NTRU-based FHE for Larger Key and Message Space

Robin Jadoul[1] Axel Mertens[1] Jeongeun Park[2] Hilder V. L. Pereira[3]

[1]COSIC, KU Leuven, Leuven, Belgium
[2]Norwegian University of Science and Technology (NTNU), Trondheim, Norway
[3]Universidade Estadual de Campinas, Campinas, Brazil

FHE

Goal:

$$\mathrm{Enc}(x) \oplus \mathrm{Enc}(y) \simeq \mathrm{Enc}(x + y)$$

$$\mathrm{Enc}(x) \otimes \mathrm{Enc}(y) \simeq \mathrm{Enc}(x \times y)$$

FHE

Goal:

$$\mathrm{Enc}(x) \oplus \mathrm{Enc}(y) \simeq \mathrm{Enc}(x + y)$$

$$\mathrm{Enc}(x) \otimes \mathrm{Enc}(y) \simeq \mathrm{Enc}(x \times y)$$

Common problem:

$$\mathrm{Enc} \ \ \text{contains noise}$$

$$\Rightarrow \text{refresh noise/bootstrap}$$

Ciphertexts

LWE

$$\text{Enc} : \mathbb{Z}_q \to \mathbb{Z}_q^n \times \mathbb{Z}_q$$

Ciphertexts

LWE

$$\text{Enc} : \mathbb{Z}_q \to \mathbb{Z}_q^n \times \mathbb{Z}_q$$

NTRU (scalar)

$$\text{Enc} : \mathcal{R}_q \to \mathcal{R}_q$$

$$(\mathcal{R}_q = \mathbb{Z}_q[X]/\langle X^N + 1\rangle)$$

Ciphertexts

LWE

$$\text{Enc} : \mathbb{Z}_q \to \mathbb{Z}_q^n \times \mathbb{Z}_q$$

NTRU (scalar)

$$\text{Enc} : \mathcal{R}_q \to \mathcal{R}_q$$

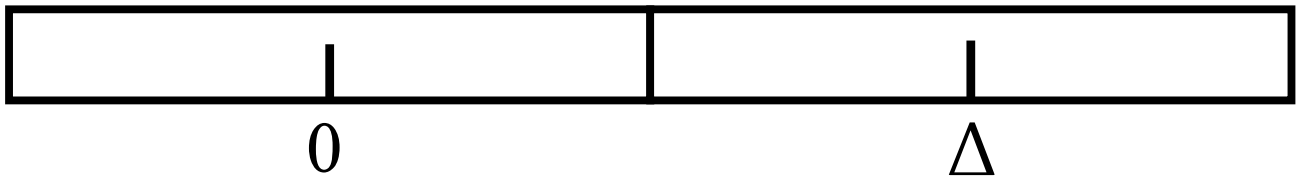
$$(\mathcal{R}_q = \mathbb{Z}_q[X]/\langle X^N + 1\rangle)$$

NTRU (vector)

$$\text{Enc} : \mathcal{R}_q \to \mathcal{R}_q^{\ell}$$

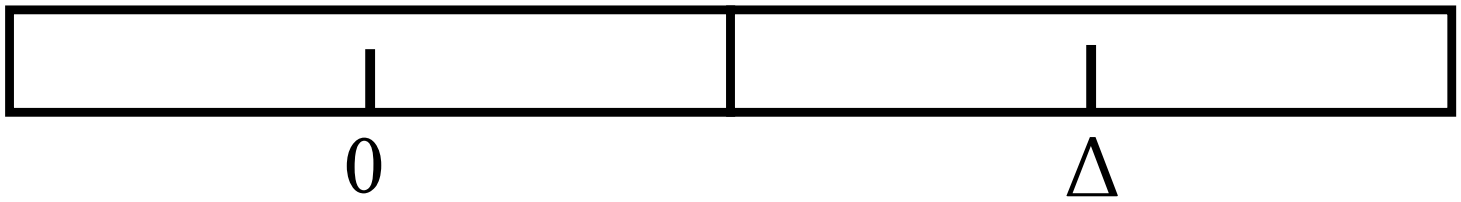
Decrypting LWE

- $\mathrm{Enc}(m) = (\boldsymbol{a}, b = \langle \boldsymbol{a}, \boldsymbol{s} \rangle + e + \Delta \cdot m)$
- $\mathrm{Dec}(\boldsymbol{a}, b) = \left\lfloor \frac{b - \langle \boldsymbol{a}, \boldsymbol{s} \rangle}{\Delta} \right\rceil$
- $e < \frac{\Delta}{2}$!



Bootstrapping

- The idea: decrypt homomorphically



$$0 \cdot X^{\frac{3}{4}N+1} + \ldots + 0 + 0 \cdot X + \ldots + 0 \cdot X^{\frac{N}{4}} + 1 \cdot X^{\frac{N}{4}+1} + 1 \cdot X^{\frac{N}{4}+2} + \ldots + 1 \cdot X^{\frac{3}{4}N}$$

- Rotate this polynomial
- $P(0) = m$
- Cannot know by how much (leaks s)
- "Blind rotation"

Blind rotation

- $P = t(X) \cdot \prod_i \mathrm{CMux}_i(a_i)$
- $\mathrm{CMux}_i(a_i) \simeq \mathrm{Enc}(X^{a_i \cdot s_i})$

Blind rotation

- $P = t(X) \cdot \prod_i \mathrm{CMux}_i(a_i)$
- $\mathrm{CMux}_i(a_i) \simeq \mathrm{Enc}(X^{a_i \cdot s_i})$
- Binary s
  - $\mathrm{CMux}_i(a_i) = 1 + \mathrm{Enc}(s_i) \cdot (X^{a_i} - 1)$

Blind rotation

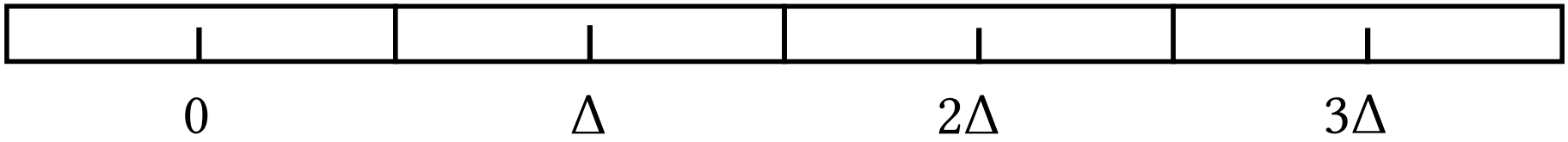
- $P = t(X) \cdot \prod_i \mathrm{CMux}_i(a_i)$
- $\mathrm{CMux}_i(a_i) \simeq \mathrm{Enc}(X^{a_i \cdot s_i})$
- Binary s
  - $\mathrm{CMux}_i(a_i) = 1 + \mathrm{Enc}(s_i) \cdot (X^{a_i} - 1)$
- General (larger) s
  - Same security, smaller LWE dimension n
  - $\Rightarrow$ more efficient bootstrapping
  - CMux: $P = 1 + \sum_{j \neq 0} \mathrm{Enc}\left(\delta_{s_i, j}\right) \cdot (X^{a_i \cdot j} - 1)$

Blind rotation

- Alternative: automorphisms of $\mathcal{R}_q$
- Introduce by Xiang et al. (Crypto'23)
- Slightly altered ciphertext
- Supports *any* key space
  - Double the number of "external products"
  - Larger evaluation keys
  - Diminishing returns from larger and larger keys

Larger message space

- From bits to $\mathbb{Z}_{2^k}$



Programmable bootstrapping

- $P = t(X) \cdot \prod_i \mathrm{CMux}_i(a_i)$
- $t(X)$ contains plain messages
- Embed lookup table

NTRU-based FHE for Larger Key and Message Space