Is Fully Homomorphic Encryption Ready for Now?

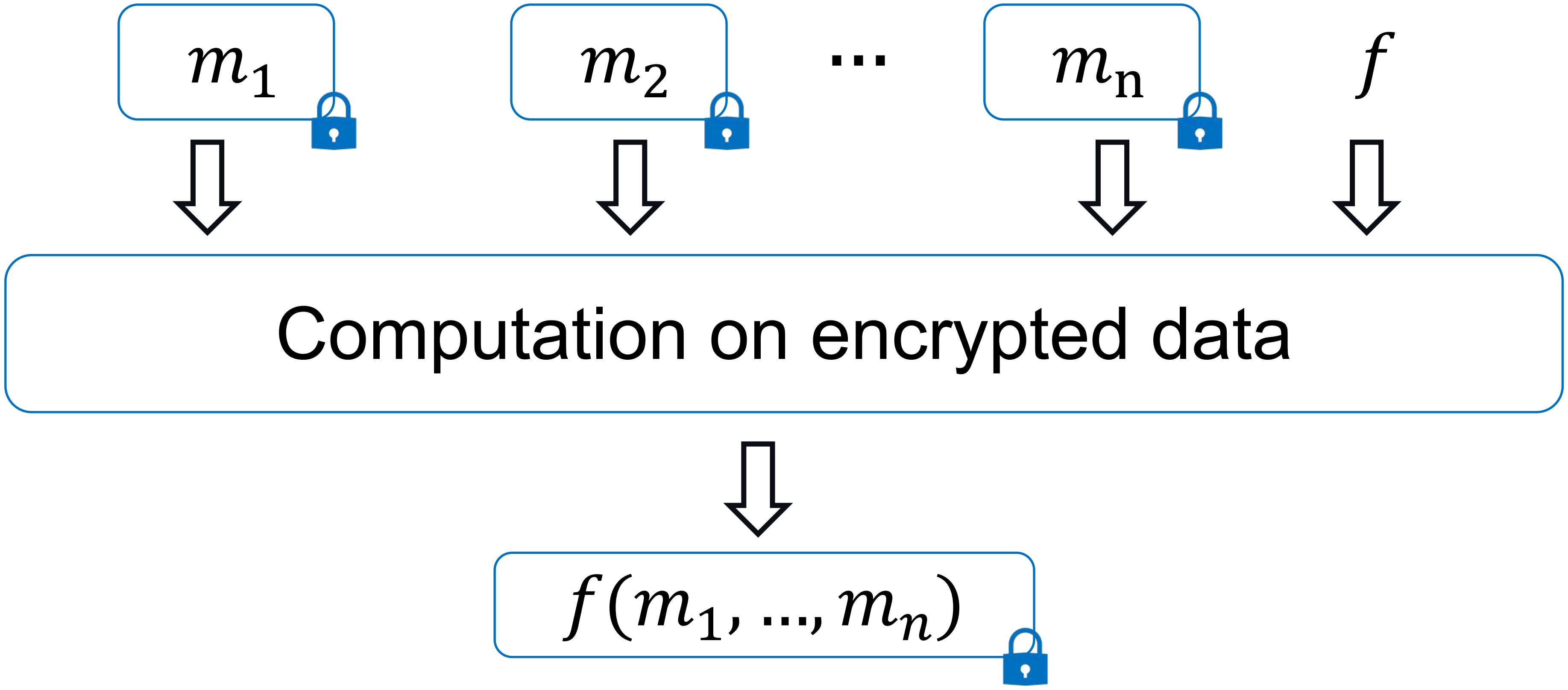
— Developments and Standards

Xianhui Lu
Institute of Information Engineering, CAS
University of Chinese Academy of Sciences

Outline

- Backgroud
- Developments
  - Evaluation Modes
  - Bootsrapping
  - Transciphering
  - Homo-Processor
- Standardization

What is Fully Homomorphic Encryption



FHE is a powerful encryption scheme that allows **computation** on **encrypted** data.

What Can FHE Do

$$\mathrm{E}_k(x), f$$

$$\mathrm{E}_k(f(x))$$

User

Cloud Server

Privacy preserving in cloud computing.

History of FHE

47 years research

16 years design

8 years basic scheme

8 years speedup+stdardard

PartialHE

ElGamal1985
Paillier1999
……

Full HE
Gentry09
Ideal Lattice
Framework

FHE
(R)LWE
BV11
BGV12
BV12

FHE
(R)GSW
GSW13
AP14
DM15
CGGI16

Fixed
Point
CKKS17

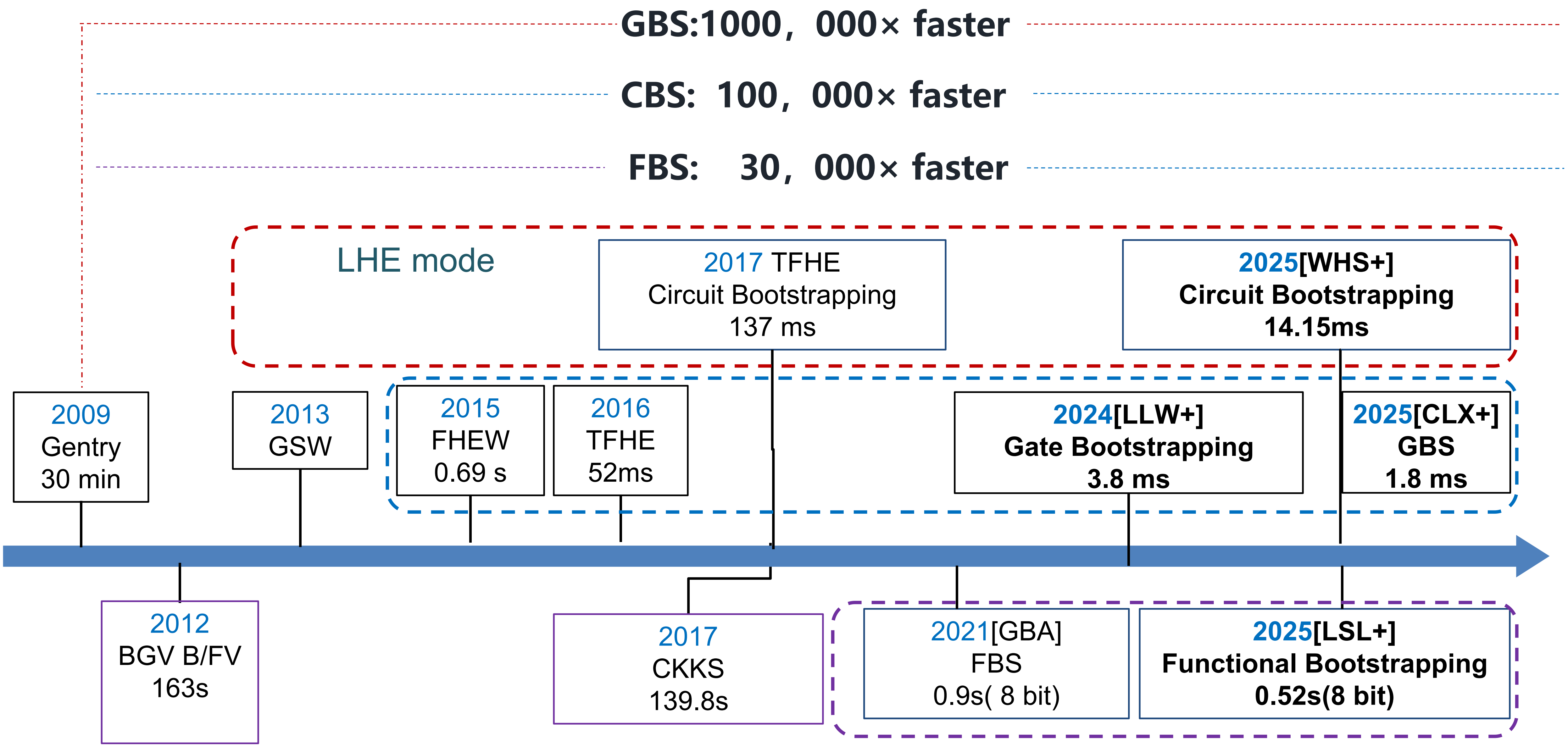
Standardization
ISO/IEC18033-6: ElGamal, Paillier
ISO/IEC 28033: BGV/BFV/CKKS/TFHE

Implementation
IBM: HELib (BGV+CKKS)
Microsoft: SEAL (BFV+CKKS)
Nicolas, Ilaria: TFHE

Evolution
Packing, Switching, Transciphering,
Bootstrapping, Compiling

1978 **2009** **2017** **2025**

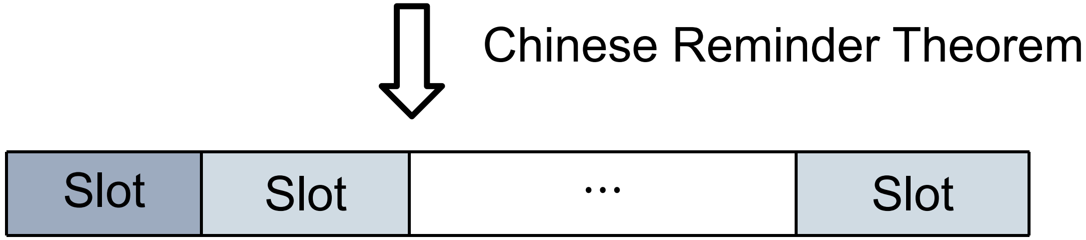
Performance Evolution of FHE



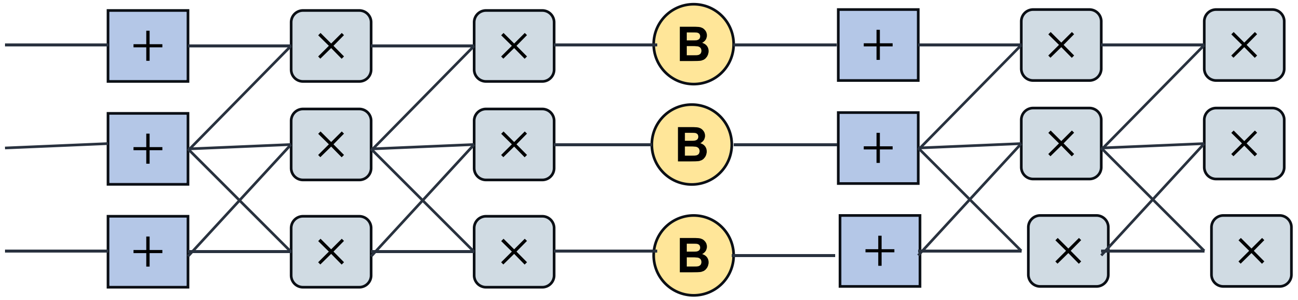
Lib	Features	Team
SEAL	**SIMD mod t & finite field vectors** **SIMD fixed point numbers,**BFV, CKKS	**Microsoft** (Kristin Lauter, Kim Laine, and Sreekanth Kannepalli)
HElib	**SIMD mod t & finite field vectors** **SIMD fixed point numbers,** BGV, CKKS	**IBM** (Shai Halevi, Victor Shoup)
HEAAN	**SIMD fixed point numbers** CKKS	Andrey Kim, Kyoohyung, Han
TFHE, TFHE-rs	**Boolean logic, Comparison** GSW13-AP14-DM15-TFHE	S. Carpov, I. Chillotti, N. Gama, M. Georgieva, M. Izabachene, https://github.com/zama-ai/tfhe-rs
FHEW	**Boolean logic, Comparison** GSW13-AP14-DM15	Léo Ducas, Daniele Micciancio
LightFHE	**Circuit Bootstrapping** Compact circuit bootstrapping, Transciphering, FHE processor instruction	Institute of Information Engineering, CAS Ruida Wang, Jincheol Ha, Xuan Shen, Xianhui Lu https://github.com/serengil/LightFHE
PALISADE	**Library for lattice cryptography** BFV, BGV, LTV, CKKS Prox Re-encryption,IB-HE, GPV Signature	**NJIT +** Partners and Collaborators: MIT, UCSD, WPI, NUS, Sabanci U, Raytheon (BBN), IBM Research, Lucent, Vencore Labs, Galois, Two Six Labs
OpenFHE	PALISADE+HELib+HEAAN+FHEW AVX-512, Python, Official Webassemly (NodeJS)	open-source project https://github.com/OpenFHEOrg

Developments of Eval Mode: SIMD+Level

- High Throughput Mode: BGV/BFV/CKKS
  - SIMD: Plaintext space: $a_0 + a_1X + \cdots + a_{n-1}X^{n-1}$



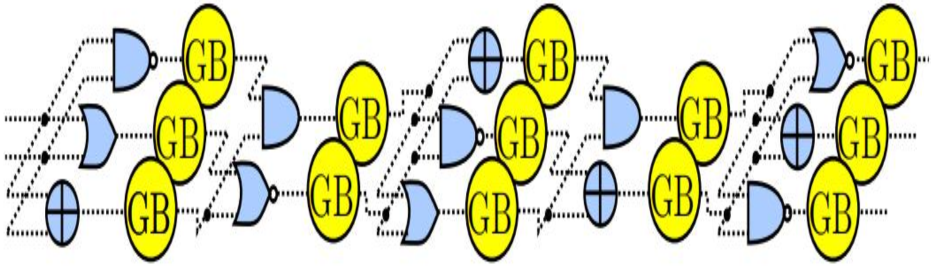
  - Level Computation Mode:



1. Zvika Brakerski, Craig Gentry, Vinod Vaikuntanathan: (Leveled) fully homomorphic encryption without bootstrapping. ITCS 2012: 309-325
2. Zvika Brakerski, Vinod Vaikuntanathan: Efficient Fully Homomorphic Encryption from (Standard) LWE. FOCS 2011: 97-106
3. Jung Hee Cheon, Andrey Kim, Miran Kim, Yong Soo Song: Homomorphic Encryption for Arithmetic of Approximate Numbers. ASIACRYPT (1) 2017: 409-437
4. Shihe Ma, Tairong Huang, Anyu Wang, Xiaoyun Wang: Accelerating BGV Bootstrapping for Large p Using Null Polynomials over $\mathbb {Z}_{p^e}$. EUROCRYPT (2) 2024: 403-432
5. Shihe Ma, Tairong Huang, Anyu Wang, Xiaoyun Wang: Faster BGV Bootstrapping for Power-of-Two Cyclotomics Through Homomorphic NTT. ASIACRYPT (1) 2024: 143-175

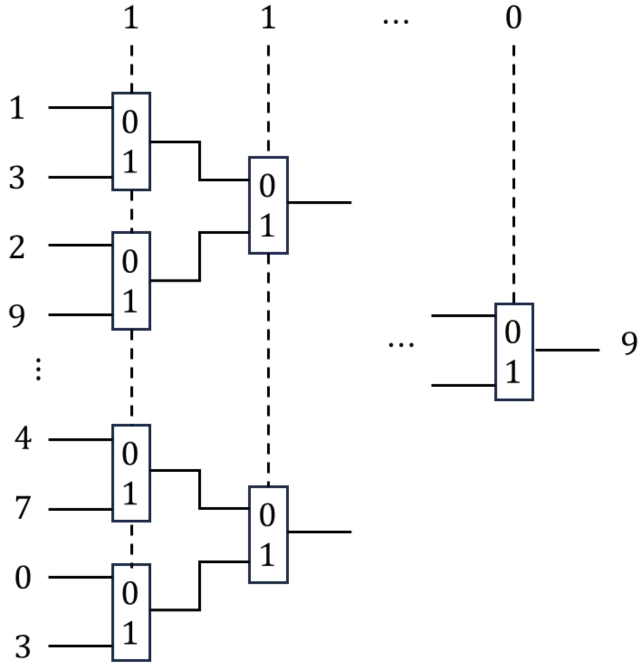
Developments of Eval Mode: Binary+Circuit

- Low Latency Mode: TFHE/FHEW
  - Boolean Gates:



  - Look up Table

x	y
0	1
1	3
2	2
253	7
254	0
255	3

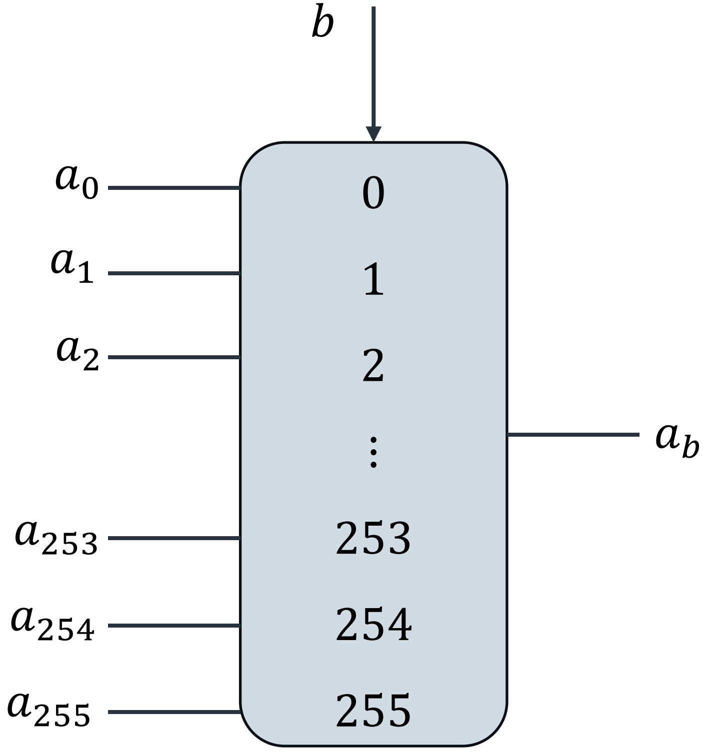


1. Craig Gentry, Amit Sahai, Brent Waters:Homomorphic Encryption from Learning with Errors: Conceptually-Simpler, Asymptotically-Faster, Attribute-Based. CRYPTO (1) 2013: 75-92
2. Léo Ducas, Daniele Micciancio: FHEW: Bootstrapping Homomorphic Encryption in Less Than a Second. EUROCRYPT (1) 2015: 617-640
3. Ilaria Chillotti, Nicolas Gama, Mariya Georgieva, Malika Izabachène:Faster Fully Homomorphic Encryption: Bootstrapping in Less Than 0.1 Seconds. ASIACRYPT (1) 2016: 3-33

Developments of Eval Mode: SIMD Bin+LUT

■ New Mode: BGV/BFV/CKKS with LUT, useful for NN and LLM

x	y
0	1
1	3
2	2
253	7
254	0
255	3



1-out-of N CMUX

Equality Testing Function：

$$g_i(x_j) = \begin{cases} 1, j = i \\ 0, j \neq i \end{cases}$$

For algebra interpolation:

$$g_i(x) = 1 - (x - i)^{p-1}$$

For arithmetic interpolation:

$$g_i(x) = \frac{\prod_{j \neq i}(x - x_j)}{\prod_{j \neq i}(x_i - x_j)}$$

$$p(x) = \sum_{i=1}^{n} y_i g_i(x)$$

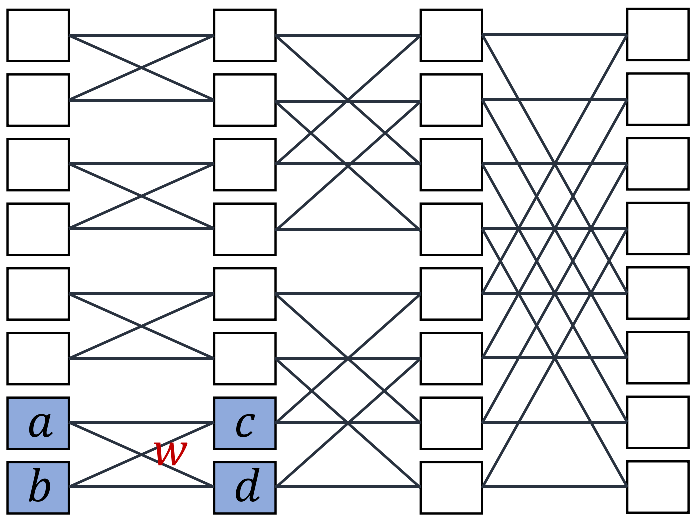
1. Zeyu Liu, Yunhao Wang: Amortized Functional Bootstrapping in Less than 7 ms, with Õ(1) Polynomial Multiplications. ASIACRYPT (6) 2023: 101-132
2. Zeyu Liu, Yunhao Wang: Relaxed Functional Bootstrapping: A New Perspective on BGV/BFV Bootstrapping. ASIACRYPT (1) 2024: 208-240
3. Andreea Alexandru, Andrey Kim, Yuriy Polyakov:General Functional Bootstrapping using CKKS. IACR Cryptol. ePrint Arch. 2024: 1623 (2024), CRYPTO2025.

Developments of Eval Mode: SIMD Bin+LUT

■ New Mode: TFHE/FHEW with SIMD, useful for NN and LLM

- Homomorphic NTT:

$$m = \boldsymbol{a} \cdot \boldsymbol{z} + b$$

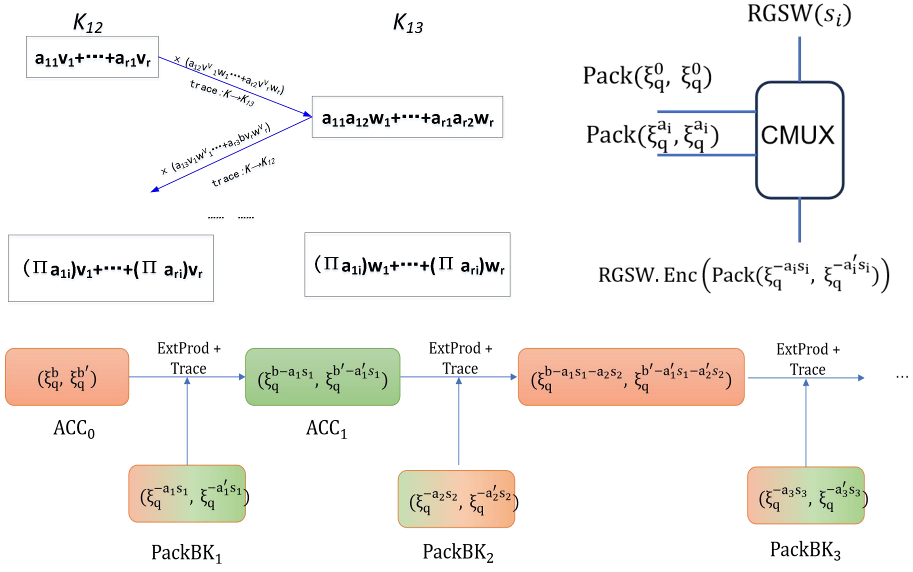


Butterfly transform $c = a + wb$

$d = a - wb$

- Tensor Ring Encoding:

$$R = R_1 \otimes R_2 \otimes R_3$$

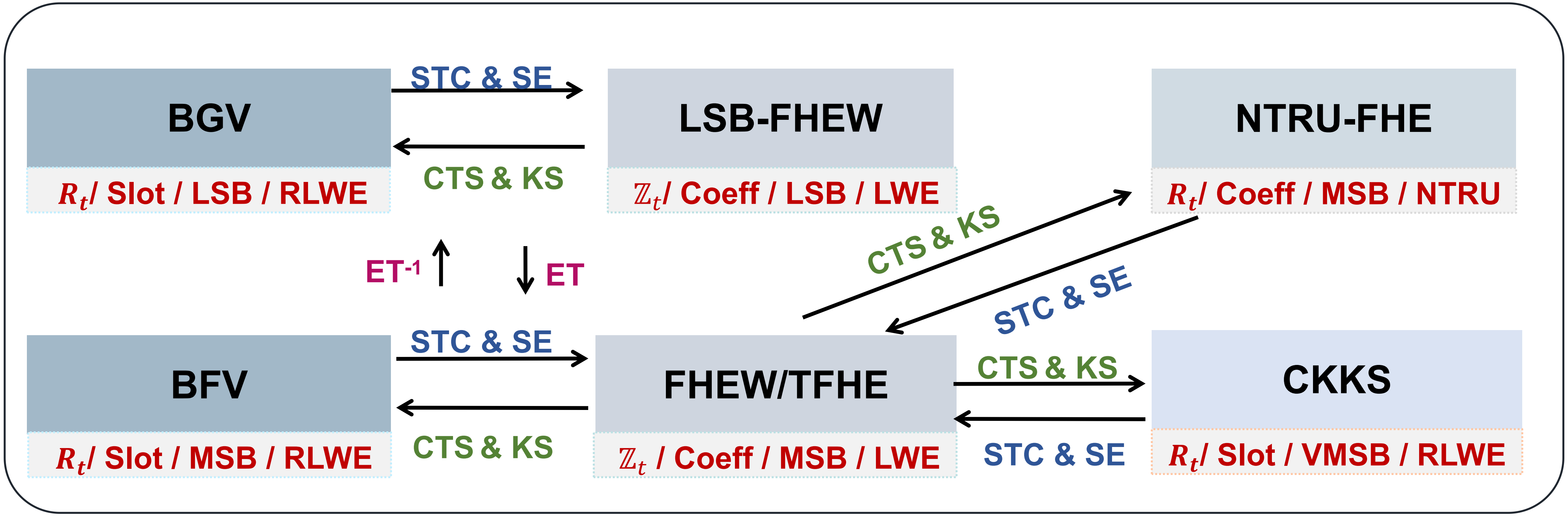


HomTrace based cross-ring bootstrapping

1. Daniele Micciancio, Jessica Sorrell: Ring Packing and Amortized FHEW Bootstrapping. ICALP 2018: 100:1-100:14
2. Antonio Guimarães, Hilder V. L. Pereira, Barry Van Leeuwen: Amortized Bootstrapping Revisited: Simpler, Asymptotically-Faster, Implemented. ASIACRYPT (6) 2023: 3-35
3. Gabrielle De Micheli, Duhyeong Kim, Daniele Micciancio, Adam Suhl:Faster Amortized FHEW Bootstrapping Using Ring Automorphisms. Public Key Cryptography (4) 2024: 322-353
4. Feng-Hao Liu, Han Wang : Batch Bootstrapping I: A New Framework for SIMD Bootstrapping in Polynomial Modulus， Eurocrypt 2023
5. Feng-Hao Liu, Han Wang : Batch Bootstrapping II: Bootstrapping in Polynomial Modulus Only Requires $\tilde{O}(1)$ FHE Multiplications in Amortization， Eurocrypt 2023

Developments of Eval Mode: Hybrid

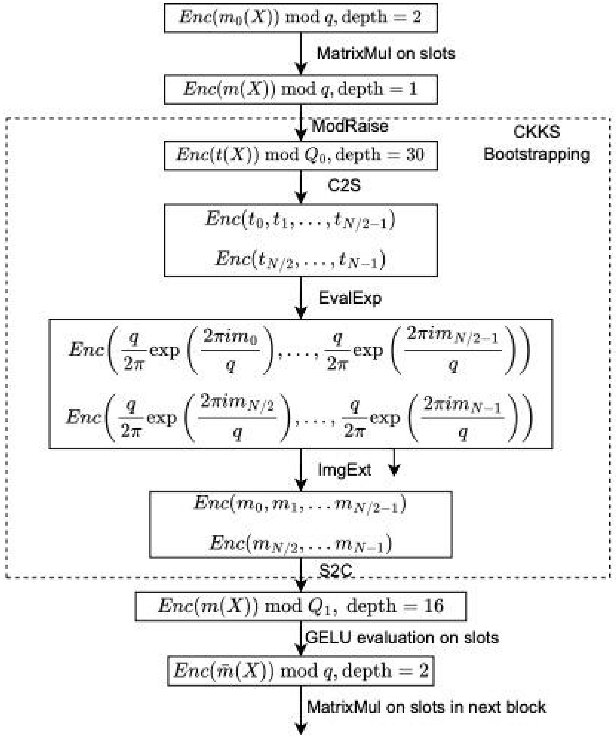
■ Switching Among Different Modes



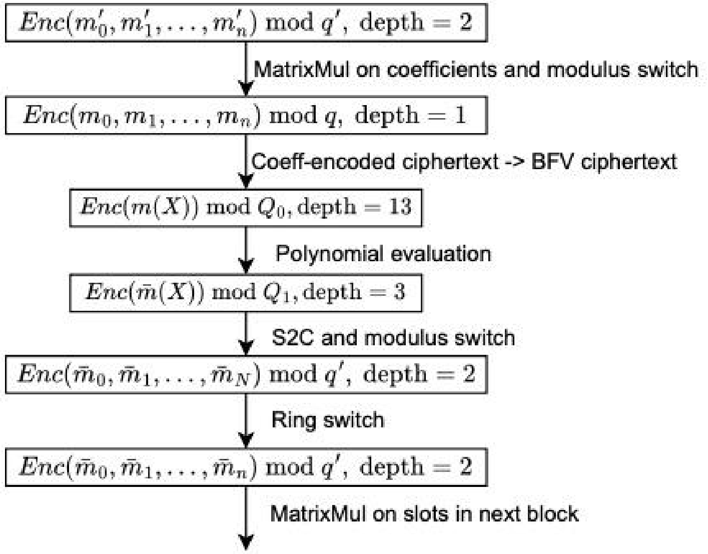
1. Christina Boura, Nicolas Gama, Mariya Georgieva, Dimitar Jetchev: CHIMERA: Combining Ring-LWE-based Fully Homomorphic Encryption Schemes. J. Math. Cryptol. 14(1): 316-338 (2020)
2. Wen-jie Lu, Zhicong Huang,Cheng Hong,Yiping Ma,Hunter Qu: PEGASUS: Bridging Polynomial and Non-polynomial Evaluations in Homomorphic Encryption.SP 2021: 1057-1073
3. Youngjin Bae, Jung Hee Cheon, Jaehyung Kim, Jai Hyun Park, Damien Stehlé: HERMES: Efficient Ring Packing Using MLWE Ciphertexts and Application to Transciphering. CRYPTO (4) 2023: 37-69

Developments of Eval Mode: Use in AI Inference

- Feedforward block inference speedup 100 times



Slot-encoded CKKS evaluation framework
depth: 30, modulus: 1763 bits



Coefficient-encoded matrix multiplication [2]

Improved and optimized functional bootstrapping

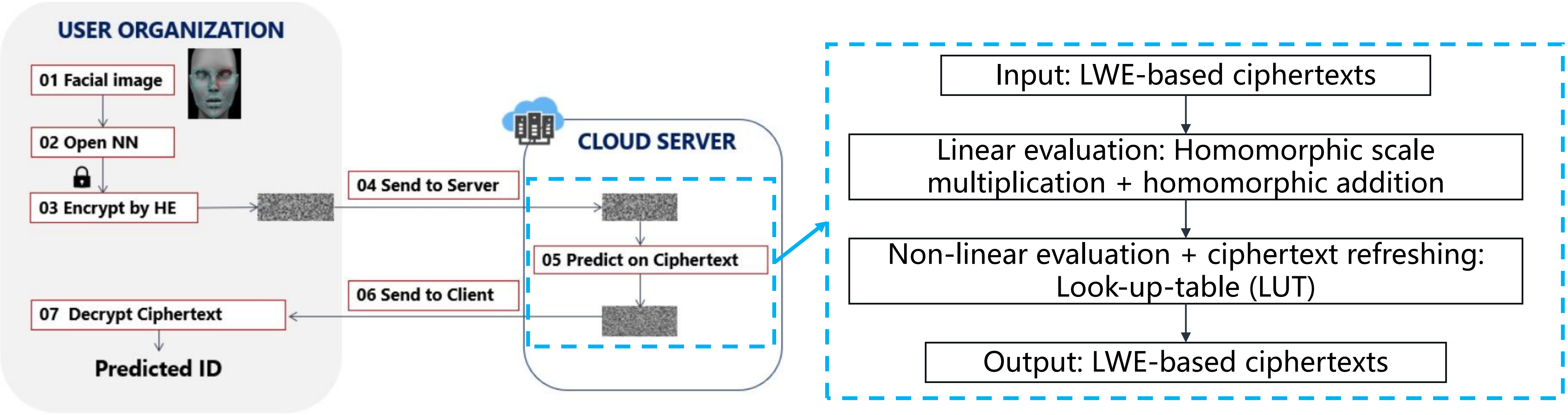
New evaluation framework
depth: 13, modulus: 669bits

When evaluated on the BERT-base model, it achieves a 100× speedup over the state-of-the-art method in the same environment.

1. Linru Zhang, Xiangning Wang, Xianhui Lu,Huaxiong Wang, Kwok-Yan Lam. LEAF: A Low-Latency Evaluation Architecture for Feedforward Block in Privacy-Preserving Transformer Inference[J]. Cryptology ePrint Archive, 2025.
2. Youngjin Bae, Jung Hee Cheon, Guillaume Hanrot, Jai Hyun Park, Damien Stehlé. Plaintext-ciphertext matrix multiplication and FHE bootstrapping: fast and fused[C]//Annual International Cryptology Conference. Cham: Springer Nature Switzerland, 2024: 387-421.

Developments of Eval Mode: Use in NN Inference

■ Practical Neural Network Inference

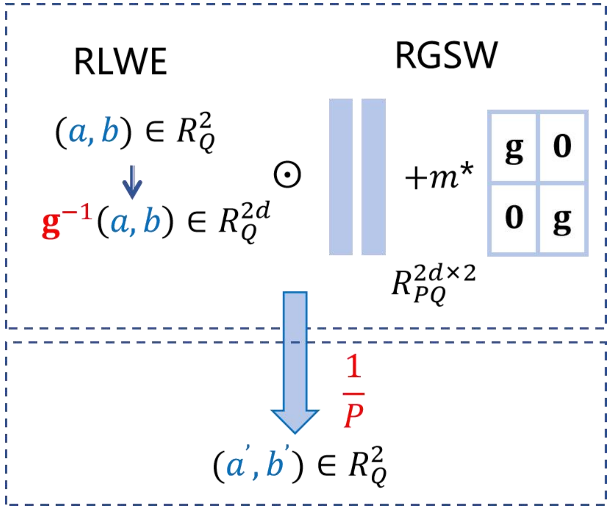


Task	Network structure	Time
hand-writing number recognition (MNIST)	Open NN: none, Private NN: 2 FC layers	0.14s
Facial recognition	Open NN: FaceNet, Private NN: 2 FC layers	0.2s
Speaker verification	Open NN: MFA-conformer, Private NN: 1 FC layer	0.6s

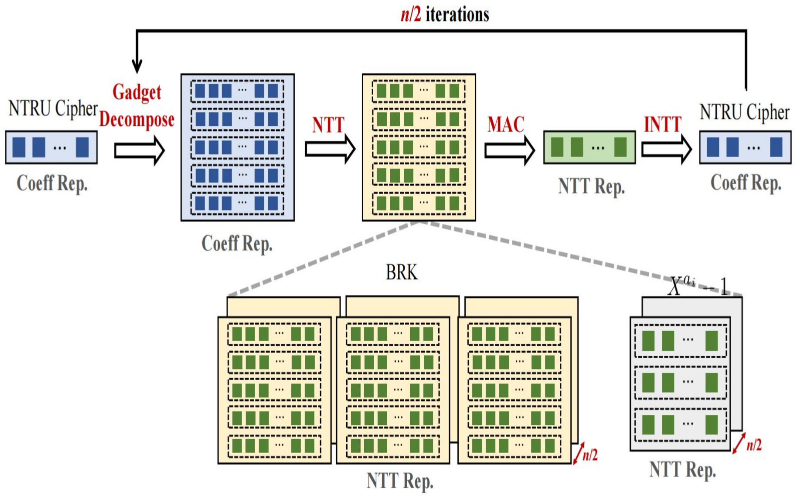
1. Kwok-Yan Lam, Xianhui Lu, Linru Zhang, Xiangning Wang, Huaxiong Wang, Si Qi Goh. Efficient FHE-based privacy-enhanced neural network for trustworthy AI-as-a-service. IEEE Transactions on Dependable and Secure Computing, 21(5), 4451-4468. (2024)
2. Library can be download from https://www.hintsight.com/

Developments of Bootstrapping

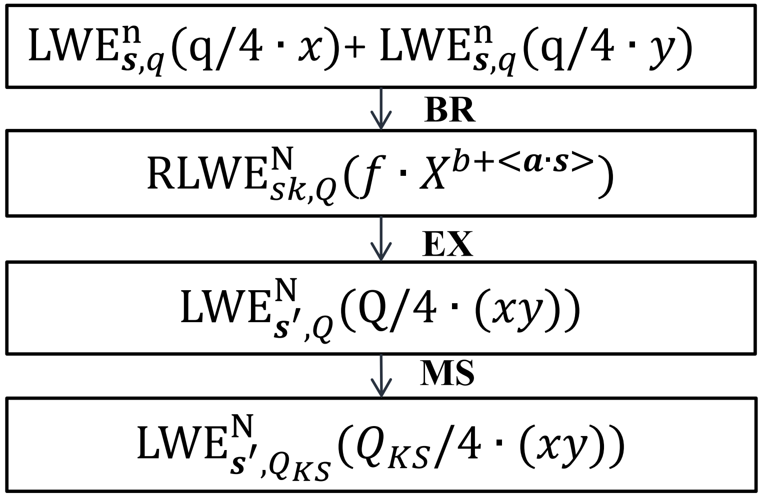
■ Gate Bootstrapping Speedup 500 times



Co-Design of
Parameter and AVX Instruction



NTRU structure to reduce
Poly-Multiplication

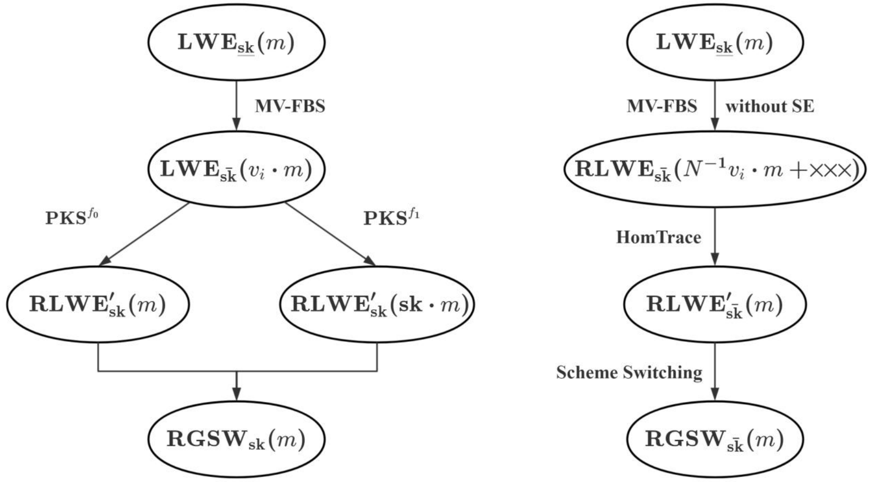


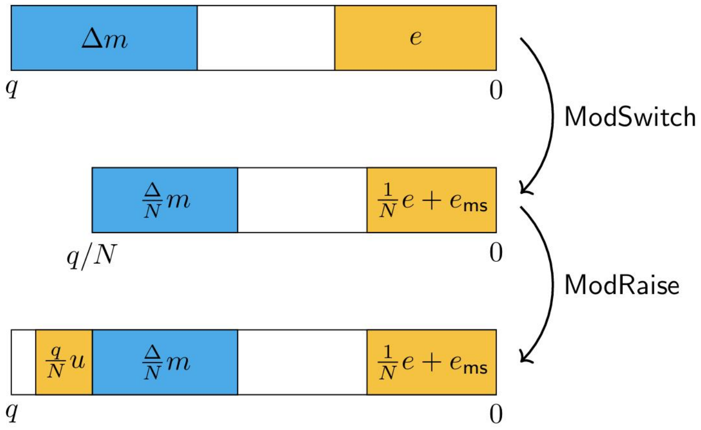
Better noise managment to
reduce parameter size

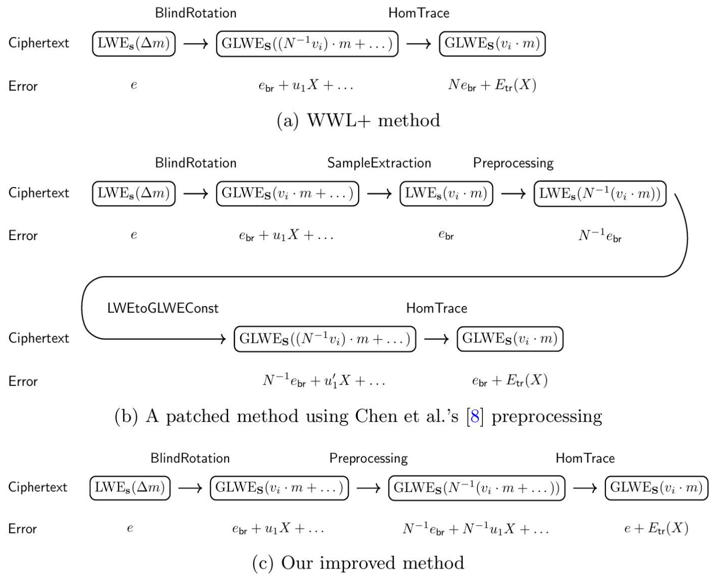
1. Léo Ducas, Daniele Micciancio: FHEW: Bootstrapping Homomorphic Encryption in Less Than a Second. EUROCRYPT (1) 2015: 617-640
2. Ilaria Chillotti, Nicolas Gama, Mariya Georgieva, Malika Izabachène:Faster Fully Homomorphic Encryption: Bootstrapping in Less Than 0.1 Seconds. ASIACRYPT (1) 2016: 3-33
3. Zhihao Li, Xianhui Lu, Zhiwei Wang, Ruida Wang, Ying Liu, Yinhang Zheng, Lutan Zhao, Kunpeng Wang and Rui Hou. Faster NTRU-based Bootstrapping in less than 4 ms. IACR Trans. Cryptogr. Hardw. Embed. Syst. TCHES2024 (3) : 418-451.
4. Chunling Chen, Xianhui Lu, Binwu Xiang, Bowen Huang, Ruida Wang, Yijian Liu: Refined Error Management for Gate Bootstrapping. (less than 2ms) ACISP (2) 2025: 252-274

Developments of Bootstrapping

■ Circuit Bootstrapping Speedup 10 times







Reduced workflow
Computaion: $O(N^2) \rightarrow O(N\log^2 N)$, 200 ×
Memory: $O(N^2)$ $O(N\log N)$,500×

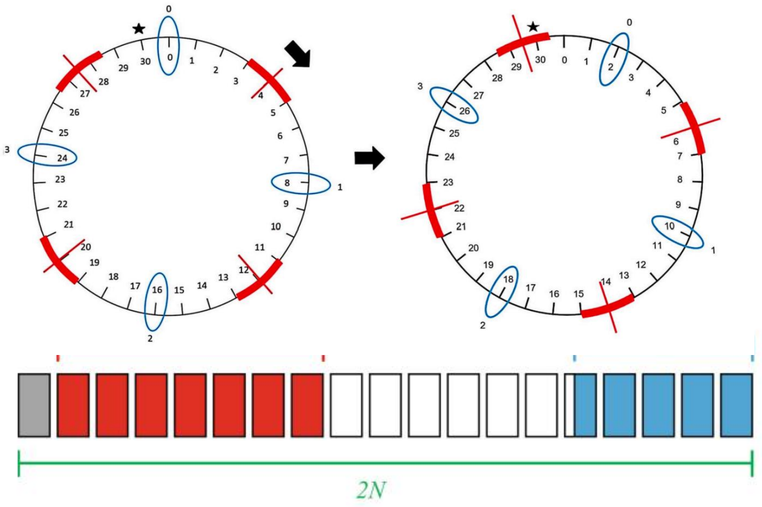
Split FFT （13ms）
Computaion: 3.5×
Memory: 37.5×

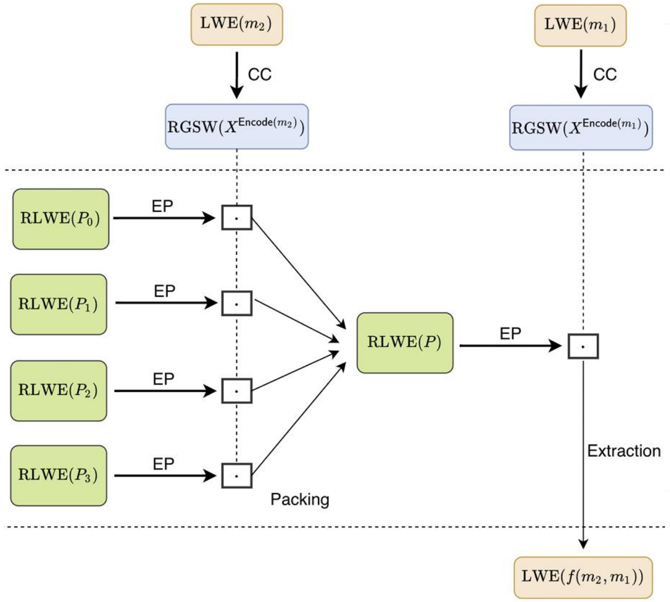
Noise managment by precomputation
Noise: N× smaller
Computation: 2.6×

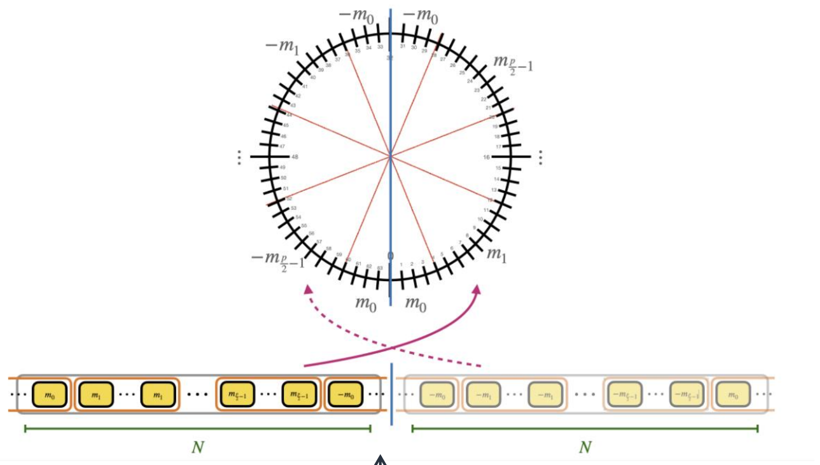
1. Ilaria Chillotti, Nicolas Gama, Mariya Georgieva, Malika Izabachène: Faster Packed Homomorphic Operations and Efficient Circuit Bootstrapping for TFHE. ASIACRYPT (1) 2017: 377-408 (137ms)
2. Ruida Wang, Yundi Wen, Zhihao Li, Xianhui Lu, Kun Liu, Kunpeng Wang, Circuit Bootstrapping: Faster and Smaller. Annual International Conference on the Theory and Applications of Cryptographic Techniques. Eurocrypt 2024: 342-372.
3. Ruida Wang, Jincheol Ha, Xuan Shen, Xianhui Lu, Chunling Chen, Kunpeng Wang, and Jooyoung Lee. FHEW-like Leveled Homomorphic Evaluation: Refined Workflow and Polished Building Blocks. Eprint 2024/1318. CCS2025.(13ms)

Developments of Bootstrapping

■ Functional Bootstrapping Speedup 1000 times







Encrypted test polynomial

Full-Domain FBS:
Overcome **negcyclic** limitation

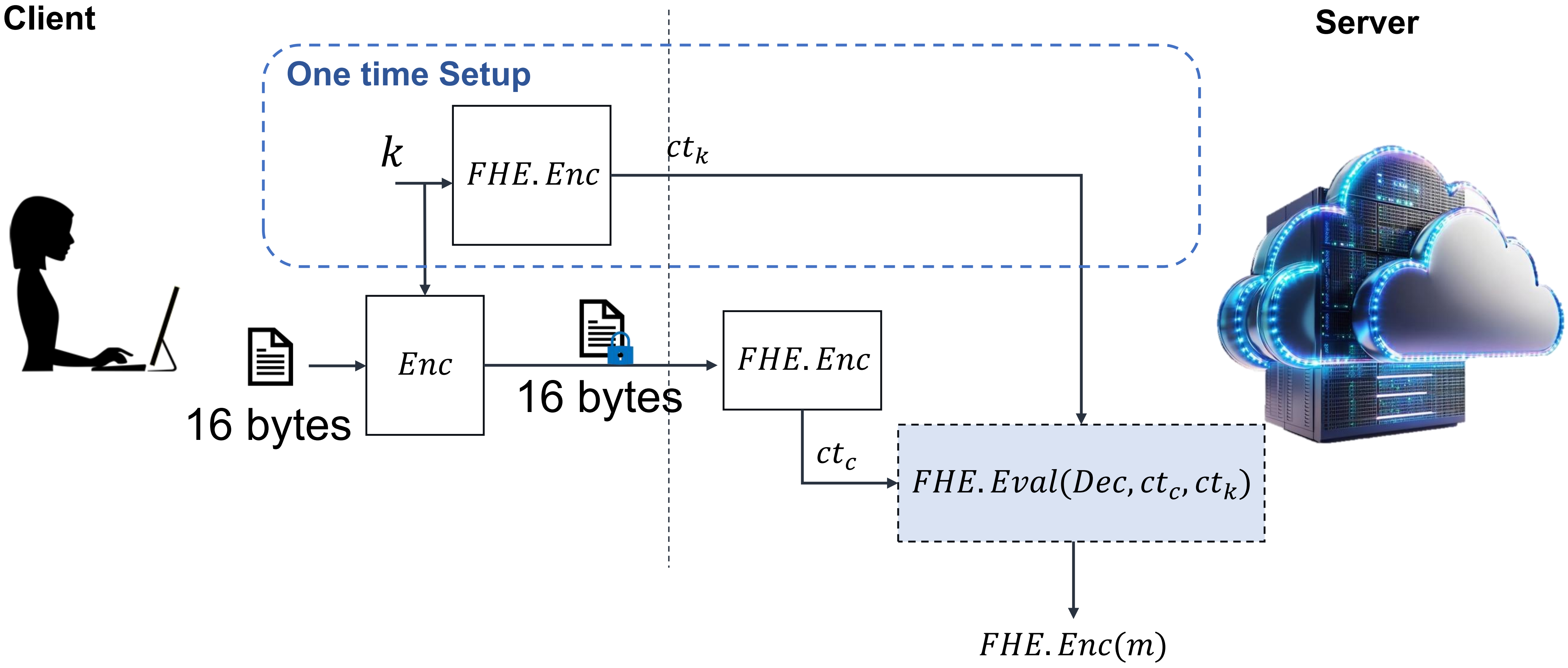
High-Precision FBS:
100-1000x faster

Private-preserving FBS:
for **private function**

[1] Ruida Wang, Xianhui Lu, Yundi Wen, Zhihao Li, Benqiang Wei, Kunpeng Wang, Lixia Luo. Full Domain Functional Bootstrapping using The Prime Cyclotomic Ring. Theoretical Computer Science 2025.
[2] Zhihao Li, Benqiang Wei, Ruida Wang, Xianhui Lu and Kunpeng Wang. Full Domain Functional Bootstrapping with Least Significant Bit Encoding. Inscrypt 2023.
[3] Zhihao Li, Xuan Shen, Xianhui Lu, Ruida Wang, Yuan Zhao, Zhiwei Wang, and Benqiang Wei. Leveled Functional Bootstrapping via External Product Tree. Eprint 2025

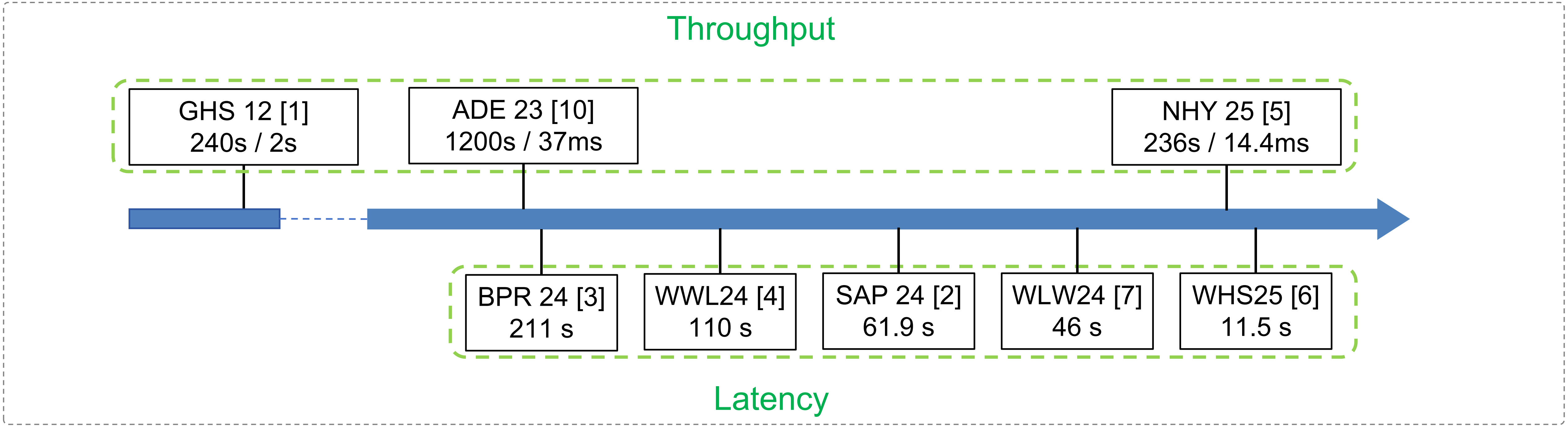
Developments of transciphering

- Minimize bandwidth by transciphering



Developments of transciphering

- AES Transciphering: throughput 16666 times, latency 20 times



[1]Craig Gentry, Shai Halevi, and Nigel P. Smart. Homomorphic evaluation of the AES circuit. CRYPTO12
[2]Leonard Schild, Aysajan Abidin, and Bart Preneel. Fast transciphering via batched and reconfigurable LUT evaluation. TCHES24.
[3]Nicolas Bon, David Pointcheval, and Matthieu Rivain. Optimized homomorphic evaluation of boolean functions. TCHES24.
[4]Ruida Wang, Yundi Wen, Zhihao Li, Xianhui Lu, Benqiang Wei, Kun Liu, and Kunpeng Wang. Circuit Bootstrapping: Faster and Smaller. EUROCRYPT24.
[5]Chao Niu, Zhicong Huang, Zhaomin Yang, Yi Chen, Liang Kong, Cheng Hong and Tao Wei. XBOOT: Free-XOR Gates for CKKS with Applications to Transcipherin. TCHES25.
[6]Ruida Wang, Jincheol Ha, Xuan Shen, Xianhui Lu, Chunling Chen, Kunpeng Wang and Jooyoung Lee. Refined TFHE Leveled Homomorphic Evaluation and Its Application. CCS25.
[7]Benqiang Wei, Xianhui Lu, Ruida Wang, Kun Liu, Zhihao Li, and Kunpeng Wang. Thunderbird: Efficient homomorphic evaluation of symmetric ciphers in 3gpp by combining two modes of TFHE. TCHES24.
[8]Anne Canteaut, Sergiu Carpov, Caroline Fontaine, Tancr`ede Lepoint, Mar´ ıa Naya-Plasencia, Pascal Paillier, and Renaud Sirdey. Stream ciphers: A practical solution for efficient homomorphic-ciphertext compression. FSE16
[9]Thibault Balenbois, Jean-Baptiste Orfila, and Nigel P. Smart. Trivial Transciphering With Trivium and TFHE. WAHC23
[10]Ehud Aharoni, Nir Drucker, Gilad Ezov, Eyal Kushnir, Hayim Shaul, and Omri Soceanu. E2e near-standard and practical authenticated transciphering. Eprint23.
[11]Jihoon Cho, Jincheol Ha, Seongkwang Kim, ByeongHak Lee, Joohee Lee, Jooyoung Lee, Dukjae Moon, and Hyojin Yoon. Transciphering framework for approximate homomorphic encryption. ASIACRYPT21
[12] Jincheol Ha, Seongkwang Kim, ByeongHak Lee, Jooyoung Lee, and Mincheol Son. Rubato: Noisy ciphers for approximate homomorphic encryption. EUROCRYPT22
[13]Chao Niu, Benqiang Wei, Zhicong Huang, Zhaomin Yang, Cheng Hong, Meiqin Wang, Tao Wei. SoK: FHE-Friendly Symmetric Ciphers and Transciphering. TCHES25
[14]Jules Baudrin, Sonia Belaïd, Nicolas Bon, Christina Boura, Anne Canteaut, Gaëtan Leurent, Pascal Paillier, Léo Perrin, Matthieu Rivain, Yann Rotella, and Samuel Tap. Transistor: a TFHE-friendly Stream Cipher. CRYPTO25

Developments of Homomorphic Processor

■ Making FHE User-Friendly

Fully Homomorpphic Encryption is complex and hard to use..

FHE Processor instruction hide complex detail of FHE from engineers

Name	Input Lang.	Schemes: BFV	Schemes: CKKS	Schemes: GSW	Ptxt. Space	Features & Optimizations: SIMD	Features & Optimizations: Params.	Features & Optimizations: Ctxt. Mnt.	Features & Optimizations: × Depth	Accessbility: Code	Accessbility: Ex.	Accessbility: Doc.	Last Major Update
ALCHEMY ([49])	Haskell	●	○	○	Arithm.	◐	◐	◐	○	●	◐	○	02/2020
Cingulata ([51])	C++	●	○	◐	Binary	○	●	◐	●	●	●	○	11/2019
E^3 ([65])	C++	●	○	●	Both	◐	○	◐	○	●	●	●	09/2020
EVA ([17])	Python	○	●	○	Arithm.	●	●	●	○	●	●	○	11/2020
Marble ([50])	C++	●	○	○	Both	◐	◐	◐	○	●	●	○	10/2018
RAMPARTS ([66])	Julia	●	○	○	Arithm.	○	●	◐	●	○	–	–	–
CHET ([67])	C++	○	●	○	Arithm.	◐	●	◐	○	○	–	–	–
nGraph-HE ([24])	Python	●	●	○	Arithm.	●	○	◐	●	●	●	●	08/2019
SEALion ([68])	Python	●	○	○	Arithm.	◐	●	◐	○	○	●	○	01/2019

Table II: Overview of existing general-purpose FHE compilers (top) and those specializing on machine learning (bottom). Note that similar schemes are summarized into families, e.g., BFV/BGV as BFV and CGGI/TFHE/FHEW as GSW.

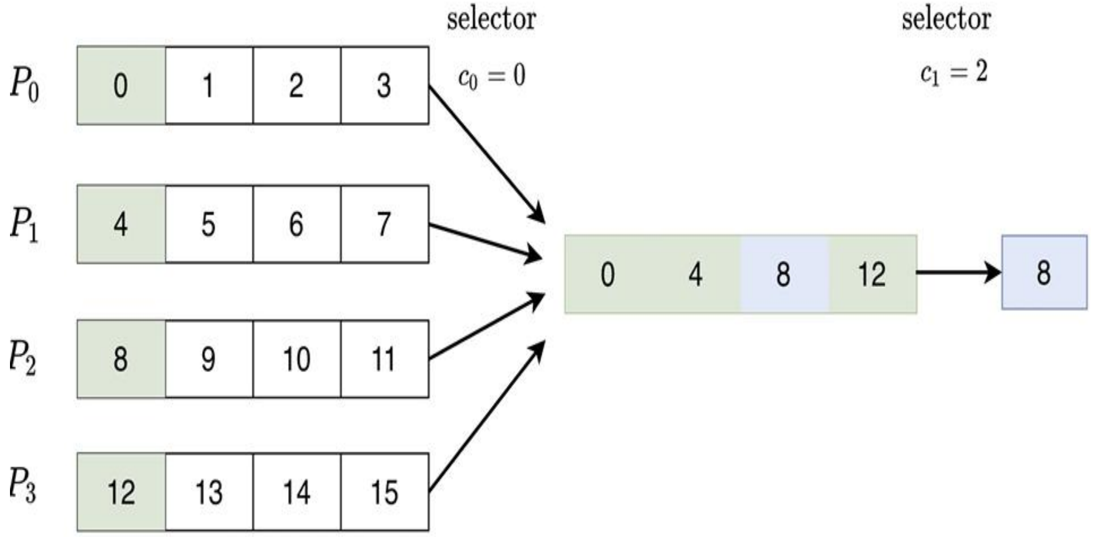
FHE Instruction Set

ANDi/ORi/XORi	AND/OR/XOR
DC	RC
(U)SHLi/(U)SHRi	(U)SHL/(U)SHR
ROLi/RORi	ROL/ROR
EQi	EQ
LT(E)i/GT(E)i	LT(E)/GT(E)
(N)CDUP	CSEL
NEG/ABS	MIN/MAX
ADDi/SUBi	ADD/SUB
ADDZ	MUL(M)i/DIV(4)i/MOD4i
MODi	MUL
MULM	DIV4
DIV	MOD4
MOD	(N)CDUPi
XOP	MINi/MAXi

1. Alexander Viand, Patrick Jattke, Anwar Hithnawi: SoK: Fully Homomorphic Encryption Compilers. SP 2021: 1092-1108

Developments of Homomorphic Processor

■ FHE Instructions based functional bootstrapping



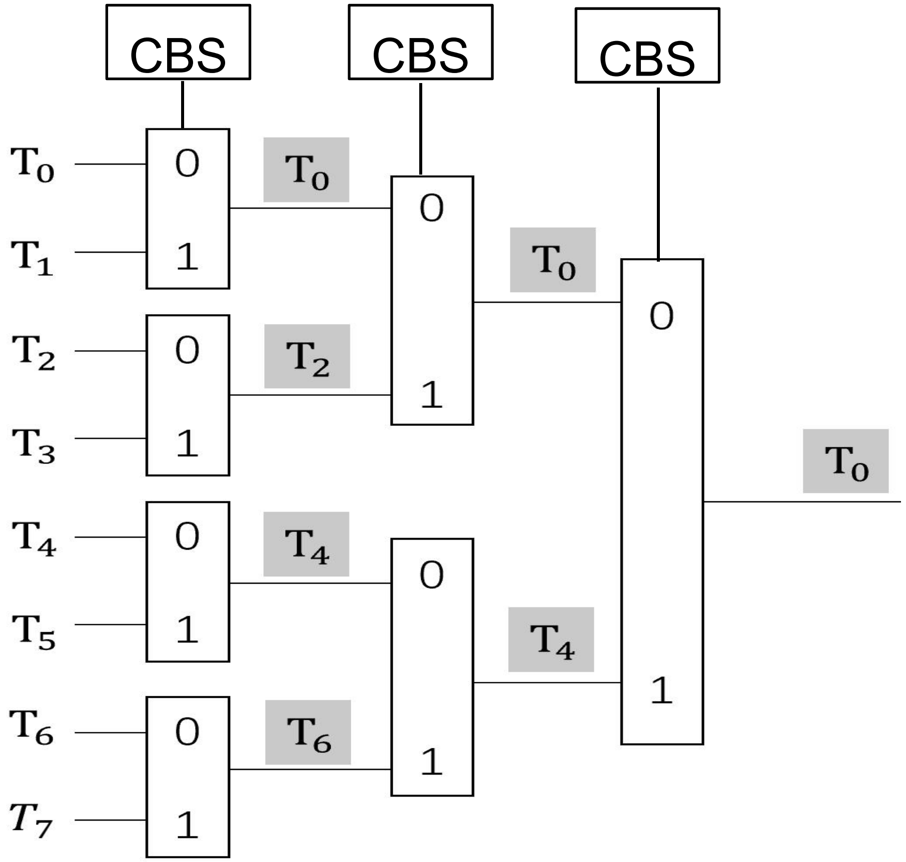
Look-up-table via
functional bootstrapping tree

Instruction	Time(ms)	Instruction	Time(ms)
ANDi/ORi/XORi	48.75	AND/OR/XOR	184.52
DC	48.75	RC	195.00
(U)SHLi/(U)SHRi	48.75	(U)SHL/(U)SHR	320.30
ROLi/RORi	97.50	ROL/ROR	480.45
EQi	48.75	EQ	276.79
LT(E)i/GT(E)i	92.26	LT(E)/GT(E)	436.94
NEG/ABS	92.26	MIN/MAX	825.12
ADDi/SUBi	92.26	ADD/SUB	344.68
ADDZ	184.52	MUL(M)i/DIV(4)i/MOD4i	92.26
MODi	160.15	MUL	504.82
MULM	1650.24	DIV4	1121.04
DIV	4801.05	MOD4	504.82
MOD	4393.73	MINi/MAXi	92.26

1. Daphné Trama, Pierre-Emmanuel Clet, Aymen Boudguiga, and Renaud Sirdey. Designing a General-Purpose 8-bit (T)FHE Processor Abstraction. TCHES 2025

Developments of Homomorphic Processor

- Up to 30x faster via circuit bootstrapping



Look-up-table via
circuit bootstrapping and Cmux tree

Instruction	Time(ms)	Instruction	Time(ms)
ANDi/ORi/XORi	36.17	AND/OR/XOR	227.05
DC	36.17	RC	144.67
(U)SHLi/(U)SHRi	36.17	(U)SHL/(U)SHR	227.05
ROLi/RORi	36.17	ROL/ROR	227.05
EQi	36.17	EQ	227.05
LT(E)i/GT(E)i	112.74	LT(E)/GT(E)	227.05
NEG/ABS	112.74	MIN/MAX	227.05
ADDi/SUBi	112.74	ADD/SUB	227.05
ADDZ	227.05	MUL(M)i/DIV(4)i/MOD4i	112.74
MODi	112.74	MUL	227.05
MULM	227.05	DIV4	227.05
DIV	227.05	MOD4	227.05
MOD	227.05	MINi/MAXi	112.74

1. Ruida Wang, Jincheol Ha, Xuan Shen, Xianhui Lu, Chunling Chen, Kunpeng Wang, and Jooyoung Lee. FHEW-like Leveled Homomorphic Evaluation: Refined Workflow and Polished Building Blocks. Eprint 2024/1318. CCS2025.

Standarization

- First ISO/IEC FHE standards 1-2 years later

ICS › 35 › 35.030

ISO/IEC 18033-6:2019 [ISO/IEC 18033-6:2019]

IT Security techniques — Encryption algorithms — Part 6: Homomorphic encryption

ABSTRACT PREVIEW

This document specifies the following mechanisms for homomorphic encryption.

— Exponential ElGamal encryption;

— Paillier encryption.

For each mechanism, this document specifies the process for:

BUY THIS STANDARD

FORMAT	LANGUAGE
✔ PDF + EPUB	English
PAPER	English

CHF 88 BUY

- **ISO/IEC-28033 Information security — Fully homomorphic encryption**

- Part 1: General (CD)
- Part 2: Mechanisms for exact arithmetic on modular integers (BGV/BFV, AWI)
- Part 3: Mechanisms for arithmetic on approximate numbers (CKKS, CD)
- Part 4: Mechanisms for arithmetic based on look-up table evaluation (DM/CGGI, DIS)
- Part 5: Mechanisms for Scheme Switching (AWI)

Is FHE Ready?

- Usability
  - Throughput Mode
  - Latency Mode
  - Hybrid Mode
- Performance
  - Gate bootstrapping less than 2 ms
  - Circuit bootstrapping less than 13 ms
  - AES transciphering latency 11 s or amortized 14 ms
  - FHE instructions 36-227 ms
- Standardization
  - ISO/IEC 28033 standards in one or two years

INSTITUE OF INFORMATION ENGINEERING, CAS

UNIVERSITY OF CHINESE ACADEMY OF SCIENCES

Thank you