AIP 加速課題
2020 年度採択研究代表者

2021 年度
年次報告書

原 祐子

東京工業大学・工学院
准教授

小型 IoT エッジデバイスの軽量暗号アーキテクチャ設計

§1. 研究成果の概要

Internet of Things (IoT) のエッジコンピューティングの普及に伴い、小型エッジデバイスの台数、および、センシングデータ量が増大し、それらのセキュリティ強化は重要な課題となっている。近年、NIST や ISO において、小型デバイスを想定した軽量暗号の標準化が進められている。本研究では、NIST/ISO 標準の軽量暗号に対象に、サイドチャネル攻撃(特に電力解析攻撃)に対して堅牢な小型・低電力プロセッサ、および、最新の攻撃技術に対するセキュリティ評価プラットフォーム開発を目指す。2021 年度は、(1) 2020 年度に引き続き軽量暗号アルゴリズムの調査、(2) 2020 年度に拡張した小型プロセッサ SubRISC+の実装改良、(3) セキュリティ評価環境の拡張を行った。(1)では、NIST の軽量暗号コンペティションのファイナリストについてアルゴリズムの特徴を分析し、小型エッジデバイスに要求されるレイテンシ・メモリ使用量等の分析を行った。(2)では、昨年度の成果として決定したプロセッサの命令セット・機能を元に、回路オーバヘッドを抑えつつ、漏洩を抑えるハードウェア設計を行った。また、最新の研究発表や提案するプロセッサのシミュレーション・FPGA 実装結果を詳細に分析し、軽量暗号ソフトウェアの実装方針を検討・整理した。(3)については、電力解析攻撃におけるシステムノイズの影響を明らかにした。研究成果を国際会議 AsianHOST で発表し、Best Paper Award を受賞した。また、(2)のプロセッサの比較対象となる既存手法の再現について、発表論文やシミュレーション結果を元に検討した。

§2. 研究実施体制

(1)原グループ

① 研究代表者:原 祐子 (東京工業大学工学院 准教授)

② 研究項目

・軽量暗号向け小型プロセッサの実装・漏洩を抑えるための改良

・軽量暗号アルゴリズムのソフトウェア実装および実装方針整理

・評価環境の拡張および比較対象再現について検討

(2)李グループ

① 主たる共同研究者:李 陽 (電気通信大学情報理工学研究科 准教授)

② 研究項目

・軽量暗号アルゴリズムの調査・まとめ

・軽量暗号アルゴリズムのソフトウェア実装

・新たな電力解析攻撃の開発・評価

【代表的な原著論文情報】

1) 伊藤 千夏, 原 祐子, 崎山 一男, 李 陽, ″GIFT 暗号を用いたソフトウェア閾値法の実装,″ 電子情報通信学会 2021 年ソサイエティ大会, 2021.

2) Rei Kudo, Takeshi Sugawara, Kazuo Sakiyama, Yuko Hara-Azumi, and Yang Li, ″Revisiting System Noise in Side-Channel Attacks: Mutual Assistant SCA vs. Genetic Algorithm,″ Asian Hardware Oriented Security and Trust Symposium (AsianHOST), pp.1-6, 2021.

3) 渡辺 陸, 楊 明宇, 原 祐子, 崎山 一男, 李 陽, ″RISC-V と SubRISC+における LED 暗号の Bitslice 実装の評価,″ 暗号と情報セキュリティシンポジウム (SCIS), 2022.

4) 楊 明宇, 卯木 あゆ美, 李 陽, 崎山 一男, 原 祐子, ″少命令セット組込みプロセッサにおける ARX 型暗号アルゴリズムの実装と評価,″ 暗号と情報セキュリティシンポジウム (SCIS) 2022.

5) 北原 知明, 日良 僚太, 原 祐子, 宮原 大輝, 李 陽, 崎山 一男, ″NIST 軽量暗号最終候補におけるソフトウェア実装性能の評価,″ 暗号と情報セキュリティシンポジウム (SCIS), 2022.