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

多項式補間による整数型準同型大小比較/除算の改良

Improvement of integer-wise homomorphic comparison and division using polynomial interpolation

森村 洸生 * 西出 隆志 *
Koki Morimura Takashi Nishide

キーワード 秘密計算，完全準同型暗号，HElib，準同型大小比較，準同型除算，多項式補間

あらまし

完全準同型暗号による、整数型の大小比較・除算演算の改善手法を提案する。完全準同型暗号には、平文をビット毎に暗号化する bit-wise 型と平文を整数のまま暗号化する integer-wise 型の 2 種類がある。本研究では、integer-wise 型の完全準同型暗号を対象とする。大小比較については、先行研究 [1] の手法に対し、多項式補間で導出する多項式を奇関数にすることで、準同型乗算の回数を半分にする方式を提案する。また除算については、先行研究 [2] の手法に対し、準同型乗算の深さを変えずに、多項式評価の回数を約半分にする手法を適用することで、処理速度を改善し、事前計算や保存しておくべき多項式係数を削減できることを示す。また、提案手法を BGV 方式を利用した FHE ライブラリである HElib で実装した。その結果、平文空間 $\mathbb{Z}_{257}$ において処理速度が従来手法と比べて約半分になることを確認した。

参考文献

[1] Narumanchi, H., Goyal, D., Emmadi, N., Gauravaram, P.“Performance Analysis of Sorting of FHE Data: Integer-Wise Comparison vs Bit-Wise Comparison” 2017 IEEE 31st International Conference on Advanced Information Networking and Applications (AINA). (March 2017)

[2] Hiroki Okada,Carlos Cid,Seira Hidano,Shinsaku Kiyomoto“Integer-wise Homomorphic Division Algorithm,” SCIS2019

* 筑波大学, 茨城県つくば市天王台 1 丁目 1-1, University of Tsukuba, 1-1-1, Tennodai, Tsukuba Shi, Ibaraki Ken