Practical Sanitization for TFHE

Intak Hwang, Seonhong Min, Yongsoo Song
Seoul National University

서 울 대 학 교
SEOUL NATIONAL UNIVERSITY

Sanitization

✓ **Sanitization**

- Sanitization 'removes' the information remaining in the noise and the mask of the input ciphertext.
- Crucial for secure 2PC construction.

✓ **Existing approaches (for TFHE)**

- [Gen09] : Noise flooding.
- [DS16] : (Several) gentle noise flooding and bootstrapping.
- [BI22], [Klu22] : Many randomized gadget decompositions.

✓ **Our Approach**

- Three-step sanitization:
  Rerandomization -> Blind Rotation -> Linear Evaluation

1.Mask rerandomization [BI22]

✓ **Simulatable zero encryption**

- Public key $pk = (pk_0, pk_1) \in R_q^2 = \left(\mathbb{Z}_q[X]/(X^N+1)\right)^2$
- Sample $e_1, e_2 \leftarrow D_{\mathbb{Z}^N,\sigma_r}$ and $e_0 \leftarrow \lfloor D_{\mathbb{R}^N,\tau_r} \rceil$.
- Compute $e_2 \cdot pk + (e_0, e_1)\ (mod\ q)$

✓ **Ciphertext distribution**

- Suppose
  - $pk_0 + pk_1 \cdot t = e_{pk}\ (mod\ q)$ with $\|e_{pk}\|$.
  - $\frac{1}{\sigma_r^2} + \frac{B^2}{\tau_r^2} \le \frac{\pi}{2\eta_\epsilon(\mathbb{Z}^{2N})^2}$
- Output ciphertext is computationally indistinguishable to a **fresh ciphertext** with noise distribution

$$\mathrm{e}_0 + e_2 \cdot e_{pk} + e_1 \cdot t$$

- In other words, the mask of the output ciphertext looks uniform to the key owner.

2.Blind Rotation (FHEW, TFHE, LMKCDEY…)

✓ **Black-box Blind Rotation**

Run the blind rotation algorithm (+key-switching) in a black-box manner, with input $(0, \vec{a}) \in \mathbb{Z}_q^{N+1}$ where the given rerandomized ciphertext is $(b, \vec{a}) \in \mathbb{Z}_q^{N+1}$.

✓ **Output ciphertext distribution**

- Recall that $\vec{a}$ looks uniform to the key-owner after the rerandomization.
- Therefore, the output ciphertext distribution of blind rotation algorithm can be simply simulated by running the blind rotation algorithm with a uniform vector.

3.Oblivious linear evaluation [dCKK+24]

✓ **Oblivious linear evaluation**

- Suppose ptxt modulus p divides the ctxt modulus q
- Given BFV ciphertext $\mathrm{ct} = (c_0, c_1) \in R_q^2$ such that

$$c_0 + c_1 \cdot t = \frac{q}{p} \cdot x + e_{ct}\ (mod\ q)$$

- Compute $r \cdot \mathrm{ct} + (b + e, 0)\ \ (mod\ q)$ where

$$r \leftarrow D_{a+p\mathbb{Z}^N,\sigma_\ell},\ e \leftarrow \lfloor D_{\mathbb{R}^N,\tau_\ell} \rceil$$

  to compute $ax + b$.
- The output noise distribution is indistinguishable to

$$\lfloor D_{\mathbb{R},\sqrt{\sigma_\tau^2 E_{ct} E_{ct}^\top + \tau_\ell^2 I}} \rceil$$

  if $\frac{1}{\sigma^2} + \frac{\|E_{ct}\|_2^2}{\tau^2} \le \frac{2\pi}{\eta_\epsilon(p\mathbb{Z}^N)^2}$ for the negacyclic matrix of ciphertext error e_{ct}.

✓ **In TFHE sanitization**

- After blind rotation, multiply $X^b \in R_4$ to the output ciphertext obliviously.
- Then, the output ciphertext is an encryption of

$$X^{b+\langle\vec{a},\vec{s}\rangle} \cdot tv.$$

- Since e_{ct} is simulatable, output of linear evaluation is also simulatable, as long as we bound the two-norm of E_{ct}.
- Add zero encryption to rerandomize the ciphertext.

Experiments

✓ **Parameters**

n	N	p	q	α	β	B	d	B'	d'
612	2048	2^2	2^{64}	$2^{50.40}$	$2^{12.65}$	2^{11}	3	2^{32}	4

Base Bootstrapping Parameters

σ_r	τ_r	σ_ℓ	τ_ℓ
$2^{10.61}$	$2^{33.29}$	$2^{7.80}$	$2^{57.18}$

Randomization Parameters

✓ **Experimental results**

	Ours	DS16	BI22	Klu22 (NTT)	Klu22 (FFT)
Sanitization	35.88ms	173.00ms	7500ms	1360ms	1330ms
Speedup	1x	4.8x	209x	37.9x	37.06x

Sanitization/Bootstrapping Latency