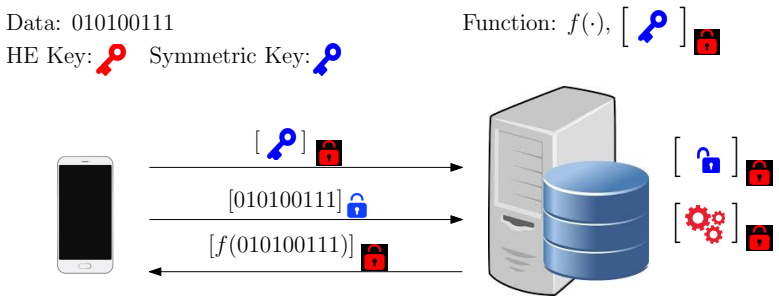
Modèle ARTISHOW:
Hybrid Homomorphic Encryption



Supervisors : Qingju WANG & Weiqiang WEN (Cybersecurity and Cryptography, INFRES)
Number of students per group : 3∼4
How many groups for this project: 1
Tags : Homomorphic encryption, Key recovery
Working language : mainly English

1 Contexte/Context

Privacy-preserving cryptographic protocols and primitives, such as homomorphic encryption (HE), have been applied to increasingly more applications in the recent decade. However, applying them to any given use case usually results in huge performance penalty, both for the runtime of the actual use case, and for the communication between the involved parties.

Looking at applications involving HE, one can use symmetric ciphers in so-called hybrid homomorphic encryption (HHE) (also called trans-ciphering) to address the large communication overhead between a client encrypting the data and a server performing the homomorphic computations. However, the reduced communication overhead then usually comes at the cost of a larger server runtime overhead, which depends on the symmetric cipher used in HHE.

2 Attendus du projet/Expectations

The aim of his project is to :

- Study the mechanism of two recent HHE friendly symmetric ciphers, namely `HERA` [4] and `Rubato` [6].
- Implement the aforementioned ciphers in popular HE protocols, specifically, `HERA` in BFV [5, 1] and BGV [2], and `Rubato` in CKKS [3], in the programming language the working group adept at.
- If time allows, this project can further implement key recovery attacks on `Rubato` and/or `HERA`, and try to propose countermeasures to resist against such attacks with the supervisors.

References

[1] Zvika Brakerski. Fully homomorphic encryption without modulus switching from classical gapsvp. In Reihaneh Safavi-Naini and Ran Canetti, editors, *CRYPTO 2012*, volume 7417 of *LNCS*, pages 868–886. Springer, 2012.

[2] Zvika Brakerski, Craig Gentry, and Vinod Vaikuntanathan. (leveled) fully homomorphic encryption without bootstrapping. In Shafi Goldwasser, editor, *Innovations in Theoretical Computer Science 2012*, pages 309–325. ACM, 2012.

[3] Jung Hee Cheon, Andrey Kim, Miran Kim, and Yong Soo Song. Homomorphic encryption for arithmetic of approximate numbers. In Tsuyoshi Takagi and Thomas Peyrin, editors, *ASIACRYPT 2017*, volume 10624 of *LNCS*, pages 409–437. Springer, 2017.

[4] Jihoon Cho, Jincheol Ha, Seongkwang Kim, ByeongHak Lee, Joohee Lee, Jooyoung Lee, Dukjae Moon, and Hyojin Yoon. Transciphering framework for approximate homomorphic encryption. In Mehdi Tibouchi and Huaxiong Wang, editors, *ASIACRYPT 2021*, volume 13092 of *LNCS*, pages 640–669. Springer, 2021.

[5] Junfeng Fan and Frederik Vercauteren. Somewhat practical fully homomorphic encryption. *IACR Cryptol. ePrint Arch.*, page 144, 2012.

[6] Jincheol Ha, Seongkwang Kim, ByeongHak Lee, Jooyoung Lee, and Mincheol Son. Rubato: Noisy ciphers for approximate homomorphic encryption. In Orr Dunkelman and Stefan Dziembowski, editors, *EUROCRYPT 2022*, volume 13275 of *LNCS*, pages 581–610. Springer, 2022.