「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

2018 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，鍵長・通信量が最も短いポスト量子暗号の一つである超特異楕円曲線同種写像（SI）暗号と，比較的短い鍵長・通信量の高い計算効率を有する Learning With Errors over Ring 問題に基づく格子暗号（R-LWE 暗号）に着目し，これらの暗号を効率的に実現するためのガロア体算術演算回路の設計を実施した．また，上記暗号と併用する共通鍵暗号として国際標準暗号 Advanced Encryption Standard（AES）のハードウェアアーキテクチャの設計を実施した．

まず，SI 暗号で用いられる巨大な標数のガロア体上の乗算を効率的に実現するために，剰余数系（RNS: Residue Number System）と呼ばれる整数表現に基づく低遅延な並列剰余乗算器を設計した．また，R-LWE 暗号おいて最も計算時間がかかる数論変換（NTT: Number Theoretic Transform）処理の低遅延なハードウェアアーキテクチャを設計した．さらに，AES ハードウェアアーキテクチャ設計においては，これまで開発してきたガロア体表現変換・演算圧縮技術に加えて乗法的オフセットと呼ばれる線形演算の最適化手法を開発した．本手法は既存のアーキテクチャに適用することでオーバーヘッド無しで 7–9%面積遅延効率を向上することが可能である．

§2. 研究実施体制

①研究者：上野　嶺（東北大学電気通信研究所　助教）
②研究項目
・ハードウェアアルゴリズムの設計
・暗号ハードウェアの安全性評