Homomorphic polynomial evaluation using Galois structure and applications to BFV bootstrapping

Hiroki Okada[2] Rachel Player[1] Simon Pohmann[1]

Royal Holloway, University of London, UK

KDDI Research, Japan

October 5, 2023

Motivation

- TFHE is great!
- But sometimes BFV can achieve better performance
  - Parallelism via slots
  - Plaintext space has more structure
- [LW23]: BFV bootstrapping for LWE (TFHE) ciphertexts

- Polynomial evaluation is fascinating
- This setting is unusual and new

BFV

Plaintext space	$R_t = R/tR$
Ciphertext space	R_q^2
Secret key	$s \in R_q$

where $R := \mathbb{Z}[X]/(X^N + 1)$

- Message m stored in highest significant bits

$$c_0 + c_1 s \approx \frac{q}{t} m$$

- Homomorphic $+, \cdot$ and Galois automorphisms

Bootstrapping BFV

Plaintext	$m \in R_t$	
Ciphertext	$(c_0, c_1) \in R_q^2$	$c_0 + c_1 s \approx \frac{q}{t} m$
Secret key	$s \in R_q$	

Assume $t = p$, $q = p^e$ (bootstrapped ciphertext).

$$\text{Decryption: } m = \left\lfloor p^{1-e}(c_0 + c_1 s) \right\rceil$$

Difficulty: Rounded division by p^{e-1}

$\Updownarrow$

Floor-division by p^{e-1}

$\Updownarrow$

Get least significant p-adic digit

Bootstrapping BFV

Plaintext	$m \in R_t$
Ciphertext	$(c_0, c_1) \in R_q^2$
Secret key	$s \in R_q$

$$\mathrm{Dec}(c_0, c_1) = \lfloor p^{1-e}(c_0 + c_1 s) \rceil$$

Theorem ([HS21])

Polynomial $f \in \mathbb{Z}[X]$ *with* $\deg(f) \leq p$ *such that*

$$f(z_0 + p^i z_1) \equiv z_0 \mod p^{i+1}.$$

for $z_0 \in \{0, ..., p-1\}$, $z_1 \in \mathbb{Z}$, $i < e$

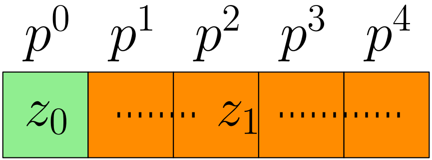
Bootstrapping BFV

Theorem ([HS21])

Polynomial $f \in \mathbb{Z}[X]$ *with* $\deg(f) \leq p$ *such that*

$$f(z_0 + p^i z_1) \equiv z_0 \mod p^{i+1}.$$

for $z_0 \in \{0, ..., p-1\}$, $z_1 \in \mathbb{Z}$, $i < e$



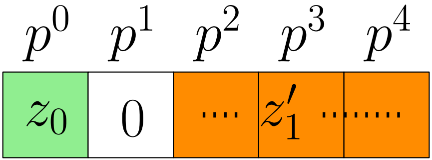
Bootstrapping BFV

Theorem ([HS21])

Polynomial $f \in \mathbb{Z}[X]$ *with* $\deg(f) \leq p$ *such that*

$$f(z_0 + p^i z_1) \equiv z_0 \mod p^{i+1}.$$

for $z_0 \in \{0, ..., p-1\}$, $z_1 \in \mathbb{Z}$, $i < e$



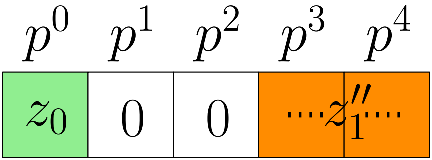
Bootstrapping BFV

Theorem ([HS21])

Polynomial $f \in \mathbb{Z}[X]$ *with* $\deg(f) \leq p$ *such that*

$$f(z_0 + p^i z_1) \equiv z_0 \mod p^{i+1}.$$

for $z_0 \in \{0, \ldots, p-1\}$, $z_1 \in \mathbb{Z}$, $i < e$



Bootstrapping BFV

Theorem ([HS21])

Polynomial $f \in \mathbb{Z}[X]$ *with* $\deg(f) \leq p$ *such that*

$$f(z_0 + p^i z_1) \equiv z_0 \mod p^{i+1}.$$

for $z_0 \in \{0, ..., p-1\}$, $z_1 \in \mathbb{Z}$, $i < e$

p^0	p^1	p^2	p^3	p^4
z_0	0	0	0	z_1'''

Bootstrapping BFV

Theorem ([HS21])

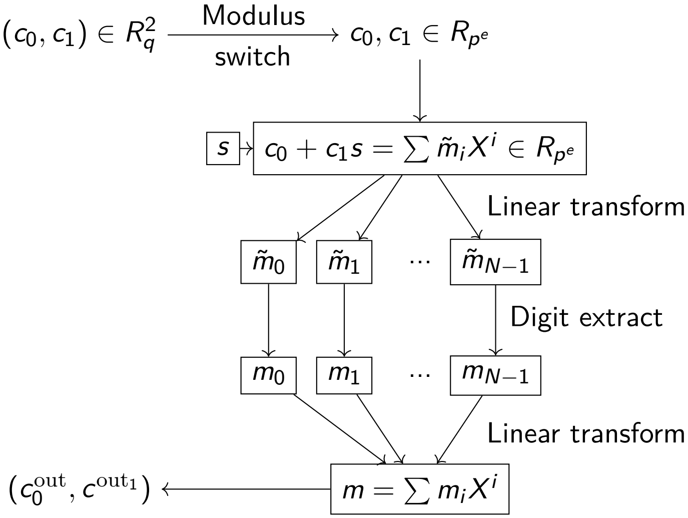
Polynomial $f \in \mathbb{Z}[X]$ *with* $\deg(f) \leq p$ *such that*

$$f(z_0 + p^i z_1) \equiv z_0 \mod p^{i+1}.$$

for $z_0 \in \{0, \ldots, p-1\}$, $z_1 \in \mathbb{Z}$, $i < e$

p^0	p^1	p^2	p^3	p^4
z_0	0	0	0	0

Bootstrapping BFV



Beware the Algebraic Number Theory!

Plaintext space slots

Plaintext Space: $R_t = \mathbb{Z}_t[X]/(X^N + 1)$

- If $X^N + 1$ factors modulo t

$$R_t \cong \bigoplus_{i=1}^{n} \underbrace{\mathbb{Z}_t[X]/(f_i)}_{\text{a ``slot''}}$$

- $\mathbb{Q}[X]/(X^N + 1)$ is Galois $\Rightarrow$ all slots isomorphic

---

$\Rightarrow$ SIMD parallelism!

Bootstrapping with Slots

Encrypt "vectors" in

$$R_t \cong \bigoplus_{i=1}^{n} \mathbb{Z}_t[X]/(f_i)$$

where $X^N + 1 = f_1 \cdots f_n \mod t$

- Perform n digit extractions in SIMD
- Only N/n digit extraction steps

Why not $n = N$?

Bootstrapping with Slots

Encrypt "vectors" in

$$R_t \cong \bigoplus_{i=1}^{n} \mathbb{Z}_t[X]/(f_i)$$

where $X^N + 1 = f_1 \cdots f_n \mod t$

- Perform n digit extractions in SIMD
- Only N/n digit extraction steps

Why not $n = N$?

$X^N + 1$ factors completely mod $p^e \Leftrightarrow p \equiv 1 \mod 2N$

Requires large p!

Digit extraction and small n

We work in "plaintext slots"

$$S = \mathbb{Z}_{p^e}[X]/(f_i)$$

Think: modulus is prime (i.e. $e = 1$) $\Rightarrow S = \mathbb{F}_{p^d}$

- Digit extraction polynomial works in $\mathbb{F}_p$
- We "waste" the rest of $\mathbb{F}_{p^d}$

Galois automorphisms

$$\mathrm{Gal}(\mathbb{F}_{p^d}/\mathbb{F}_p) = \{\sigma : \mathbb{F}_{p^d} \to \mathbb{F}_{p^d} \mid \sigma \text{ automorphism}\}$$

- This is a group
- Cyclic, generated by Frobenius automorphism

$$\pi : \mathbb{F}_{p^d} \to \mathbb{F}_{p^d}, \quad x \mapsto x^p$$

- Has an analogue for Galois rings (i.e. the p^e-case)
- Relationship with Galois group of R resp. R_p is given by the splitting behavior of (p) in the cyclotomic number field $\mathbb{Q}[X]/(X^N + 1)$.

The algebraic norm

Defined as

$$N(x) := \prod_{i=0}^{d-1} \pi^i x$$

Observation 1: If $x \in \mathbb{F}_p$ and $\alpha \in \mathbb{F}_{p^d}$, then

$$N(\alpha - x) = \mathrm{MinPoly}(\alpha)(x)$$

The algebraic norm

Defined as

$$N(x) := \prod_{i=0}^{d-1} \pi^i x$$

Observation 1: If $x \in \mathbb{F}_p$ and $\alpha \in \mathbb{F}_{p^d}$, then

$$N(\alpha - x) = \mathrm{MinPoly}(\alpha)(x)$$

Observation 2: We can compute $N(x)$ as

$$\left.\begin{aligned} x_0 &:= x \\ x_1 &:= x_0 \cdot \pi x_0 = x \cdot \pi x \\ x_2 &:= x_1 \cdot \pi^2 x_1 = x \cdot \pi x \cdot \pi^2 x \cdot \pi^3 x \\ &\dots \end{aligned}\right\} \log d \text{ mults!}$$

The algebraic norm (cont'd)

Observation 1

$N(\alpha - x) = \mathrm{MinPoly}(\alpha)(x)$

Observation 2

Can compute $N(x)$ with $\log(d)$ multiplications

If we find $\alpha \in \mathbb{F}_{p^d}$ such that

$\mathrm{MinPoly}(\alpha) =$ Digit Extraction Poly

- Requires $p \leq d$
- Digit extraction in $\log(p)$ mults!
- Classical method (Paterson Stockmeyer) uses $2\sqrt{p}$ mults
- Can be used for many polynomials!

It is faster!

Evaluate digit extraction poly via $N(\alpha_{\text{digit extract}} - x)$

- Assuming $p \leq d$
- Using $\log(p)$ mults

$$N = 2^{15}, \quad p = 257, \quad d = 256, \quad n = 128, \quad e = 2$$

	Key switches	Time (our impl)	Time [CH18]
Lin. Transform 1	22	7.9s	-
Lin. Transform 2	30	8.6s	-
Digit Extract	17	5.6s	-
Total	69	22.1s	36.8s

(timings for slim bootstrapping)

Future Directions

- What about parameters with $t = p^r$, $1 < r < e$?
  - Concurrent progress by [CH18; Gee+23]
- Evaluating multiple polynomials at same point?
- What if $\mathrm{degree} > d$?

Thank you for your attention!

[CH18] Hao Chen and Kyoohyung Han. "Homomorphic Lower Digits Removal and Improved FHE Bootstrapping". 2018.

[Gee+23] Robin Geelen, Ilia Iliashenko, Jiayi Kang, and Frederik Vercauteren. "On Polynomial Functions Modulo p^e and Faster Bootstrapping for Homomorphic Encryption". 2023.

[HS21] Shai Halevi and Victor Shoup. "Bootstrapping for HElib". (2021).

[LW23] Zeyu Liu and Yunhao Wang. *Amortized Functional Bootstrapping in less than 7ms, with* $\tilde{O}(1)$ *polynomial multiplications*. 2023.