Improvement of Full Domain Functional Bootstrapping

2310005 Gaku Amamiya

Fully Homomorphic Encryption (FHE), referred to as the "Holy Grail" of cryptography, is an encryption scheme that allows arbitrary computations to be performed on encrypted data. Here, arbitrary computations can be expressed as combinations of basic operations such as AND, OR, and NOT, which in turn can be represented using addition and multiplication. Since FHE allows addition and multiplication on encrypted data, it enables the computation of arbitrary operations.

This property makes it promising for applications in privacy-preserving computing, such as performing machine learning on encrypted data or executing computations in outsourced computing protocols while keeping the client' s data encrypted.

However, repeated homomorphic operations cause noise to accumulate in the ciphertext, leading to decryption failure. Therefore, FHE requires an operation called Bootstrapping to reduce noise. In conventional schemes, Bootstrapping could not be performed within a practical time frame, making it the biggest challenge in achieving practical FHE. Since Gentry first realized FHE in 2009, various schemes have been proposed and improved, but practical implementation has yet to be achieved.

Recently, a type of FHE called Torus Fully Homomorphic Encryption (TFHE), proposed by Chillotti et al., has achieved fast execution of 1-bit Gate Bootstrapping in approximately 10 milliseconds. Furthermore, an extension of Bootstrapping in TFHE, known as Functional Bootstrapping, exists. Functional Bootstrapping not only reduces noise but also enables the evaluation of arbitrary functions using a Look-Up Table. As a result, it is more efficient to evaluate nonlinear functions directly using Functional Bootstrapping to process a Look-Up Table rather than approximating them by combining basic operations through Gate Bootstrapping.

However, in TFHE's Functional Bootstrapping, the domain of the function must be restricted to evaluate an arbitrary function. Full Domain Functional Bootstrapping (FDFB) is an approach that eliminates this limitation, allowing the function' s domain to cover the entire plaintext space of the ciphertext. Existing FDFB methods required at least two Blind Rotations, two Sample Extractions, and two Key Switchings. In this study, we propose a method that achieves FDFB using only two Blind Rotations and two simple Sample Extractions.