A introduction to multilinear maps and their attacks using the example of CLT13

Lukas Kempf

2021-12-10

Outline

- Multilinear maps
- CLT13
- DH with CLT13
- Attacking CLT13

Diffie-Hellman key exchange

Let G be finite cyclic group with generator g.

Alice	Bob
Choose random $a \in \mathbb{N}$.	Choose random $b \in \mathbb{N}$.
Broadcast g^a.	Broadcast g^b.

Shared key: $(g^b)^a = (g^a)^b$

Diffie-Hellman key exchange

Let G be finite cyclic group with generator g.

Alice	Bob
Choose random $a \in \mathbb{N}$. Broadcast g^a.	Choose random $b \in \mathbb{N}$. Broadcast g^b.

Shared key: $(g^b)^a = (g^a)^b$

Attacker knows g^a and g^b.

$\Rightarrow$ Obtaining g^{ab} from this must be hard (CDH assumption).

Diffie-Hellman key exchange

Let G be finite cyclic group with generator g.

Alice	Bob
Choose random $a \in \mathbb{N}$. Broadcast g^a.	Choose random $b \in \mathbb{N}$. Broadcast g^b.

Shared key: $(g^b)^a = (g^a)^b$

Attacker knows g^a and g^b.

$\Rightarrow$ Obtaining g^{ab} from this must be hard (CDH assumption).

Alternative stronger assumption: Given g^a and g^b it must be hard to differentiate g^{ab} from random (DDH assumption).

Multilinear maps

Definition (Multilinear Map Boneh et al. 2003)

A map $e : G_1^n \leftarrow G_2$ is a *n-multilinear map* if it satisfies the following properties:

1. G_1 and G_2 are groups of the same prime order
2. if $a_1, \ldots, a_n \in \mathbb{Z}$ and $x_1, \ldots, x_n \in G_1$ then

$$e\left(x_1^{a_1}, \ldots, x_n^{a_n}\right) = e(x_1, \ldots, x_n)^{a_1 \ldots a_n}$$

3. if $g \in G_1$ is a generator of G_1 then $e(g, \ldots, g)$ is a generator of G_2.

Why multilinear maps matter

- DH key-exchange between multiple parties in one round [2].
- Existence of cryptographic multilinear maps linked to the existence of indistinguishability obfuscation [1].
- Building block for time-lock encryption [8].

DH with multilinear maps

Let $e : G_1^n \leftarrow G_2$ be a n-multilinear map and g a generator of G_1.

Each of the $n+1$ parties chooses $a_i \in \mathbb{N}$ and broadcasts $h_i = g^{a_i}$.

$$\begin{aligned} e(h_2, \ldots, h_{n+1})^{a_1} &= e(h_1, h_3, \ldots, h_{n+1})^{a_2} = \ldots \\ &= e(h_1, \ldots, h_n)^{a_{n+1}} = e(g, \ldots, g)^{a_1 \cdots a_{n+1}} \end{aligned}$$

DH with multilinear maps

Let $e : G_1^n \leftarrow G_2$ be a n-multilinear map and g a generator of G_1.

Each of the $n+1$ parties chooses $a_i \in \mathbb{N}$ and broadcasts $h_i = g^{a_i}$.

$$
\begin{aligned}
e(h_2, \ldots, h_{n+1})^{a_1} = e(h_1, h_3, \ldots, h_{n+1})^{a_2} = \ldots \\
= e(h_1, \ldots, h_n)^{a_{n+1}} = e(g, \ldots, g)^{a_1 \cdots a_{n+1}}
\end{aligned}
$$

Security assumption: Given $g, g^{a_1}, \ldots, g^{a_{n+1}} \in G_1$ it is hard to compute $e(g, \ldots, g)^{a_1 \cdots a_{n+1}} \in G_2$ (MDH assumption).

How to construct such maps?

"The central open problem posed in this paper is the construction of cryptographic multilinear map generators when $n > 2$." (Boneh et al. 2003)

How to construct such maps?

"The central open problem posed in this paper is the construction of cryptographic multilinear map generators when $n > 2$." (Boneh et al. 2003)

"We also give evidence that such maps might have to either come from outside the realm of algebraic geometry, or occur as 'unnatural' computable maps arising from geometry." (Boneh et al. 2003)

Chinese remainder theorem

Theorem (Chinese remainder theorem over the integers)

Let $\{p_1, \ldots, p_n\}$ be pairwise coprime integers and $N = \prod_i^n$. Then there exists a ring isomorphism $\mathbb{Z}_N \cong \mathbb{Z}_{p_1} \times \cdots \times \mathbb{Z}_{p_n}$.

More concretely we have maps

$$f : x \longmapsto (x \bmod p_1, \ldots, x \bmod p_n)$$

and

$$g : (x_1, \ldots, x_n) \longmapsto \sum_{i=1}^{n} 1_{p_i} x_i$$

where 1_{p_i} is chosen so that $f\left(1_{p_i}\right)$ is 1 in exactly the i-th component and $f \circ g = \mathrm{id}$.

Notation: $x = \mathrm{CRT}_{(p_i)}\left(x_i\right)$

Graded encoding schemes

Basically: Encoding ring elements with noise.

For every $r \in R$ and degree $n \in \mathbb{N}$ we have multiple possible encodings $S_n^{(r)}$.

Addition is possible: For $v_1 \in S_n^{(r_1)}$ and $v_2 \in S_n^{(r_2)}$ we have $v_1 + v_2 \in S_n^{(r_1+r_2)}$.

Multiplication is possible: For $v_1 \in S_{n_1}^{(r_1)}$ and $v_2 \in S_{n_2}^{(r_2)}$ we have $v_1 \cdot v_2 \in S_{n_1+n_2}^{(r_1 \cdot r_2)}$ if $n_1 + n_2$ is small enough.

CLT13 — Idea

Section based on the paper of Coron, Lepoint, and Tibouchi 2013.

- Use CRT to hide computations in the smaller rings by doing them concurrently in the larger ring
- Generate n primes $p_1, \ldots, p_n$ for CRT and compute $x_0 \coloneqq \prod_i^n p_i$
- Generate “small” primes $g_1, \ldots, g_n$
- Let $r_1, \ldots, r_n$ be “small” integers
- Let z be random integer
- Let κ be max encoding level

Encoding of vector $m \in \mathbb{Z}^n$ in level k:

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

CLT13 — Idea

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

Zero-test parameter:

$$p_{zt} = \sum_{i=1}^{n} h_i \left(z^\kappa \cdot g_i^{-1} \bmod p_i \right) \cdot \prod_{i' \neq i} p_{i'} \mod x_0$$

CLT13 — Idea

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

Zero-test parameter:

$$p_{zt} = \sum_{i=1}^{n} h_i \left(z^\kappa \cdot g_i^{-1} \bmod p_i \right) \cdot \prod_{i' \neq i} p_{i'} \mod x_0$$

Applying the zero-test to a κ-level encoding c:

$$p_{zt} \cdot c = \sum_{i=1}^{n} h_i \left(r_i + m_i \cdot (g_i^{-1} \bmod p_i) \right) \cdot \prod_{i' \neq i} p_{i'} \mod x_0$$

CLT13 — Idea

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

Adding encodings:

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

Multiplying encodings:

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

CLT13 — Public key

8 different parameters dependent on security parameter.

Notation: $\mathcal{R}$ means random number of appropriate size.

Public key pubKey:

- x_0
- p_{zt}
- τ random level-1 encodings of zero $\{x_j\}$ meaning $x_j = \mathrm{CRT}_{(p_i)}\left(\frac{\mathcal{R}g_i}{z}\right)$
- n more random level-1 encodings of zero
- ℓ random level-0 encodings of random values $\{x'_j\}$ meaning $x'_j = \mathrm{CRT}_{(p_i)}\left(\mathcal{R}g_i + \mathcal{R}\right)$
- Level-1 encoding of 1 $y = \mathrm{CRT}_{(p_i)}\left(\frac{\mathcal{R}g_i+1}{z}\right)$

CLT13 — More operations

$\mathbf{samp}(\text{pubKey})$: Pick random subset of $\{x'_j\}$ and add together.

$\mathbf{enc}(\text{pubKey}, c, k)$: Raise level-0 encoding c to level k by multiplying with y^k.

$\mathbf{reRand}(\text{pubKey}, c)$: Re-randomize level-1 encoding c (simplified version). Add to c sum of random subset of $\{x_j\}$.

$\mathbf{isZero}(\text{pubKey}, c)$: Test if level-$\kappa$ encoding c is zero (simplified version) by checking if $c \cdot p_{zt}$ is small enough.

$\mathbf{ext}(\text{pubKey}, c)$: Collect most significant bits of $c \cdot p_{zt}$ (simplified version).

DH with CLT13

Key exchange between $\kappa + 1$ parties.

Each party i: Let $a_i = \mathbf{samp}(\mathrm{pubKey})$ be secret random value and broadcast

$$h_i = \mathbf{reRand}(\mathrm{pubKey}, \mathbf{enc}(\mathrm{pubKey}, a_i, 1))$$

Shared encoding:

$$a_1 h_2 \dots h_{\kappa+1} = h_1 a_2 h_3 \dots h_{\kappa+1} = \dots = h_1 \dots h_\kappa a_{\kappa+1}$$

Shared value can be obtained by extraction.

CLT13 — Hardness assumption

Definition (Graded Descicional Diffie-Hellman (GDDH))

Consider following process:

1. Generate a public key pubKey with security parameter λ
2. Choose $a_j = \mathbf{samp}(\mathrm{pubKey})$ for all $1 \leq j \leq \kappa + 1$
3. Set $u_j = \mathbf{reRand}(\mathrm{pubKey}, \mathbf{enc}(\mathrm{pubKey}, 1, a_j))$ for all $1 \leq j \leq \kappa + 1$
4. Choose $b = \mathbf{samp}(\mathrm{pubKey})$
5. Set $v = \mathbf{reRand}(\mathrm{pubKey}, \mathbf{enc}(\mathrm{pubKey}, \kappa, \prod_{i=1}^{\kappa+1} a_i))$
6. Set $w = \mathbf{reRand}(\mathrm{pubKey}, \mathbf{enc}(\mathrm{pubKey}, \kappa, b))$

The GDDH assumption states that an attacker with runtime polynomial in λ has only negligible chance to differentiate v and w given the u_j and pubKey.

Section based on the paper of Cheon et al. 2014.

Definition (CRT-ACD Problem)

Let $n, \eta, \varepsilon \in \mathbb{N}$. Let χ_ε be distribution over $(-(2^\varepsilon), 2^\varepsilon) \cap \mathbb{Z}$. For given η-bit primes $p_1, \dots, p_n$ define

$$D_{\chi_\varepsilon,\eta,n}(p_1, \dots, p_n) = \left\{\mathrm{CRT}_{(p_i)}(r_i) \mid r_i \to \chi_\varepsilon\right\}.$$

CRT-ACD Problem: Given many samples from $D_{\chi_\varepsilon,\eta,n}(p_1, \dots, p_n)$ and $x_0 = \prod_{i=1}^n p_i$ find all p_i.

Attacking CLT13 — CRT-ACD

Section based on the paper of Cheon et al. 2014.

Definition (CRT-ACD Problem)

Let $n, \eta, \varepsilon \in \mathbb{N}$. Let χ_ε be distribution over $(-(2^\varepsilon), 2^\varepsilon) \cap \mathbb{Z}$. For given η-bit primes $p_1, \ldots, p_n$ define

$$D_{\chi_\varepsilon,\eta,n}(p_1, \ldots, p_n) = \left\{ \mathrm{CRT}_{(p_i)}(r_i) \mid r_i \to \chi_\varepsilon \right\}.$$

CRT-ACD Problem: Given many samples from $D_{\chi_\varepsilon,\eta,n}(p_1, \ldots, p_n)$ and $x_0 = \prod_{i=1}^{n} p_i$ find all p_i.

Let $\hat{p}_i = x_0/p_i$. $\hat{P} = \mathrm{CRT}_{(p_i)}(\hat{p}_i)$ is called auxillary input.

Lemma

Given $a = \mathrm{CRT}_{(p_i)}(r_i) \to D_{\chi_\varepsilon,\eta,n}(p_1, \ldots, p_n)$ *and* $\hat{P} = \mathrm{CRT}_{(p_i)}(\hat{p}_i)$ *it holds that*

$$\hat{P} \cdot a \bmod x_0 = \mathrm{CRT}_{(p_i)}(\hat{p}_i \cdot r_i) = \sum_{i=1}^{n} \hat{p}_i \cdot r_i$$

if $\varepsilon + \log n + 1 < \eta$.

Attacking CLT13 — CRT-ACD

Lemma

Given $a = \mathrm{CRT}_{(p_i)}(r_i) \to D_{\chi_\varepsilon,\eta,n}(p_1, \ldots, p_n)$ *and* $\hat{P} = \mathrm{CRT}_{(p_i)}(\hat{p}_i)$ *it holds that*

$$\hat{P} \cdot a \bmod x_0 = \mathrm{CRT}_{(p_i)}(\hat{p}_i \cdot r_i) = \sum_{i=1}^{n} \hat{p}_i \cdot r_i$$

if $\varepsilon + \log n + 1 < \eta$.

Sketch of proof: Consider second equation modulo p_i. Ensure that left side is smaller that x_0. Result follows from uniqueness of CRT.

Attacking CLT13 — CRT-ACD

Let $a = \mathrm{CRT}_{(p_i)}(a_i)$, $b = \mathrm{CRT}_{(p_i)}(b_i)$. Assume lemma is applicable:

$$ab\hat{P} \bmod x_0 = \sum a_i b_i \hat{p}_i$$

Attacking CLT13 — CRT-ACD

Let $a = \mathrm{CRT}_{(p_i)}(a_i)$, $b = \mathrm{CRT}_{(p_i)}(b_i)$. Assume lemma is applicable:

$$ab\hat{P} \bmod x_0 = \sum a_i b_i \hat{p}_i$$

As matrix equation:

$$ab\hat{P} \bmod x_0 = \begin{pmatrix} a_1 & a_2 & \cdots & a_n \end{pmatrix} \begin{pmatrix} \hat{p}_1 & 0 & \cdots & 0 \\ 0 & \hat{p}_2 & \cdots & 0 \\ 0 & 0 & \ddots & 0 \\ 0 & 0 & \cdots & \hat{p}_n \end{pmatrix} \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix}$$

Attacking CLT13 — CRT-ACD

Collecting more samples ($1 \le i, j \le n$):

$$a_i = \mathrm{CRT}_{(p_k)}\left(a_{k,i}\right), b = \mathrm{CRT}_{(p_k)}\left(b_k\right), c_j = \mathrm{CRT}_{(p_k)}\left(c_{k,j}\right)$$

Stating matrix equations:

$$w_{i,j} = \begin{pmatrix} a_{1,i} & a_{2,i} & \cdots & a_{n,i} \end{pmatrix} \begin{pmatrix} b_1 \hat{p}_1 & 0 & \cdots & 0 \\ 0 & b_2 \hat{p}_2 & \cdots & 0 \\ 0 & 0 & \ddots & 0 \\ 0 & 0 & \cdots & b_n \hat{p}_n \end{pmatrix} \begin{pmatrix} c_{1,j} \\ c_{2,j} \\ \vdots \\ c_{n,j} \end{pmatrix}$$

$$w'_{i,j} = \begin{pmatrix} a_{1,i} & a_{2,i} & \cdots & a_{n,i} \end{pmatrix} \begin{pmatrix} \hat{p}_1 & 0 & \cdots & 0 \\ 0 & \hat{p}_2 & \cdots & 0 \\ 0 & 0 & \ddots & 0 \\ 0 & 0 & \cdots & \hat{p}_n \end{pmatrix} \begin{pmatrix} c_{1,j} \\ c_{2,j} \\ \vdots \\ c_{n,j} \end{pmatrix}$$

Attacking CLT13 — CRT-ACD

$$w_{i,j} = \begin{pmatrix} a_{1,i} & a_{2,i} & \cdots & a_{n,i} \end{pmatrix} \begin{pmatrix} b_1\hat{p}_1 & 0 & \cdots & 0 \\ 0 & b_2\hat{p}_2 & \cdots & 0 \\ 0 & 0 & \ddots & 0 \\ 0 & 0 & \cdots & b_n\hat{p}_n \end{pmatrix} \begin{pmatrix} c_{1,j} \\ c_{2,j} \\ \vdots \\ c_{n,j} \end{pmatrix}$$

Collecting $w_{i,j}$ and $w'_{i,j}$ into matrices $\mathbf{W}$ and $\mathbf{W}'$:

$$\mathbf{W} = \mathbf{A}^T \cdot \mathrm{diag}(b_1\hat{p}_1, \ldots, b_n\hat{p}_n) \cdot C$$
$$\mathbf{W}' = \mathbf{A}^T \cdot \mathrm{diag}(\hat{p}_1, \ldots, \hat{p}_n) \cdot C$$

Attacking CLT13 — CRT-ACD

$$w_{i,j} = \begin{pmatrix} a_{1,i} & a_{2,i} & \cdots & a_{n,i} \end{pmatrix} \begin{pmatrix} b_1\hat{p}_1 & 0 & \cdots & 0 \\ 0 & b_2\hat{p}_2 & \cdots & 0 \\ 0 & 0 & \ddots & 0 \\ 0 & 0 & \cdots & b_n\hat{p}_n \end{pmatrix} \begin{pmatrix} c_{1,j} \\ c_{2,j} \\ \vdots \\ c_{n,j} \end{pmatrix}$$

Collecting $w_{i,j}$ and $w'_{i,j}$ into matrices $\mathbf{W}$ and $\mathbf{W}'$:

$$\mathbf{W} = \mathbf{A}^T \cdot \mathrm{diag}(b_1\hat{p}_1, \ldots, b_n\hat{p}_n) \cdot C$$
$$\mathbf{W}' = \mathbf{A}^T \cdot \mathrm{diag}(\hat{p}_1, \ldots, \hat{p}_n) \cdot C$$

Assume $\mathbf{A}$ and $\mathbf{C}$ are invertible:

$$\mathbf{W} \cdot \mathbf{W}'^{-1} = \mathbf{A}^T \cdot \mathrm{diag}(b_1, \ldots, b_n) \cdot \mathbf{A}^{T^{-1}}$$

$$\mathbf{W} \cdot \mathbf{W}'^{-1} = \mathbf{A}^T \cdot \mathrm{diag}(b_1, \ldots, b_n) \cdot \mathbf{A}^{T^{-1}}$$

Calculating eigenvalues of $\mathbf{W} \cdot \mathbf{W}'^{-1}$ yields $B = \{b_1, \ldots, b_n\}$.

Attacking CLT13 — CRT-ACD

$$\mathbf{W} \cdot \mathbf{W'}^{-1} = \mathbf{A}^T \cdot \mathrm{diag}(b_1, \ldots, b_n) \cdot \mathbf{A}^{T^{-1}}$$

Calculating eigenvalues of $\mathbf{W} \cdot \mathbf{W'}^{-1}$ yields $B = \{b_1, \ldots, b_n\}$.

Assume are b_i pairwise distinct:

$$\gcd(b - b_i, x_0) = p_i$$

Attacking CLT13 — Adapting the attack

Recall:

$$p_{zt} = \sum_{i=1}^{n} h_i \left(z^{\kappa} \cdot g_i^{-1} \bmod p_i \right) \cdot \prod_{i' \neq i} p_{i'} \mod x_0$$

Attacking CLT13 — Adapting the attack

Recall:

$$p_{zt} = \sum_{i=1}^{n} h_i \left(z^{\kappa} \cdot g_i^{-1} \bmod p_i \right) \cdot \prod_{i' \neq i} p_{i'} \mod x_0$$

Let $a = \mathrm{CRT}_{(p_i)}\left(r_i g_i / z^{\kappa}\right)$ be top-level encoding of 0.

$$p_{zt} \cdot a \bmod x_0 = \mathrm{CRT}_{(p_i)}\left(\hat{p}_i h_i r_i\right) = \sum_{i=1}^{n} \hat{p}_i h_i r_i$$

Attacking CLT13 — Adapting the attack

Recall:

$$p_{zt} = \sum_{i=1}^{n} h_i \left(z^\kappa \cdot g_i^{-1} \bmod p_i \right) \cdot \prod_{i' \neq i} p_{i'} \mod x_0$$

Let $a = \mathrm{CRT}_{(p_i)} \left(r_i g_i / z^\kappa \right)$ be top-level encoding of 0.

$$p_{zt} \cdot a \bmod x_0 = \mathrm{CRT}_{(p_i)} \left(\hat{p}_i h_i r_i \right) = \sum_{i=1}^{n} \hat{p}_i h_i r_i$$

We get similar attack by spanning

$$x'_j \cdot x'_1 \cdot x_k \cdot y^{\kappa-1} \cdot p_{zt} \bmod x_0 \text{ and } x'_j \cdot x_k \cdot y^{\kappa-1} \cdot p_{zt} \bmod x_0$$

for $1 \leq j, k \leq n$.

Current state

TODO: Slide really needed? Or just link to website? Or just CLT type constructions? CLT13 and improvement CLT15 broken in regards to GDDH [4, 3]. iO based on CLT13 has been broken in multiple cases [7, 6].

MZ17 (based on CLT13) is still standing regarding the GDDH assumption [9].

Lattice based approaches have been successfully attacked regarding GDDH and iO.

More (partially outdated) info: `https://malb.io/are-graded-encoding-schemes-broken-yet.html`

Why this topic?

DESCRIPTION

We identified a group of individuals who we suspect of insider trading and have captured their communication. However, they seem to use a fancy cryptographic construction called CLT13 to do their key exchange in just one round. Can you help us decrypt their secret?

Public files

Author

lukas|RedRocket

POINTS

500 + 480 Points (3 solves)

[1] Martin R Albrecht et al. "Multilinear maps from obfuscation". In: *Journal of Cryptology* (2020), pp. 1–34.

[2] Dan Boneh and Alice Silverberg. "Applications of multilinear forms to cryptography". In: *Contemporary Mathematics* 324.1 (2003), pp. 71–90.

[3] Jung Hee Cheon et al. *Cryptanalysis of the New CLT Multilinear Map over the Integers*. Cryptology ePrint Archive, Report 2016/135. `https://ia.cr/2016/135`. 2016.

[4] Jung Hee Cheon et al. *Cryptanalysis on the Multilinear Map over the Integers and its Related Problems*. Cryptology ePrint Archive, Report 2014/906. `https://ia.cr/2014/906`. 2014.

[5] Jean-Sebastien Coron, Tancrede Lepoint, and Mehdi Tibouchi. *Practical Multilinear Maps over the Integers*. Cryptology ePrint Archive, Report 2013/183. `https://ia.cr/2013/183`. 2013.

[6] Jean-Sebastien Coron and Luca Notarnicola. *Cryptanalysis of CLT13 Multilinear Maps with Independent Slots*. Cryptology ePrint Archive, Report 2019/309. `https://ia.cr/2019/309`. 2019.

[7] Jiseung Kim and Changmin Lee. *Cryptanalysis of FRS Obfuscation based on the CLT13 Multilinear Map*. Cryptology ePrint Archive, Report 2019/1254. `https://ia.cr/2019/1254`. 2019.

[8] Jia Liu et al. "How to build time-lock encryption". In: *Designs, Codes and Cryptography* 86.11 (2018), pp. 2549–2586.

[9] Fermi Ma and Mark Zhandry. *The MMap Strikes Back: Obfuscation and New Multilinear Maps Immune to CLT13 Zeroizing Attacks*. Cryptology ePrint Archive, Report 2017/946. `https://ia.cr/2017/946`. 2017.