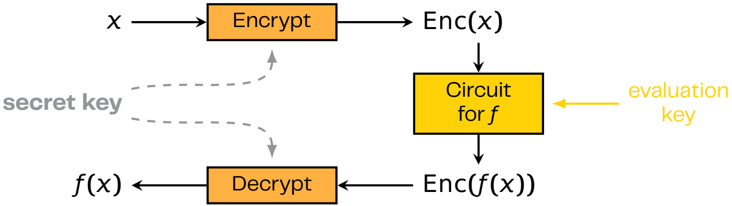
Marc Joye

March 2023

On NTRU-ν-um Modulo $X^N - 1$

ZAMA

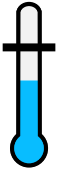
FHE :: Fully Homomorphic Encryption



Remark: Any private-key FHE scheme can easily be turned into a public-key FHE scheme

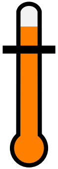
FHE :: Controlling the Noise

Enc(x)



✔ valid ciphertext

Enc(x)



✖ incorrect decryption

Noise accumulates over time

Gentry's Recryption (a.k.a. Bootstrapping)

$$\mathrm{Enc}_{sk}(x) \longrightarrow \boxed{f(\cdot)} \longrightarrow \mathrm{Enc}_{sk}(f(x))$$

Application: Recryption

with $c \leftarrow \mathrm{Enc}_{sk_1}(m)$

$$\mathrm{Enc}_{sk_2}(sk_1) \longrightarrow \boxed{\mathrm{Dec}(\cdot, c)} \longrightarrow \mathrm{Enc}_{sk_2}(\mathrm{Dec}(sk_1, c))$$

$$= \mathrm{Enc}_{sk_2}(m)$$

Application to TFHE

with $c \leftarrow \mathrm{Enc}_{sk_1}(m)$

$$\mathrm{Enc}_{sk_2}(sk_1) \longrightarrow \boxed{\mathrm{Dec}(\cdot, c)} \longrightarrow \mathrm{Enc}_{sk_2}(m)$$

(bootstrapping key)

- Gentry's recryption enables bootstrapping ciphertexts
- **How to round over encrypted data?**

TLWE encryption

1. $\boldsymbol{a} \xleftarrow{\$} \mathbb{T}_q^n$
2. $\mu^* := \mu + e \in \mathbb{T}_q$
3. $b \leftarrow \mu^* + \langle \boldsymbol{s}, \boldsymbol{a} \rangle$

TLWE decryption

1. $\mu^* \leftarrow b - \langle \boldsymbol{s}, \boldsymbol{a} \rangle$
2. round μ^*

Polynomials to the Rescue

Proposition

Let $\mathfrak{M}$ be a module. For any polynomial $\upsilon \in \mathfrak{M}[X]/(X^N + 1)$

$$\upsilon(X) = v_0 + v_1 X + \cdots + v_j X^j + \cdots + v_{N-1} X^{N-1}$$

it holds that

$$X^{-j} \cdot \upsilon(X) = v_j + \ldots$$

(i.e., is a polynomial with constant term v_j)

Illustration :: 2-digit Rounding

μ^*		μ
0.00	$\rightarrow$	0.0
0.01	$\rightarrow$	0.0
0.02	$\rightarrow$	0.0
$\vdots$		$\vdots$
0.09	$\rightarrow$	0.1
0.10	$\rightarrow$	0.1
0.11	$\rightarrow$	0.1
$\vdots$		$\vdots$
0.19	$\rightarrow$	0.2
0.20	$\rightarrow$	0.2
0.21	$\rightarrow$	0.2
$\vdots$		$\vdots$
0.29	$\rightarrow$	0.3

$$\boxed{\upsilon(X) = v_0 + \cdots + v_{N-1}X^{N-1} \implies X^{-j} \cdot \upsilon(X) = v_j + \ldots}$$

- $N = 32$ (power of 2)
- $\upsilon(X) = \begin{aligned}[t] & 0.0 + 0.0\,X + 0.0\,X^2 + \cdots + 0.0\,X^4 \\ & + 0.1\,X^5 + \cdots + 0.1\,X^{10} + \cdots + 0.1\,X^{14} \\ & + 0.2\,X^{15} + \cdots + 0.2\,X^{20} + \cdots + 0.2\,X^{24} \\ & + 0.3\,X^{25} + \cdots + 0.3\,X^{29} \end{aligned}$

$\forall \mu^* \in [\![0.00, 0.29]\!]$

$$X^{-100\,\mu^*} \cdot \upsilon(X) = \mu + \ldots$$

Implementation :: RLWE vs. NTRU

RLWE

1. $a \xleftarrow{\$} \mathcal{R}_q$
2. $\mu^* := \Delta m + e$ with $e \leftarrow \chi$
3. $b \leftarrow s\,a + \mu^*$

$$\rightsquigarrow \boldsymbol{c} = (a, b) \in \mathcal{R}_q \times \mathcal{R}_q$$

NTRU

1. $e_1 \xleftarrow{\$} \chi$
2. $\mu^* := \Delta m + e_2$ with $e_2 \leftarrow \chi$
3. $c \leftarrow \dfrac{e_1}{f} + \mu^*$

$$\rightsquigarrow c \in \mathcal{R}_q$$

where

RLWE $\mathcal{R} = \mathbb{Z}[X]/(X^N + 1)$ with N a power of 2

NTRU $\mathcal{R} = \mathbb{Z}[X]/(X^N + 1)$ as for RLWE, or
$\mathcal{R} = \mathbb{Z}[X]/(X^N - 1)$ with N prime

and $\mathcal{R}_q = \mathcal{R}/q\mathcal{R}$

Concurrent Works

Charlotte Bonte, Ilia Iliashenko, Jeongeun Park, Hilder V. L. Pereira, and Nigel P. Smart

FINAL: Faster FHE instantiated with NTRU and LWE

In *ASIACRYPT 2022*, pp. 188–215

Cryptology ePrint Archive 2022/074

Kamil Kluczniak

NTRU-ν-um: Secure Fully Homomorphic Encryption from NTRU with Small Modulus

In *ACM CCS 2022*, pp. 1783–1797

Cryptology ePrint Archive 2022/089

NTRUnium Modulo $X^N - 1$ :: Encryption

$$c \leftarrow \frac{e}{f} + \Delta m \pmod{q, X^N - 1} \quad \text{where } e = e_1 + e_2 f$$

where

$$\begin{cases} f \text{ is the private key} \\ e_1, e_2 \text{ are error polynomials} \end{cases}$$

such that

- f is invertible in and has random coefficients (uniformly) chosen in $\{-1, 0, 1\}$
- $\Delta = q/p$ for some $p \mid q$ and $m \in \mathcal{R}_p$

NTRUnium Modulo $X^N - 1$ :: Decryption

$$c \leftarrow \frac{e}{f} + \Delta m \pmod{q, X^N - 1} \quad \text{where } e = e_1 + e_2 f$$

3–step process:

1. $d \leftarrow c\,f = e + \Delta m\, f$
2. $\bar{d} \leftarrow \lceil d/\Delta \rfloor \pmod{p}$
3. $m \leftarrow \bar{d}\, f^{-1} \in \mathcal{R}_p$

Correctness of decryption requires $\|e\|_\infty < \Delta/2$

Definition

'Mildly noisy' samples: $\|e\|_\infty \ll \frac{\Delta}{2\sqrt{N}}$

Attacking Mildly Noisy Ciphertexts

$$c \leftarrow \frac{e}{f} + \Delta m \pmod{q, X^N - 1} \quad \text{with } \|e\|_\infty \ll \frac{\Delta}{2\sqrt{N}}$$

Since $(X-1) \mid (X^N - 1)$

$$c \leftarrow \frac{e}{f} + \Delta m \pmod{q, X - 1}$$

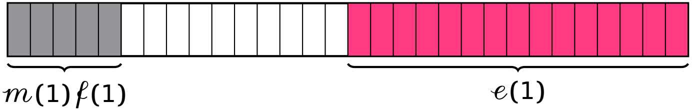
and thus

$$\begin{aligned} d(1) := c(1) \cdot f(1) &\equiv e(1) + \Delta m(1) \cdot f(1) \\ &\equiv e(1) + \Delta \cdot (m(1) \cdot f(1) \bmod p) \pmod{q} \end{aligned}$$

Attacking Mildly Noisy Ciphertexts

$$c \leftarrow \frac{e}{f} + \Delta m \pmod{q, X^N - 1} \quad \text{with } \|e\|_\infty \ll \frac{\Delta}{2\sqrt{N}}$$

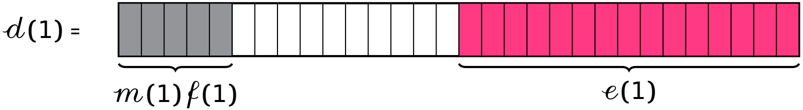
$d(1) =$



$$\begin{aligned} d(1) := c(1) \cdot f(1) &\equiv e(1) + \Delta m(1) \cdot f(1) \\ &\equiv e(1) + \Delta \cdot (m(1) \cdot f(1) \bmod p) \pmod{q} \end{aligned}$$

Attacking Mildly Noisy Ciphertexts

$$c \leftarrow \frac{e}{f} + \Delta m \pmod{q, X^N - 1} \quad \text{with } \|e\|_\infty \ll \frac{\Delta}{2\sqrt{N}}$$



1. Initialize $\mathcal{L} = \{0, \ldots, N\}$
2. Obtain a mildly noisy ciphertext c
3. For each candidate value $f(1) \in \mathcal{L}$, do the following:
   a. check whether $d(1) := c(1)f(1)$ satisfies above form
   b. if not, disregard candidate $f(1)$ and update $\mathcal{L} \leftarrow \mathcal{L} \setminus \{f(1)\}$
4. If $\#\mathcal{L} > 1$ go to Step 2

Bootstrapping Keys :: Key Recovery Attack

- For gadget parameters B and ℓ

$$\boldsymbol{bsk}[i] \leftarrow \left(\mathrm{NTRU}(s_i B^j)\right)_{0\le j\le \ell-1} \in (\mathcal{R}_q)^{\ell} \qquad (1 \le i \le n)$$

- $\mathrm{Var}(\mathrm{Err}(\mathcal{C}_{\mathrm{bootstrapped}}))$ has a term of the form

$$\varrho \cdot \sigma_{bsk}^2 \quad \text{where } \varrho = \tfrac{1}{12}\, n\, N\, \ell\, (B^2 - 1)$$

$$\implies \sqrt{\varrho} \cdot \sigma_{bsk} \ll \Delta/2$$

NTRUnium bootstrapping keys are mildly noisy ciphertexts

$\rightsquigarrow$ Key recovery attack: secret key bits s_i can be recovered using $\mathscr{P}(1)$

Validation :: Numerical Experiments

- Source code available for computer algebra system GP/Pari*

*Available at URL `http://pari.math.u-bordeaux.fr/`

NTRUnium Parameter Sets

Binary LWE keys

	q	N	$\sqrt{\varrho}$
NTRU–ν–um–C–11–B	2^{30}	$2^{11}-9$	$2^{15.64}$
NTRU–ν–um–C–12–B	2^{38}	$2^{12}-3$	$2^{18.14}$
NTRU–ν–um–C–13–B	2^{41}	$2^{13}-1$	$2^{19.68}$
NTRU–ν–um–C–14–B	2^{42}	$2^{14}-3$	$2^{20.23}$

Ternary LWE keys

	q	N	$\sqrt{\varrho}$
NTRU–ν–um–C–11–T	2^{30}	$2^{11}-9$	$2^{14.40}$
NTRU–ν–um–C–12–T	2^{38}	$2^{12}-3$	$2^{20.46}$
NTRU–ν–um–C–13–T	2^{42}	$2^{13}-1$	$2^{20.20}$
NTRU–ν–um–C–14–T	2^{42}	$2^{14}-3$	$2^{20.70}$

Contact and Links

marc@zama.ai

zama.ai

Github

Community links

ZAMA