Theme: Security

Topic: Advanced Topics On TFHE-like Fully Homomorphic Encryption

Background

Fully homomorphic encryption (FHE) cryptosystems allow us to compute on encrypted data. Most of the modern FHE schemes fall into two categories:

- Schemes like CKKS/BFV are designed to handle arithmetic functions, and they are hard to support non-linear functions, such as comparison or absolute value.
- Schemes like TFHE are designed to handle boolean functions, which in theory could support any arbitrary computations.

However, there are still strong limitations for the TFHE-like scheme to be practical:

- Not efficient for arithmetic operations. In contrast, CKKS/BFV schemes can do matrix multiplication efficiently, which is crucial in privacy-preserving machine learning.
- Big key size. TFHE-like schemes often require evaluation keys with hundreds of megabytes, even if we only want to compute a single gate. This restricts the usability, especially when the resources are constrained.

Target

FHEW/TFHE like scheme that supports boolean (or other types of non linear) functions. Furthermore, it should have better usability, examples include but not limited to:

- Provide a better compatibility with the arithmetic FHEs such as ckks and bfv scheme, such as switching the ciphertext between different schemes without decryption.
- Be more compact and efficient so as to run on resource-constrained devices.

Related Research Topics

- TFHE: https://github.com/tfhe/tfhe
- FHEW : https://github.com/lducas/FHEW

Suggested Collaboration Method

AIR (Alibaba Innovative Research), one-year collaboration project.