The 28th Annual Meeting in Mathematics (AMM 2024)
Department of Mathematics Statistics and Computer,
Faculty of Science, Ubon Ratchathani University,
Thailand

Safeguarding Data Privacy: Exploring Full Homomorphic Encryption

Alain Jean Alherbe[1,†]

[1]Department of Mathematics Statistics and Computer, Faculty of Science
Ubon Ratchathani University, Ubon Ratchathani 34190, Thailand

Abstract

Encryption is the process of securing the confidentiality of stored or transmitted data. It involves encoding the information in such a way that only authorized parties can access it. There are several cryptography architectures designed to ensure secure data transmission and storage. For example, Advanced Encryption Standard (AES) and Secure Hash Algorithm (SHA). When data is transmitted over the internet with those architectures, there is a risk of interception by unauthorized parties and sensitive information can be compromised, leading to security and privacy breaches. Full Homomorphic Encryption (FHE) is an innovative encryption technique that enables computations to be performed on encrypted data without the need for decryption. This means that sensitive information remains private while computations are carried out on the encrypted data, ensuring that the output is also encrypted. TenSEAL is a software library developed by Google. It is specifically designed for building homomorphic applications requiring secure computations on sensitive data. This library enables the implementation of secure computations while maintaining the confidentiality of the underlying data. We provide an overview of FHE, examine the benefits and limitations of using TenSEAL, and demonstrate the procedure of using the library to perform basic computations on encrypted data.

[†] Keynote Speaker.
Email: alain.j@ubu.ac.th