革新的コンピューティング技術の開拓
2018 年度採択研究者

2019 年度
実績報告書

上野　嶺

東北大学電気通信研究所
助教

バッテリレス無線センサネットワークのためのポスト量子暗号計算技術

§1. 研究成果の概要

本年度は，(1) 前年度に設計した剰余数系（RNS: Residue Number System）に基づく巨大標数のガロア体向け低遅延剰余乗算器のバックエンド最適化および性能評価を行った．その結果，同種写像（Supersingular Isogeny）に基づく耐量子計算機暗号 SIDHp503 と呼ばれる方式の主要な演算である虚二次拡大体上の乗算を約 380 ナノ秒で実行可能となることを確認した．これはこれまでで同等のパラメータおよびデバイスにおける既存の最も高速な SIDHp503 ハードウェアの約 401 ナノ秒に対し約 5%低遅延である．

さらに本年度は，(2) 暗号文上で確率的乗算と確率的加算の両方が評価可能な確率的準同型暗号（PHE: Probabilistic Homomorphic Encryption）を開発した（図 1）．準同型暗号とは暗号文を復号することなくある2つの暗号文の平文の和や積に対応する暗号文を現実的な時間と無視できる失敗確率で生成可能な暗号を指す．これまで，任意回の乗算を評価可能な完全準同型暗号（FHE）は数 MB 以上の鍵長とブートストラップと呼ばれる計算コストが非常に重い処理が必要になりその実装コストの改善が課題であった．本年度に開発した PHE はストカスティック計算と呼ばれる確率的乗算と加算をブートストラップ無しで任意回評価可能であるとともに，PHE は単演算準同型暗号（単演算 HE）や制限付き準同型暗号（SHE）などの既存の公開鍵暗号を用いて構成されるためそれらと同等の鍵長で実装可能である（表 1）．一方で，PHE で評価結果の平文にはストカスティック計算に由来する誤差が含まれる．したがって，PHE ではストカスティック計算の誤差が許容できる応用においては実装効率の観点から優位となる．本年度は，PHE 上で準同型評価を行った結果の平文に含まれる誤差の基礎的評価を行うとともに，いくつかの公開鍵暗号を用いて PHE の実装評価を行った．実装効率の観点から耐量子計算機暗号の一種である格子暗号が PHE の構成に適していることを確認した．

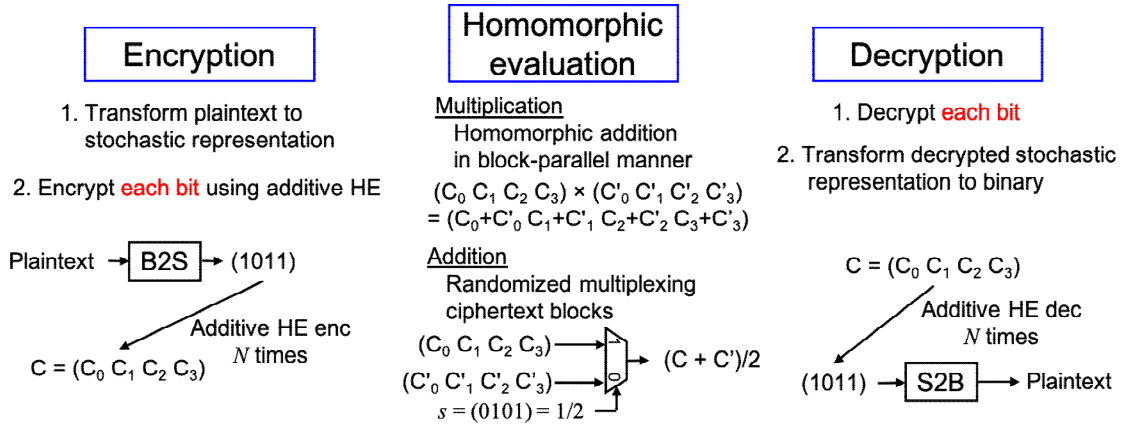

図 1：PHE の概要

表 1：単演算 HE，SHE，FHE，そして PHE の比較

	Arithmetic flexibility	Computational complexity	Key size	Ciphertext size
単演算HE	×	○	○	○
SHE	△	△	△	△
FHE	○	×	×	×
PHE	○ （ただし復号した平文に誤差を含む）	単演算HEと同等 （ストカスティック数値のビット長に対し線形）		