IoT が拓く未来
2020 年度採択研究者

2020 年度
年次報告書

五十部 孝典

兵庫県立大学 大学院応用情報科学研究科
准教授

# IoT 機器の長期的な安全性確保のためのビヨンド軽量暗号の開拓

## §1. 研究成果の概要

本年度は、軽量ホワイトボックス暗号技術の開発を行った。具体的には、IoT 機器が攻撃者にコントロールされた場合でも安全性を保障する技術である「ホワイトボックス暗号」とIoT 機器等のデバイスで効率的に実装可能な「軽量暗号技術」の開発を実施した。

ホワイトボックス暗号に関しては、攻撃者が IoT デバイスを完全にコントロール可能な状況でも安全性を保障するため、暗号演算をテーブルアクセスのみから実現し、各テーブルに鍵を隠す技術を開発した。これにより、メモリ上には鍵は出現せず、攻撃者は秘密鍵を取得することができない。さらに、テーブル自体の取得を防ぐため、暗号化関数としての機能を維持したまま、セキュアにテーブルを更新可能な”Updatable Whitebox Cryptography”の理論を構築した。この理論をもとに実際の暗号アルゴリズム Yoroi を設計し、論文を投稿した。

軽量暗号技術についての具体的な成果としては、「低遅延暗号」と「低回路規模暗号」の技術を開発した。低遅延暗号技術としては、低遅延非線形関数の設計と、全体の繰り返し数を抑えるための技術である 2-branch construction を開発した。これらの技術を用いて低遅延暗号 Orthros を設計し、デファクトスタンダード暗号の AES と比較し、1/10 の遅延での暗号化が可能となった。この成果は、共通鍵暗号技術のトップジャーナルである ToSC 2021 に採録された。また、低回路規模暗号に関しては、ストリーム暗号において必要なレジスタサイズを抑える技術である Double key filtering と呼ばれる技術を開発し、実際の暗号アルゴリズム Atom を設計した。Atom は 128 bit security のストリーム暗号としては、世界最軽量を達成し、結果は ToSC 2021に採録された。さらに、軽量暗号の新しい解析、安全性手法として、比較的 Diffusion speed が遅い関数に対して non-random なふるまいを効率的に発見する技術を開発し、Gimli と呼ばれる著名な暗号技術に対して適応し、暗号解析の記録を更新した。この成果も、ToSC 2021 に採録されている。

【代表的な原著論文情報】

1) Subhadeep Banik, Takanori Isobe, Fukang Liu, Kazuhiko Minematsu and Kosei Sakamoto, ″Orthros: A Low-Latency PRF″, IACR Trans. Symmetric Cryptol (ToSC/FSE), 2021, no.1, pp.37-77, 2021.

2) Subhadeep Banik, Andrea Caforio, Takanori Isobe, Fukang Liu, Willi Meier, Kosei Sakamoto and Santanu Sarkar, ″Atom: A Stream Cipher with Double Key Filter″, IACR Trans. Symmetric Cryptol (ToSC/FSE),no.1, pp.5-36, 2021.

3) Fukang Liu, Takanori Isobe and Willi Meier, ″Exploiting Weak Diffusion of Gimli: Improved Distinguishers and Preimage Attacks″, IACR Trans. Symmetric Cryptol (ToSC/FSE), no.1, pp.185-216, 2021.