

Cryptanalysis of the multilinear map over the integers

Jung Hee Cheon¹, Kyoohyung Han¹, [Changmin Lee](#)¹,
Hansol Ryu¹, Damien Stehlé²

¹Seoul National University

²ENS de Lyon

April 28, 2015



Background

A κ -multilinear map is a map $e : G_1 \times \dots \times G_\kappa \rightarrow G_T$, which has the following property:

$$e(g_1, \dots, \alpha \cdot g_i, \dots, g_\kappa) = \alpha \cdot e(g_1, \dots, g_\kappa) \quad \text{for } 1 \leq i \leq \kappa.$$

Multilinear map is a very useful tool in cryptography.

- ▶ N -multipartite key exchange [BS03]
- ▶ Efficient broadcast encryption [BS03]
- ▶ Key homomorphic PRF [BLMR14]
- ▶ Obfuscation [GLSW14]

For a long time, however, constructing a multilinear map has been an open problem.

Known Cryptographic Multilinear Maps

Recently, 2-type of cryptographic (approximate) multilinear maps are constructed.

One by Garg, Gentry, and Halevi (Eurocrypt 2013).

- First plausible Multilinear map
- uses ideal lattices

The other by Coron, Lepoint, and Tibouchi (Crypto 2013).

- Similar to GGH scheme
- uses basic integer arithmetic

These are inspired from well-known FHE schemes.

Some security assumptions enabled by multilinear maps

- **Graded Computational Diffie Hellman problem (GCDH)**

Given $(\kappa + 1)$ encodings of $\{m_i\}_{0 \leq i \leq \kappa}$, compute an encoding of

$$\prod_{i=0}^{\kappa} m_i.$$

- **The Subgroup Membership problem (SubM)**

Given an encoding of m and a subgroup G' of a plaintext group G , determine whether m is sampled in G' or not.

- **The Decision Linear problem (DLIN)**

Given $(\kappa + 1) \times (\kappa + 1)$ encodings of $\{m_{ij}\}$, determine whether matrix $(m_{ij})_{\{0 \leq i, j \leq \kappa\}}$ is full rank or not.

SubM and DLIN do not hold in GGH.

GCDH, SubM, DLIN are expected to hold in CLT.

Applications of [CLT13] scheme

Many applications are based on CLT scheme exploiting the conjectured hardness of DLIN and SubM.

- [ABP14] Disjunctions for hash proof systems: New constructions and applications
- [BP13] Verifier-based password-authenticated key exchange: New models and constructions
- [BLMR14] Key homomorphic PRFs and their applications
- [GGHZ14b] Fully secure functional encryption without obfuscation
- [GLW14] Witness encryption from instance independent assumptions
- [GLSW14] Indistinguishability obfuscation from the multilinear subgroup elimination assumption
- etc...

Result

Given instance of CLT's, one can find all secret parameters of the CLT scheme in **polynomial time** with overwhelming probability.

Warm-up: Naive CLT, Description and Cryptanalysis

Naive Approach: Encoding

- $\mathcal{P} := \mathbb{Z}_g$, $\mathcal{C} := \mathbb{Z}_p$, $\text{GCD}(g, p) = 1$ with $g \ll p$
- Secret: $z \in \mathcal{C}$, $g, h, r_i, r_y \in \mathbb{Z}$ ($r_y, r_i \ll p$ and $h \leq \sqrt{p}$)
- Public: $q, (x_1, \dots, x_\tau, y, P_{zt}) \in \mathcal{C}^{\tau+2}$
 - ▶ Sampling: $m \leftarrow \mathbb{Z}$, m is small integer.
 - ▶ Encoding: For $y := \left[\frac{r_y g + 1}{z} \right]_p$, $x_i := \left[\frac{r_i g + 0}{z} \right]_p$,
$$\text{enc}_1(m) := m \cdot y + \sum b_j x_j = \left[\frac{rg + m}{z} \right]_p$$
 - ▶ Zero testing parameter: $P_{zt} := \left[\frac{hz^\kappa}{g} \right]_p$

Naive Approach: Mul and Zero Testing

- Multiplication: Given $c_i = \frac{1}{z}(\hat{r}_i g + m_i) = \text{enc}_1(m_i)$,

$$\prod_{i=1}^{\kappa} c_i = \frac{1}{z^{\kappa}}(\hat{r}g + \prod_{i=1}^{\kappa} m_i) = \text{enc}_{\kappa}(\prod_{i=1}^{\kappa} m_i).$$

- Zero testing: Given a level- κ encoding $c = \frac{1}{z^{\kappa}}(rg + m)$, and

$$P_{zt} = \frac{hz^{\kappa}}{g},$$

$$[P_{zt} \cdot c]_p = \begin{cases} hr & \ll p \text{ if } m = 0 \\ [h(mg^{-1} + r)]_p & \approx p \text{ otherwise.} \end{cases}$$

- Fact: If $a \equiv b \pmod{p}$, $0 \leq b < p$, then $[a]_p = b$.

A $(\kappa + 1)$ -partite key exchange

- User U_i publishes an encoding of m_i , $\text{enc}_1(m_i)$, for his secret message m_i .
- Upon receiving all other encodings, user U_i computes

$$\Delta_i := [P_{zt} \cdot m_i \cdot \prod_{j \neq i} \text{enc}_1(m_j)]_p.$$

- For any i, k , we have $\Delta_i - \Delta_k = [P_{zt} \cdot \text{enc}_\kappa(0)]_p = hr \ll p$.
- That is, $\text{MSB}_\alpha(\Delta_i) = \text{MSB}_\alpha(\Delta_k)$ for each i and k , which is the shared secret of $\kappa + 1$ users.

Attack of Naive Scheme-GCD algorithm

Since $x_j = \text{enc}_1(0)$ and $y = \text{enc}_1(1)$ are public,
we can generate a level- κ encoding of zero: $[x_j \cdot y^{\kappa-1}]_p$, then

$$\begin{aligned}[x_j \cdot y^{\kappa-1} \cdot P_{zt}]_p &= \left[\frac{r_j g}{z} \left(\frac{r_y g + 1}{z} \right)^{\kappa-1} \cdot \frac{h z^\kappa}{g} \right]_p \\ &= [r_j (r_y g + 1)^{\kappa-1} h]_p = r_j (r_y g + 1)^{\kappa-1} h.\end{aligned}$$

It always has a factor h for $1 \leq j \leq n$.

Similarly, we can get gh , and hence g . Broken !

Genuine CLT

From naive to genuine CLT

	Base ring R	$\mathcal{P} = R/gR$	$\mathcal{C} = R/qR$
Naive	\mathbb{Z}	\mathbb{Z}_g	\mathbb{Z}_p
CLT	$\prod_{i=1}^n \mathbb{Z}$	$\prod_{i=1}^n \mathbb{Z}_{g_i}$	$\prod_{i=1}^n \mathbb{Z}_{p_i}$

Notation:

- $\text{CRT}_{(p_i)}(r_i)$ defined as the unique integer in $\left(-\frac{1}{2} \prod_{i=1}^n p_i, \frac{1}{2} \prod_{i=1}^n p_i\right]$ which is congruent to $r_i \pmod{p_i}$ for all $i \in \{1, \dots, n\}$
- $x_0 = \prod_{i=1}^n p_i$

CLT scheme: Algebraic Setup

- $\mathcal{P} := \prod_{i=1}^n \mathbb{Z}_{g_i}$, $\mathcal{C} := \prod_{i=1}^n \mathbb{Z}_{p_i} \equiv \mathbb{Z}_{x_0}$, $\text{GCD}(g_i, p_i) = 1$ in \mathbb{Z}
- Secret: $z \in \mathcal{C}$, $g_i, h_i, p_i, r_i, r_{ij}, \tilde{r}_{ki} \in \mathbb{Z}$ ($r_i, r_{ij}, \tilde{r}_{ki}, g_i \ll q_i$ and $h_i \leq \sqrt{p_i}$)
- Public: $x_0, (x'_1, \dots, x'_\tau, x_1, \dots, x_\tau, y, P_{zt}) \in \mathcal{C}^{2\tau+2}$
 - ▶ Sampling: For $x'_k := \text{CRT}_{(p_i)}(\tilde{r}_{ki})$, $\text{CRT}_{(p_i)}(m_i) = \sum_{k=1}^{\tau} b_k x'_k$
 - ▶ Encoding: For $y := \text{CRT}_{(p_i)}\left(\frac{r_i g_i + 1}{z}\right)$, $x_j := \text{CRT}_{(p_i)}\left(\frac{r_{ij} g + 0}{z}\right)$,
 $\text{enc}_1(\vec{m}) := \text{CRT}_{(p_i)}(m_i) \cdot y + \sum b'_j x_j$
 - ▶ Zero testing parameter: $P_{zt} := \sum_{i=1}^n \left[\frac{h_i z^{\kappa}}{g_i} \right]_{p_i} \frac{x_0}{p_i}$

Zero testing in CLT scheme

Lemma (Zero Testing Parameter)

$$\left[\text{CRT}_{(p_i)}(r_i) \cdot \sum_{i=1}^n a_i \frac{x_0}{p_i} \right]_{x_0} = \left[\sum_{i=1}^n r_i a_i \frac{x_0}{p_i} \right]_{x_0} \quad \text{for } x_0 = p_1 \dots p_n$$

- Given a level- κ encoding and P_{zt}

$$c = \text{CRT}_{(p_i)} \left(\frac{r_i g_i + m_i}{z^\kappa} \right), \quad P_{zt} = \sum_{i=1}^n \left[\frac{h_i z^\kappa}{g_i} \right]_{p_i} \frac{x_0}{p_i},$$

$$[c \cdot P_{zt}]_{x_0} = \begin{cases} \sum_{i=1}^n h_i r_i \frac{x_0}{p_i} & \ll x_0 \quad \text{if } (m_1, \dots, m_n) = 0 \\ \left[\sum_{i=1}^n h_i (m_i g_i^{-1} + r_i) \frac{x_0}{p_i} \right]_{x_0} & \approx x_0 \quad \text{otherwise} \end{cases}$$

Attack Algorithm

Trivial Approach

- When we perform zero testing, $[c^{(\kappa)} \cdot P_{zt}]_{x_0}$'s entry has the following form:

$$[c^{(\kappa)} \cdot P_{zt}]_{x_0} = \sum_{i=1}^n h_i r_i \frac{x_0}{p_i}. \quad \text{(an integer equation!)}$$

- $[c^{(\kappa)} P_{zt}]_{x_0} = \sum_{i=1}^n h_i r_{ij} \frac{x_0}{p_i}$ is a linear equation for $h_1 \frac{x_0}{p_1}, \dots, h_n \frac{x_0}{p_n}$.
- Cannot apply the GCD algorithm to recover $h_i \frac{x_0}{p_i}$.

Idea of our work

- Suppose we have a matrix equation by collecting n^2 quadratic forms:

$$(a_{ij})_{ij} = \left(\sum_{k=1}^n r_{ik} A_k r'_{kj} \right)_{ij} = (r_{ik})_{ik} \cdot \begin{pmatrix} A_1 & & \\ & \ddots & \\ & & A_n \end{pmatrix} \cdot (r'_{kj})_{kj}$$

- Assume another matrix equation with different diagonal entries:

$$(b_{ij})_{ij} = \left(\sum_{k=1}^n r_{ik} B_k r'_{kj} \right)_{ij} = (r_{ik})_{ik} \cdot \begin{pmatrix} B_1 & & \\ & \ddots & \\ & & B_n \end{pmatrix} \cdot (r'_{kj})_{kj}$$

- $(a_{ij})_{ij} \cdot (b_{ij})_{ij}^{-1} = (r_{ik})_{ik} \cdot \begin{pmatrix} A_1/B_1 & & \\ & \ddots & \\ & & A_n/B_n \end{pmatrix} \cdot (r_{ik})_{ik}^{-1}$

- Hence we can easily recover A_i/B_i by computing eigenvalues.

Build Equations

- For fixed j and k , by multiplying x'_j, x_k, x'_1, y , generate a level- κ encoding of zero and apply P_{zt} :

$$\begin{aligned} [x'_j \cdot x'_1 \cdot x_k \cdot y^{\kappa-1} \cdot P_{zt}]_{x_0} &= \sum_{i=1}^n \tilde{r}_{ij} \tilde{r}_{i1} r_{ik} \left((r_i \cdot g_i + 1)^{\kappa-1} h_i \frac{x_0}{p_i} \right) \\ &= \sum_{i=1}^n \tilde{r}_{ij} (\tilde{r}_{i1} H_i) r_{ik}. \end{aligned}$$

- This equation is a **quadratic form of \tilde{r}_{ij}, r_{ik}** . Hence

$$\begin{pmatrix} \tilde{r}_{1j} & \cdots & \tilde{r}_{nj} \end{pmatrix} \cdot \begin{pmatrix} \tilde{r}_{11} H_1 & & \\ & \ddots & \\ & & \tilde{r}_{n1} H_n \end{pmatrix} \cdot \begin{pmatrix} r_{1k} \\ \vdots \\ r_{nk} \end{pmatrix}.$$

Build Equations

- Changing the indices j and k , compute $[x'_j \cdot x'_1 \cdot x_k \cdot y^{\kappa-1} \cdot P_{zt}]_{x_0}$, and compose a matrix W_1

$$\begin{aligned}
 W_1 &= \begin{pmatrix} \tilde{r}_{11}\tilde{r}_{11}H_1r_{11} & \tilde{r}_{12}\tilde{r}_{21}H_2r_{12} & \dots & \tilde{r}_{1n}\tilde{r}_{n1}H_nr_{1n} \\ \tilde{r}_{21}\tilde{r}_{11}H_1r_{21} & \tilde{r}_{22}\tilde{r}_{21}H_2r_{22} & \dots & \tilde{r}_{2n}\tilde{r}_{n1}H_nr_{2n} \\ & \vdots & & \\ \tilde{r}_{n1}\tilde{r}_{11}H_1r_{n1} & \tilde{r}_{n2}\tilde{r}_{21}H_2r_{n2} & \dots & \tilde{r}_{nn}\tilde{r}_{n1}H_nr_{nn} \end{pmatrix} \\
 &= \underbrace{\begin{pmatrix} \tilde{r}_{11} & \dots & \tilde{r}_{n1} \\ \vdots & \ddots & \vdots \\ \tilde{r}_{1n} & \dots & \tilde{r}_{nn} \end{pmatrix}}_{\tilde{R}} \cdot \underbrace{\begin{pmatrix} \tilde{r}_{11}H_1 & & \\ & \ddots & \\ & & \tilde{r}_{n1}H_n \end{pmatrix}}_{\text{diag}} \cdot \underbrace{\begin{pmatrix} r_{11} & \dots & r_{1n} \\ \vdots & \ddots & \vdots \\ r_{n1} & \dots & r_{nn} \end{pmatrix}}_R.
 \end{aligned}$$

Build Equations

- By replacing x'_1 by x'_2

$$[x'_j \cdot \textcolor{red}{x}'_1 \cdot x_k \cdot y^{\kappa-1} \cdot P_{zt}]_{x_0} \rightarrow [x'_j \cdot \textcolor{red}{x}'_2 \cdot x_k \cdot y^{\kappa-1} \cdot P_{zt}]_{x_0},$$

we obtain

$$W_2 = \tilde{R} \cdot \text{diag}(\textcolor{red}{r}_{12}H_1, \dots, \textcolor{red}{r}_{n2}H_n) \cdot R.$$

- From W_1 and W_2 , we can get

$$W_1 \cdot W_2^{-1} = \tilde{R} \cdot \text{diag}(\tilde{r}_{11}/\tilde{r}_{12}, \dots, \tilde{r}_{n1}/\tilde{r}_{n2}) \cdot \tilde{R}^{-1}.$$

Its eigenvalues are $\tilde{r}_{11}/\tilde{r}_{12}, \dots, \tilde{r}_{n1}/\tilde{r}_{n2}$.

Solve Equations

- Recover $\tilde{r}_{i1}/\tilde{r}_{i2}$, the eigenvalues of matrix $W_1 \cdot W_2^{-1}$.
- Recover p_i : By definition,
 - ▶ $x'_1/x'_2 = \tilde{r}_{i1}/\tilde{r}_{i2} \pmod{p_i}$.
 - ▶ p_i divides $(x'_1\tilde{r}_{i2} - x'_2\tilde{r}_{i1})$ and $x_0 = \prod_{i=1}^n p_i$.

Hence, $\text{GCD}(x'_1\tilde{r}_{i2} - x'_2\tilde{r}_{i1}, x_0) = p_i$ with high probability.

- By repeating this for $i = 1$ to n , we can find all the **secret p_i 's**.

Attack Complexity

- Our attack consists of three steps of computing
 - ▶ Build a matrix
 - ▶ Recover $\tilde{r}_{i1}/\tilde{r}_{i2}$
 - ▶ Recover p_i
- The complexity is dominated by matrix computation of size $n = \Theta(\kappa\lambda^2)$ for κ multilinear map with security parameter λ .
- In case that R or \tilde{R} is singular, repeat this procedure with different set of n level-1 encodings of zero or n level-0 encodings.

Further Work

- After this work, the authors of CLT has modified their scheme. But it has no complete security proof yet. It would be an interesting problem to analyze or prove the security of the modified CLT.
- Recently, GGH scheme is also under the attack. So it is very important to analyze the security of multilinear maps *without* encodings of zero.

