Cryptanalysis of the New CLT Multilinear Map over the Integers

Jung Hee Cheon[1], Pierre-Alain Fouque[2,3], Changmin Lee[1],
Brice Minaud[2], Hansol Ryu[1]

[1]Seoul National University, Seoul, Korea

[2]Université de Rennes 1, Rennes, France

[3]Institut Universitaire de France, Paris, France

May 11, 2016

Multilinear Maps

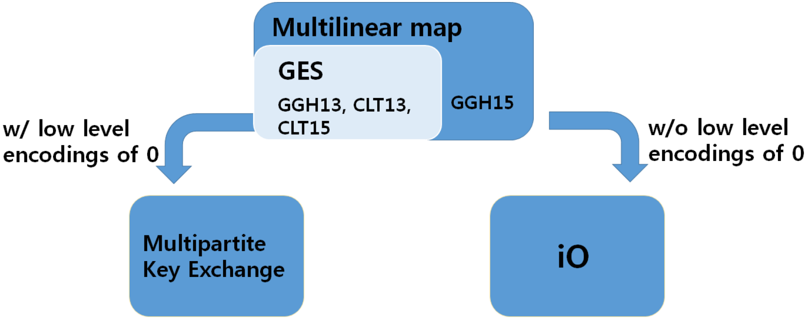
A κ-multilinear map is a map $e : G_1 \times \cdots \times G_\kappa \to G_T$, which has the following property:

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

Hardness Assumptions

MDDH: Given $(\kappa + 1)$ encodings of $m_0, \cdots, m_\kappa$ and encoding of m, determine whether $m = \prod_0^\kappa m_i$.

Applications



+ Witness encryption, functional encryption, efficient broadcast encryption, ...

Multilinear Maps over the Integers

Scheme	Attack
CLT13	CHLRS15
GGHZ14, BWZ14	$CGH^{+}15$
CLT15	

Vs. from ideal lattices:

- Conceptual simplicity
- Relative efficiency
- Wide range of presumed hard problems

Multilinear Maps over the Integers

Scheme	Attack
CLT13	CHLRS15
GGHZ14, BWZ14	CGH^+15
CLT15	Ours

Vs. from ideal lattices:

- Conceptual simplicity
- Relative efficiency
- Wide range of presumed hard problems

Result

Given instance of CLT15's, one can find all secret parameters of CLT15 scheme in polynomial time with overwhelming probability.

CLT15 Multilinear Map

CLT15: Construction

Algebraic setting:

- Secret: Primes $p_1, \cdots, p_n$ and $g_1, \cdots, g_n$ with $g_i \ll p_i$
  $x_0 = \prod_i p_i$ and invertible $z \in \mathbb{Z}_{x_0}$
- Public: Zero-testing modulus N with $N \gg x_0$

Encoding:

- Level-k encoding of $(m_1, \cdots, m_n) \in \mathbb{Z}_{g_1} \times \cdots \times \mathbb{Z}_{g_n}$ is

$$e = \mathrm{CRT}_{(p_i)}\left(\frac{r_i g_i + m_i}{z^k}\right) + a x_0 \equiv \frac{r_i g_i + m_i}{z^k} \bmod p_i.$$

CLT15: Zero-testing

Define $u_i = \left[\frac{g_i}{z^\kappa}\left(\frac{x_0}{p_i}\right)^{-1}\right]_{p_i}\frac{x_0}{p_i}$, $v_i = [p_{zt} \cdot u_i]_N$ for $i = 1, \cdots, n$ and $v_0 = [p_{zt} \cdot x_0]_N$. Then

$$e = \mathrm{CRT}_{(p_i)}\left(\frac{r_i g_i + m_i}{z^\kappa}\right) = \sum_i [r_i + m_i/g_i]_{p_i} u_i + a x_0,$$

and $|v_i| \approx N/p_i, |v_0| \ll N$. So

$$[p_{zt} \cdot e]_N = \left[\sum_i [r_i + m_i/g_i]_{p_i} v_i + a v_0\right]_N.$$

If e is an encoding of zero,

$$\begin{aligned}[p_{zt} \cdot e]_N &= \left[\sum_i [r_i + 0/g_i]_{p_i} v_i + a v_0\right]_N \\ &= \sum_i r_i v_i + a v_0 \qquad \ll N.\end{aligned}$$

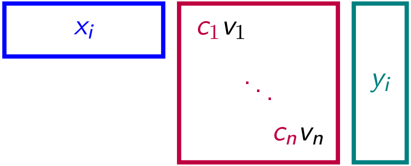
CHLRS Attack: When x_0 is Known

Given $x = \mathrm{CRT}_{(\mathrm{p_i})}(\mathrm{x_i g_i / z}), \mathrm{y} = \mathrm{CRT}_{(\mathrm{p_i})}(\mathrm{y_i / z^{\kappa - 1}}), \mathrm{c} = \mathrm{CRT}_{(\mathrm{p_i})}(\mathrm{c_i})$, compute

$$e = xcy \bmod x_0 = \mathrm{CRT}(\mathrm{x_i c_i y_i g_i / z^{\kappa}}),$$

$$[p_{zt} \cdot e]_N = \sum_i x_i c_i v_i y_i + a v_0, \text{ and}$$

$$[p_{zt} \cdot e]_N \equiv_{v_0} \sum_i x_i c_i v_i y_i.$$



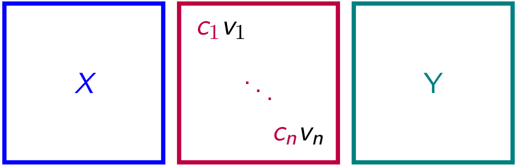
CHLRS Attack: When x_0 is Known

Given $x = \mathrm{CRT}_{(\mathrm{p_i})}(\mathrm{x_i g_i / z}), \mathrm{y} = \mathrm{CRT}_{(\mathrm{p_i})}(\mathrm{y_i / z^{\kappa-1}}), \mathrm{c} = \mathrm{CRT}_{(\mathrm{p_i})}(\mathrm{c_i})$, compute

$$e = xcy \bmod x_0 = \mathrm{CRT}(\mathrm{x_i c_i y_i g_i / z^{\kappa}}),$$

$$[p_{zt} \cdot e]_N = \sum_i x_i c_i v_i y_i + a v_0, \text{ and}$$

$$[p_{zt} \cdot e]_N \equiv_{v_0} \sum_i x_i c_i v_i y_i.$$



From this matrix equation, we can get c_i. Then $(c - c_i)$ is a multiple of p_i.

CHLRS Attack: When x_0 is Unknown

We can not reduce the size of encoding.

$$e = xcy = \sum_i x_i c_i y_i u_i + a x_0,$$

$$[p_{zt} \cdot e]_N = \Big[\sum_i x_i c_i y_i v_i + a v_0 \Big]_N,$$

and $\sum_i x_i c_i y_i v_i + a v_0 > N$, since $a \approx x_0^2$.

- Previous attack does not work.
- Correctness of zero-testing does not hold.

Need to reduce the size of encodings in order to performing zero-testing.

CLT15: Multiplication using Ladder

- Note that for given level-s encoding $e = \mathsf{CRT}_{(\mathsf{p_i})}\big(\frac{\mathsf{r_i g_i + m_i}}{\mathsf{z^s}}\big)$ and level-$(\kappa - s)$ encoding $e' = \mathsf{CRT}_{(\mathsf{p_i})}\big(\frac{\mathsf{r_i' g_i + m_i'}}{\mathsf{z^{\kappa - s}}}\big)$,

$$e \cdot e' \equiv_{x_0} \mathsf{CRT}_{(\mathsf{p_i})}\Big(\frac{\mathsf{r_i'' g_i + m_i m_i'}}{\mathsf{z^\kappa}}\Big).$$

  However, the size of $e \cdot e' \approx x_0^2$.

- Ladder in each level: encodings of zero

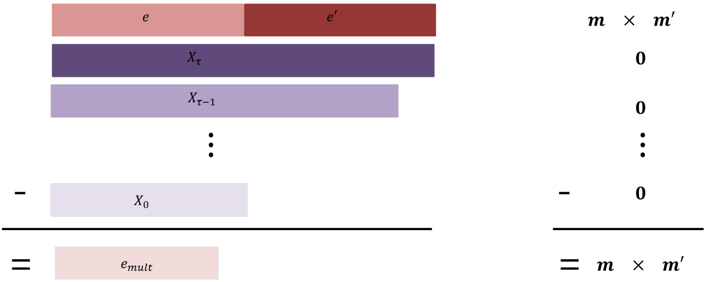
$$X_0 < X_1 < \cdots < X_{\gamma'} \text{ with } X_j \approx 2^j x_0.$$

CLT15: Multiplication using Ladder

Multiplication of two encodings e and e':

$$e_{mult} = e \cdot e' - \sum_j b_j X_j^{(t)} \equiv \frac{\tilde{r}_i g_i + m_i m'_i}{z^t} \bmod p_i, \quad b_j \in \{0, 1\},$$

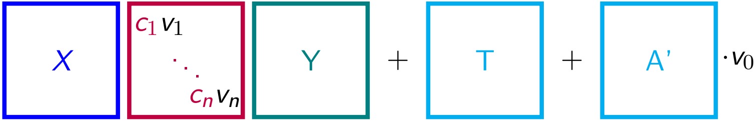
$e_{mult} \approx x_0$.



CHLRS Attack: Using Ladder

Given $x = \mathrm{CRT}_{(p_i)}(x_i g_i / z), y = \mathrm{CRT}_{(p_i)}(y_i / z^{\kappa-1}), c = \mathrm{CRT}_{(p_i)}(c_i)$, compute

$$e = xyc - \sum b_j X_j = \sum (x_i c_i y_i + t_i) u_i + a' x_0 \text{ and}$$
$$[p_{zt} \cdot e]_N = \sum_i (x_i c_i y_i + t_i) v_i + a' v_0.$$



T and A are unknown matrices, so it looks hard to obtain c_i.

Cryptanalysis of CLT15

Attack Idea

Compute $v_0 \in \mathbb{Z}$ and recover x_0.

$$p_{zt} \cdot (e - \sum_j b_j X_j) \bmod N = \sum_i (r_i + t_i) v_i + a v_0.$$

1. Remove t_i using $p_{zt} \cdot X_j$.
2. Compute $v_0 \in \mathbb{Z}$ from several equations modulo unknown v_0.

Step 1: Remove t_i

$$p_{zt} \cdot (e - \sum_j b_j X_j) \bmod N = \sum_i (r_i + t_i) v_i + (a + a') v_0$$
$$= \Big(\sum_i r_i v_i + a v_0 \Big) + \boxed{\sum_i t_i v_i + a' v_0}$$

Define a map ϕ,

$$\phi : \sum r_i u_i + a x_0 \longmapsto \sum r_i v_i + a v_0,$$

and compute $\phi(-\sum_j b_j X_j) = \boxed{\sum t_i v_i + a' v_0}$.

Step 1: Remove t_i

$$p_{zt} \cdot (e - \sum_j b_j X_j) \bmod N = \sum_i (r_i + t_i) v_i + (a + a') v_0$$

$$= \Big(\sum_i r_i v_i + a v_0 \Big) + \boxed{\sum_i t_i v_i + a' v_0}$$

Define a map ϕ,

$$\phi : \sum r_i u_i + a x_0 \longmapsto \sum r_i v_i + a v_0,$$

and compute $\phi(-\sum_j b_j X_j) = \boxed{\sum t_i v_i + a' v_0}$.

Step 1: Remove t_i

Proposition 1

If e is an encoding of zero and $e \approx x_0$, then

$$\phi(e) = p_{zt} \cdot e \bmod N.$$

Proposition 2

Let $e = \sum r_i u_i + a x_0, e' = \sum r'_i u_i + a' x_0$. If $\forall i, -p_i/2 < r_i + r'_i \leq p_i/2$, then

$$\phi(e + e') = \phi(e) + \phi(e').$$

The conditions in Proposition 2 are also required for the correctness of the scheme to hold.

Step 1: Remove t_i

$$\phi\big(\sum b_j X_j\big) = \sum b_j \cdot \phi(X_j)$$

Compute individual $\phi(X_j)$.

1. $\phi(X_0) = p_{zt} \cdot X_0 \bmod N$ by Prop 1.
2. $\phi(X_1 - X_0) = \phi(X_1) - \phi(X_0)$ by Prop 2 since $(X_1 - X_0)$ is small.
3. Continue this process to get all $\phi(X_j)$'s.

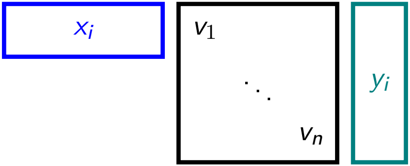
$$X \begin{pmatrix} c_1 v_1 & & \\ & \ddots & \\ & & c_n v_n \end{pmatrix} Y + T + A' \cdot v_0$$


X
c1 v1
cn vn
Y
+
A
·v0

Step 2: Compute v_0

$$x = \mathrm{CRT}\left(\frac{\mathrm{x_i g_i}}{\mathrm{z}}\right),\ \mathrm{y} = \mathrm{CRT}\left(\frac{\mathrm{y_i}}{\mathrm{z}^{\kappa-1}}\right)$$

$$\phi(xy) = \sum x_i v_i y_i + a^* v_0$$

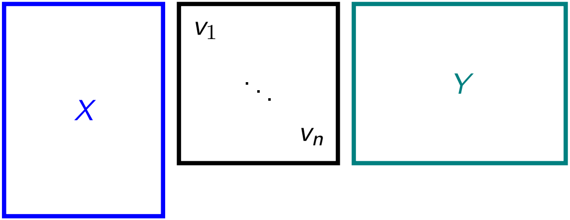


in $\mathbb{Z}_{v_0}$

Step 2: Compute v_0

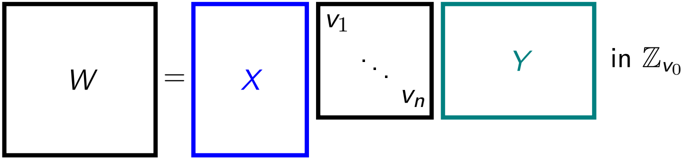
$$x = \mathrm{CRT}\left(\frac{\mathrm{x_i g_i}}{\mathrm{z}}\right),\ \mathrm{y} = \mathrm{CRT}\left(\frac{\mathrm{y_i}}{\mathrm{z}^{\kappa-1}}\right)$$

$$\phi(xy) = \sum x_i v_i y_i + a^* v_0$$



in $\mathbb{Z}_{v_0}$

Step 2: Compute v_0



- W is not a full rank matrix when embedded into $\mathbb{Z}_{v_0}$, then v_0 divides $\det(W)$.
- Compute v_0 and $x_0 = v_0 \cdot p_{zt}^{-1} \bmod N$

Summary of Current Multilinear Maps

	Scheme	Attack	
		Key Exchange (w/ Lowlevel enc(0))	iO (w/o Lowlevel enc(0))
Ideal Lattice	GGH13	HJ16	ABD16, CJL16, MSZ16
Integers	CLT13	CHLRS15	?
	CLT15	Our work	
Graph-Induced	GGH15	CLLT15	?

- MSZ16: only for a basic iO scheme
- ABD16, CJL16: break quantumly or upto degree $\lambda^{3-\epsilon}$ in time $< 2^\lambda$

Further works:

Cryptanalyze CLT13, GGH15 without low-level encoding of zero.

Design a new multilinear map with reduction to standard hard problems.

Thank you