NTRU-based Bootstrapping for MK-FHEs

without using Overstretched Parameters

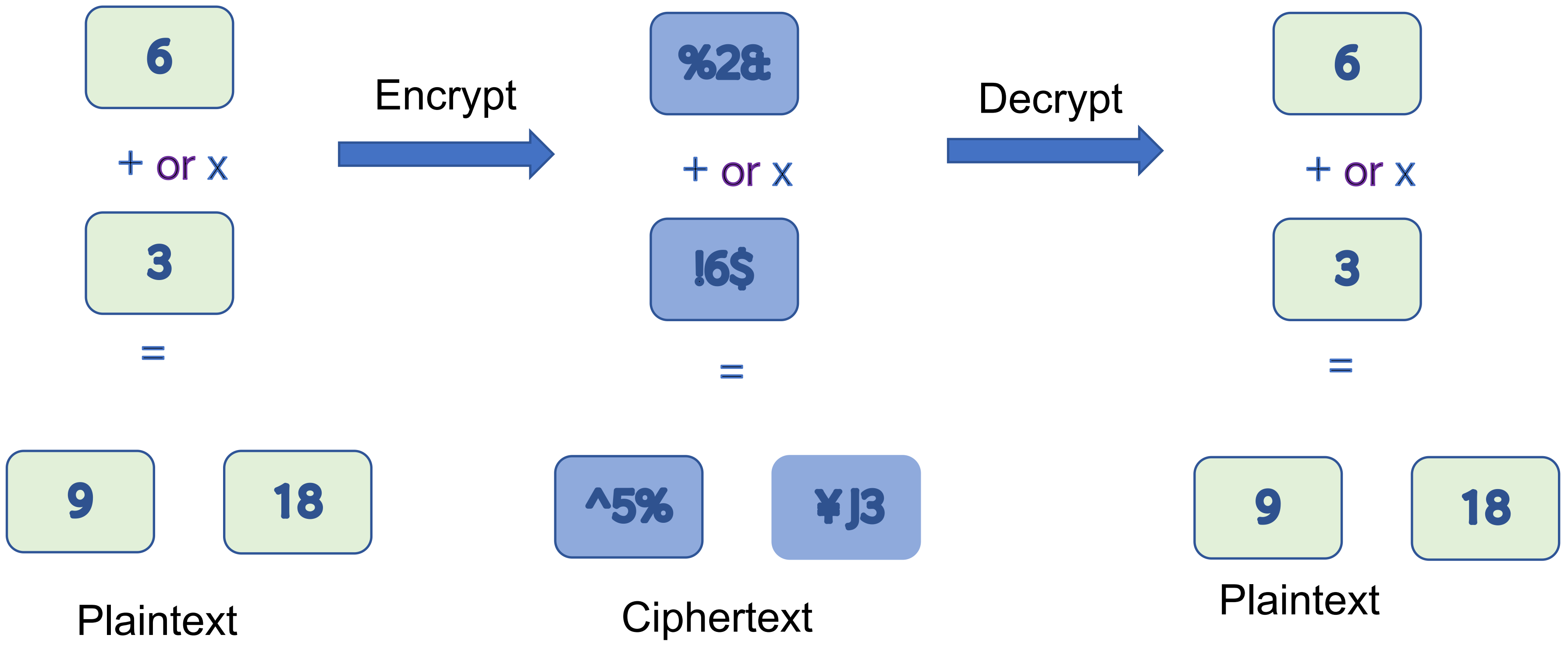
Binwu Xiang, Jiang Zhang, Kaixing Wang, Yi Deng, Dengguo Feng

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

SKLC
State Key Laboratory of Cryptology

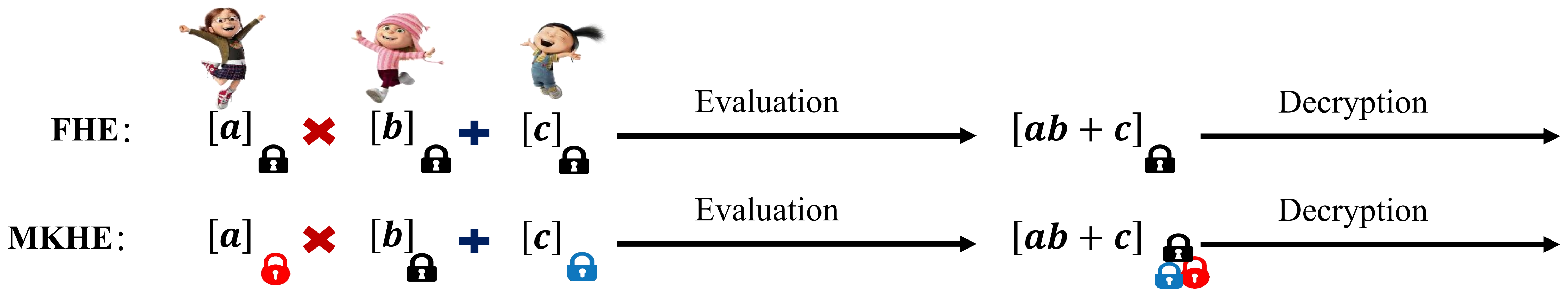
中国科学院大学
University of Chinese Academy of Sciences

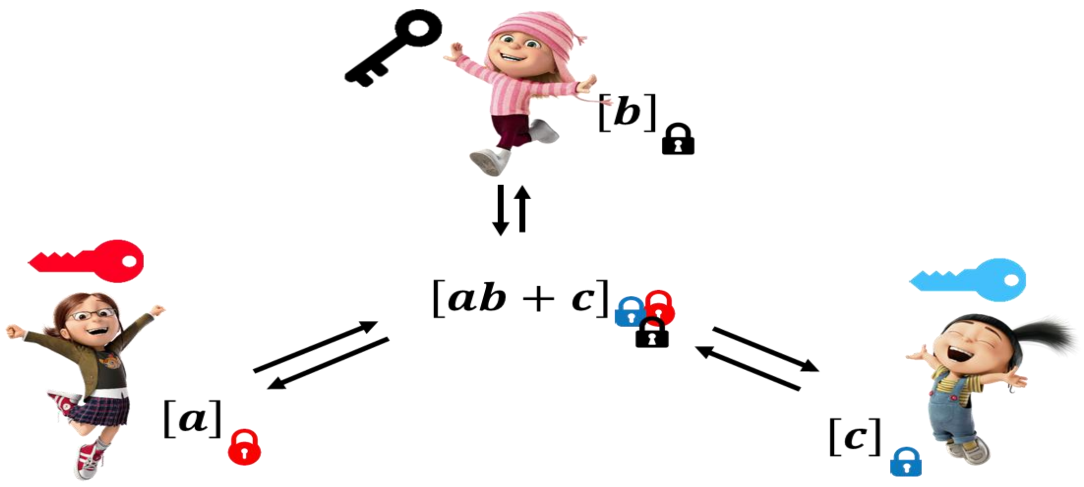
Fully Homomorphic Encryption (FHE)



- '**holy grail of cryptography**', allows arbitrary operations on ciphertext without decryption.
- **Applications**: PPML (Privacy-Preserving Machine Learning);PIR (Private Information Retrieval); PSI (Private Set Intersection); MPC (Multi-Party Computation)

Multi-Key Fully Homomorphic Encryption





- **Non-interactive** key generation and encryption.
- **Distributed** decryption.
- Time/space complexity is typically related to k.

Previous Works

- Theoretical studies
  - LTV12, CM15, MW16, PS16, BP16, CZW17
  - No implementations
- Practical schemes
  - TFHE/FHEW-like: CCS19, KMS24, FHE with bootstrapping
  - CKKS/BFV-like: CDKS19, KKLSS22, Level MK-FHE

Why (Mostly) (R)LWE-based Scheme, very few relying on NTRU?

Previous Works

RLWE problem

- Secret: $s \in R$
- $a \leftarrow U(R_q)$
- $e \leftarrow \chi$
- $b = a \cdot s + e \bmod q$

$(a, b) \approx_c U(R_q^2)$

NTRU problem

- Secret: $\mathrm{f} \in R$, with small coefficients, f^{-1} exist
- $\mathrm{g} \leftarrow \chi$
- $\mathrm{c} = \mathrm{g} \cdot \mathrm{f}^{-1} \bmod q$

$\mathrm{c} \approx_c U(R_\mathrm{q})$

Constructing schemes based on the NTRU assumption seem to naturally offer advantages.

Previous Works

➢ Early Work

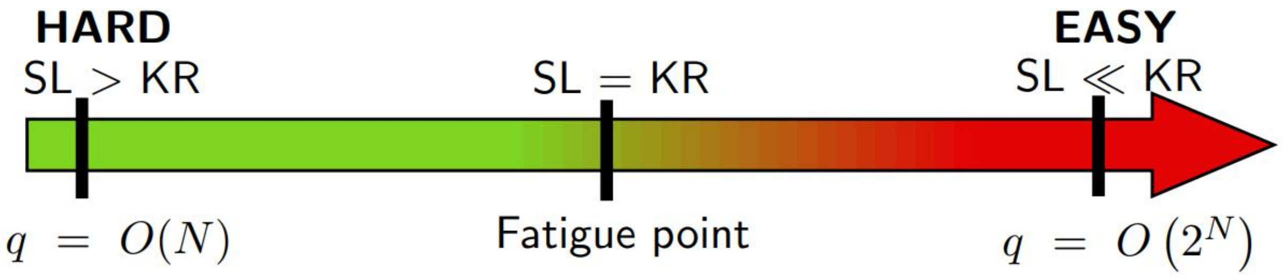
[LTV12] more efficient than the corresponding RLWE-based schemes BGV.

$$R_q := \mathbb{Z}_q[X]/\langle X^N + 1\rangle \text{ with } q \in \Omega(2^N).$$

➢ NTRU Attacks[DW21]

Key recovery attacks (KR): exponential time in N.

Sublattice attacks (SL): hardness varies depending on q, fatigue point ($q = O(n^{2.484})$).



[LTV12] L´opez-Alt, A., Tromer, E., Vaikuntanathan, V.: On-the-fly multiparty computation on the cloud via multikey fully homomorphic encryption. In STOC
[DW21] L. Ducas and W. van Woerden. NTRU fatigue: How stretched is overstretched? In ASIACRYPT 2021

Our result

- Motivation: Design an NTRU-based MK-FHE scheme that supports a super-constant number of participants (keys)
- Challenge: Existing schemes suffer exponential noise growth, requiring parameters beyond the fatigue point.
- Our Result:
  - ✓ New NTRU-base MK-FHE: **sub-linear** keys without overstretched NTRU parameters.
    - First Layer: matrix NTRU-based encryption supporting multi-key NAND, $q = O(k \cdot n^{1.5})$, linear in k.
    - Second Layer: NTRU-based encryption enabling efficient hybrid product for gate bootstrapping.
  - ✓ Fast bootstrapping for MK-LWE ciphertext with small key size
  - ✓ New LWEs to LWEs key switching :
    - reduce Key Size from $\boldsymbol{O}(\boldsymbol{n}^2)$ to $\boldsymbol{O}(\boldsymbol{n})$ bits
    - almost without extra computational overhead

First-layer Matrix NTRU-based Multi-Key Encryption

- Setup: Each i-th party samples
  - ✓ $\boldsymbol{sk}$: an invertible matrix $\boldsymbol{F_i} \in Z_{\mathrm{q}}^{\mathrm{n \times n}}$
  - ✓ $\boldsymbol{evk_i}$: $\left(\boldsymbol{e_i} + \left(\frac{5q}{8}, \boldsymbol{0}\right)\right) \boldsymbol{F_i^{-1}} \in Z_q^n$
- Single-key ciphertext : $\boldsymbol{c_i} = \left(\boldsymbol{e'_i} + \left(\frac{q}{4}\mathrm{m}, \boldsymbol{0}\right)\right) \boldsymbol{F_i^{-1}} \in Z_q^n$
  - ✓ The security relies on the MNTRU problem $\boldsymbol{C} = \boldsymbol{G} \cdot \boldsymbol{F}^{-\boldsymbol{1}} \bmod \mathrm{q} \approx_{\mathrm{c}} U\left(Z_{\mathrm{q}}^{\mathrm{n \times n}}\right)$
  - ✓ We just use the first row of $\boldsymbol{C}$ to define the ciphertext $\boldsymbol{c_i}$
  - ✓ Decryption: $\boldsymbol{c}_{\mathrm{i}} \cdot \boldsymbol{col_0}(\boldsymbol{F}_{\mathrm{i}})$

First-layer Matrix NTRU-based Multi-Key Encryption

- **MK-Ciphertext** : The concatenation of each party.
  - ✓ MK secret: $(\boldsymbol{F_1}, \boldsymbol{F_2}, \cdots, \boldsymbol{F_k}) \in Z_q^{kn\times n}$.
  - ✓ Ciphertext: $(\boldsymbol{c_1}, \boldsymbol{c_2}, \dots, \boldsymbol{c_k}) \in Z_q^{kn}$ with $\boldsymbol{c_1} \cdot \boldsymbol{col_0}(\boldsymbol{F_1}) + \dots + \boldsymbol{c_k} \cdot \boldsymbol{col_0}(\boldsymbol{F_k}) \approx \frac{\mathrm{q}}{\boldsymbol{4}}\mathrm{m}$
- **MK-NAND** : Extended multi-key ciphertext via **Linear Combination.**
  - ✓ eg. k=2, $\boldsymbol{c}' = (\boldsymbol{c}_1', \boldsymbol{c}_2') = (\boldsymbol{evk_1}, \boldsymbol{0}) - (\boldsymbol{c_1}, \boldsymbol{0}) - (\boldsymbol{0}, \boldsymbol{c_2})$ (NAND)
  - ✓ output ciphertext contains a large noise $e' < q/8$
  - ✓ Decryption: $\boldsymbol{c_1} \cdot \boldsymbol{col_0}(\boldsymbol{F_1}) + \boldsymbol{c_2} \cdot \boldsymbol{col_0}(\boldsymbol{F_2}) = \frac{\mathrm{q}}{\boldsymbol{2}}\boldsymbol{NAND}(\boldsymbol{m_1}, \boldsymbol{m_2})$

Bootstrapping matrix NTRU-based Multi-Key Ciphertexts

- First, we start with $(\boldsymbol{c_1}, \boldsymbol{c_2}, \ldots, \boldsymbol{c_k}) \in Z_q^{kn}$ and construct a NTRU-based Hybrid Product :
  - ✓ Input:
    - MK-NTRU ciphertext $ct = (c_1, \ldots, c_k) \in R^{\mathrm{k}}$ such that $c_1 s_1 + \ldots + c_k s_k \approx \mu$ mod q
    - A uni-encryption $(\boldsymbol{d}_{\mathrm{i}} = \mathbf{a}\mathrm{r_i} + \boldsymbol{g}\mu_i + \boldsymbol{e_1},\ \boldsymbol{f}_{\mathrm{i}} = (\boldsymbol{e_2} + \boldsymbol{g}\mathrm{r})/s_i)$;
    - The public key $\{\boldsymbol{pk_i} =- \boldsymbol{a}\mathrm{s_i} + \boldsymbol{e}\}$ **for** $i \in [1, k]$
  - ✓ Output a new MK-NTRU encryption $ct' = (c_1{}', \ldots, c_k{}')$ of $\mu\mu_{\mathrm{i}}$
  - ✓ The security relies on the Hint-NTRU problem in [EEN+24].

[EEN+24] Plover: Masking-friendly hash-and-sign lattice signatures. In: EUROCRYPT 2024.

Bootstrapping matrix NTRU-based Multi-Key Ciphertexts

- First, we start with $(\boldsymbol{c_1}, \boldsymbol{c_2}, \ldots, \boldsymbol{c_k}) \in Z_q^{kn}$ and construct a NTRU-based Hybrid Product :
  - ✓ Input:
    - MK-NTRU ciphertext $ct = (c_1, \ldots, c_k) \in R^{\mathrm{k}}$ such that $c_1 s_1 + \ldots + c_k s_k \approx \mu$ mod q
    - A uni-encryption $(\boldsymbol{d}_{\mathrm{i}} = \mathbf{a}\mathrm{r}_{\mathrm{i}} + \boldsymbol{g}\mu_i + \boldsymbol{e_1},\ \boldsymbol{f}_{\mathrm{i}} = (\boldsymbol{e_2} + \boldsymbol{g}\mathrm{r})/s_i)$;
    - The public key $\{\boldsymbol{pk_i} = -\boldsymbol{a}\mathrm{s}_{\mathrm{i}} + \boldsymbol{e}\}$ **for** $i \in [1, k]$
  - ✓ Output a new MK-NTRU encryption $ct' = (c_1{}', \ldots, c_k{}')$ of $\mu\mu_{\mathrm{i}}$
  - ✓ The security relies on the Hint-NTRU problem in [EEN+24].
    - $\{(\mathbf{h} = \mathbf{e}_1/s, \mathbf{a}, \mathbf{b} = \mathbf{a} \cdot s + \mathbf{e}_2) | s \leftarrow \chi'_s, \mathbf{e}_1, \mathbf{e}_2 \leftarrow \chi_e'^d, \mathbf{a} \leftarrow R_Q^d\}$,
    - $\{(\mathbf{u}, \mathbf{v}, \mathbf{w}) | \mathbf{u}, \mathbf{v}, \mathbf{w} \leftarrow R_Q^d\}$.

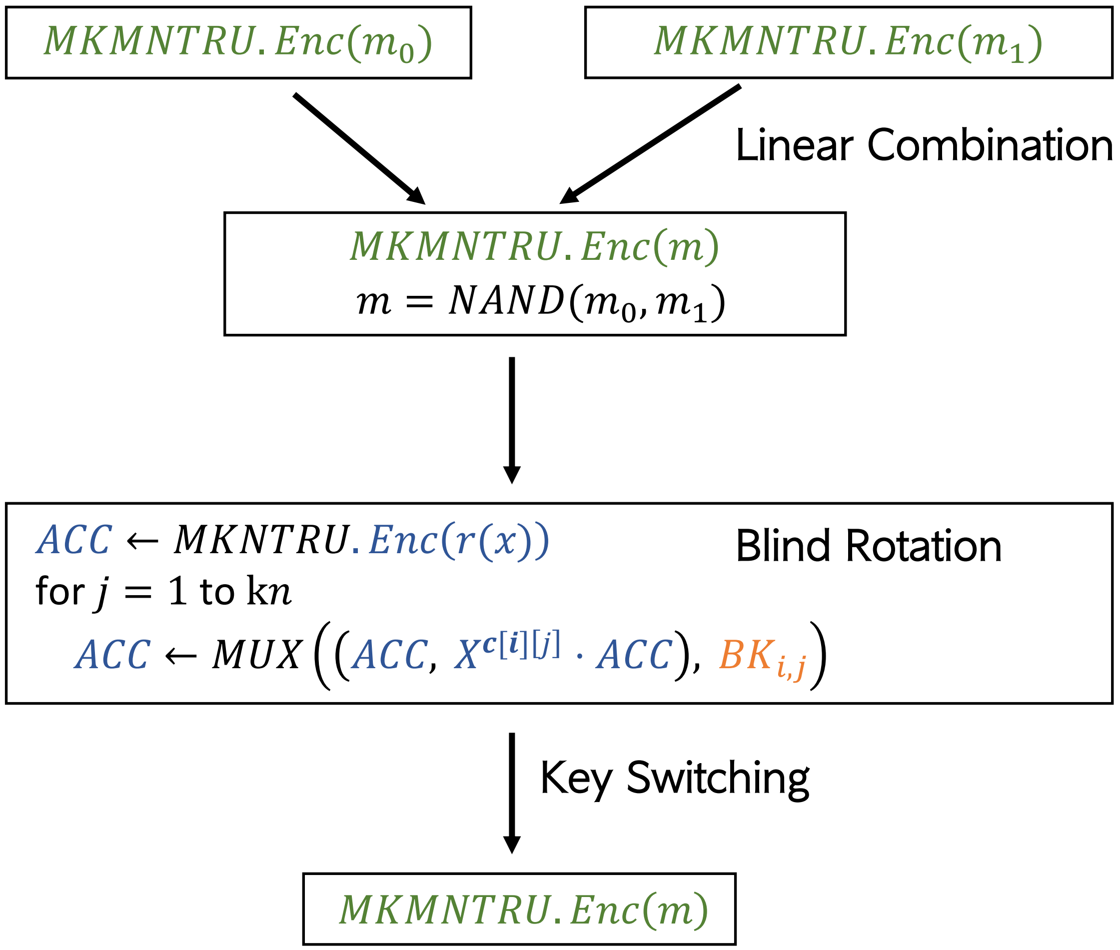
[EEN+24] Plover: Masking-friendly hash-and-sign lattice signatures. In: EUROCRYPT 2024.

Bootstrapping matrix NTRU-based Multi-Key Ciphertexts

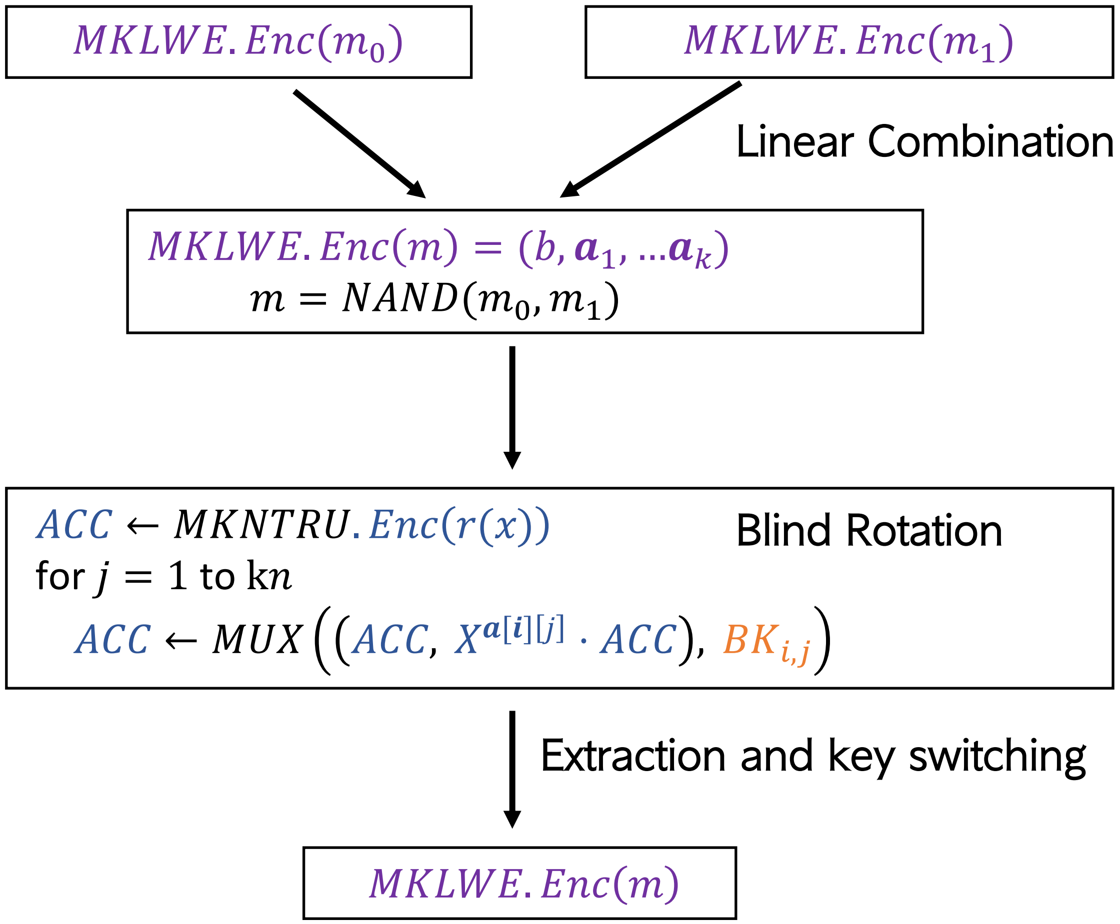
- First, we start with $(\boldsymbol{c_1}, \boldsymbol{c_2}, ..., \boldsymbol{c_k}) \in Z_q^{kn}$ and construct a NTRU-based Hybrid Product :
  - ✓ Input:
    - MK-NTRU ciphertext $ct = (c_1, ..., c_k) \in R^{\mathrm{k}}$ such that $c_1 s_1 + \ldots + c_k s_k \approx \mu \bmod q$
    - A uni-encryption $(\boldsymbol{d}_{\mathrm{i}} = \mathbf{a}\mathrm{r}_{\mathrm{i}} + \boldsymbol{g}\mu_i + \boldsymbol{e_1},\ \boldsymbol{f}_{\mathrm{i}} = (\boldsymbol{e_2} + \boldsymbol{g}\mathrm{r})/s_i)$;
    - The public key $\{\boldsymbol{pk_i} =- \boldsymbol{a}\mathrm{s}_{\mathrm{i}} + \boldsymbol{e}\}$ **for** $i \in [1, k]$
  - ✓ Output a new MK-NTRU encryption $ct' = (c_1{}', ..., c_k{}')$ of $\mu\mu_{\mathrm{i}}$
  - ✓ The security relies on the Hint-NTRU problem in [EEN+24].
- After n iterations, we obtain an MK-NTRU encryption of $r(X)X^{\boldsymbol{c_1} \cdot \boldsymbol{col_0}(\boldsymbol{F_1}) + \ldots + \mathbf{c}_{\mathrm{k}} \cdot \boldsymbol{col_0}(\boldsymbol{F}_{\mathrm{k}})}$
- Then, we propose a key switching to switch the MK-NTRU ciphertext to the MK-MNTRU

[EEN+24] Plover: Masking-friendly hash-and-sign lattice signatures. In: EUROCRYPT 2024.

Bootstrapping matrix NTRU-based Multi-Key Ciphertexts



Bootstrapping LWE-based Multi-Key Ciphertexts



Bootstrapping LWE-based Multi-Key Ciphertexts

- Ciphertext Structure: $(\boldsymbol{b}, \boldsymbol{a}_1, \ldots, \boldsymbol{a}_k) \in \boldsymbol{Z}_q^{kN+1}$
- Goal: Switch the secret key from $(\mathbf{1}, \boldsymbol{s}_1, \ldots, \boldsymbol{s}_k) \in \boldsymbol{Z}_q^{kN+1}$ to $(\mathbf{1}, \boldsymbol{z}_1, \ldots, \boldsymbol{z}_k) \in \boldsymbol{Z}_q^{kn+1}$
- Previous Approach.
  - ✓ Key Generation: A set of LWE ciphertexts of

$$LWE_{z_i}\left(vB_{\mathrm{ks}}^{l} s_{i,j}\right) \quad j \in Z_N,\ l \in z_{d_{ks}},\ v \in Z_{B_{ks}}$$

- Our Approach : Pack N LWE key-switching keys into a single RLWE ciphertext.
  - ✓ Key Generation: Use RLWE ciphertexts to encrypt sequentially
  - ✓ Key Switching : Extract almost free coefficients using the index
  - ✓ Applicable to single-key LWEs to LWEs key switching
  - ✓ Key Size: from $\boldsymbol{O}(\boldsymbol{n}^2)$ to $\boldsymbol{O}(\boldsymbol{n})$ bits

Comparison

Compared to Existing NTRU-based MK-FHE Schemes

Scheme	Noise	Modulus
[LTV12]	$\widetilde{O}(n^k)$	$O(2^{n^\varepsilon})$
[CO17]	$\widetilde{O}(n^k)$	$O(2^{n^\varepsilon})$
Ours	$\widetilde{O}(kn^{1.5})$	$O(kn^{1.5})$

k: Number of parties ; n: Lattice dimension; q: Ciphertext modulus; $\varepsilon \in (0, 1)$

Supporting Sub-linear Number of Participants Below the Fatigue Point

[LTV12] López-Alt A, Tromer E, Vaikuntanathan V. On-the-fly multiparty co-mputation on the cloud via multikey fully homomorphic encryption[C]//Proceedings of the forty-fourth annual ACM symposium on Theory of computing. 2012:1219-1234.

[CO17] Chongchitmate W, Ostrovsky R. Circuit-private multi-key FHE[C]//IACR International Workshop on Public Key Cryptography. Berlin, Heidelberg: Springer Berlin Heidelberg, 2017: 241-270.

Comparison

Compared to other TFHE/FHEW-like schemes

Scheme	Time (s)				Key Size(MB)			
	$k = 2$	$k = 4$	$k = 8$	$k = 16$	$k = 2$	$k = 4$	$k = 8$	$k = 16$
CCS19	0.07	0.33	1.19		89.21	96.38	102.94	
KMS24	0.14	0.44	1.17	2.86	214.61	285.22	250.06	285.31
Ours	0.05	0.21	0.54	2.61	13.89	13.89	13.89	13.89
X	1.4/2.8	1.6/2.1	2.2/2.2	1.1	6.5/15.5	6.9/20.5	7.4/18	20.5

[CCS19] Chen H, Chillotti I, Song Y. Multi-key homomorphic encryption fromTFHE[C]//Advances in Cryptology–ASIACRYPT 2019, Part II 25. Springer International Publishing, 2019: 446-472.
[KMS24] Kwak, H., Min, S., Song, Y. (2024). Towards Practical Multi-key TFHE: Parallelizable, Key-Compatible, Quasi-linear Complexity. In: Public-Key Cryptography – PKC 2024. PKC 2024. Lecture Notes in Computer Science, vol 14604. Springer, Cham.

Conclusion

- NTRU-based multi key FHE
  - without using Overstretched Parameters
  - Fast bootstrapping and small key size
  - Support a sub-linear number k

Thanks!

xiangbinwu@iie.ac.cn

https://github.com/SKLC-FHE/MKFHE