T19-458

東北大学シーズ紹介

# 暗号化されたデータの高速演算方式

**データを暗号化したままで、既存の方法より高速で演算処理が可能**

## 概要

本技術は、確率的計算方式を用いてデータを暗号化状態のまま演算処理する技術です。暗号化状態のデータを演算処理するには、従来完全準同型暗号(FHE: Fully Homomorphic Encryption)といった技術が用いられますが、演算処理時間が膨大になるといった課題がありました。本技術は、確率的計算手法を用いた加算及び乗算を回数制限無く利用可能であり、既存の方式に比して、演算処理時間を短縮することが可能です。

## 応用分野例

以下のような分野への応用が考えらます。
機械学習/深層学習
データマイニング
プライバシー保護統計処理

特許データシート
関連特許番号 (整理番号)： 特願2019-232752 (T19-458)
発明者：本間　尚文、上野　嶺

## 従来方式との性能比較

| 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.

## 連絡先

株式会社　東北テクノアーチ
TEL 022-222-3049　　FAX 022-222-3419
問い合わせはこちらからお願いします。