Analysis of Homomorphic Encryption Algorithms

Hushchyn Bohdan-Danylo

Kharkiv National University of Radio Electronics, 14 Nauky Ave, Kharkiv UA-61166, Ukraine, bohdan-danylo.hushchyn@nure.ua

Abstract. *Modern methods of homomorphic encryption are considered. Homomorphic encryption schemes are analyzed according to the type and complexity of operations they support. Homomorphic encryption schemes based on lattice problems, such as the BGV scheme and the CKKS scheme, are analyzed. These schemes are believed to be resistant to both classical and quantum attacks.*

Keywords: *Homomorphic Encryption, PHE, SHE, FHE, quantum attack, machine learning.*

I. Introduction and Problem Statement

At present, information is increasingly important in all life processes, and artificial intelligence systems are gaining more and more development. At the same time, threats to information security are constantly growing. In these conditions, it becomes increasingly important to ensure the confidentiality of information. Common cryptographic approaches often require a trade-off between security and the ability to analyze and process data. In cases of using artificial intelligence and machine learning methods, this often becomes a major problem. The use of homomorphic encryption provides a solution to this problem by allowing computations to be performed on encrypted data without the need to decrypt it before use. Homomorphic encryption and machine learning are two important technologies that help increase the level of privacy and data protection in cases where artificial intelligence is used [1].

Thus, the analysis of modern methods of homomorphic encryption becomes relevant.

II. Problem Solution and Results

Homomorphic encryption is a type of encryption method that allows you to perform calculations on encrypted data without first decrypting it with a secret key. The calculation results also remain encrypted and can only be decrypted by the owner of the private key [2].

The concept of partially homomorphic encryption was first introduced by Rivest, Adleman, and Dertouzos in 1978, and this work is considered the introduction of homomorphic encryption. The subject has since made tremendous progress, leading to the creation of Fully Homomorphic Encryption (FHE) techniques by Gentry in 2009 [2, 3].

Homomorphic encryption schemes are classified according to the type and complexity of operations they support. These categories include [4, 5]:

1. Partially Homomorphic Encryption (PHE): Allows only one mathematical operation (such as addition or multiplication) to be performed on the encrypted data. Examples are the RSA cryptosystem for multiplication operations and the Paillier cryptosystem for addition operations.

2. Somewhat Homomorphic Encryption (SHE): Allows addition and multiplication operations, but only a certain number of times. The limitations are related to the accumulation of noise during encryption operations, which can eventually make the ciphertext impossible to decipher.

3. Fully Homomorphic Encryption (FHE): Allows you to perform any computation on ciphertexts, including an unlimited number of addition and multiplication operations. FHE algorithms use techniques such as bootstrapping to limit the accumulation of noise, ensuring that ciphertext remains decipherable even after multiple operations.

Gentry's design relies on lattice-based cryptography and introduces the concept of bootstrapping to control noise growth. Bootloading is a process that involves homomorphic decryption and then re-encryption of the ciphertext within the scheme itself to reduce noise and ensure further operations.

Examples of FHE schemes are the BGV (Brakerski-Gentry-Vaikuntanathan) scheme. It is based on the original Gentry design and improves efficiency by optimizing noise control. Another algorithm is the FV (Fan-Vercauteren) scheme, which was introduced in 2012 and uses the circular learning-with-error (RLWE) problem for better performance. In 2017, the CKKS (Cheon-Kim-Kim-Song) scheme was developed, which supports approximate arithmetic on encrypted data and makes it suitable for applications that require operations with real numbers.

Homomorphic encryption (HE) schemes, like other cryptographic systems, face potential vulnerability to quantum attacks. The main concern is the dependence of many HE schemes on the complexity of certain mathematical problems, which may be undermined by advances in quantum computing [6].

Many homomorphic encryption schemes, such as the BGV scheme and the CKKS scheme, are based on lattice problems such as learning with error (LWE) and ring learning with error (RLWE). These schemes are currently believed to be resistant to both classical and quantum attacks.

III. Conclusions

Thus, the main advantages of homomorphic encryption are the ability to perform calculations on encrypted data without the need to decrypt them. A review of modern homomorphic encryption algorithms has shown that they have already made significant progress, but there are still some limitations, particularly in terms of performance and computational cost. Some homomorphic encryption schemes are resistant to both classical and quantum attacks.

References

[1] Lee, Joon-Woo, et al. "Privacy-preserving machine learning with fully homomorphic encryption for deep neural network." iEEE Access 10 (2022): 30039-30054.

[2] Halevi, S., & Shoup, V. (A Full Introduction to Homomorphic Encryption). 2013. IBM Research. 92 pages.

[3] Gentry, C. Fully Homomorphic Encryption Using Ideal Lattices. 2009. Proceedings of the 41st Annual ACM Symposium on Theory of Computing. 1098 pages.

[4] Yi, X., Paulet, R., Bertino, E., Yi, X., Paulet, R., & Bertino, E. (2014). Homomorphic encryption (pp. 27-46). Springer International Publishing

[5] Coron, J.-S., Naccache, D., & Tibouchi, M. (Homomorphic Encryption). 2011. Springer. 142 pages.

[6] Brakerski, Z., & Vaikuntanathan, V. (Efficient Fully Homomorphic Encryption from (Standard) LWE). 2014. SIAM Journal on Computing, 43(2), 831-871. 40 pages.