An intro to multilinear maps and their attacks using the example of CLT13

Lukas Kempf

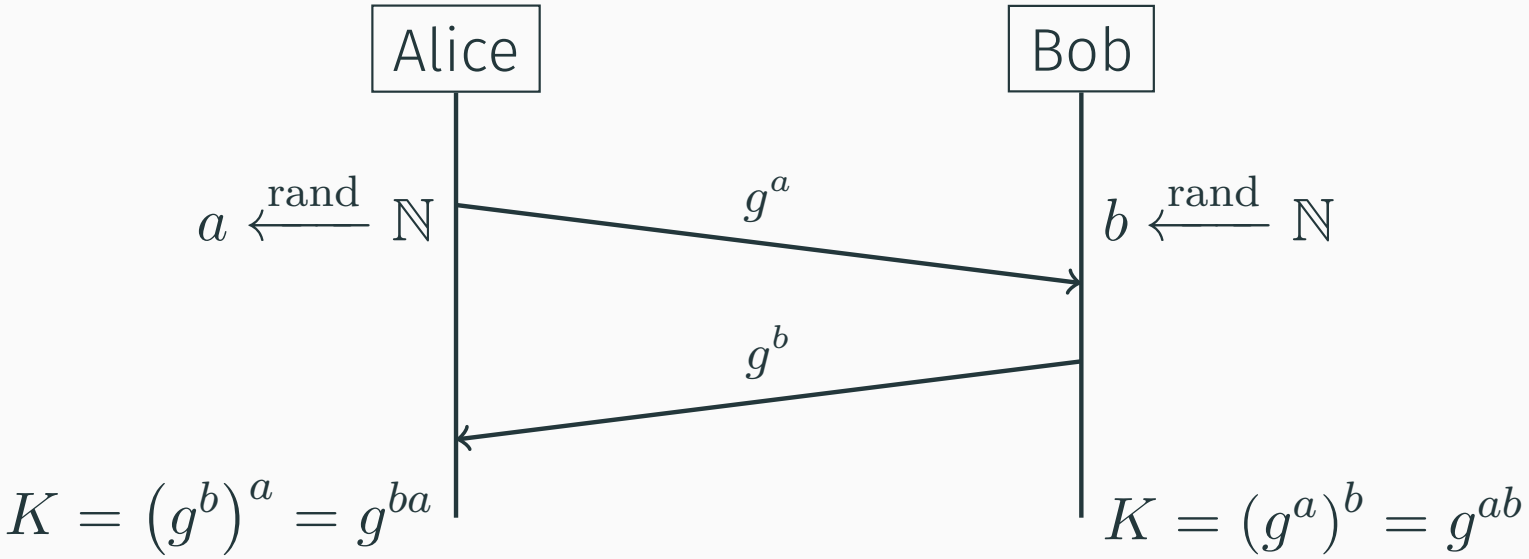
2021-12-10

Outline

- Multilinear maps
- CLT13
- DH with CLT13
- Attacking CLT13
- State of multilinear maps

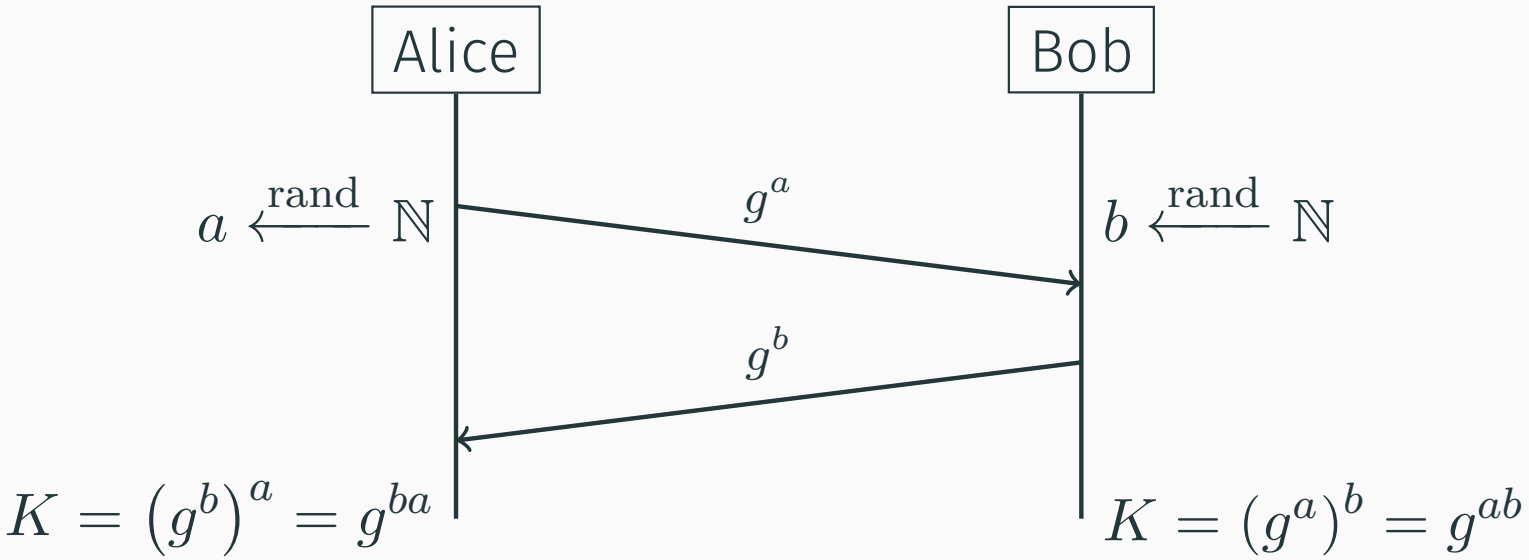
Diffie-Hellman key exchange

Let G be finite cyclic group with generator g.



Diffie-Hellman key exchange

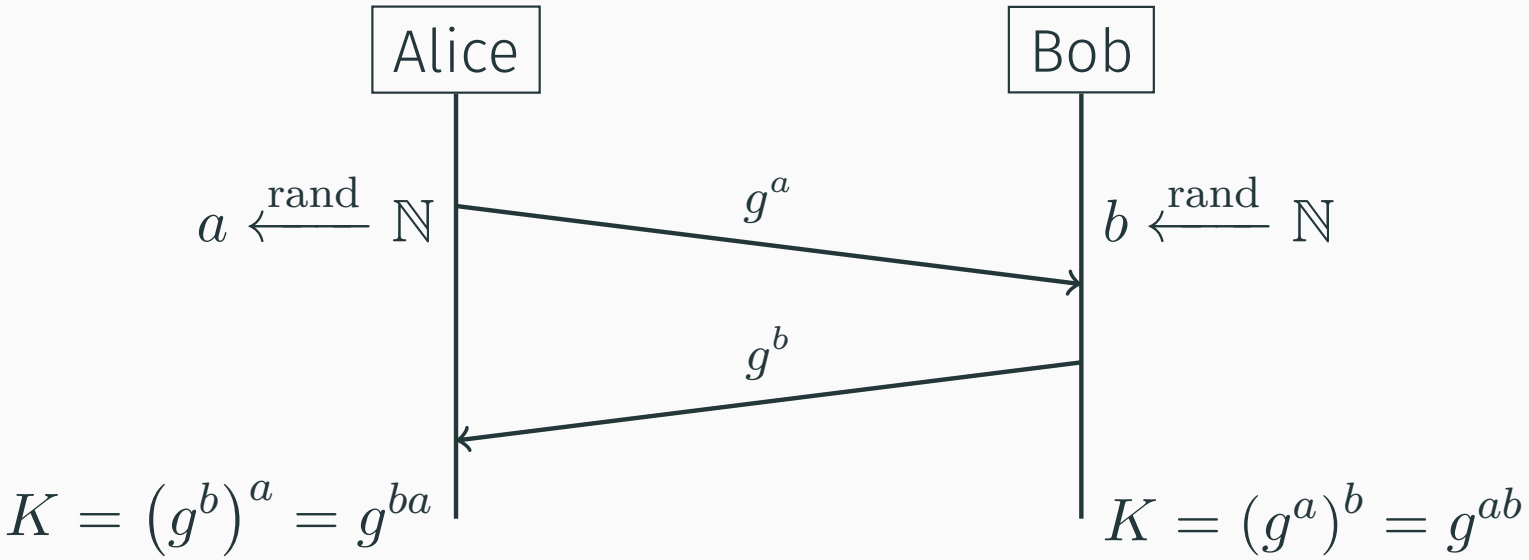
Let G be finite cyclic group with generator g.



$\Rightarrow$ Obtaining g^{ab} from g^a and g^b this must be hard (computational assumption).

Diffie-Hellman key exchange

Let G be finite cyclic group with generator g.



$\Rightarrow$ Obtaining g^{ab} from g^a and g^b this must be hard (computational assumption).

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

Multilinear maps

Definition (Multilinear Map Boneh et al. 2003)

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

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

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

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

DH with multilinear maps

With multilinear maps: DH between multiple parties in one round.

DH with multilinear maps

With multilinear maps: DH between multiple parties in one round.

Let $e : G_1^\kappa \to G_2$ be a κ-multilinear map and g a generator of G_1.

Each of the $\kappa + 1$ parties chooses $a_i \xleftarrow{\text{rand}} \mathbb{N}$ and broadcasts $f_i = g^{a_i}$.

$$e(f_2, \ldots, f_{\kappa+1})^{a_1} = e(f_1, f_3, \ldots, f_{\kappa+1})^{a_2} = \cdots$$
$$= e(f_1, \ldots, f_\kappa)^{a_{\kappa+1}} = e(g, \ldots, g)^{a_1 \cdots a_{\kappa+1}}$$

DH with multilinear maps

With multilinear maps: DH between multiple parties in one round.

Let $e : G_1^\kappa \to G_2$ be a κ-multilinear map and g a generator of G_1.

Each of the $\kappa + 1$ parties chooses $a_i \xleftarrow{\text{rand}} \mathbb{N}$ and broadcasts $f_i = g^{a_i}$.

$$e(f_2, \ldots, f_{\kappa+1})^{a_1} = e(f_1, f_3, \ldots, f_{\kappa+1})^{a_2} = \ldots$$
$$= e(f_1, \ldots, f_\kappa)^{a_{\kappa+1}} = e(g, \ldots, g)^{a_1 \cdots a_{\kappa+1}}$$

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

How to construct such maps?

"The central open problem posed in this paper is the construction of cryptographic multilinear map generators when $\kappa > 2$." (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 $\kappa > 2$." (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)

Graded encoding schemes

Somewhat similar to homomorphic encodings.

For every $r \in R$ and level $t \in \mathbb{N}$ we have a set $S_t^{(r)}$ of possible encodings.

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

Multiplication is possible: For $v_1 \in S_{t_1}^{(r_1)}$ and $v_2 \in S_{t_2}^{(r_2)}$ we have $v_1 \cdot v_2 \in S_{t_1+t_2}^{(r_1 \cdot r_2)}$ if $t_1 + t_2 \leq \kappa$, the maximum level.

Interpretation of graded multilinear maps

Let $v \in S_t^{(r)}$ be a level t encoding of $r \in \mathbb{Z}$. Let G_1 be a group with generator g.

For $t = 0$ interpret v as a scalar r.

For $t = 1$ interpret v as group element $g^r \in G_1$.

Interpretation of graded multilinear maps

Let $v \in S_t^{(r)}$ be a level t encoding of $r \in \mathbb{Z}$. Let G_1 be a group with generator g.

For $t = 0$ interpret v as a scalar r.

For $t = 1$ interpret v as group element $g^r \in G_1$.

Let v_1 and v_2 be two level-1 encodings of r_1 and r_2. Interpret $v_1 + v_2$ as $g^{r_1+r_2}$. Interpret $v_1 \cdot v_2$ as evaluation of some multilinear pairing $e(g^{r_1}, g^{r_2}) = e(g, g)^{r_1 \cdot r_2}$.

Interpretation of graded multilinear maps

Let $v \in S_t^{(r)}$ be a level t encoding of $r \in \mathbb{Z}$. Let G_1 be a group with generator g.

For $t = 0$ interpret v as a scalar r.

For $t = 1$ interpret v as group element $g^r \in G_1$.

Let v_1 and v_2 be two level-1 encodings of r_1 and r_2. Interpret $v_1 + v_2$ as $g^{r_1+r_2}$. Interpret $v_1 \cdot v_2$ as evaluation of some multilinear pairing $e(g^{r_1}, g^{r_2}) = e(g, g)^{r_1 \cdot r_2}$.

$\Rightarrow$We can see $e(g, g)$ as the generator of some group G_2 of level-2 encodings.

Chinese remainder theorem

Theorem (Chinese remainder theorem over the integers)

Let $\{p_1, \ldots, p_n\}$ be pairwise coprime integers and $M = \prod_i^n p_i$. Then there exists a unique ring isomorphism

$\mathbb{Z}_M \cong \mathbb{Z}_{p_1} \times \cdots \times \mathbb{Z}_{p_n}$.

More concretely we have maps

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

and

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

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

Notation: $x = \mathrm{CRT}_{(p_i)}([x_i])$

CLT13 — Idea

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

- Use CRT to operate in small secret rings while only one large value is public
- Generate n primes $p_1, \ldots, p_n$ for CRT and compute $M := \prod_i^n p_i$
- Generate "small" primes $g_1, \ldots, g_n$
- Let $r_1, \ldots, r_n$ be "small" integers (noise)
- Let d be random integer
- Let κ be max encoding level

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

$$c \equiv \frac{r_i \cdot g_i + m_i}{d^t} \mod p_i$$

CLT13 — Idea

$$c \equiv \frac{r_i \cdot g_i + m_i}{d^t} \mod p_i$$

Adding encodings:

$$\frac{r_i \cdot g_i + m_i}{d^t} + \frac{r'_i \cdot g_i + m'_i}{d^t} \equiv \frac{(r_i + r'_i) \cdot g_i + m_i + m'_i}{d^t} \mod p_i$$

Multiplying encodings:

$$\frac{r_i \cdot g_i + m_i}{d^t} \cdot \frac{r'_i \cdot g_i + m'_i}{d^{t'}} \equiv \frac{r_i^\dagger \cdot g_i + m_i \cdot m'_i}{d^{t+t'}} \mod p_i$$

CLT13 — Idea

$$c \equiv \frac{r_i \cdot g_i + m_i}{d^t} \mod p_i$$

Zero-test parameter:

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

CLT13 — Idea

$$c \equiv \frac{r_i \cdot g_i + m_i}{d^t} \mod p_i$$

Zero-test parameter:

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

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

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

CLT13 — Public key

Security parameter λ influences multiple internal parameters (omitted).

Notation: rand means random number of appropriate size.

Public key pubKey (simplified):

- $M := \prod_i^n p_i$
- p_{zt}
- Level-1 encodings of zero $\{z_j\}$ meaning $z_j = \mathrm{CRT}_{(p_i)}\left(\left[\frac{\mathrm{rand} \cdot g_i}{d}\right]\right)$
- Level-0 encodings of random values $\{x'_j\}$ meaning $x'_j = \mathrm{CRT}_{(p_i)}\left([\mathrm{rand} \cdot g_i + \mathrm{rand}]\right)$
- Level-1 encoding of 1 $y = \mathrm{CRT}_{(p_i)}\left(\left[\frac{\mathrm{rand} \cdot g_i + 1}{d}\right]\right)$

CLT13 — More operations

$\mathbf{samp}(\mathrm{pubKey})$: To get random level-0 encoding pick random subset of $\{x'_j\}$ and add together.

CLT13 — More operations

$\mathbf{samp}(\mathrm{pubKey})$: To get random level-0 encoding pick random subset of $\{x'_j\}$ and add together.

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

CLT13 — More operations

$\mathbf{samp}(\mathrm{pubKey})$: To get random level-0 encoding pick random subset of $\{x'_j\}$ and add together.

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

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

DH with CLT13 — First idea

Key exchange between $\kappa + 1$ parties.

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

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

Shared encoding:

$$\mathbf{ext}(a_1 f_2 \cdots f_{\kappa+1}) = \mathbf{ext}(f_1 a_2 f_3 \cdots f_{\kappa+1}) = \cdots = \mathbf{ext}(f_1 \cdots f_\kappa a_{\kappa+1})$$

DH with CLT13 — First idea

Key exchange between $\kappa + 1$ parties.

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

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

Shared encoding:

$$\mathbf{ext}(a_1 f_2 \cdots f_{\kappa+1}) = \mathbf{ext}(f_1 a_2 f_3 \cdots f_{\kappa+1}) = \cdots = \mathbf{ext}(f_1 \cdots f_\kappa a_{\kappa+1})$$

Problem: $f_i \cdot y^{-1} \equiv a_i \cdot y \cdot y^{-1} \equiv a_i \mod M$!

DH with CLT13

Solution: Add noise to the encoding.

$\mathbf{reRand}(\mathrm{pubKey}, c)$: Re-randomize level-1 encoding c by adding sum of random subset of $\{z_j\}$ to c (simplified).

DH with CLT13

Solution: Add noise to the encoding.

$\mathbf{reRand}(\mathrm{pubKey}, c)$: Re-randomize level-1 encoding c by adding sum of random subset of $\{z_j\}$ to c (simplified).

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

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

DH with CLT13

Solution: Add noise to the encoding.

$\mathbf{reRand}(\mathrm{pubKey}, c)$: Re-randomize level-1 encoding c by adding sum of random subset of $\{z_j\}$ to c (simplified).

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

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

Shared encoding doesn't change:

$$\mathbf{ext}(a_1 f_2 \cdots f_{\kappa+1}) = \mathbf{ext}(f_1 a_2 f_3 \cdots f_{\kappa+1}) = \cdots = \mathbf{ext}(f_1 \cdots f_\kappa a_{\kappa+1})$$

CLT13 — Hardness assumption

Given a public key pubKey with security parameter λ generate:

Real encoding:

1. Choose random level-0 encoding a_j for all $1 \leq j \leq \kappa + 1$.
2. Set $u_j = \mathbf{reRand}(\mathrm{pubKey}, \mathbf{enc}(\mathrm{pubKey}, 1, a_j))$ to obtain level-1 encoding for all $1 \leq j \leq \kappa + 1$.
3. Set $v = \mathbf{reRand}(\mathrm{pubKey}, \mathbf{enc}(\mathrm{pubKey}, \kappa, \prod_{i=1}^{\kappa+1} a_i))$.

CLT13 — Hardness assumption

Given a public key pubKey with security parameter λ generate:

Real encoding:

1. Choose random level-0 encoding a_j for all $1 \leq j \leq \kappa + 1$.
2. Set $u_j = \mathbf{reRand}(\mathrm{pubKey}, \mathbf{enc}(\mathrm{pubKey}, 1, a_j))$ to obtain level-1 encoding for all $1 \leq j \leq \kappa + 1$.
3. Set $v = \mathbf{reRand}(\mathrm{pubKey}, \mathbf{enc}(\mathrm{pubKey}, \kappa, \prod_{i=1}^{\kappa+1} a_i))$.

Random encoding:

1. Choose random level-0 encoding b.
2. Set $w = \mathbf{reRand}(\mathrm{pubKey}, \mathbf{enc}(\mathrm{pubKey}, \kappa, b))$.

The GDDH assumption states that a polynomial attacker has only negligible chance to differentiate v and w given the u_j and pubKey.

Attacking CLT13 — CRT-ACD

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

Before attacking CLT13 we look at a simpler but similar problem:

Definition (CRT-ACD Problem)

Let $n, \eta, \varepsilon \in \mathbb{N}$. For given η-bit primes $p_1, \ldots, p_n$ define the distribution

$$D_{\varepsilon,\eta,n}(p_1, \ldots, p_n) = \left\{ \mathrm{CRT}_{(p_i)}\left([r_i]\right) \mid r_i \xleftarrow{\text{rand}} (-2^{\varepsilon}, 2^{\varepsilon}) \cap \mathbb{Z} \right\}.$$

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

Attacking CLT13 — CRT-ACD

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

Before attacking CLT13 we look at a simpler but similar problem:

Definition (CRT-ACD Problem)

Let $n, \eta, \varepsilon \in \mathbb{N}$. For given η-bit primes $p_1, \ldots, p_n$ define the distribution

$$D_{\varepsilon,\eta,n}(p_1, \ldots, p_n) = \left\{ \mathrm{CRT}_{(p_i)}\left([r_i]\right) \mid r_i \xleftarrow{\text{rand}} (-2^{\varepsilon}, 2^{\varepsilon}) \cap \mathbb{Z} \right\}.$$

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

Let $\hat{p}_i = M/p_i$. $\hat{P} = \mathrm{CRT}_{(p_i)}\left([\hat{p}_i]\right)$ is called auxillary input. This can be seen as simpler version of p_{zt}.

Attacking CLT13 — CRT-ACD

Lemma

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

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

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

Attacking CLT13 — CRT-ACD

Lemma

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

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

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

$\Rightarrow$ Reduces modular arithmetics to linear equation.

Attacking CLT13 — CRT-ACD

Lemma

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

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

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

$\Rightarrow$ Reduces modular arithmetics to linear equation.

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

Attacking CLT13 — CRT-ACD

We now clevery apply the reduction to linear equations to recover the secret p_i.

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

$$ab\hat{P} \bmod M = \sum_{i=1}^{n} a_i b_i \hat{p}_i$$

Attacking CLT13 — CRT-ACD

We now clevery apply the reduction to linear equations to recover the secret p_i.

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

$$ab\hat{P} \bmod M = \sum_{i=1}^{n} a_i b_i \hat{p}_i$$

As matrix equation:

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

Attacking CLT13 — CRT-ACD

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

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

Using the samples to state matrix equations:

$$w_{i,j} = a_i \cdot \hat{P} b \cdot c_j \bmod M = \begin{pmatrix} a_{1,i} & \cdots & a_{n,i} \end{pmatrix} \begin{pmatrix} b_1\hat{p}_1 & \cdots & 0 \\ 0 & \ddots & 0 \\ 0 & \cdots & b_n\hat{p}_n \end{pmatrix} \begin{pmatrix} c_{1,j} \\ \vdots \\ c_{n,j} \end{pmatrix}$$

$$w'_{i,j} = a_i \cdot \hat{P} \cdot c_j \bmod M = \begin{pmatrix} a_{1,i} & \cdots & a_{n,i} \end{pmatrix} \begin{pmatrix} \hat{p}_1 & \cdots & 0 \\ 0 & \ddots & 0 \\ 0 & \cdots & \hat{p}_n \end{pmatrix} \begin{pmatrix} c_{1,j} \\ \vdots \\ c_{n,j} \end{pmatrix}$$

Attacking CLT13 — CRT-ACD

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

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

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

with $\mathbf{A}^T = (a_{k,i})$ and $\mathbf{C} = (c_{k,j})$.

Attacking CLT13 — CRT-ACD

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

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

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

with $\mathbf{A}^T = (a_{k,i})$ and $\mathbf{C} = (c_{k,j})$.

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

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

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 $B = \{b_1, \ldots, b_n\}$ by the spectral theorem.

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 $B = \{b_1, \ldots, b_n\}$ by the spectral theorem.

Assume are b_i pairwise distinct:

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

Attacking CLT13 — Adapting the attack

Recall:

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

Attacking CLT13 — Adapting the attack

Recall:

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

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

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

Lemma applies because for encodings of 0 $p_{zt} \cdot a$ is short enough.

Attacking CLT13 — Adapting the attack

Recall:

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

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

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

Lemma applies because for encodings of 0 $p_{zt} \cdot a$ is short enough.

We get similar attack by spanning

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

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

Why multilinear maps matter

- DH key-exchange between multiple parties in one round.
- Efficient message broadcast to subset of recipients.
- Existence of cryptographic multilinear maps linked to the existence of indistinguishability obfuscation.
- Building block for time-lock encryption.

Current state of multilinear maps

CLT13 and improvement CLT15 broken in regards to GDDH. iO based on CLT13 has been broken in multiple cases.

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

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`

Conclusion

- Multilinear maps are building block for a lot of new and interesting constructions.
- Current known instantiations are quite complex.
- Many have been broken.
- Existence of practical and secure multilinear maps still unknown.
- $\Rightarrow$ Lots of ongoing research.

Why this topic?

- Topic was chosen as basis for CTF-Challenge originally.
- Plan: Implement DH with CLT13 and let players implement the attack.

Why this topic?

- Topic was chosen as basis for CTF-Challenge originally.
- Plan: Implement DH with CLT13 and let players implement the attack.
- However: Calculating eigenvalues of larger matrix with large integers is a bit slow.
- Solution: Use weak re-randomization instead.
- If you like applying cryptography it might be fun to look at CTFs.