Tohoku Univ. Technology

High-speed computational method for encrypted data

Achieving higher computational speed than conventional methods without decryption

Overview

This technology is a decryption-free processing method for encrypted data by probability arithmetic way. Conventional FHE (Fully Homomorphic Encryption) method is able to deal with encrypted data, however, the extremely time-consuming computation makes it problematic. This invention utilizes probability arithmetic way for unlimited times of additions and multiplications. Accordingly, the costing time for computation is much decreased compared with conventional methods.

Product Application

- ☐ Machine learning / Deep learning
- ☐ Data mining
- ☐ Statistical analysis of protected private data

This invention vs. conventional methods

Method	Scheme	Number of Mult.	Key Length	Note
Additive HE	Lifted EC ElGamal	N/A	32Bytes	-
SHE	Ring-LWE	1-15	20K-13M Bytes	Parameters where plaintext is given by 0 or 1
FHE	TFHE*	∞	16MBytes	Bootstrapping requires 13 ms per bit
PHE	This technology	∞	32Bytes	Decoded plaintext contains noise due to stochastic computing

*I. Chillotti, M. Georgieva, and M. Lzabach´ene, “TFHE: Fast fully homomorphic encryption over the torus,” J. Cryptol., pp.891–905, 2019.

IP Data

IP No. : PCT/JP2020/045643
Inventor : HONMA Naofumi, UENO Rei
Admin No. : T19-458

Contact

Tohoku Techno Arch Co., Ltd.
TEL +81 222 3049 Please visit CONTACT here