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

2020 年度
年次報告書

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，(i) 剰余数系に基づく同種写像暗号の高速ハードウェア実装，(ii) Quotient Pipelining モンゴメリ乗算に基づく同種写像暗号向け高面積遅延効率乗算器の設計・評価，(iii) ポスト量子暗号の実装攻撃に対する脆弱性の評価を行った．鍵長・通信量が最も小さいポスト同種写像暗号の方式の一つである同種写像暗号では，３つ以上の有限体乗算を並列で実行することが困難なため，同種写像暗号の高速化には有限体乗算の低遅延化が本質的に重要となる．(i) では，剰余数系と呼ばれる冗長表現に基づくハードウェアアーキテクチャを設計し，さらにその乗算器の内部演算を展開して並列に行うことで高速な同種写像暗号ハードウェアを設計した．提案手法はこれまでで最速の既存手法よりも約 37%高速に同種写像暗号を実行可能なことを確認した．これは本研究者が知る同種写像暗号モジュールの中で最速である．さらに，(ii) では，(i) に対し面積遅延効率の観点から最適化した乗算器を設計し，基礎的な評価を行った．FPGA および ASIC での実装評価の結果から，設計した乗算器は既存手法に対して面積遅延の観点から最も効率的に同種写像暗号を実行できる可能性があることを確認した．加えて，(iii) では，ポスト量子暗号の組み込み応用においてセキュリティ上非常に重要となる実装攻撃に対する脆弱性の評価を行った．特に，機器の暗号演算を実行中の消費電力や漏洩電磁波から秘密情報を推測するサイドチャネル攻撃などを中心として調査を行った．結果として，現実的な実験環境と確率で秘密鍵が漏洩する可能性があることを発見し，発見した攻撃に対する対策の検討を行った．