Fully homomorphic encryption (FHE) schemes

Khanh Nguyen, Dung Duong, and Willy Susilo

Instutute of Cybersecurity and Cryptology, University of Wollongong, Australia

October 22, 2022

1 Preliminaries

Learning with error (LWE).

Theorem 1 *content.*

Lemma 1 *x+y=z*

Lemma 1.1 *z-r+t=3*

Ring Learning with error (RLWE). Lemma.

2 FHE schemes

2.1 BV scheme

The BV scheme was introduce by Brakerski and Vinod Vaikuntanathan in [BV14] (LWE) and [BV11] (RLWE).

2.2 BGV scheme

[BGV14]

2.3 BFV scheme

In , **B**rakerski [Bra12] proposed a FHE scheme based on LWE problem. Then, **F**an Junfeng and **V**ercauteren Frederik [FV12] introduced RLWE version of Brakerski's scheme. The scheme is called BFV.

BFV scheme

Let R = Z

- Key generation:
- Encryption:
- Decryption:
- Homomorphic operations
  - Add
  - MultConst
  - Mult

References

[BGV14] Zvika Brakerski, Craig Gentry, and Vinod Vaikuntanathan. (leveled) fully homomorphic encryption without bootstrapping. *ACM Transactions on Computation Theory (TOCT)*, 6(3):1–36, 2014.

[Bra12] Zvika Brakerski. Fully homomorphic encryption without modulus switching from classical gapsvp. In *Annual Cryptology Conference*, pages 868–886. Springer, 2012.

[BV11] Zvika Brakerski and Vinod Vaikuntanathan. Fully homomorphic encryption from ring-lwe and security for key dependent messages. In *Annual cryptology conference*, pages 505–524. Springer, 2011.

[BV14] Zvika Brakerski and Vinod Vaikuntanathan. Efficient fully homomorphic encryption from (standard) lwe. *SIAM Journal on computing*, 43(2):831–871, 2014.

[FV12] Junfeng Fan and Frederik Vercauteren. Somewhat practical fully homomorphic encryption. *Cryptology ePrint Archive*, 2012.