [GGH12].

3.1 Basic Ideas

The construction of Garg, Gentry and Halevi works in a polynomial ring $R = \mathbb{Z}[X]/(X^n + 1)$, where n is chosen to be large enough and such that $X^n + 1$ is irreducible, and choosing a secret ring element $g \in R$. Then a principal ideal $I = \langle g \rangle \subset R$ is generated along with an integer q and another randomly generated secret element $z \in R/qR$.

The set of all level-i encodings is $S_i = \{c/z^i \in R_q : \|c\| < q^{1/8}\}$, while the set of all level-i encodings of a coset $e + I$ is $S_i^{e+I} = \{c/z^i \in R_q : c \in e + I, \|c\| < q^{1/8}\}$.

The basic idea is to start with an encoding $d \in R/I$ of a message at level-0, and a level-1 encoding $y = [a/z]_q$ of $1 + I$, where $a \in 1 + I$, where y will be published.

For each level-i, we get that $\boldsymbol{u}_i = [dy^i]_q = [\frac{da^i}{z^i}]_q$ is a level-i encoding. The numerator of $\boldsymbol{u}_i$ is $da^i \in d + I$, and can be shown to have norm at most $q^{1/8}$, so by definition $\boldsymbol{u}_i$ is indeed a level-i encoding of $d + I$.

The problem here is that from a level-i encoding e_i of d, we can easily get d. This is avoided by randomizing the above operation.

The MDDH, which is the equivalent of DDH for multilinear maps, is believed to be hard in this construction. However, the equivalent of other hardness assumptions on bilinear maps are easy. For example, given enough level-1 encodings of 0 and 1, we can have a "weak discrete log" procedure for level-i, $i < \kappa$ encodings. This idea can lead to a basis of the ideal lattice I ([GGH12]).

3.2 Operations

Addition and Multiplication Suppose we have $k \leq \kappa$ elements $x_1, x_2, \cdots, x_k$ with level-1 encodings $u_i = x_i/z \in R_q$. Let $a = max\|x_i\|$. Then the choice of short x_i's will mean that $\kappa a < a^\kappa \ll q$. Moreover, by the triangle inequality, $\|\sum_{i=1}^k x_i\| \leq \sum_{i=1}^k \|x_i\| \leq ka \leq \kappa a \ll q$, and we also have $\|\prod_{i=1}^k x_i\| = \prod_{i=1}^k \|x_i\| \leq a^k \leq a^\kappa \ll q$. Hence there won't be any reductions modulo q. So by setting

$$u_{add} = \sum_{i=1}^{k} u_i = \frac{\sum_{i=1}^k x_i}{z}$$

$$u_{mul} = \prod_{i=1}^{k} u_i = \frac{\prod_{i=1}^k x_i}{z^k}$$

we can see that the encoding of a summation can be done by summing the encodings, and similarly for multiplication by later raising the denominator to the correct power k.

Then a κ-multilinear map $e(x_1, x_2, \cdots, x_\kappa)$ of $x_1, x_2, \cdots, x_\kappa$ can be defined as a product of the level-1 encodings of $x_1, x_2, \cdots, x_\kappa$.

Zero Testing As we have seen, even without the randomization process, every "plaintext" can be encoded in several different ways for a certain encoding level. The zero test essentially checks if an encoding is in the set of level-k encodings of $0 + I = I$. This is difficult to achieve, so the requirement is relaxed to allow a negligible probability of non-zero encodings passing the zero test.

A zero test can be used to do an equality test: a, b are level-k encodings of the same "plaintext" iff $a - b$ passes the zero test.

Extraction The extraction algorithm ideally is such that for any $u_1, u_2 \in S_k^{(\alpha)}$, the extraction output is the same string $s \in \{0,1\}^\lambda$.

As with the zero testing, this is difficult to achieve, and the requirement is relaxed such that level-k encodings of the same element will have the same extraction output, except for a negligible probability.

3.3 Parameters

Garg, Gentry and Halevi give approximate parameters as follows (security parameter λ):

- $\kappa \leq poly(\lambda)$
- $n = O(\kappa\lambda^2)$
- $q \approx 2^{n/\lambda}$
- $m = O(n^2)$

4 Multilinear Maps Construction without Ideal Lattices

In this section, we will review the recent multilinear maps construction of [CLT13].

4.1 Basic Ideas

The scheme of Coron, Lepoint and Tebouchi start by generating n large secret primes p_i, n small secret primes g_i, and a random secret integer z modulo $x = \prod_{i=1}^{n} p_i$. The value x defined here will also be public. The scheme works with messages from the ring $R = \mathbb{Z}_{g_1} \times \mathbb{Z}_{g_2} \times \cdots \times \mathbb{Z}_{g_n}$. However, as the values g_i are secret, the user sees the scheme to encode messages from the n-dimensional vector $\mathbb{Z}^n$. The level-k encoding of $m = (m_i)$ results in $c \in \mathbb{Z}_x$ such that for $1 \leq 1 \leq n$,

$$c \equiv \frac{r_i \cdot g_i + m_i}{z^k} \mod p_i$$

By the Chinese Remainder Theorem, this value will be unique modulo x. However, a user of the scheme will not know the values g_i, p_i so cannot normally do the encodings themselves. As in the [GGH12] scheme, this is solved y giving access to a set of random level-0 encodings, which enables a level-0 encoding of a message m.

Encoding a message m at higher levels is done by giving access to a level-1 encoding of $(1, 1, \cdots 1)$, that is an integer y that satisfies

$$y \equiv \frac{r_i \cdot g_i + 1}{z^k} \mod p_i$$

for $1 \leq i \leq n$ and small random integers $r_i \in [-2^{\rho/2}, 2^{\rho/2}]$. The value y is also computed by using the construction method of the Chinese Remainder Theorem. Given a level-0 encoding c of m, a level-k encoding can then be given as $c_k = c \cdot y_k \mod x_0$. As in [GGH12], this will need to be re-randomized, or else $c = \frac{c_k}{y^k}$ can be computed, and from here the message m can be extracted.

4.2 Operations

Addition and Multiplication As in [GGH12], given messages $x_1, x_2, \cdots, x_k$ with level-1 encodings $u_1, u_2, \cdots, u_k$, we can get encodings of sums and products respectively by summing and multiplying the encodings. Specifically,

$$u_{add} = \sum_{i=1}^{k} u_i \mod x$$

$$u_{mul} = \prod_{i=1}^{k} u_i \mod x$$

Then a κ-multilinear map $e(x_1, x_2, \cdots, x_\kappa)$ of $x_1, x_2, \cdots, x_\kappa$ can be defined as a product of the level-1 encodings of $x_1, x_2, \cdots, x_\kappa$.

Zero Testing The zero testing works by computing a vector $w = f(m)$ such that if m is the zero vector, then $\|w\|_\infty$ is small enough to pass the zero test, else it is a large value.

As before, the zero test can also be used to do an equality test: a, b are level-k encodings of the same message $m \in R$ iff $a - b$ passes the zero test.

Extraction The extraction method is similar to [GGH12].

4.3 Parameters

Coron, Lepoint and Tebouchi give approximate parameters as follows (security parameter λ):

- $\rho = \Omega(\lambda)$
- $\alpha = \lambda$
- $n = \omega(\eta \log \lambda)$

where ρ is the number of bits for the randomness r_i, α is the number of bits for the small primes g_i, and η is the number of bits for the large primes p_i.

5 Applications and Challenges

5.1 Application: Non-interactive Key Agreement

Multilinear maps can be used to generalize the Joux tripartite Diffie-Hellman protocol into $N = \kappa+1$ parties [CLT13].

Here, the public parameters will be generated with $\kappa = N - 1$ and an appropriate security parameter λ.

Each party P_i creates a secret (level-0) encoding c_i sampled randomly, then publishes a corresponding rerandomized level-1 encoding c_i'.

Once this is done, each party computes the product of his c_i and everyone else's c_j' to get $C_i = c_i \prod_{i \neq j} c_j' \mod x$, which is a level $N - 1 = \kappa$ encoding. The shared key can then be obtained using the extraction operation.

We can see here that each party only sends one ring element to be published, and retrieves $N-1$ ring elements.

However, this is not efficient: the public key for [CLT13] contains at least $n \cdot \alpha$ encodings, where each encoding is of size $n \cdot \eta$ bits. Hence the public key size is not smaller than $(n \cdot \alpha) \cdot (n \cdot \eta) = n^2 \cdot \alpha \cdot \eta$ bits. If we take α, η such that $\alpha \cdot \eta \geq n$, the public key is then at least n^3 bits long, which is unacceptable.

In [CLT13], this is resolved by doing some optimizations which make this solution more practical. The implementation seems to be less secure, as it removes some nice properties such as the uniformity of the sampling algorithm. The size of the public key is a common obstacle in finding practical applications for multilinear maps.

5.2 Challenges

Here we will discuss some unresolved questions that have occurred in this survey. This will be a good starting point for future work in multilinear maps.

1. We have not really analyzed much in complexity, outside the parameters such as public key size for the schemes. In particular, we have not seen the cost of doing a multilinear map of degree κ.
2. We have not discussed much about the security of the two schemes. It is known that the best current attacks on [GGH12] are lattice attacks that make use of the fact that the construction is based on ideal lattices. In comparison, [CLT13] seems to avoid these attacks simply by not using ideal lattices. However, we do not know if some other attacks work would well in the [CLT13] scheme. Both [GGH12] and [CLT13] have detailed cryptanalysis of their schemes.

6 Conclusion

We have seen two constructions of multilinear maps based on lattices. The two schemes have many similarities, but in general the second scheme is more efficient than the first. This is mainly due to the change of encoding domain from ideal lattices to integers. The security of both schemes has not been well studied, which is why both papers describing the schemes give a comprehensive security analysis, which we have not discussed in this paper.

We have also seen how multilinear maps can be useful to perform some cryptographic protocols more efficiently. However, the current results are not yet practical, and it will be something that has to be enhanced significantly in future work on multilinear maps. It is hoped that future work can also expand the range of applications of multilinear maps.

References

CLT13. Jean-Sebastien Coron, Tancrede Lepoint, and Mehdi Tibouchi. Practical Multilinear Maps over the Integers. Technical Report 2013/183, April 1, 2013. Available at http://eprint.iacr.org/2013/183.

GGH12. Sanjam Garg, Craig Gentry, and Shai Halevi. Candidate Multilinear Maps from Ideal Lattices. Technical Report 2012/610, October 29, 2012. Available at http://eprint.iacr.org/2012/610.

MR08. Daniele Micciancio and Oded Regev. Lattice-based Cryptography, 2008.