Circuit Bootstrapping: Faster and Smaller

Ruida Wang, Yundi Wen, Zhihao Li, Xianhui Lu, Benqiang Wei, Kun Liu and Kunpeng Wang

1. State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing, China.
2. School of Cyber Security, University of Chinese Academy of Sciences, Beijing, China.
3. Academy of Mathematics and Systems Science, Chinese Academy of Sciences, Beijing, China.

中国科学院信息工程研究所
INSTITUTE OF INFORMATION ENGINEERING,CAS

中国科学院大学
University of Chinese Academy of Sciences

AMSS
Academy of Mathematics and Systems Science,CAS

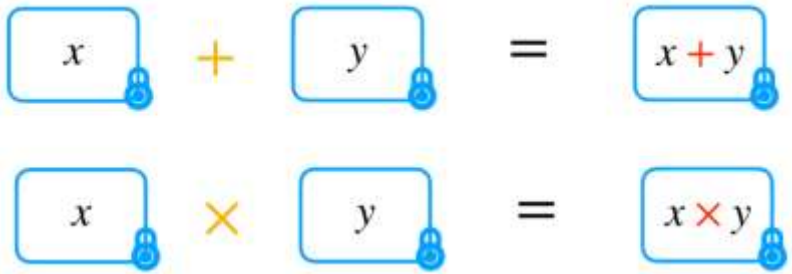
Outline

- **Background**
  - Fully Homomorphic Encryption
  - FHEW/TFHE Scheme
  - FHEW/TFHE Bootstrapping
- **LHE Evaluation Mode**
- **Improved Circuit Bootstrapping**
- **Performance**
- **Discussion**
- **Q&A**

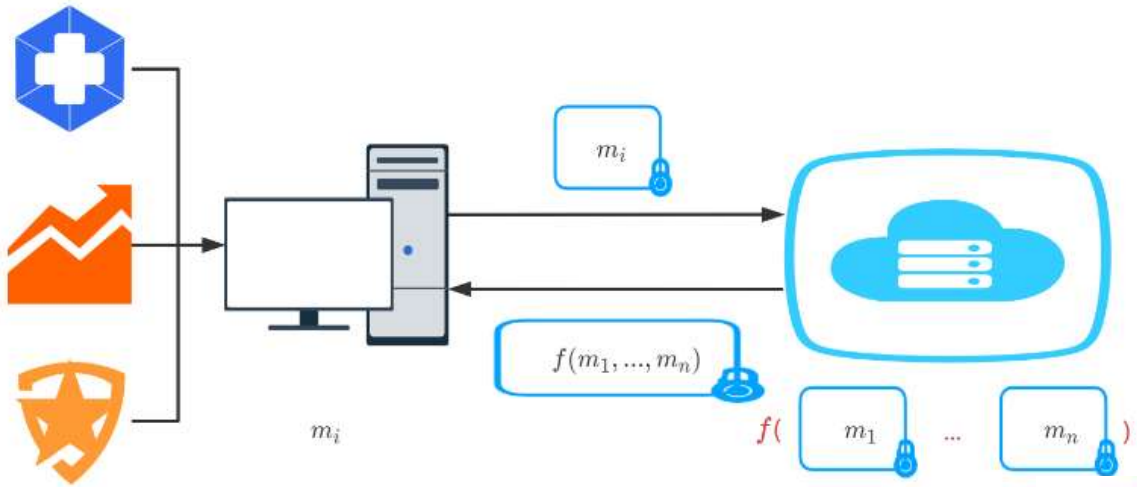
中国科学院信息工程研究所
INSTITUTE OF INFORMATION ENGINEERING,CAS

Fully Homomorphic Encryption

- FHE: Allows computations on encrypted data without decryption.

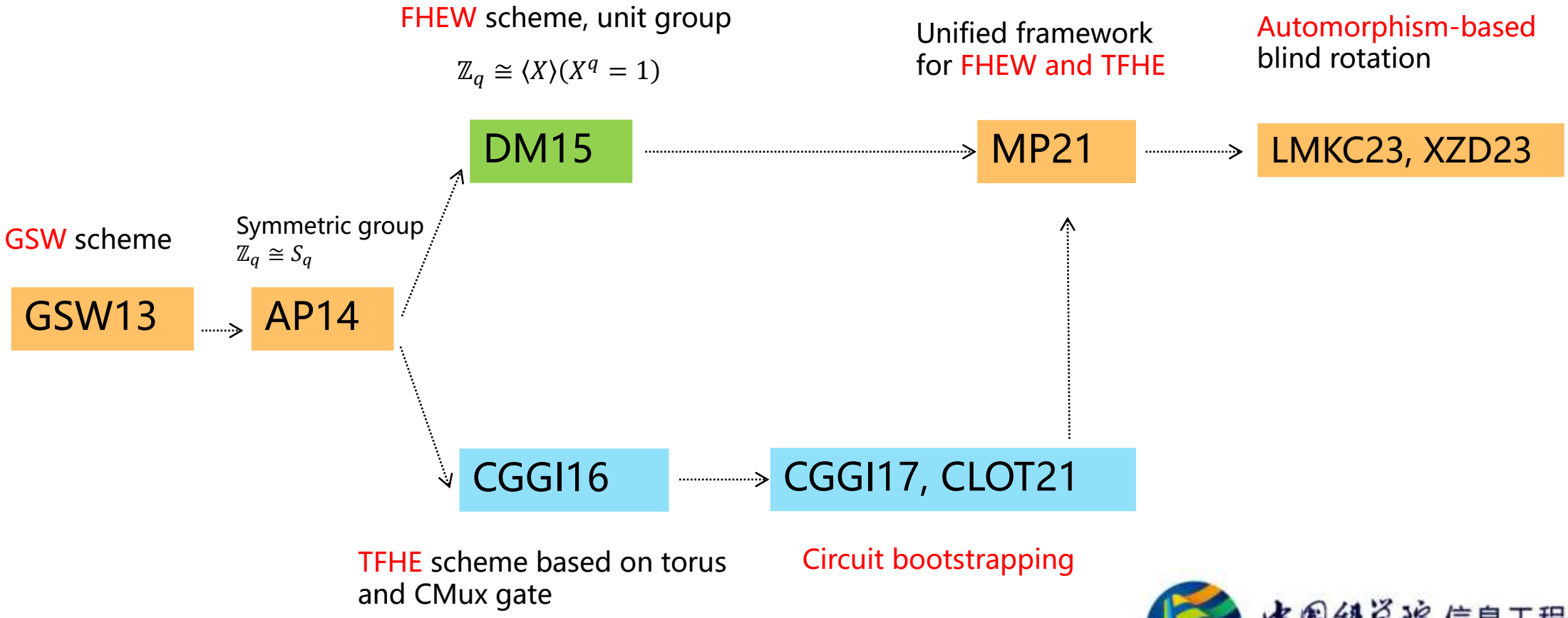


- Applications: Secure cloud computing, Privacy-Preserving ML, …



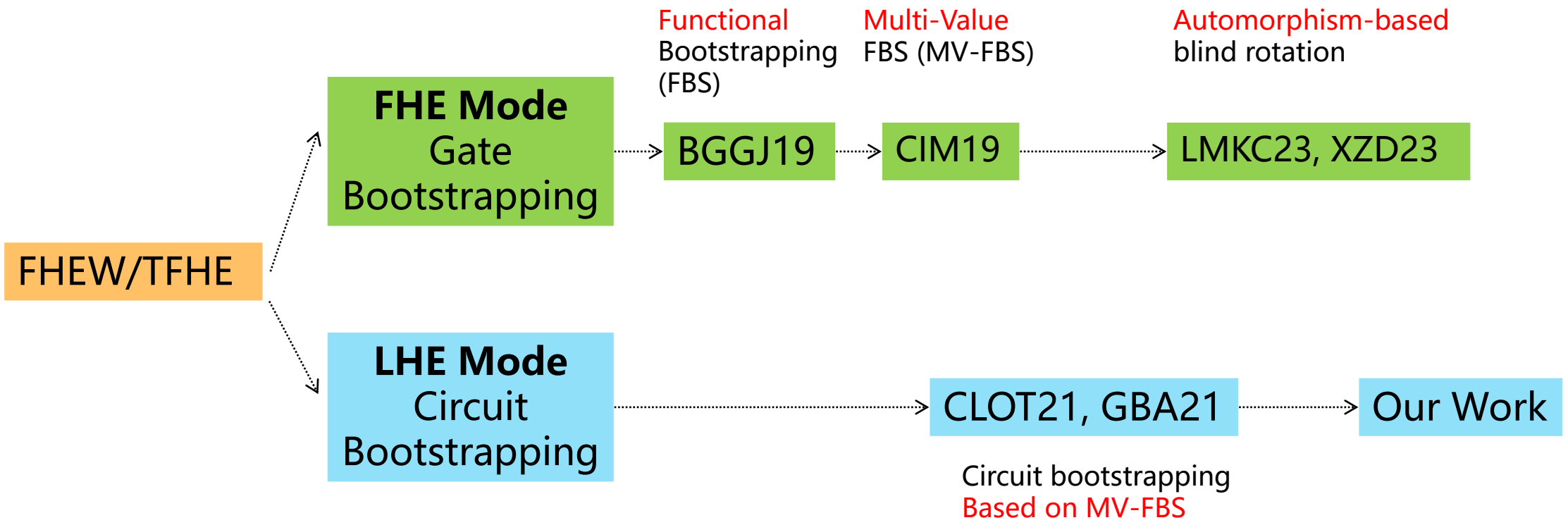
FHEW/TFHE Scheme

- FHEW/TFHE: Similar to, unified framework in [MP21].
- Known for bootstrapping efficiency.



FHEW/TFHE Bootstrapping

- Bootstrapping gate-by-gate: **F**ully **h**omomorphic **e**valuation mode.
- "Sleepy Field" : **L**eveled **h**omomorphic **e**valuation mode.



Outline

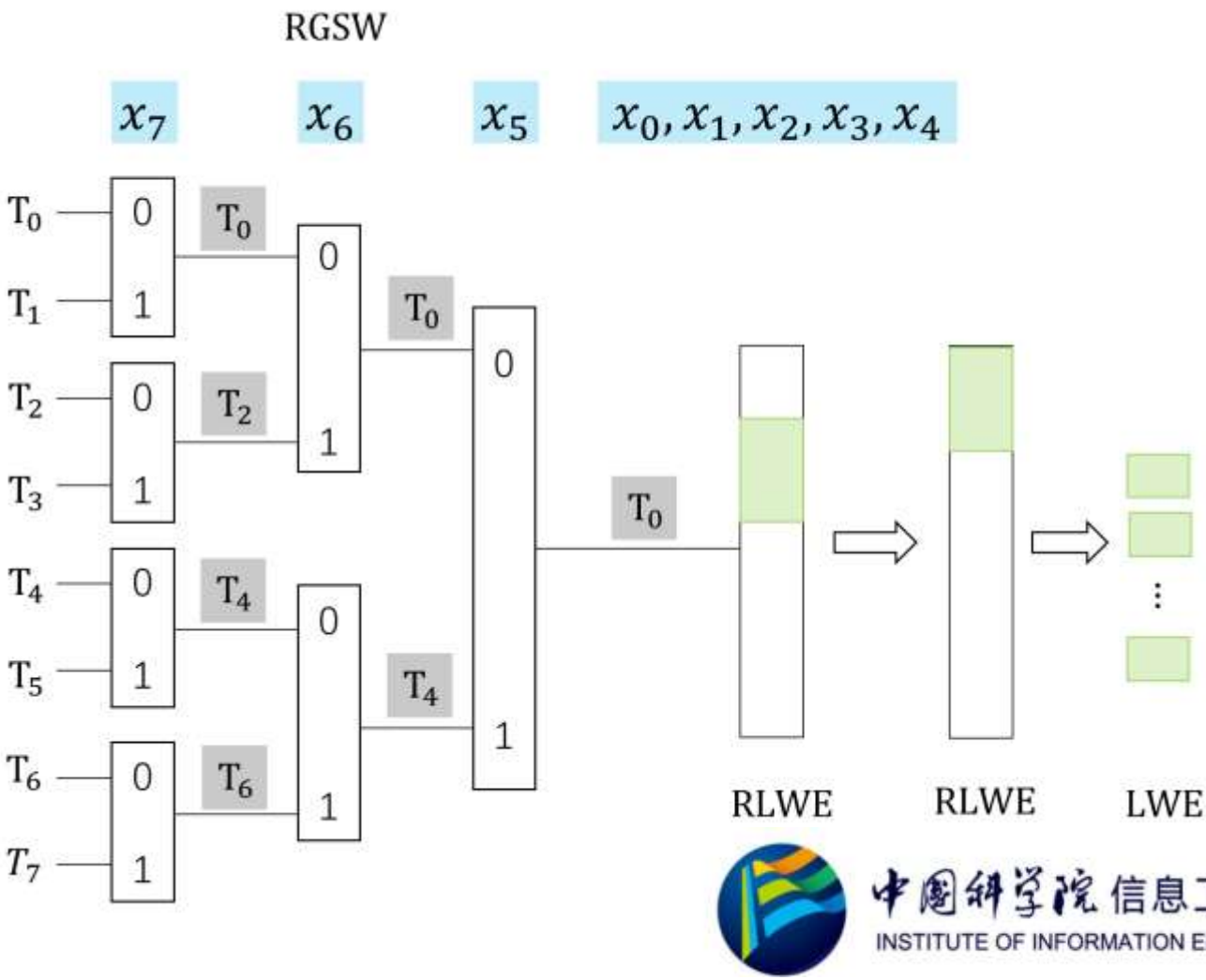
- **Background**
- **LHE Evaluation Mode**
  - Look-Up-Table Via CMUX Gate
  - Circuit Bootstrapping (CGGI17, CLOT21)
- **Improved Circuit Bootstrapping**
- **Performance**
- **Discussion**
- **Q&A**

LUT Via CMUX Gate

- Input: RGSW
- Output: LWE

CMUX: $\mathrm{RGSW}(x_7) \boxdot (\mathrm{RLWE}(\mathrm{T}_1) - \mathrm{RLWE}(\mathrm{T}_0)) + \mathrm{RLWE}(\mathrm{T}_0)$

x_0	$\cdots$	x_7	f_0	$\cdots$	f_{31}
0	$\cdots$	0	$\sigma_{0,0}$	$\cdots$	$\sigma_{0,31}$
1	$\cdots$	0	$\sigma_{1,0}$	$\cdots$	$\sigma_{1,31}$
0	$\cdots$	0	$\sigma_{2,0}$	$\cdots$	$\sigma_{2,31}$
1	$\cdots$	0	$\sigma_{3,0}$	$\cdots$	$\sigma_{3,31}$
$\vdots$	$\cdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
0	$\cdots$	1	$\sigma_{252,0}$	$\cdots$	$\sigma_{252,31}$
1	$\cdots$	1	$\sigma_{253,0}$	$\cdots$	$\sigma_{253,31}$
0	$\cdots$	1	$\sigma_{254,0}$	$\cdots$	$\sigma_{254,31}$
1	$\cdots$	1	$\sigma_{255,0}$	$\cdots$	$\sigma_{255,31}$



LUT Via CMUX Gate

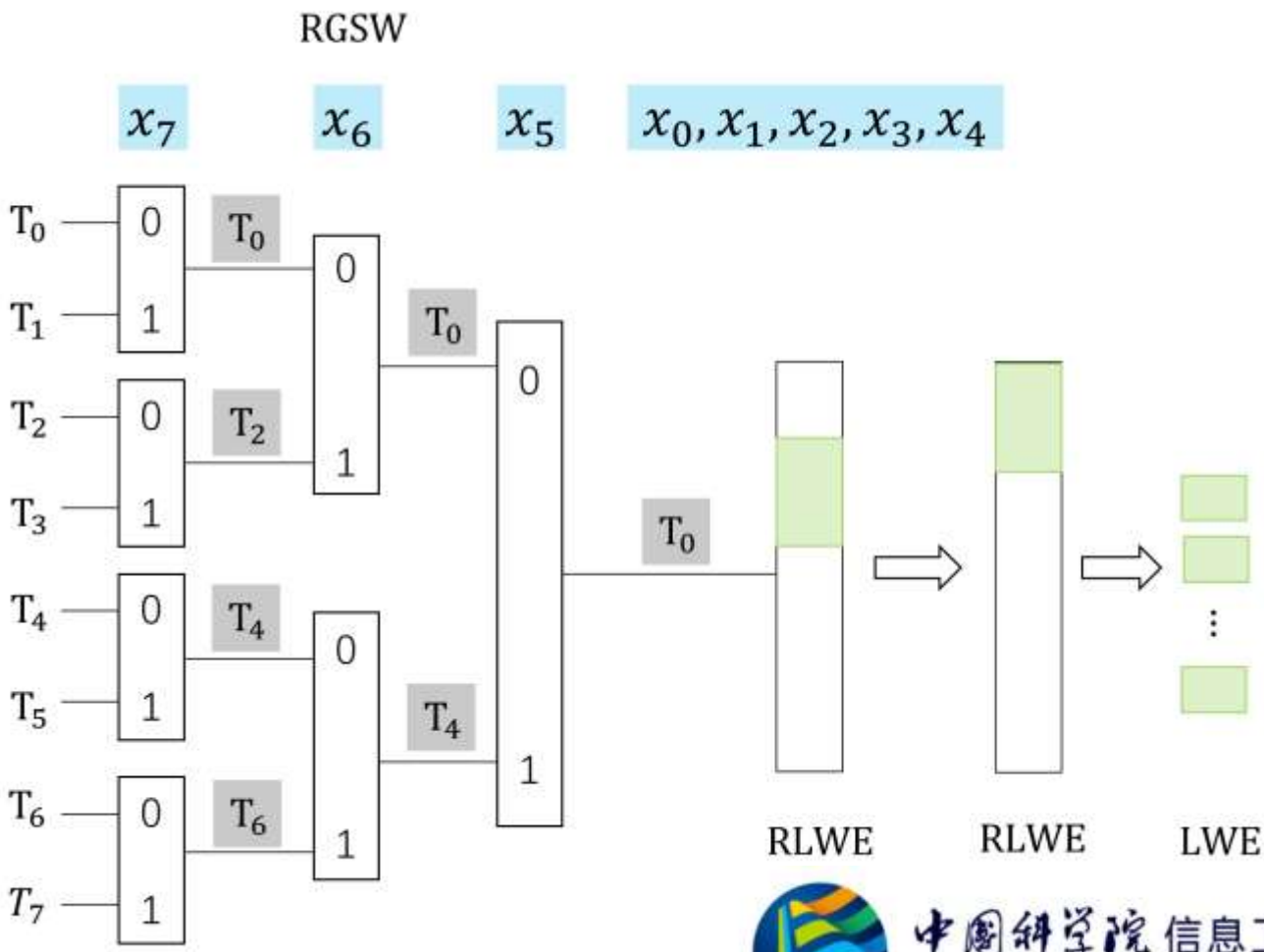
- Input: RGSW
- Output: LWE

CMUX: $\mathrm{RGSW}(x_7) \boxdot (\mathrm{RLWE}(\mathrm{T}_1) - \mathrm{RLWE}(\mathrm{T}_0)) + \mathrm{RLWE}(\mathrm{T}_0)$

x_0	$\cdots$	x_7	f_0	$\cdots$	f_{31}
0	$\cdots$	0	$\sigma_{0,0}$	$\cdots$	$\sigma_{0,31}$
1	$\cdots$	0	$\sigma_{1,0}$	$\cdots$	$\sigma_{1,31}$
0	$\cdots$	0	$\sigma_{2,0}$	$\cdots$	$\sigma_{2,31}$
1	$\cdots$	0	$\sigma_{3,0}$	$\cdots$	$\sigma_{3,31}$
$\vdots$	$\cdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
0	$\cdots$	1	$\sigma_{252,0}$	$\cdots$	$\sigma_{252,31}$
1	$\cdots$	1	$\sigma_{253,0}$	$\cdots$	$\sigma_{253,31}$
0	$\cdots$	1	$\sigma_{254,0}$	$\cdots$	$\sigma_{254,31}$
1	$\cdots$	1	$\sigma_{255,0}$	$\cdots$	$\sigma_{255,31}$

T_0

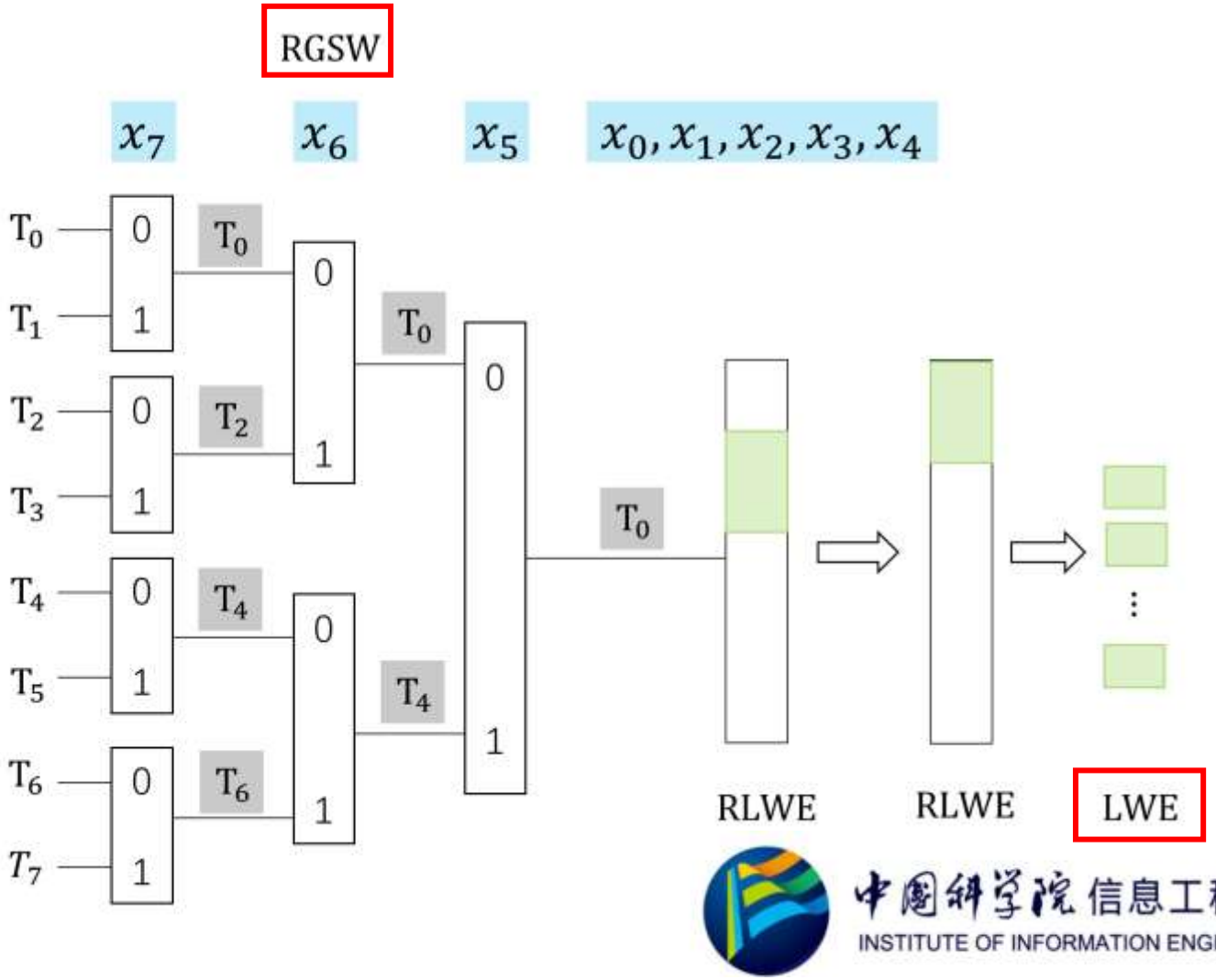
T_7



LUT Via CMUX Gate

- Low-noise RGSW → high-noise LWE.
- Noise? Composability?

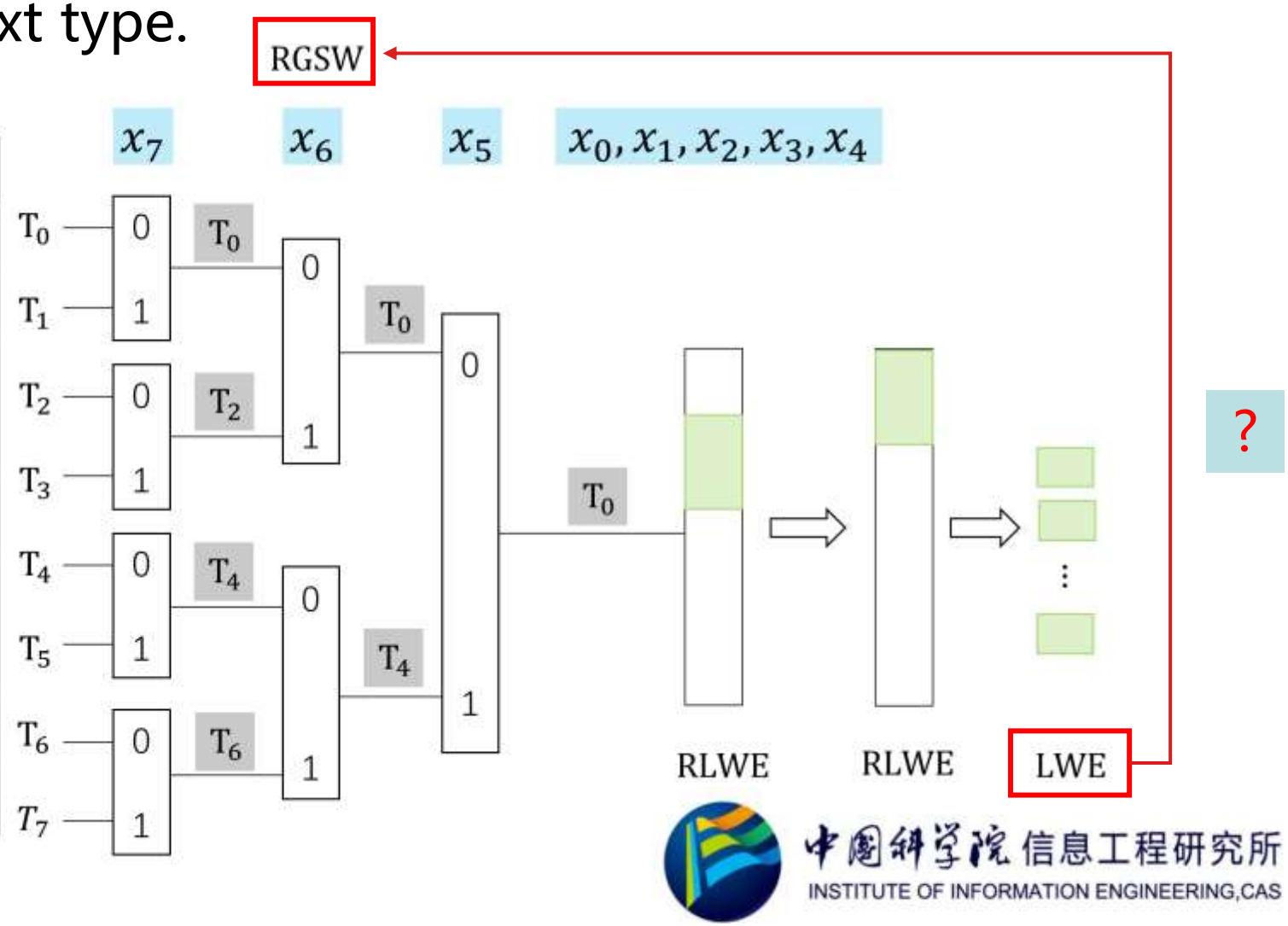
x_0	$\cdots$	x_7	f_0	$\cdots$	f_{31}
0	$\cdots$	0	$\sigma_{0,0}$	$\cdots$	$\sigma_{0,31}$
1	$\cdots$	0	$\sigma_{1,0}$	$\cdots$	$\sigma_{1,31}$
0	$\cdots$	0	$\sigma_{2,0}$	$\cdots$	$\sigma_{2,31}$
1	$\cdots$	0	$\sigma_{3,0}$	$\cdots$	$\sigma_{3,31}$
$\vdots$	$\cdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
0	$\cdots$	1	$\sigma_{252,0}$	$\cdots$	$\sigma_{252,31}$
1	$\cdots$	1	$\sigma_{253,0}$	$\cdots$	$\sigma_{253,31}$
0	$\cdots$	1	$\sigma_{254,0}$	$\cdots$	$\sigma_{254,31}$
1	$\cdots$	1	$\sigma_{255,0}$	$\cdots$	$\sigma_{255,31}$



Circuit Bootstrapping

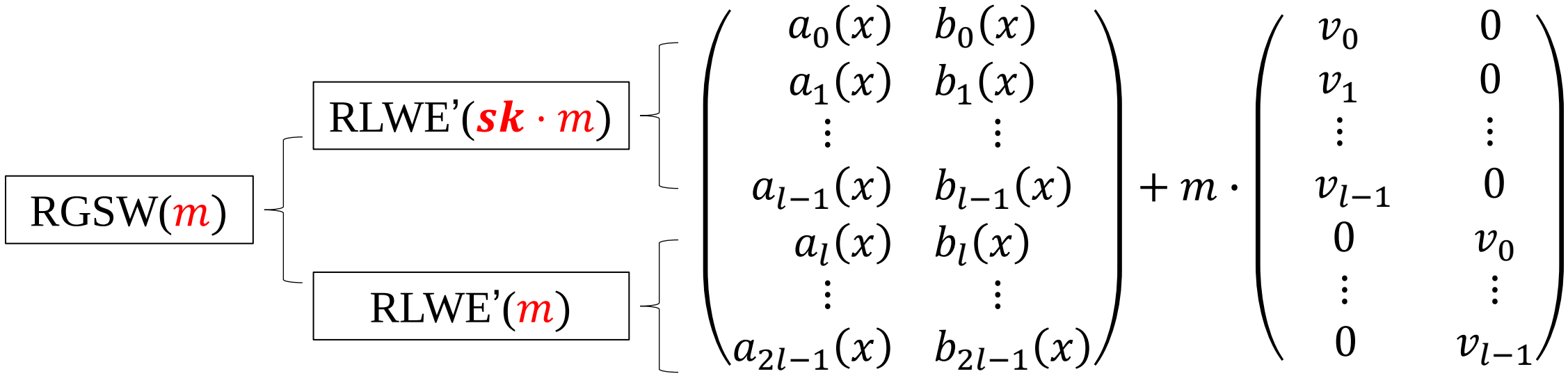
- Goal 1: Refresh noise.
- Goal 2: Convert ciphertext type.

x_0	$\cdots$	x_7	f_0	$\cdots$	f_{31}
0	$\cdots$	0	$\sigma_{0,0}$	$\cdots$	$\sigma_{0,31}$
1	$\cdots$	0	$\sigma_{1,0}$	$\cdots$	$\sigma_{1,31}$
0	$\cdots$	0	$\sigma_{2,0}$	$\cdots$	$\sigma_{2,31}$
1	$\cdots$	0	$\sigma_{3,0}$	$\cdots$	$\sigma_{3,31}$
$\vdots$	$\cdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
0	$\cdots$	1	$\sigma_{252,0}$	$\cdots$	$\sigma_{252,31}$
1	$\cdots$	1	$\sigma_{253,0}$	$\cdots$	$\sigma_{253,31}$
0	$\cdots$	1	$\sigma_{254,0}$	$\cdots$	$\sigma_{254,31}$
1	$\cdots$	1	$\sigma_{255,0}$	$\cdots$	$\sigma_{255,31}$



RGSW Construction

- An RGSW ciphertext consists of two decomposed RLWE ciphertexts.
- Circuit Bootstrapping: From **LWE** to refreshed **Gadget RLWEs**.



Gadget Vector: $(v_0, \dots, v_l)$

Gadget RLWE: $\mathrm{RLWE'}(m) = (\mathrm{RLWE}(v_0 \cdot m), \dots, \mathrm{RLWE}(v_{l-1} \cdot m))$

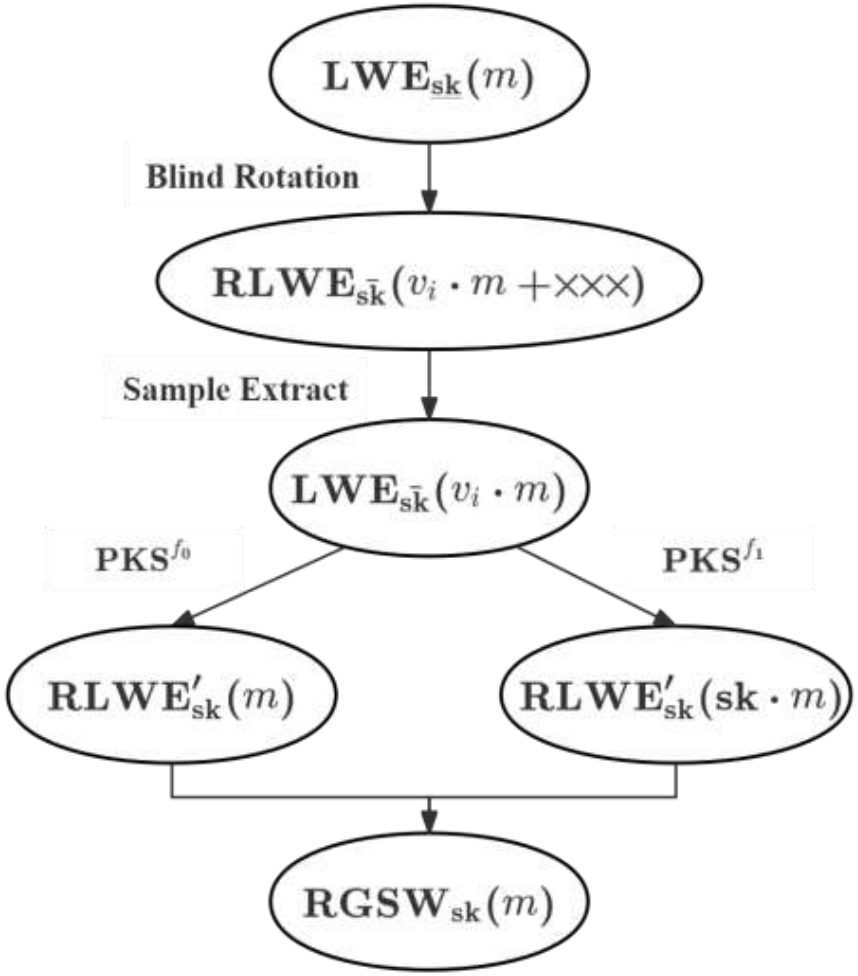
Outline

- Background
- LHE Evaluation Mode
- Improved Circuit Bootstrapping
  - Conversion over the Polynomial Ring
  - Improved Automorphism-Based Blind Rotation
- Performance
- Discussion
- Q&A

中国科学院信息工程研究所
INSTITUTE OF INFORMATION ENGINEERING,CAS

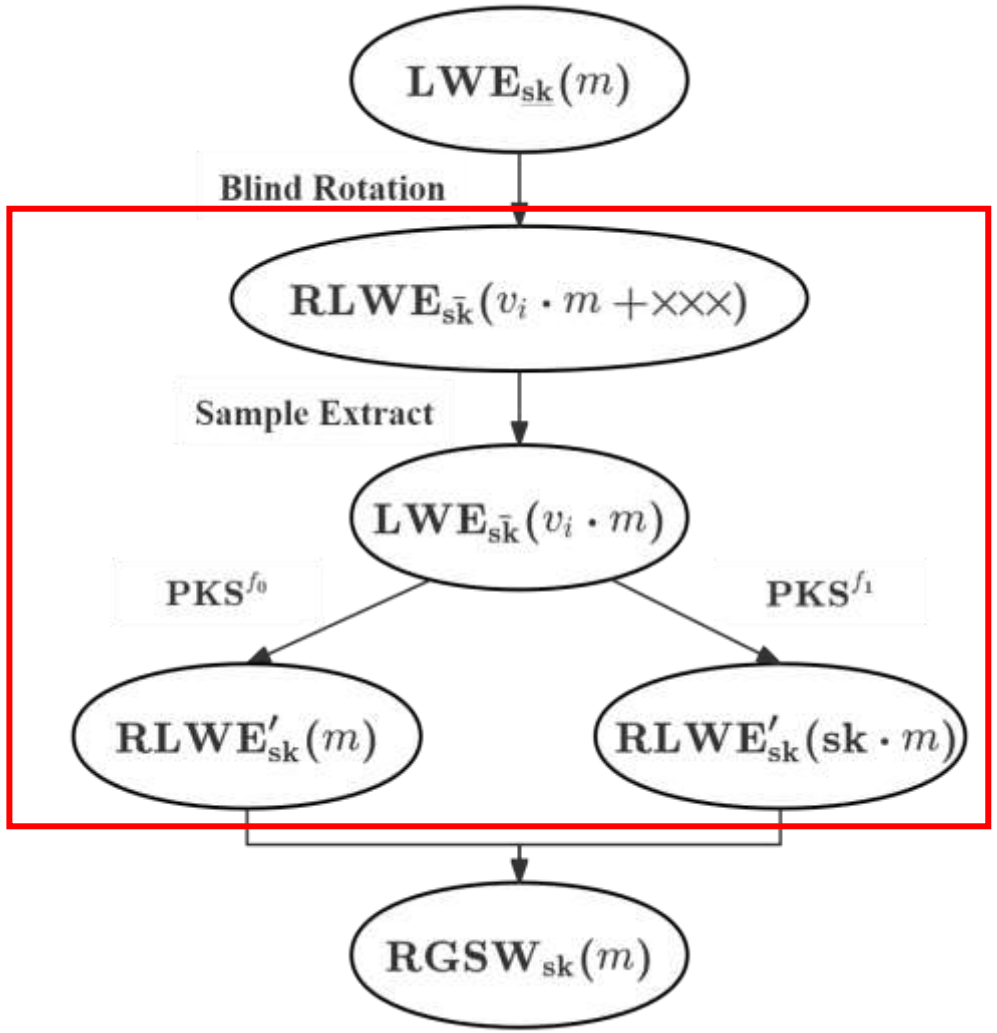
Original Idea

- Using (MV) functional bootstrapping to refresh the noise.
- Using **private key switching** to convert from LWE to RLWE’ .



Original Idea

- Conversion step accounts for more than 70% CBS time.

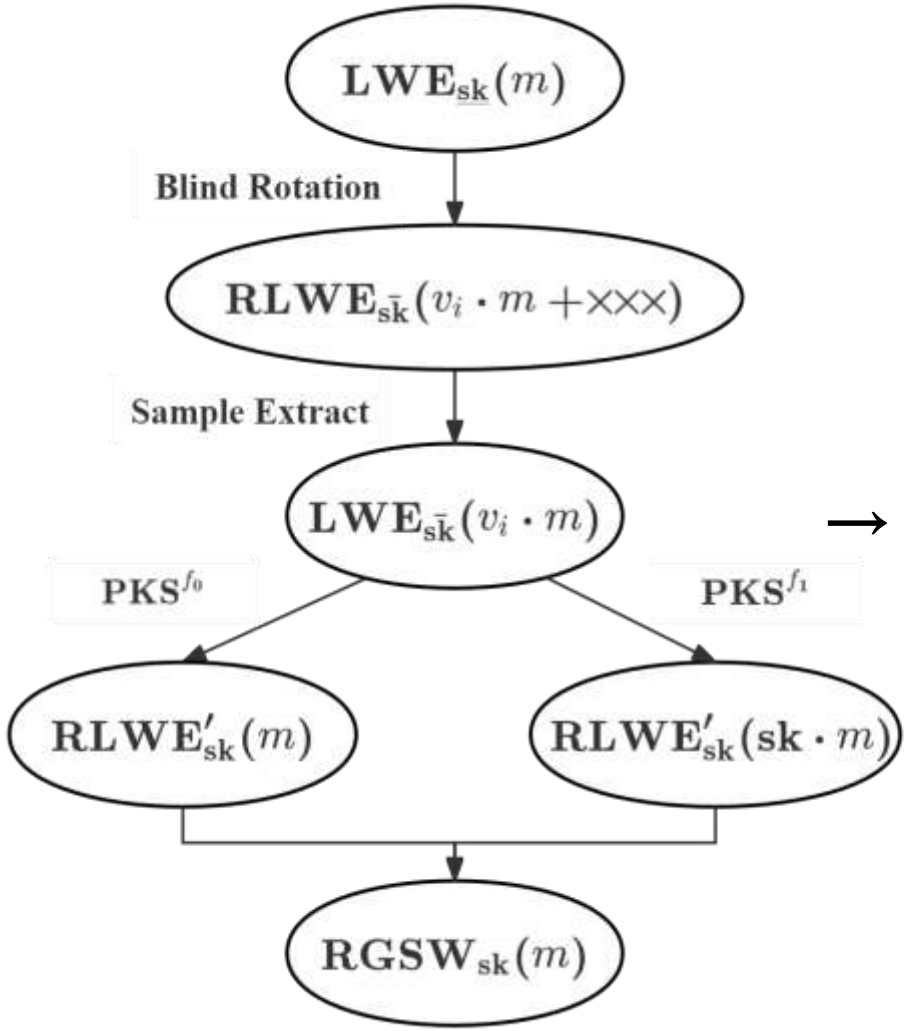


RLWE→LWE→RLWE

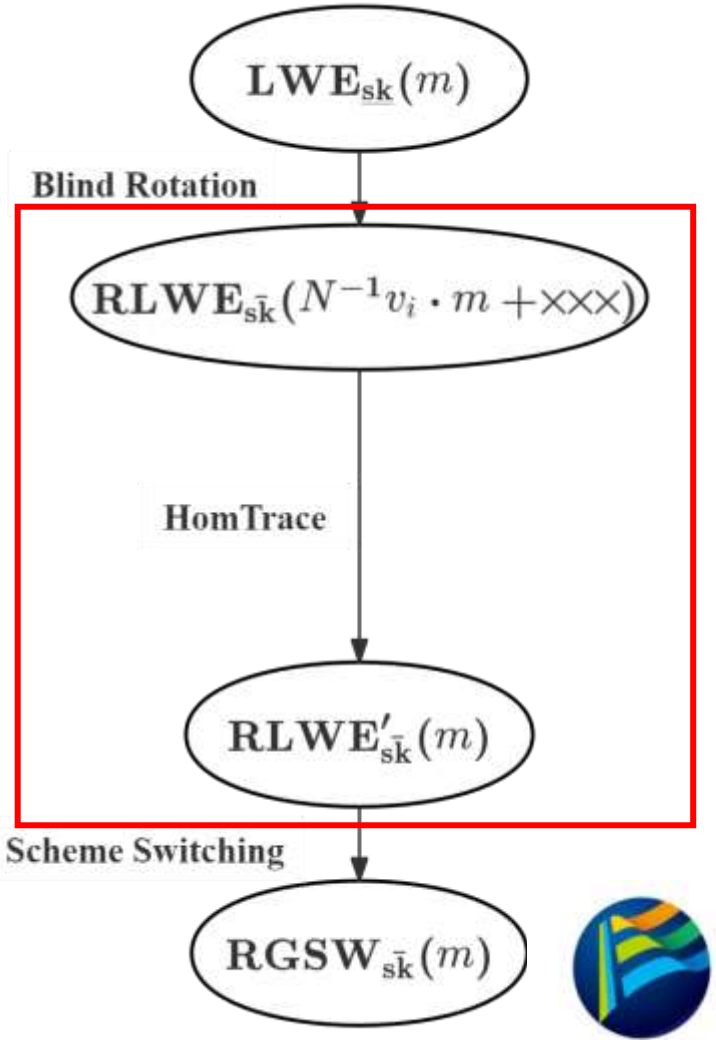
Expensive!

Conversion over the Polynomial Ring

- Our idea: Avoid switching between LWE and RLWE.



→

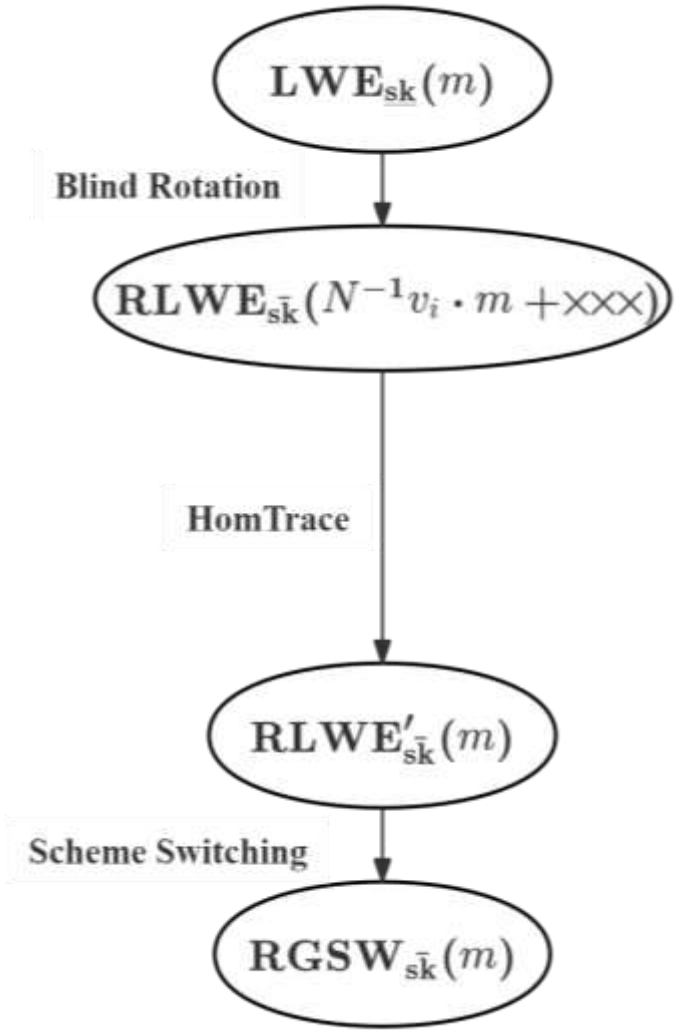


Ring Structure

中国科学院信息工程研究所
INSTITUTE OF INFORMATION ENGINEERING,CAS

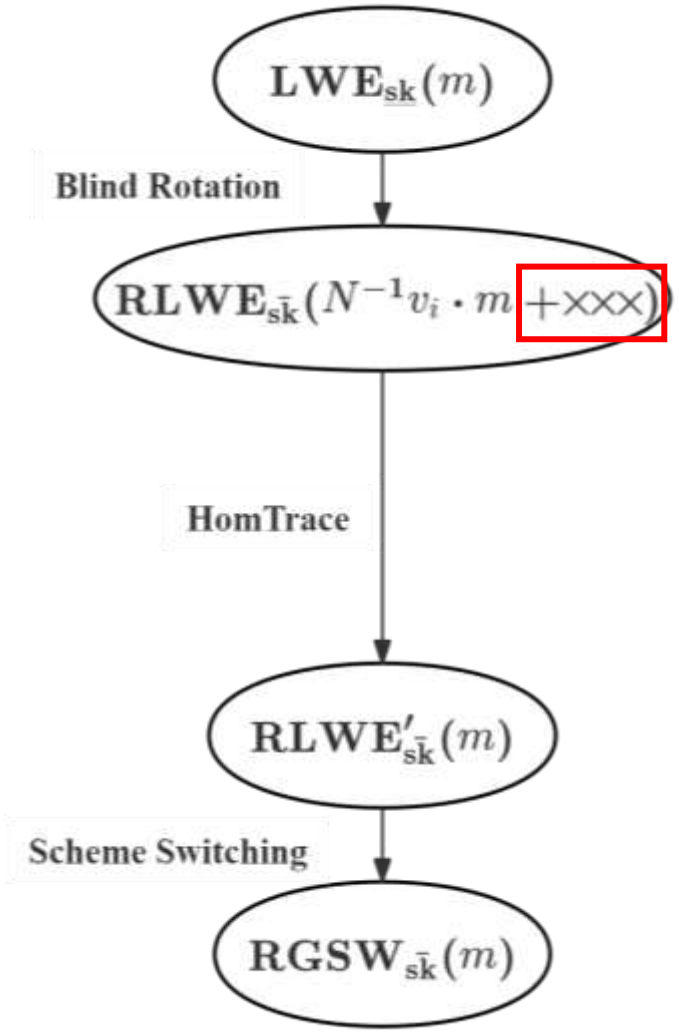
Conversion over the Polynomial Ring

- Key problem: there are some redundant terms after blind rotation.



Conversion over the Polynomial Ring

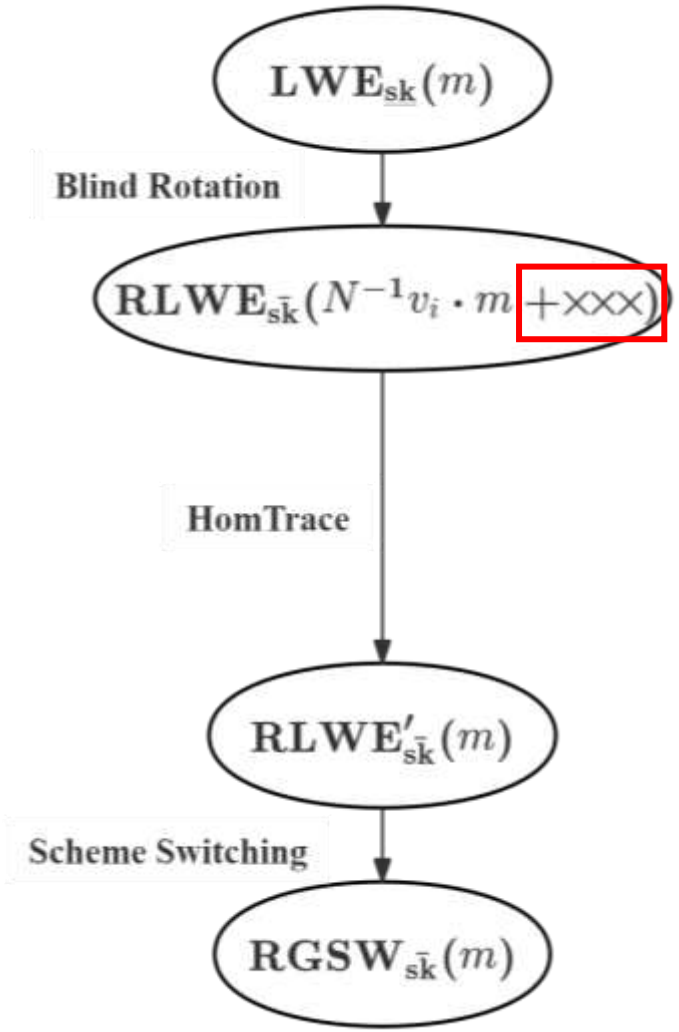
- Key problem: there are some **redundant terms** after blind rotation.



Redundant Power of X!

Conversion over the Polynomial Ring

- Solution: use HomTrace to turn them to 0.

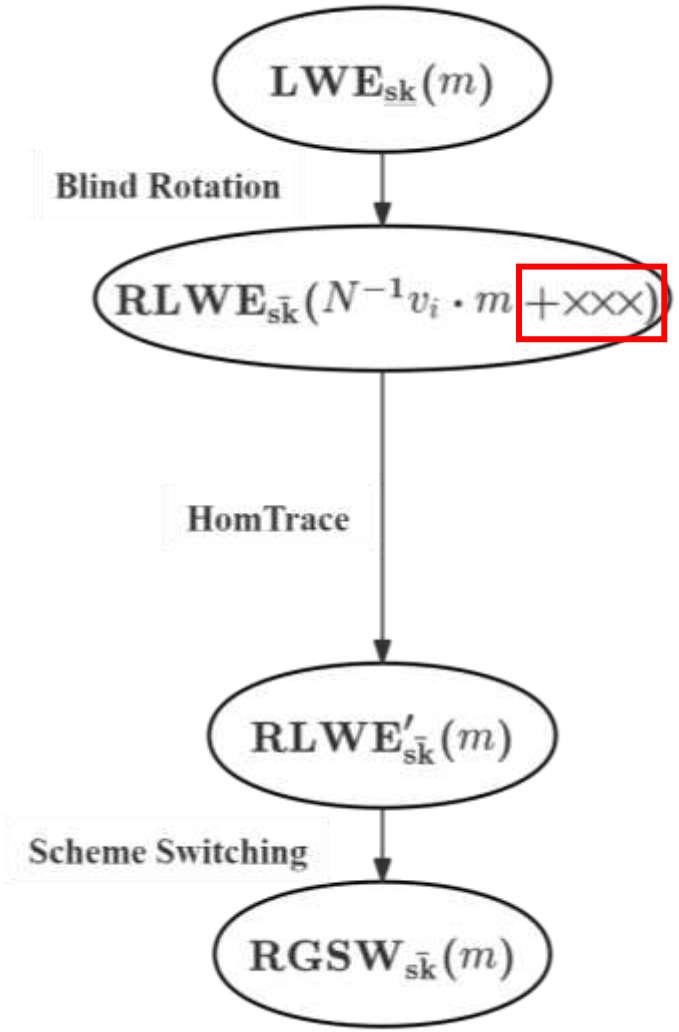


Trace Property:

$$\prod_{t=\log \bar{N}-1}^{0} \phi_t(\bar{N}^{-1}v_i \cdot m + y_1 X + \ldots + y_{\bar{N}-1}X^{\bar{N}-1}) = v_i \cdot m.$$

Conversion over the Polynomial Ring

- Solution: use HomTrace to turn them to 0.

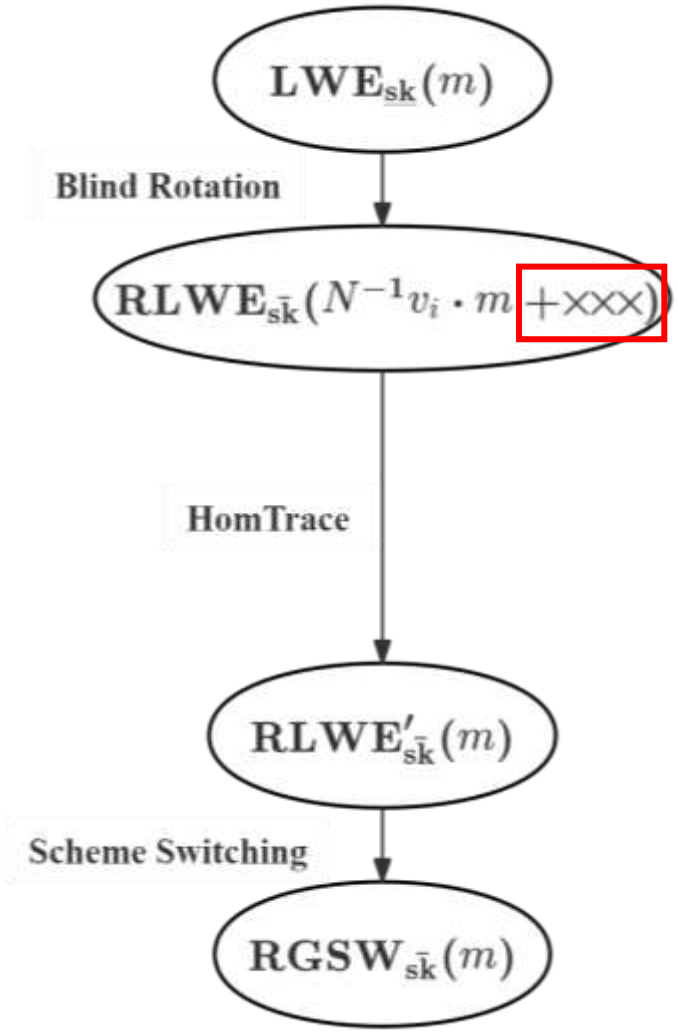


Trace Property:

$$\prod_{t=\log \bar{N}-1}^{0} \phi_t(\bar{N}^{-1}v_i \cdot m + y_1 X + \ldots + y_{\bar{N}-1}X^{\bar{N}-1}) = v_i \cdot m.$$

Conversion over the Polynomial Ring

- Solution: decompose HomTrace to $\log N$ HomAuto.



Trace Property:

$$\prod_{t=\log \bar{N}-1}^{0} \phi_t(\bar{N}^{-1}v_i \cdot m + y_1 X + \ldots + y_{\bar{N}-1}X^{\bar{N}-1}) = v_i \cdot m.$$

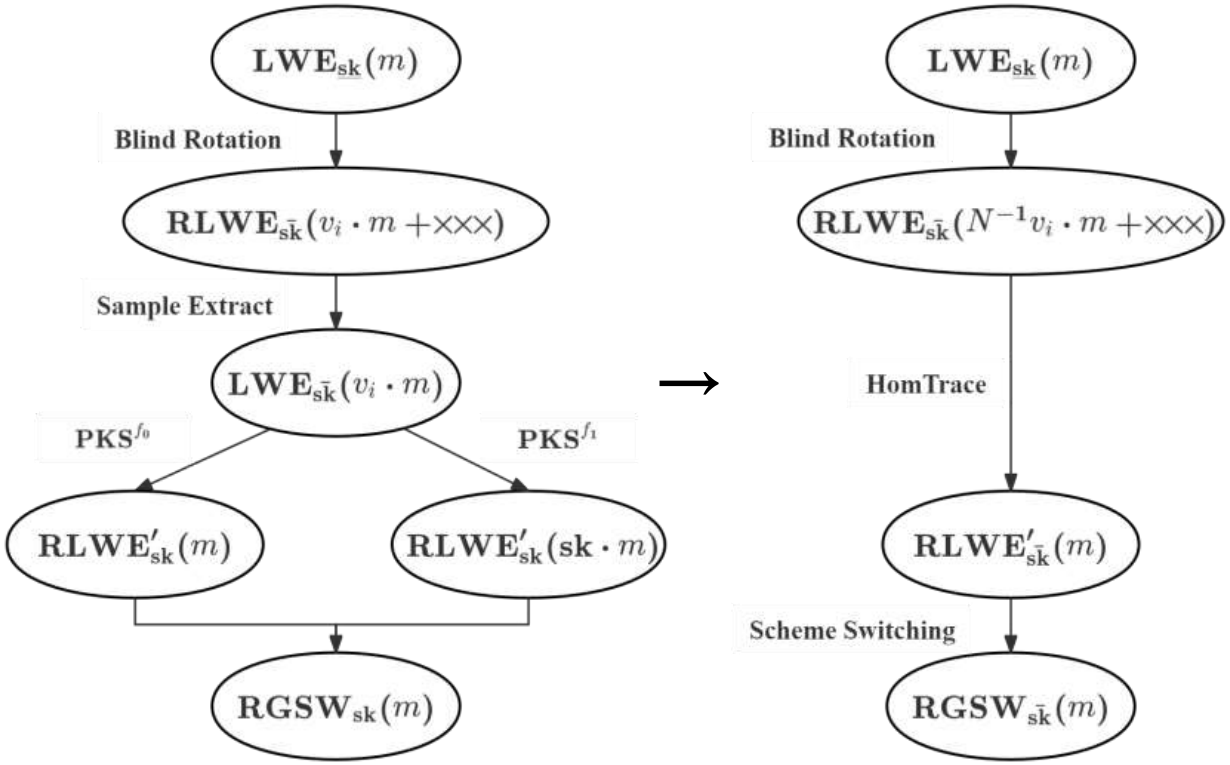
Tower Case Decomposition:

$$\prod_{t=j}^{0} \phi_t(X^i) = \phi_j \circ \cdots \circ \phi_0(X^i) = \begin{cases} 0, & k \le j \le \log \bar{N}, \\ 2^{j+1}, & 0 \le j < k. \end{cases}$$

中国科学院信息工程研究所
INSTITUTE OF INFORMATION ENGINEERING,CAS

Conversion over the Polynomial Ring

- Faster and Smaller.



Computational Complexity:

$O(N^2) \rightarrow O(N \log^2 N)$,

Key Size:

$O(N^2 \log Q) \rightarrow O(N \log N \log Q)$.

Automorphism-Based Blind Rotation

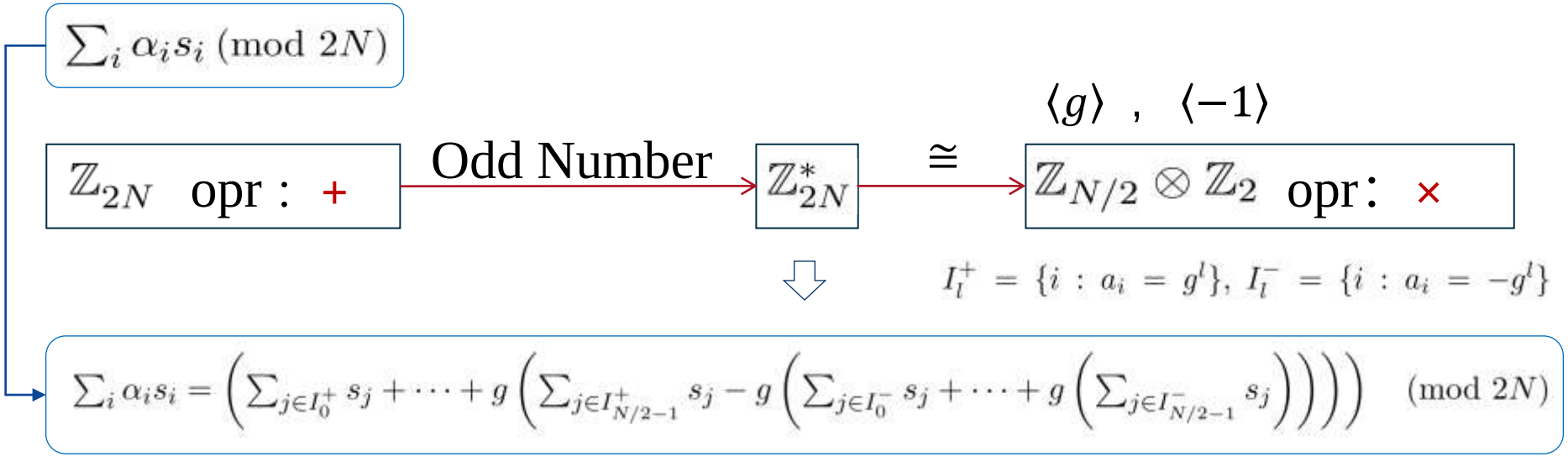
- LMKC23：choose odd numbers.
- Convert operations from an additive group to a multiplicative group.

$\sum_i \alpha_i s_i \pmod{2N}$

$\mathbb{Z}_{2N}$ opr：+ → Odd Number → $\mathbb{Z}_{2N}^*$ → $\cong$ → $\langle g \rangle$ ， $\langle -1 \rangle$ → $\mathbb{Z}_{N/2} \otimes \mathbb{Z}_2$ opr：×

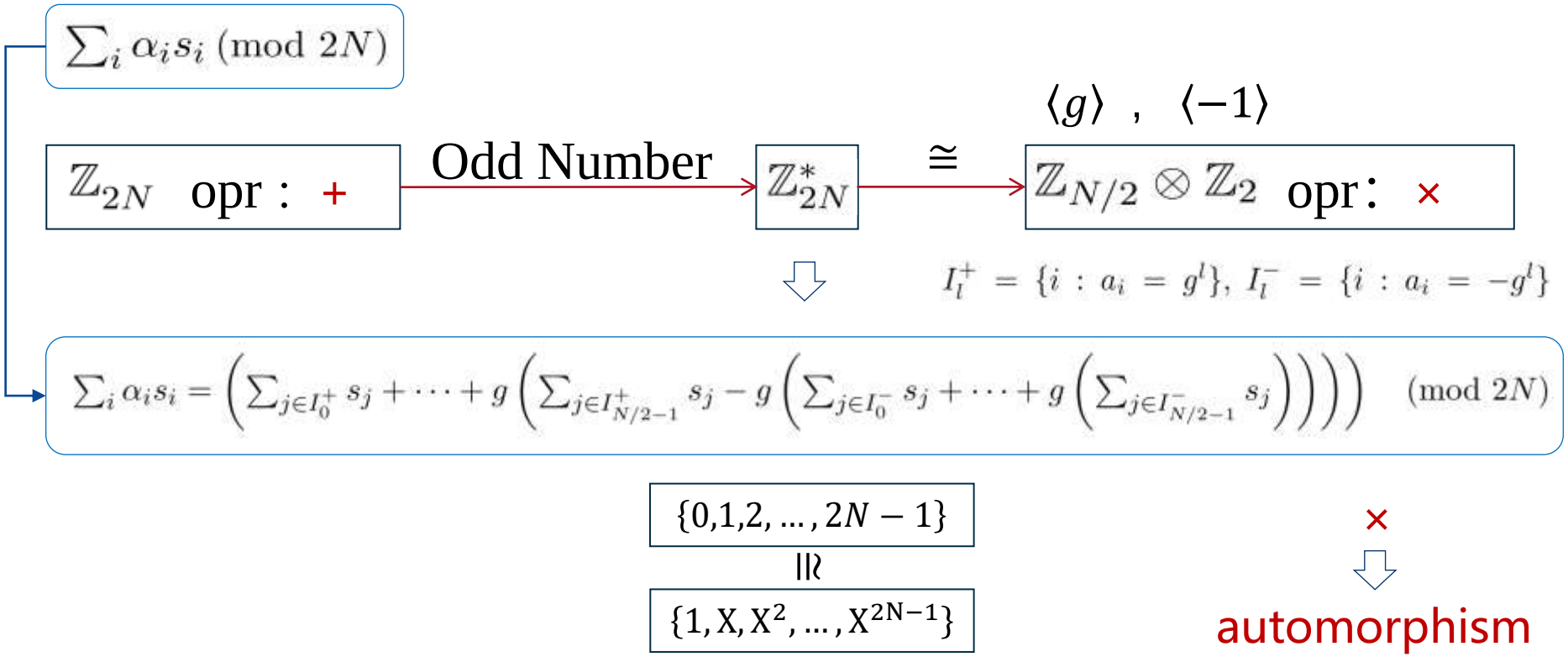
Automorphism-Based Blind Rotation

- LMKC23：choose odd numbers.
- Convert operations from an additive group to a multiplicative group.



Automorphism-Based Blind Rotation

- Map these elements to the powers of X.
- Then the multiplications are computed through automorphisms.



Automorphism-Based Blind Rotation

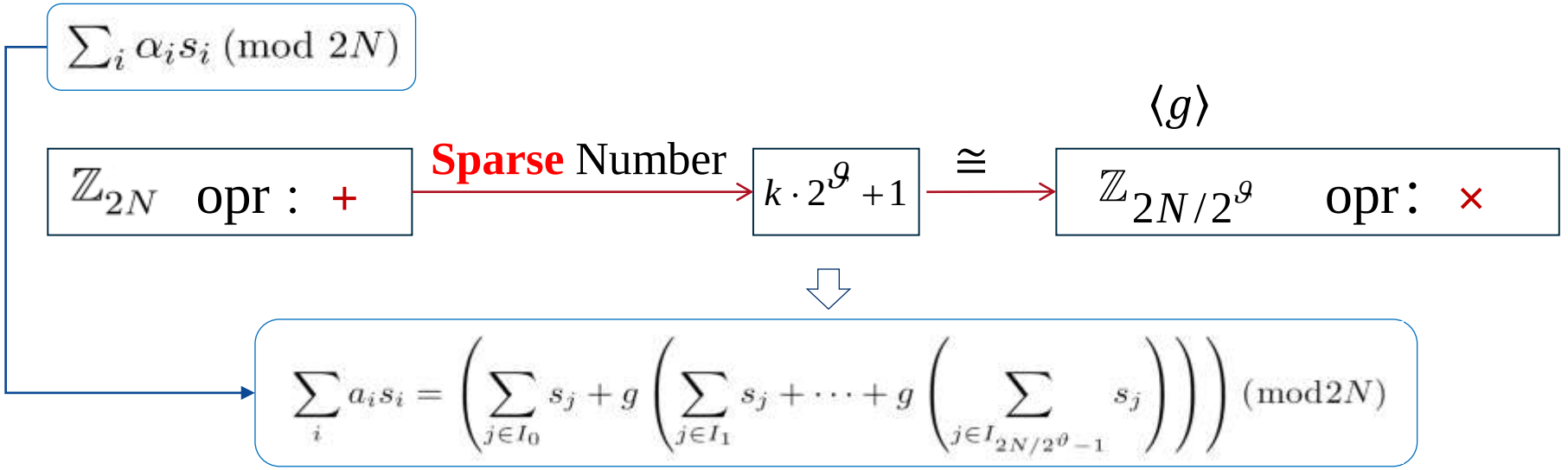
- Our improved method：choose more sparse numbers.
- Convert operations to a new multiplicative group.

$\sum_i \alpha_i s_i \pmod{2N}$

$\mathbb{Z}_{2N}$ opr：+ → **Sparse** Number → $k \cdot 2^{\vartheta} + 1$ → $\cong$ → $\mathbb{Z}_{2N/2^{\vartheta}}$ opr：× (over $\langle g \rangle$)

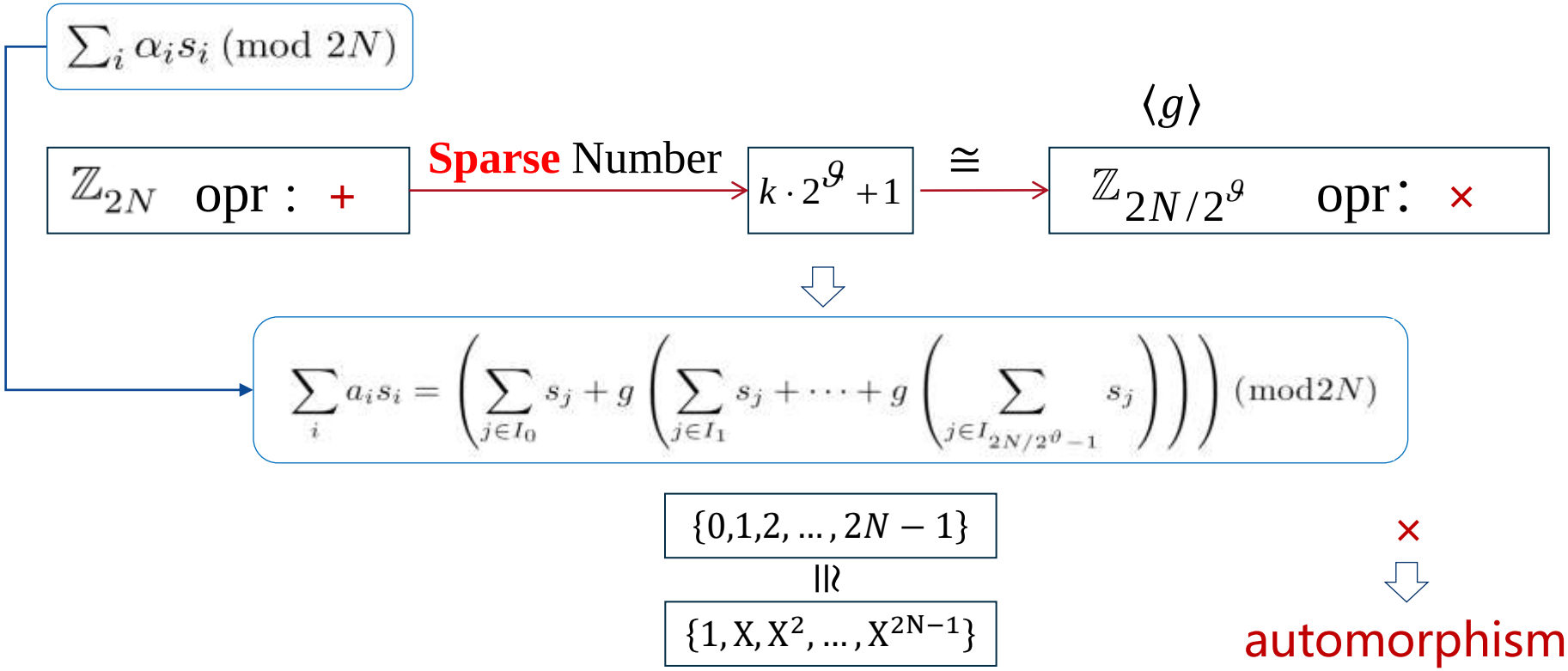
Automorphism-Based Blind Rotation

- Our improved method：choose more sparse numbers.
- Convert operations to a new multiplicative group.



Automorphism-Based Blind Rotation

- Advantages: less automorphisms.
- Sparse blind rotation implies Muti-Value FBS for circuit bootstrapping.



Outline

- Background
- LHE Evaluation Mode
- Improved Circuit Bootstrapping
- Performance
- Discussion
- Q&A

Performance

■ **Implementation**: https://github.com/LightFHE/CircuitBootstrap

- **Based Library**: OpenFHE
- **Environment**: 11th Gen Intel(R) Core(TM) i5-11500 @ 2.70GHz, 32 GB RAM

Parameter for Security						
λ	Q	N	q	n	σ_{fresh}	$Prob$
128 bit	54 bit	2048	1024	571	3.2	2^{-32}

Performance (with adjusted parameters)					
Sets	$Base_{ep}$	$Base_{trace}$	$Base_{ss}$	Run Time	Key Size
I	17 bit	17 bit	28 bit	98 ms	60 MB
II	13 bit	17 bit	28 bit	126 ms	90 MB
III	10 bit	13 bit	28 bit	158 ms	121 MB

中国科学院信息工程研究所
INSTITUTE OF INFORMATION ENGINEERING,CAS

Performance

■ **Implementation**: https://github.com/LightFHE/CircuitBootstrap

- **Based Library**: OpenFHE
- **Environment**: 11th Gen Intel(R) Core(TM) i5-11500 @ 2.70GHz, 32 GB RAM

Parameter for Security						
λ	Q	N	q	n	σ_{fresh}	$Prob$
128 bit	54 bit	2048	1024	571	3.2	2^{-32}

Comparison					
Original			Ours		
Method	Run Time	Key Size	Sets	Run Time	Key Size
TFHE	877 ms	479 MB	II	126 ms (7×)	90 MB (5×)
TFHE_{pre}	484 ms	2720 MB	III	158 ms (3×)	121 MB (25×)

Outline

- Background
- LHE Evaluation Mode
- Improved Circuit Bootstrapping
- Performance
- Discussion
- Q&A

Discussion

- Compare with TFHE-lib, TFHEpp, MOSFHET.
  - AVX-512
  - NTT vs FFT
- Wake up the “Sleepy Field”.
  - Batching , LUT through “batching RGSW”？
  - Transciphering [WWLL+23, WLWL+24]
  - TT-network, spiking network …

[WWLL+23] Benqiang Wei, Ruida Wang, Zhihao Li, Qinju Liu, Xianhui Lu. Fregata: Faster Homomorphic Evaluation of AES via TFHE. Information Security Conference, 2023:392-412.
[WLWL+24] Benqiang Wei, Xianhui Lu , Ruida Wang, Kun Liu, Zhihao Li, Kunpeng Wang. Thunderbird: Efficient Homomorphic Evaluation of Symmetric Ciphers in 3GPP by combining two modes of TFHE. IACR Trans. Cryptogr. Hardw. Embed. Syst. 2024(3).

中国科学院信息工程研究所
INSTITUTE OF INFORMATION ENGINEERING,CAS

Outline

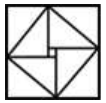
- **Background**
  - Fully Homomorphic Encryption
  - FHEW/TFHE Scheme
  - FHEW/TFHE Bootstrapping
- **LHE Evaluation Mode**
  - Look-Up-Table Via CMUX Gate
  - Circuit Bootstrapping (CGGI17, CLOT21)
- **Improved Circuit Bootstrapping**
  - Conversion over the Polynomial Ring
  - Improved Automorphism-Based Blind Rotation
- **Performance**
- **Discussion**
- **Q&A**

Thank you for listening!

Contact: wangruida@iie.ac.cn

中国科学院信息工程研究所
INSTITUTE OF INFORMATION ENGINEERING,CAS

中国科学院大学
University of Chinese Academy of Sciences



AMSS
Academy of Mathematics and Systems Science,CAS