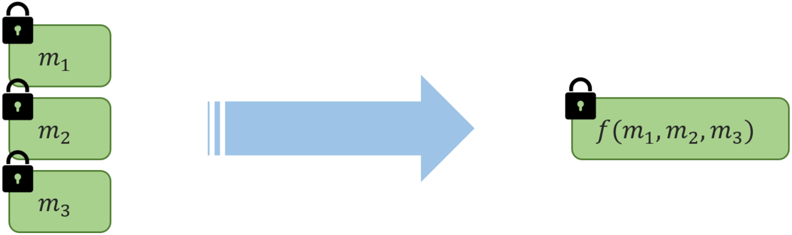
Faster TFHE Bootstrapping with Block Binary Keys

Changmin Lee[1], **Seonhong Min**[2], Jinyeong Seo[2], Yongsoo Song[2]

[1]Korea Institute for Advanced Study, Seoul
[2]Seoul National University, Seoul

Fully Homomorphic Encryption



- **Fully Homomorphic Encryption (FHE)** supports arbitrary function evaluation on encrypted data.
- **Various Applications**: privacy preserving machine learning, private information retrieval, private set intersection ...

Learning with Errors

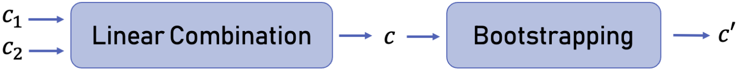
- The most efficient FHEs to date are built on **Learning with Errors (LWE)** problem and its ring-variant **Ring-LWE (RLWE)**.
- **LWE**: $(\mathbf{a}, b) \approx_c \mathcal{U}(\mathbb{Z}_q^{n+1})$
  - $\mathbf{a} \leftarrow \mathcal{U}(\mathbb{Z}_q^n)$, $\mathbf{s} \in \mathbb{Z}^n$, $e \leftarrow$ small dist' over $\mathbb{Z}$
  - $b = -\langle \mathbf{a}, \mathbf{s} \rangle + e \pmod q$
- **RLWE**: $(a, b) \approx_c \mathcal{U}(R_q^2)$
  - Variant of LWE over $R_q = R/qR$ where $R = \mathbb{Z}[X]/(X^N + 1)$
  - $a \leftarrow \mathcal{U}(R_q)$, $s \in R$, $e \leftarrow$ small dist' over R
  - $b = -a \cdot s + e \pmod q$
- FHE schemes based on LWE/RLWE
  - BGV / BFV / CKKS
  - **TFHE** / FHEW

TFHE description

- FHE scheme that supports bits operations (NAND, AND, OR...).
- **Secret Key**:
  - LWE secret $\mathbf{s} = (s_1, \ldots, s_n)$
  - RLWE secret $t = \sum_{i=1}^{N} t_i X^{i-1}$
  - Vectorized secret $\mathbf{t} = (t_1, \ldots, t_N)$
  - All keys are sampled from **binary distribution**
- **Encoding**: $m \in \{-1, 1\} \mapsto \mu = \frac{q}{8} m \in \mathbb{Z}_q$
- **Decoding**: $\begin{cases} 1 & \text{if } \mu > 0 \\ -1 & \text{otherwise} \end{cases}$
- **Encryption**: $c = (b, \mathbf{a}) \in \mathbb{Z}_q^{n+1}$ for $\mathbf{a} \leftarrow \mathcal{U}(\mathbb{Z}_q^n)$, $e \leftarrow$ small dist., $b = -\langle \mathbf{a}, \mathbf{s} \rangle + \mu + e$.
- **Decryption**: $b + \langle \mathbf{a}, \mathbf{s} \rangle = \mu + e$

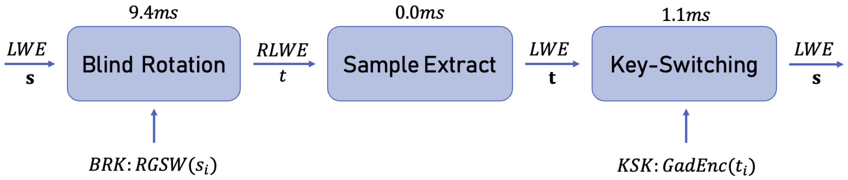
Homomorphic Gate Evaluation

- Each bit operation consists of the following pipeline:



- **Linear Combination** : The linear combination corresponding to a Boolean gate is evaluated.
  - ex) NAND : $c = (\frac{q}{8}, \mathbf{0}) - c_1 - c_2$
  - output ciphertext contains a **large noise** e.
- **Bootstrapping** : Reduces the size of noise for further evaluation.
  - ex) $\|e\| < \frac{q}{8} \to \|e'\| < \frac{q}{16}$

TFHE Bootstrapping



- **Blind Rotation** : Homomorphically computes the decryption circuit on the exponent of X *i.e.*, $X^{b+\langle \mathbf{a},\mathbf{s}\rangle}$.
  - Need Blind Rotation Key : Encryptions of s_i $(1 \leq i \leq n)$
- **Sample Extract** : Extract an LWE ciphertext from the resulting RLWE ciphertext.
- **Key-Switching** : Switch the secret key of the LWE ciphertext.
  - Need Key-Switching Key : Encryptions of t_i $(1 \leq i \leq N)$

Our Contribution

Motivation : Most FHE schemes (BGV/FV/CKKS) make an additional assumption on key structure to obtain better efficiency.

- BGV/FV : Small noise growth in homomorphic multiplication.
- CKKS : Small depth for bootstrapping.

Our Result : We adapt similar approach to accelerate TFHE bootstrapping.

1. **Faster Blind Rotation**
   - Sample LWE key from **block binary key distribution**
   - Reduce the number of iterations.
2. **Compact Key-Switching**
   - Re-use the LWE key as a part of RLWE key
   - Improve both time and space complexity

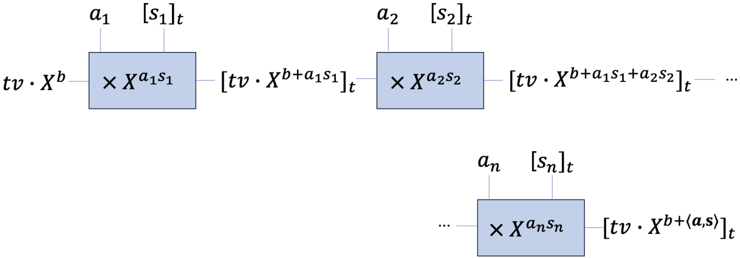
Blind Rotation

Functionality

- Homomorphic evaluation of $tv \cdot X^{b+\sum_{i=1}^{n} a_i s_i} = tv \cdot X^{\frac{q}{8}m+e} \in R_q$.
  - $tv = -\frac{q}{8}(1 + X + \cdots + X^{N-1}) \in R_q$.
  - Constant term of $tv \cdot X^{\frac{q}{8}m+e} = \frac{q}{8}m$.

- Homomorphically multiply monomials $X^{a_i s_i}$ to $tv \cdot X^b$ iteratively.
- We need **n homomorphic multiplications** total.

Previous Blind Rotation



- $X^{a_i s_i} = \begin{cases} X^{a_i} & (s_i = 1) \\ 1 & (s_i = 0) \end{cases} = 1 + (X^{a_i} - 1)s_i$
  - Using this **key formula**, we have $[X^{a_i s_i}]_t = 1 + (X^{a_i} - 1)[s_i]_t$
  - We iteratively multiply one monomial $X^{a_i s_i}$ for **n** times.

Observation

- Can we multiply 2 monomials simultaneously?

$$
\begin{aligned}
&X^{a_1 s_1 + a_2 s_2} \\
&\quad = (1 + (X^{a_1} - 1)s_1)(1 + (X^{a_2} - 1)s_2) \\
&\quad = 1 + (X^{a_1} - 1)s_1 + (X^{a_2} - 1)s_2 + (X^{a_1} - 1)(X^{a_2} - 1)s_1 s_2
\end{aligned}
$$

- With this formula, the number of homomorphic mult reduces by **half**.
  - Requires RGSW encryption of $s_1 s_2$
  - $+$ the number of linear evaluation grows.
- What if we can ignore the case where $s_1 = s_2 = 1$?
  - No additional blind rotation keys are required.
  - The number of linear evaluation remains same.
- **Generalization**: How about ℓ monomials?
  $\rightarrow$ Possible. If $\mathbf{s}$ is sampled from **Block Binary Key Distribution**...

Block Binary Keys

Definition (Block Binary Key)

- $n = k\ell$ for two positive integers $k, \ell > 0$
- $\mathbf{s} = (B_1, \ldots, B_k) \in \{0,1\}^n$
- $B_i \leftarrow \mathcal{U}((1,0,\ldots,0),\ldots,(0,0,\ldots,1),(0,\ldots,0))$
- **At most one 1 in each block**

1	0	0	0	**1**	0	0	0	0	**1**	0	0	0	0	**1**	0	**1**	0

Figure: Block Binary Key with $\ell = 3$ and $k = 6$

Block Binary Keys

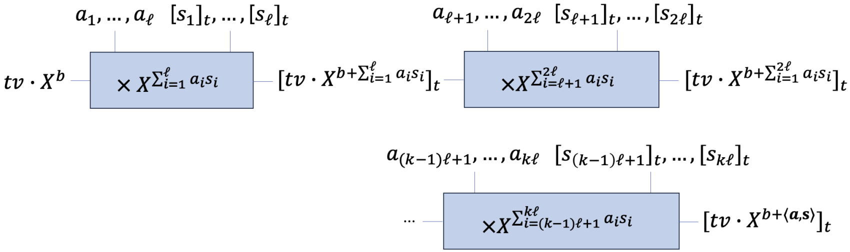
- $$X^{a_1 s_1} = \begin{cases} X^{a_1} & (s_1 = 1) \\ 1 & (s_1 = 0) \end{cases}$$
  $$= 1 + (X^{a_1} - 1)s_1$$

  $\rightarrow$ Multiply 1 monomial with 1 mult and 1 add.

- $$X^{\sum_{i=1}^{\ell} a_i s_i} = \begin{cases} X^{a_1} & (s_1 = 1, s_2 = 0, \ldots, s_\ell = 0) \\ \vdots & \\ X^{a_\ell} & (s_1 = 0, s_2 = 0, \ldots, s_\ell = 1) \\ 1 & (s_1 = 0, s_2 = 0, \ldots, s_\ell = 0) \end{cases}$$
  $$= 1 + \sum_{i=1}^{\ell} (X^{a_i} - 1)s_i$$

  $\rightarrow$ Multiply ℓ monomials with 1 mult and ℓ add.

Our Blind Rotation



- Iteratively multiplies ℓ monomials with one homomorphic multiplication.
- Only **k** homomorphic multiplications are required!!
- However, not direct ℓ-times speedup due to other operations.

Security of Block Binary Keys

- **Asymptotic Security** : If the entropy of key distribution is sufficiently large, LWE is secure (Goldwasser et al).
  - Entropy of block binary keys : $(\ell + 1)^k$
- **Concrete Security** : We conducted cryptanalysis considering the best-known lattice attacks.
  - Classical Dual
  - Meet-in-the-Middle
  - Taylor-made

Parameters

- We set the parameters with 128-bit security level.
- As ℓ **grows**, $n = k\ell$ **grows** as well to secure enough entropy.

$n = k\ell$	N	ℓ	Dual	MitM	Taylor-made
630	1024	2	128.8	139.7	128.8
687	1024	3	128.3	128.2	126.7
788	1024	4	128.6	128.0	127.4

Key-Switching

Functionality

- Switch the secret key of LWE ciphertext from $\mathbf{t}$ to $\mathbf{s}$.

- For LWE ciphertext $\mathbf{c} = (b, a_1, \ldots, a_N)$ encrypted under $\mathbf{t}$, we compute $\mathbf{c}' = (b, 0, \ldots, 0) + \sum_{i=1}^{N} a_i \cdot \mathrm{Enc}_{\mathbf{s}}(t_i)$.
  - $\mathrm{Enc}_{\mathbf{s}}(t_i)$: Gadget encryptions of t_i under $\mathbf{s}$ $(1 \leq i \leq N)$.
  - $Dec_{\mathbf{s}}(\mathbf{c}') \approx b + \sum_{i=1}^{N} a_i t_i = Dec_{\mathbf{t}}(\mathbf{c})$.
- **Complexity**
  - Time : **N** homomorphic scalar multiplications.
  - Space: **N** key-switching keys

Compact Key-Switching

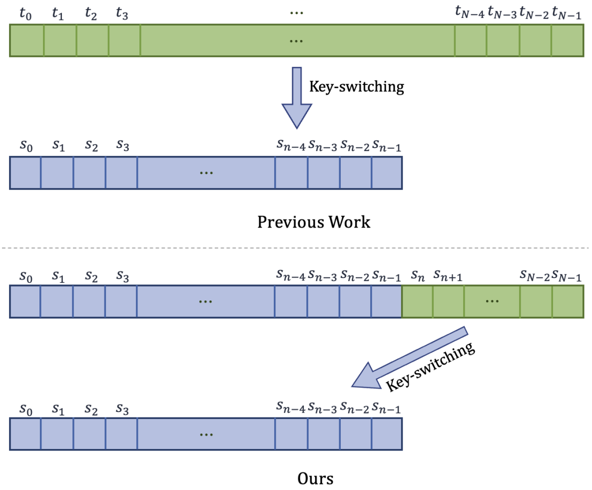
- If $t_i = s_i$ $(1 \le i \le n)$, we can replace $\mathbf{c}'$ by

$$(b, a_1, \ldots, a_n) + \sum_{i=n+1}^{N} a_i \cdot \mathrm{Enc}_{\mathbf{s}}(t_i)$$

  - $Dec_{\mathbf{s}}(\mathbf{c}') \approx b + \sum_{i=1}^{n} a_i s_i + \sum_{i=n+1}^{N} a_i t_i = b + \sum_{i=1}^{N} a_i t_i = Dec_{\mathbf{t}}(\mathbf{c})$.

- **Complexity**
  - Time : $\mathbf{N} - \mathbf{n}$ scalar multiplications
  - Space : $\mathbf{N} - \mathbf{n}$ key-switching keys

Compact Key-Switching

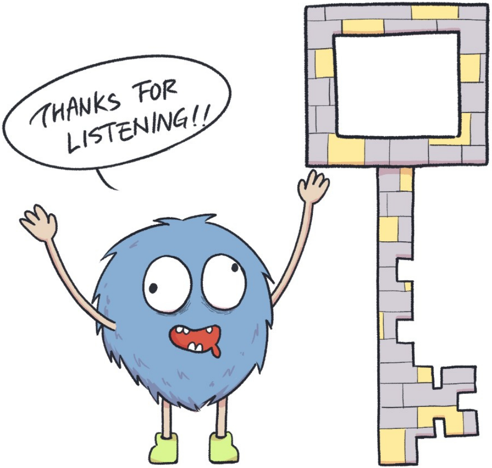


Implementation & Result

	ℓ	n	Bootstrapping	Key Size
TFHE	$\cdot$	630	10.5 *ms*	109 MB
Ours	2	630	7.0 *ms*	60 MB
	3	687	6.5 *ms*	
	4	788	6.7 *ms*	

Table: 128-bit Security level

- Implemented based on **the TFHE library**.
- We achieve **1.5-1.6x** SPEEDUP!
- Key size is reduced by **1.8x**!
- Source code is available at **github.com/SNUCP/blockkey-tfhe**


THANKS FOR LISTENING!!