PROC. INTERNAT. CONF. SCI. ENGIN. ISSN 1504607797
Volume 4, February 2021 E-ISSN 1505707533
Page x

Homomorphic Encryption and Its Application in Modern Day World

Artrim Kjamilji
Sabanci University, Istanbul-Turkey
Email: artrimk@sabanciuniv.edu

Abstract. As IPv6 drastically increased the number of devices connected to the internet from 8.4 billion in 2013 to around 30 billion in 2020, it enabled different entities such as governmental, health, research institutions, hospitals, banks or even individuals to generate and collect data that is expected to be 44 ZB in 2020, up from 4.4 ZB in 2013. In this sense, banks collect different information about users' transactions, which can be utilized to track fraud transactions or tax evasions, however in the process they compromise users' privacy by looking into private data such as credit card numbers, amount of money transferred, etc. Research labs and facilities collect samples of human genomes of individuals, which can be used to detect patterns in genes responsible for diseases, pandemics, etc., but in the process they violate the privacy of those individuals since the genome data reveals sensitive private information related to the same individual, such as fingerprints, biometric data, country or family origin etc. Hospitals and health facilities collect data about patient diseases, which can be utilized to correctly diagnose un-diagnosed patients, but in the process they jeopardize patients' private data which is protected by law. To mitigate those problems, the above mentioned entities use homomorphic encryption (HE) schemes to encrypt those private data before storing them to third parties. They do so since HE schemes allow processing and calculations to be done on encrypted data (ciphertext) without decrypting it. To this ends, HE allow the entities to retrieve beneficial information from those data without compromising their privacy, objectives which a few years ago were considered to be mutually exclusive.

We give the mathematical problems assumed to be hard upon which several HE schemes are based on, such as discrete logarithm, quadratic residue, Ring Learning With Errors (RLWE), etc. Since RLWE is proven to be secure under quantum computers, HE schemes based on RLWE (such as FV and BGV) are part of the so called post-quantum cryptography. Then we introduce the three types of HE schemes, namely 1) partially HE schemes (such as elGamal and Paillier), which allow only one type of homomorphic operation on the ciphertext (either addition or multiplication), which are represented with cryptosystems; 2) Somewhat homomorphic schemes (such as the FV scheme), that allow two types of operations on the ciphertexts (usually addition and multiplication), but the number of such operations is limited, and 3) Fully homomorphic schemes (such as BGV) that allow un-limited numbers of two types of operations on the ciphertexts (usually addition and multiplication). Finally, we give some real world application of HE schemes, such as: privacy-preserving finance, private genome analysis, secure e-voting, privacy-preserving machine learning and data mining algorithms, cryptocurrencies, private database querying, secure graph theory, etc.