AIP 加速課題
2020 年度採択研究代表者

2020 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。

2020 年度は、(1)軽量暗号の調査・選定、(2)研究代表者が ACT-I 加速課題で開発した小型プロセッサ SubRISC+を基とした拡張、(3)セキュリティ評価環境の構築、(4) SciFoS 活動による研究・市場動向の調査、(5)SubRISC+プロトタイプの有用性を実証した。

(1)では、軽量暗号のソフトウェア・ハードウェア実装にかかるコスト(回路面積、メモリ使用量)および処理効率を調査し、対象とすべきアルゴリズムを選定した。

(2)では、(1)の調査結果を受け、SubRISC＋の命令セットを拡張した。また、暗号アルゴリズムの効率的な処理に関わる機能を検討し、拡張の方針を定めた。

(3)では、(2)の拡張を受けて、ソフトウェア開発環境(主にコンパイラとシミュレータ)を拡張した。また、比較対象として、ISO 標準の軽量暗号 Chaskey-12 の専用回路を FPGA 実装し、その脆弱性を明らかにした。さらに、最新の電力解析攻撃(機械学習を用いる手法等)の評価環境を構築した。

(4)では、セキュリティを専門とする企業の研究者・開発者にヒアリングを行い、本研究のアプローチの有用性・妥当性を調査・確認した。

(5)では、SubRISC＋プロトタイプの電力・エネルギー効率の実証結果に関して、プレスリリース発表を行った。

§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

・SubRISC+(ACT-I 研究成果)の脆弱性解析

・軽量暗号に適したプロセッサ改良(主に命令セット・命令フォーマット)の検討・実装

・軽量暗号 Chaskey-12 の FPGA 実装

・ハードウェア/ソフトウェアの統合評価環境構築

(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（NIST Competition）の調査・選定
・軽量暗号 LED のソフトウェア実装
・セキュリティ評価環境構築
・ハードウェア/ソフトウェアの統合評価環境構築