SCIS 2022 2022 Symposium on
Cryptography and Information Security
Osaka, Japan & Online, Jan. 18 – 21, 2022
The Institute of Electronics,
Information and Communication Engineers

整数型平文空間における非線形 2 変数準同型演算の高速化
An efficient algorithm for non-linear two-variate homomorphic evaluation on integer-wise plaintext space

前田 大輔 * 西出 隆志 *
Daisuke Maeda Takashi Nishide

キーワード 秘密計算，完全準同型暗号，準同型除算

あらまし

完全準同型暗号での除算に代表される非線形 2 変数 Integer-wise 型演算を考える．Integer-wise 型演算では平文はビット毎ではなく整数として暗号化される．先行研究として多項式評価を用いる岡田らの方式 [2] がある．岡田らの方式は SIMD 演算もサポートできる利点があるが，入力整数 bit 長に対し実行時間が指数関数的に増加するため，最大で 257 という比較的小さな平文空間のみを対象としていた．

本論文では BFV 方式のパッキング手法を使いつつも SIMD 演算を犠牲にすることでより大きな平文空間 (2^{15}) を扱える手法を提案する．我々による岡田らの改良版方式 (スロット数 2^{15}) の実行時間見積り (約 55 日) に対し，提案手法の実行時間は 306 秒となっており，より現実的な時間で実行可能なことを PALISADE[1] での実装により確認した．

参考文献

[1] PALISADE Lattice Cryptography Library (release 1.11.5). `https://palisade-crypto.org/`, 2021.

[2] Hiroki Okada, Carlos Cid, Seira Hidano, and Shinsaku Kiyomoto. Linear depth integer-wise homomorphic division. In *IFIP International Conference on Information Security Theory and Practice*, pages 91–106. Springer, 2018.

* 筑波大学, 茨城県つくば市天王台 1 − 1 − 1 , University of Tsukuba, Ibaraki Prefecture, Tsukuba, Tennnodai, 1-1-1, 305-8571, Japan.