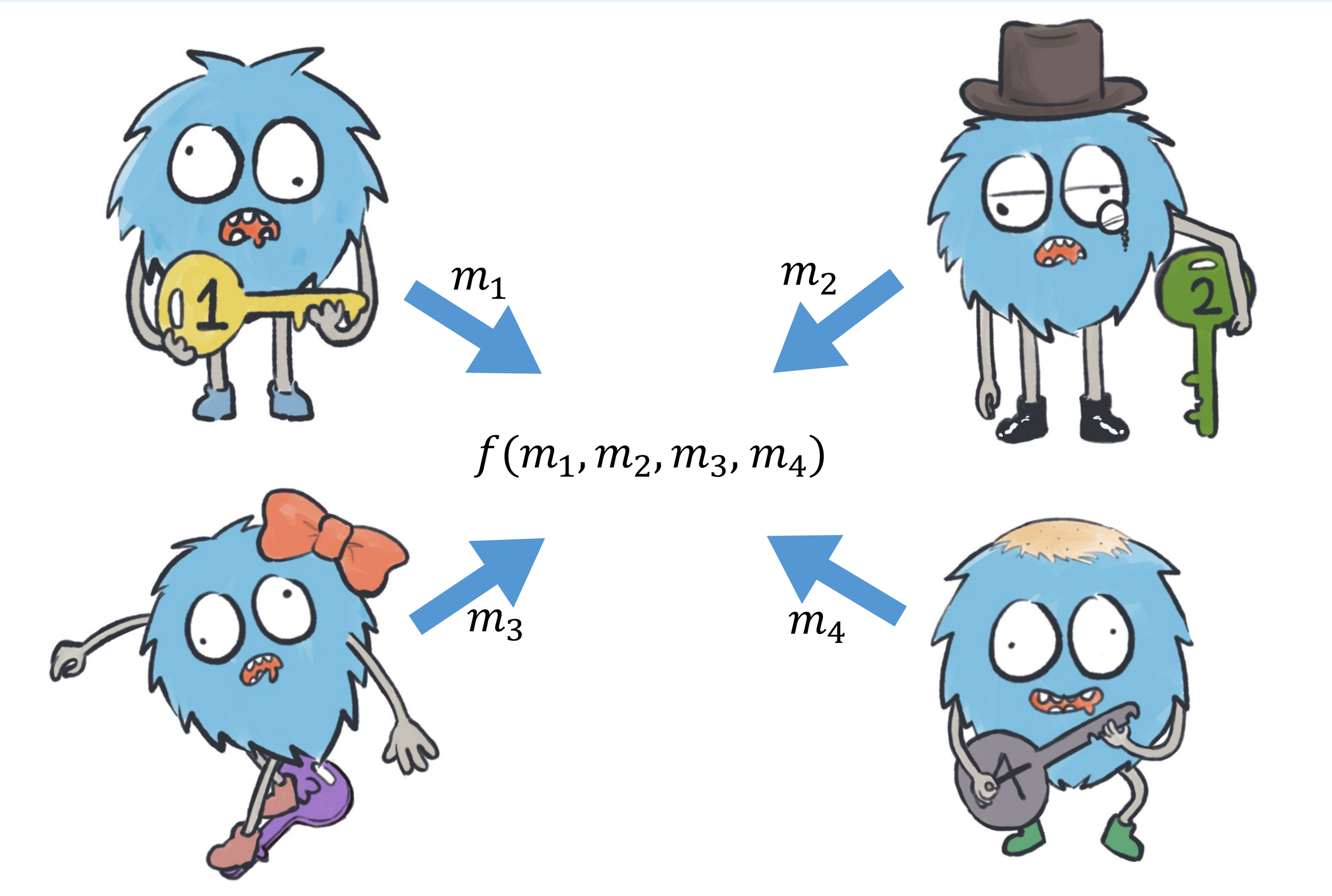
TOWARDS PRACTICAL MULTI-KEY TFHE

Parallelizable, Key-Compatible, Quasi-Linear Complexity

Hyesun Kwak, Seonhong Min, Yongsoo Song
Seoul National University

서울대학교
SEOUL NATIONAL UNIVERSITY

Multi-Key (Fully) Homomorphic Encryption



An **MKHE** scheme is a cryptosystem based on FHE which enables us to perform homomorphic evaluations between messages encrypted under different secret keys.

Prior work by Chen, Chillotti, Song [CCS19]

The main contribution of this paper is **Hybrid Product**, which is a homomorphic multiplication between **Uni-Encryption** and an MK-RLWE ciphertext of $\tilde{O}(kn)$ time complexity where k, n denotes the number of associated parties and the length of ciphertext, respectively.

- **Uni-Encryption** is a structured **single-key** RGSW ciphertext, having CRS (common reference string) as its randomness.
- Replacing the **External Products** and **RGSW keys** in BlindRotate algorithm in TFHE with **Hybrid Products** and **Uni-Encryption**, the authors could achieve $\tilde{O}(k^2n^2)$ time complexity.

Contribution 1 Improved Hybrid Product

We improve the **Hybrid Product** by a factor of almost two. We observed that we can rearrange the order of the operations and as a result, we can reduce the number of decompositions from $4k+4$ to $2k+4$. The noise growth from this improved method is slightly smaller than the original method, although the difference is almost negligible.

Contribution 2 Generalized External Product

We introduce a new multiplication operation that multiplies an **arbitrary single-key RGSW (RLEV)** ciphertext to a **MK-RLWE** ciphertext.

- Recall that the external product homomorphically **multiplicates the message to each component** of the ciphertext.

$$\varphi_t(\mathbf{c} \boxtimes \mathbf{C}) \approx \mu \cdot \varphi_t(\mathbf{c}) \approx \varphi_t(\mu \cdot \mathbf{c})$$

- Similarly, we multiplicate the single-key RGSW (RLEV) to **each component** of the MK-RLWE ciphertext. However, the resulting ciphertext is encrypted under the **tensor product** of the **single key** and the **multi-key**.
- We can resolve this issue from exploiting the **relinearization** technique. The **owner of the single key** publishes the relinearization key in the form of the **Uni-Encryption** and then relinearize the resulting ciphertext with Hybrid Product. The time complexity of this operation is $\tilde{O}(kn)$.

New BlindRotate algorithm

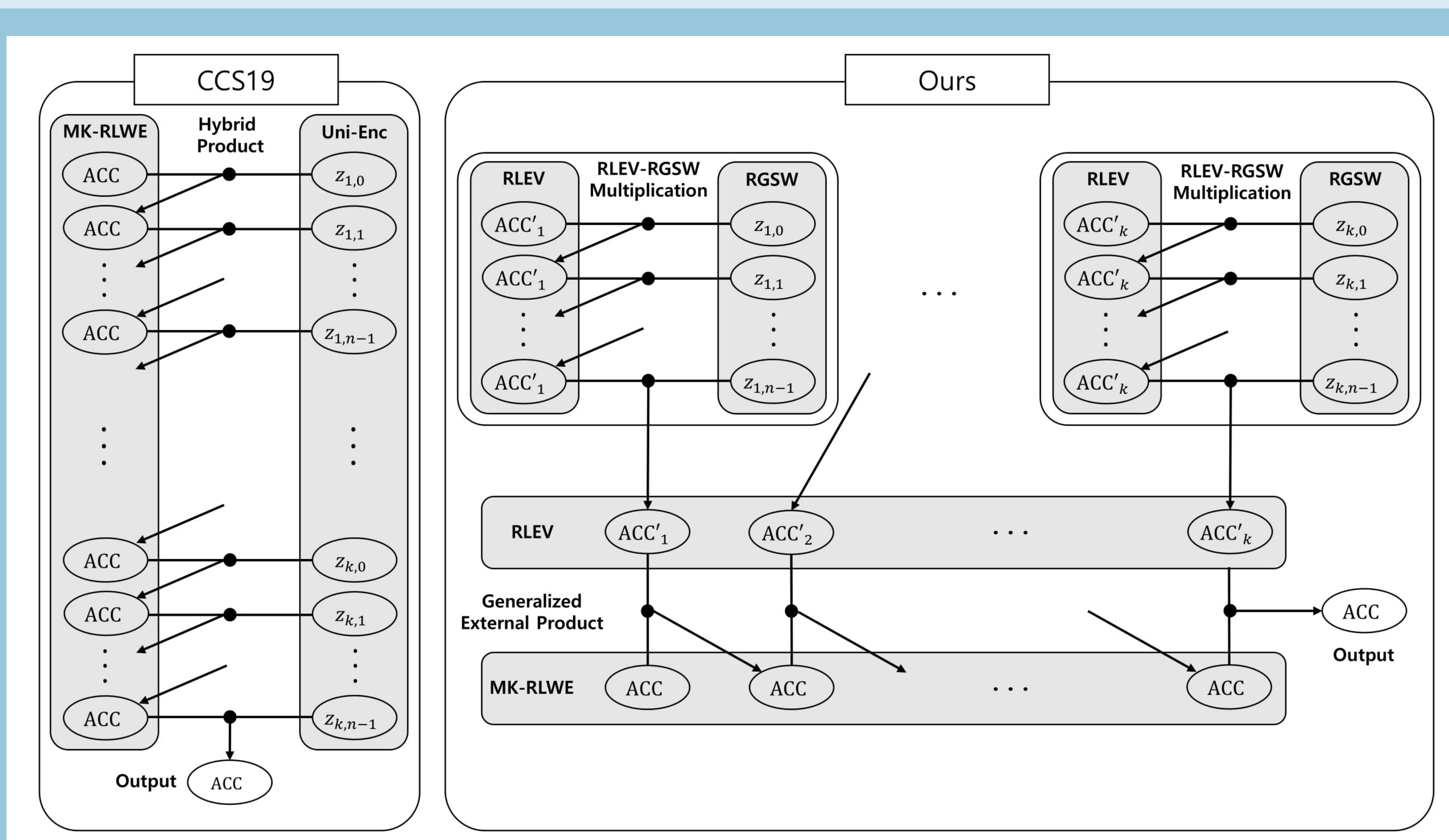
We improve the MK-TFHE scheme from the generalized external product. The vague outline of our scheme is as follows.

1. **Perform Blind Rotation with single-key RGSW (RLEV) accumulators for each party.**
2. **Multiplicate each party's RGSW (RLEV) accumulator to the test vector using the generalized external product.**

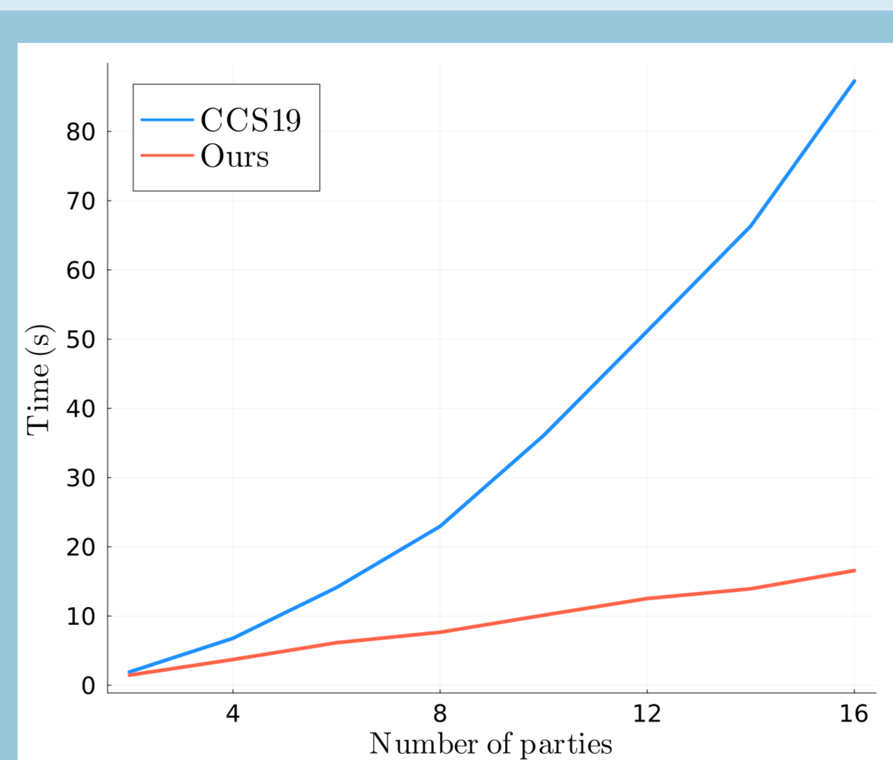
- The time complexity for the first phase is $\tilde{O}(dkn^2)$ where d is the length of the RGSW accumulator, and the time complexity for the second phase is $\tilde{O}(k^2n)$. In typical settings, k is much smaller than n, therefore our scheme is **quasi-linear** to the number of parties.
- Since the accumulators are independently generated, the phase 1 can be **algorithmically parallelized**, with $\tilde{O}(dn^2 + k^2n)$ time complexity.
- The blind rotation key is **compatible to the single-key TFHE scheme** and each party only needs to publish one additional relinearization key.

Experiments

Our algorithmic improvements overwhelm its disadvantage and **outperform** the previous scheme. As expected, our bootstrapping achieves **almost linear time complexity** with respect to the number of parties, compared to the quadratic growth of CCS19 scheme.



High-level overview of the blind rotation algorithms from CCS19 and Ours.



The time elapsed in NAND algorithms Of Ours and CCS19 with 16 parties.