FHE Reading Group - January 20
Linear Transform in in BFV (Bootstrapping)

Simon Pohmann

January 21, 2023

Where do we use it?

$$
\begin{tikzcd}
& & & \text{Input ciphertext } (c_0, c_1) \arrow[d] & \\
\mathrm{bk} \arrow[rrr] & & & \text{Noisy message } \tilde{m} = c_0 + c_1 s \arrow[dll] \arrow[dl] \arrow[dr] & \\
& \tilde{m}_0 \arrow[dd] & \tilde{m}_1 \arrow[dd] & \cdots & \tilde{m}_{N-1} \arrow[dd] \\
& & & \text{digit extraction} & \\
& m_0 \arrow[drr] & m_1 \arrow[dr] & \cdots & m_{N-1} \arrow[dl] \\
& & & \text{Result } m &
\end{tikzcd}
$$

SIMD via slots

Plaintext space is $\mathcal{P} = R/p^e R$, where $R = \mathbb{Z}[X]/(X^N + 1)$;
Assume $e = 1$
$\Rightarrow \mathcal{P} = \mathbb{F}_p[X]/(X^N + 1)$

Remark
$X^N + 1$ is irreducible in $\mathbb{Z}$

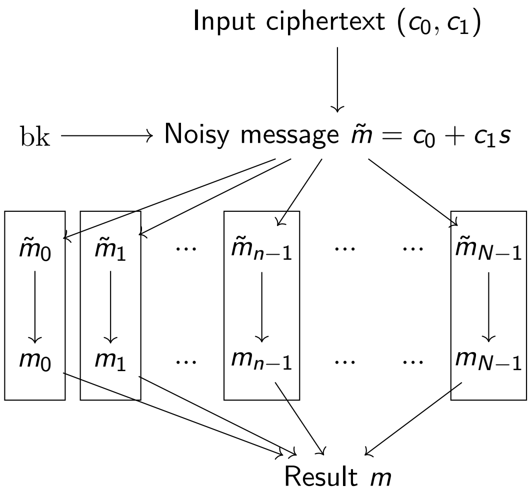
Proposition

- $X^N + 1 \equiv f_1 \ldots f_n \mod p$ *where* $n = \mathrm{ord}_{(\mathbb{Z}/2N\mathbb{Z})^*}(p)$
- *f_i irreducible of degree $d = N/n$*

$$\Rightarrow \quad \mathcal{P} \cong \bigoplus_{i=1}^{n} \mathbb{F}_{p^d}$$

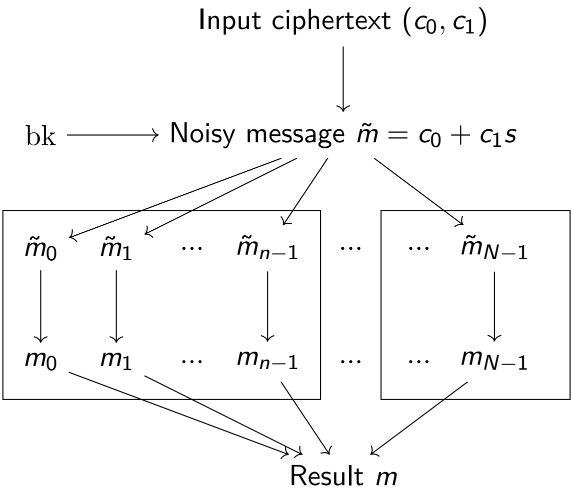
One operation in $\mathcal{P} \approx n$ operations, one on each slot $\mathbb{F}_{p^d}$

Using it



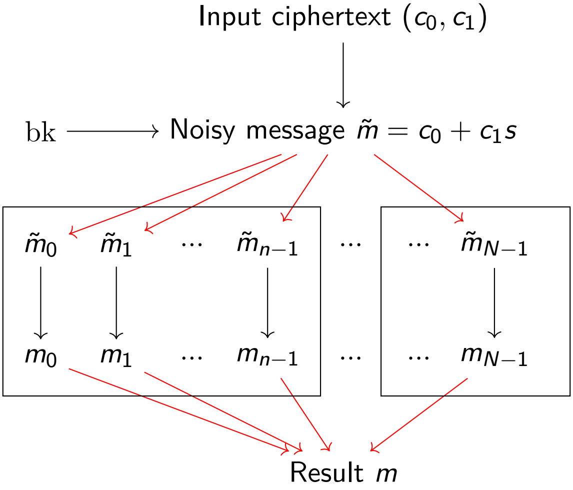
N digit extractions

Using it (cont'd)



N/n digit extractions

Using it (cont'd)



"Evaluation map"

The “Evaluation map”

$$\begin{aligned} \text{“Evaluation map”}: \quad \mathcal{P} &\rightarrow \bigoplus \mathbb{F}_{p^d} \cong \mathcal{P} \\ \sum a_i X^i &\mapsto (a_i)_{0\leq i<d} \end{aligned}$$

It is $\mathbb{F}_p$-linear!

Proposition

The $\mathbb{F}_p$-vector space

$$\mathcal{L} := \{f : \mathcal{P} \rightarrow \mathcal{P} \mid f \ \mathbb{F}_p\text{-linear}\}$$

is spanned by

$$\begin{aligned} &\{m_k : \alpha \mapsto X^k \alpha \mid k \in \{0, \ldots, N-1\}\} \\ \circ \ &\{\sigma_k : X \mapsto X^k \mid k \in (\mathbb{Z}/2N\mathbb{Z})^*\} \end{aligned}$$

Computing linear transforms

Proposition

The $\mathbb{F}_p$-vector space

$$\mathcal{L} := \{f : \mathcal{P} \to \mathcal{P} \mid f \ \mathbb{F}_p\text{-linear}\}$$

is spanned by

$$\begin{gathered}\{m_k : \alpha \mapsto X^k \alpha \mid k \in \{0, \dots, N-1\}\} \\ \circ \ \{\sigma_k : X \mapsto X^k \mid k \in (\mathbb{Z}/2N\mathbb{Z})^*\}\end{gathered}$$

$\Rightarrow$ Every $\mathbb{F}_p$-linear map can be written as

$$\alpha \mapsto \sum_{k \in (\mathbb{Z}/2N\mathbb{Z})^*} a_k \sigma_k(\alpha)$$

where $a_k \in \mathcal{P}$

More intuitive structure - or how to find the a_k

- $k \in \langle p \rangle \subseteq (\mathbb{Z}/2N\mathbb{Z})^* \Rightarrow \sigma_k$ is Frobenius within each slot
- Otherwise $\Rightarrow \sigma_k$ permutes slots (up to inter-slot auto.)

We have

$$(\mathbb{Z}/2N\mathbb{Z})^*/\langle p \rangle = \langle g_1 \rangle \times \ldots \times \langle g_r \rangle$$

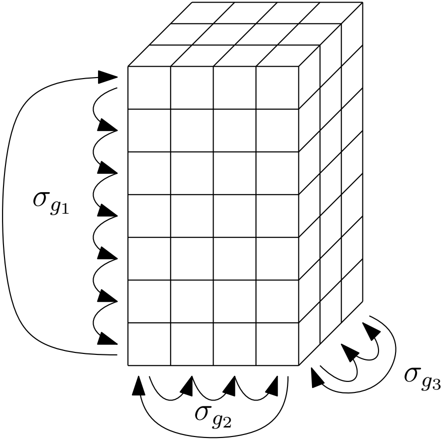
$\Rightarrow (\mathbb{Z}/2N\mathbb{Z})^*/\langle p \rangle$ has structure of an r-dimensional hypercube

We fix a "slot 0" (arbitrarily) $\Rightarrow$ Slots inherit hypercube structure

$$S : \mathcal{P} \xrightarrow{\sim} \bigoplus_{l \in (\mathbb{Z}/2N\mathbb{Z})^*/\langle p \rangle} \mathbb{F}_{p^d}$$

More intuitive structure - or how to find the a_k (cont'd)

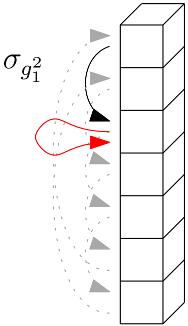
Example: $r = 3$, $(\mathrm{ord}(g_1), \mathrm{ord}(g_2), \mathrm{ord}(g_3)) = (7, 4, 2)$



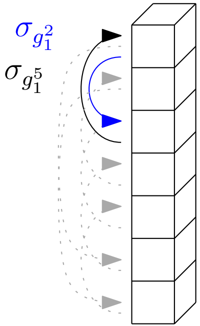
Good and bad dimensions

Problem: $k \notin \langle p \rangle \Rightarrow \sigma_k$ permutes slots **(up to inter-slot auto.)**

Slots have no “natural” generator / $\mathbb{F}_{p^d}$ unique only up to iso. - what do we mean by inter-slot automorphism?



$\rightarrow$ can be “defined away”



$\sigma_{g_1^5} \circ \sigma_{g_1^2}$ stays in slot

$\sigma_{g_1^5} \circ \sigma_{g_1^5}$ might not be identity

Good and bad dimensions (cont'd)

We require that $\sigma_{g_i^{d_i}}$ is identity (d_i hypercube length)

Proposition

$\sigma_{g_i^{d_i}} = \mathrm{id} \quad \Leftrightarrow \quad \mathrm{ord}_{(\mathbb{Z}/2N\mathbb{Z})^*}(g_i) = d_i.$
(note that $d_i = \mathrm{ord}_{(\mathbb{Z}/2N\mathbb{Z})^*/\langle p \rangle}$)

- If this is the case, we call the i-th dimension *good*
- Otherwise, we call it *bad*

Remark

If i-th dim is bad, we can still compute the rotation as

$$\alpha \mapsto \sigma_{g_1^{\delta}}(\alpha \cdot e) + \sigma_{g_1^{D-\delta}}(\alpha \cdot (1 - e))$$

where

$$D = \mathrm{ord}_{(\mathbb{Z}/2N\mathbb{Z})^*}(g_1)$$

and e is 1 in the first $d_i - \delta$ slots, and 0 in the others

Good and bad dimensions (cont'd)

- Some dimensions are good, some bad
- Rotation in good dimension: 1 Galois op
- Rotation in bad dimension: 2 Galois ops

Proposition

We can choose the g_i such that only one dimension is bad

So far: Rotations along a hypercube axis are easier to understand than the action of the group $(\mathbb{Z}/2N\mathbb{Z})^*$ via σ.

Back to the evaluation map

We want to write the evaluation map as a linear transform

We explain the map

$$\mathrm{Eval} : \mathcal{P} \cong \bigoplus \mathbb{F}_{p^d} \to \mathcal{P}, \quad (a_i) \mapsto \sum a_i X^i$$

Remark

There are "intermediate representations" in the decomposition

$$\mathcal{P} \cong \bigoplus^{d_1} \bigoplus^{d_2} \dots \bigoplus^{d_r} \mathbb{F}_{p^d}$$

Let

$$\mathcal{P}_i = \bigoplus^{d_i} \dots \bigoplus^{d_r} \mathbb{F}_{p^d} \quad \Rightarrow \quad \mathcal{P} = \bigoplus^{d_1} \dots \bigoplus^{d_{i-1}} \mathcal{P}_i$$

Back to the evaluation map (cont'd)

$$\mathrm{Eval} : \mathcal{P} \cong \bigoplus \mathbb{F}_{p^d} \to \mathcal{P}, \quad (a_i) \mapsto \sum a_i X^i$$

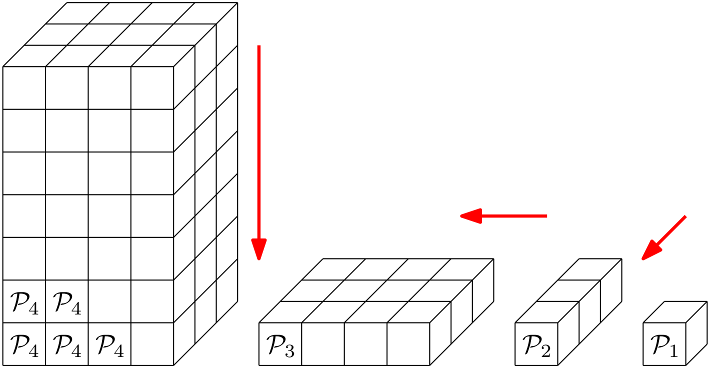
Do Eval along one hypercube dim:

$$\begin{aligned}\mathrm{Eval}_i : \bigoplus^{d_1} \dots \bigoplus^{d_i} \mathcal{P}_{i+1} &\to \bigoplus^{d_1} \dots \bigoplus^{d_{i-1}} \mathcal{P}_i \\ \left((a_{j_1,\dots,j_i})_{j_i}\right)_{j_1,\dots,j_{i-1}} &\mapsto \left(\sum_{j_i} a_{j_1,\dots,j_i} \zeta_i^{j_i}\right)_{j_1,\dots,j_{i-1}}\end{aligned}$$

where $\zeta_i = X^{d_{i+2} \dots d_r}$

$$\Rightarrow \quad \mathrm{Eval} = \mathrm{Eval}_1 \circ \dots \circ \mathrm{Eval}_r$$

Back to the evaluation map (cont'd)



Why all of this?

We can just solve a (huge) linear system to find $a_k \in \mathcal{P}$ such that

$$\alpha \mapsto \sum_{k \in (\mathbb{Z}/2N\mathbb{Z})^*} a_k \sigma_k(\alpha)$$

is the transform.

Two Reasons

- The system is not easy to solve (irrelevant in practice)
- Performance!
  - In some cases, we can compute Eval_i with 1 resp. 2 autos.!
  - Runtime: $2\log_2(n)$ autos. instead of n (or $2\sqrt{n}$)!
  - Which cases? dimension is good!

Good dimensions and the factorization of Eval

Problem: $k \notin \langle p \rangle \Rightarrow \sigma_k$ permutes slots **(up to inter-slot auto.)**

Slots have no "natural" generator / $\mathbb{F}_{p^d}$ unique only up to iso. - what do we mean by inter-slot automorphism?

Well, I think $\overline{X}$ is a "natural" generator!

- Good dimension: Only one auto. for rotation $\Rightarrow$ instead of $\overline{X}$, we use $\overline{X}^k$ such that k cancels out after all rotations
- Bad dimension: Two autos. so it is impossible that k cancels out w.r.t. two different rotations

Good dimensions and the factorization of Eval (cont'd)

- Good dimension: Only one auto. for rotation $\Rightarrow$ instead of $\overline{X}$, we use $\overline{X}^k$ such that k cancels out after all rotations
- Bad dimension: Two autos. so it is impossible that k cancels out w.r.t. two different rotations

$$\mathrm{Eval}'_i : \bigoplus_{j_1} \dots \bigoplus_{j_i} \mathcal{P}_{i+1} \ \rightarrow \ \bigoplus_{j_1} \dots \bigoplus_{j_{i-1}} \mathcal{P}_i$$

$$(a_{j_1,\dots,j_i})_{j_1,\dots,j_i} \ \mapsto \ \left(\sum_{j_i=0}^{d_i-1} a_{j_1,\dots,j_i} (\overline{X}^{g_i^{d_i-j_i}}) \ \overline{X}^{\left(\Delta_i j_i \underbrace{g_1^{j_i} \dots g_i^{j_i}}_{\text{``correction factor''}}\right)} \right)_{j_1,\dots,j_{i-1}}$$

where $\Delta_i = d_r \dots d_{i+1}$.

Summary

What we did talk about

- Galois group $(\mathbb{Z}/2N\mathbb{Z})^*$ acts on $\mathbb{F}_p[X]/(X^N + 1)$
- "Hypercube structure" as simplification of that action
- Describing the evaluation map in that framework

What we only sketched

- Implementation of Eval'_i
- Why Eval'_i is impossible in bad dimensions