IoT が拓く未来
2020 年度採択研究者

2021 年度
年次報告書

五十部 孝典

兵庫県立大学 大学院情報科学研究科
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

2021 度は、IoT デバイスにおいて攻撃者が物理的にデバイスにアクセス可能で、タイミングや電力等のサイドチャネル情報を十分に得られた場合でも、安全性を保障する暗号技術の開発を目標に研究を推進した。具体的には (1)IoT デバイス向けの軽量暗号の安全性評価、 (2)IoT 向けの暗号の設計の 2 点を実施した。

(1)に関しては、(2)の安全な暗号の設計のために暗号の自動評価ツールの作成をした。具体的には、差分、線形、不能差分、積分攻撃、代数攻撃などの主要な解析技術のツールを混合整数線形計画法の solver を用いて作成した。また、ツールを用いて実際に既存の暗号技術の厳密な安全性評価を実施した。代表的な成果としては、LowMC と Rasta に対する解析結果で、暗号分野のトップ会議 CRYPTO[1], ASIACRYPT[2]に採録された。さらに AEGIS に対する解析では FSE 2022 の Best Paper Award を受賞した[3]

(2)に関しては、(1)で作成した暗号の自動評価ツールを用いて、IoT 機器で脅威となるになるタイミング情報、電力消費量、メモリリークなどの実装攻撃に耐性のある暗号アルゴリズムの開発をソフトウェア向けとハードウェア向けにそれぞれ設計した。ソフトウェア向けの実装攻撃に耐性のある暗号アルゴリズムとして、タイミング攻撃に耐性のある constant-time 実行可能なアルゴリズム Rocca を設計した。Rocca は SIMD 命令のみで実行可能な構成でありキャッシュを用いることなく入力に依らず同じ時間で暗号演算が実行可能である。結果は、共通鍵分野のトップジャーナル ToSC に採録された[4]。また、その設計理論についてまとめた成果は国際ジャーナル IET 採録された[5]。ハードウェア向けの実装攻撃に耐性のある暗号アルゴリズムとしては、スペースハード暗号 Qubicle を開発し、現在国際論文誌へ投稿中である。Qubicle はテーブル内に秘密鍵を隠すことでメモリリークに対しての安全性を達成している。また、ハードウェアで低消費電力で実行可能な暗号の設計理論についてまとめた論文は共通鍵分野のトップ会議 ToSC に採録された。

【代表的な原著論文情報】

[1]Fukang Liu, Takanori Isobe, Willi Meier, ″Cryptanalysis of Full LowMC and LowMC-M with Algebraic Techniques″ Advances in Cryptology (CRYPTO) 2021, Lecture Note in Computer Science, Part 3, vol. 12827, pp. 368-401, 2022.

[2]Fukang Liu, Santanu Sarkar, Willi Meier and Takanori Isobe, ″Algebraic Attacks on Rasta and Dasta Using Low-Degree Equations″, Advanced in Cryptology (ASIACRYPT) 2021, Lecture Note in Computer Science, Part 1, vol. 13090, pp. 214--240}, Springer, 2021.

[3]Fukang Liu, Takanori Isobe, Willi Meier and Kosei Sakamoto, ″Weak Keys in Reduced AEGIS and Tiaoxin″, IACR Trans. Symmetric Cryptol (ToSC/FSE),no.2, pp.104-139, 2021

[4]Kosei Sakamoto, Fukang Liu, Yuto Nakano, Shinsaku Kiyomoto and Takanori Isobe, ″Rocca: An Efficient AES-based Encryption Scheme for Beyond 5G″, IACR Trans. Symmetric Cryptol (ToSC/FSE), 2021, issue 2, pp.1-30, 2021.

[5]Rentaro Shiba, Kosei Sakamoto and Takanori Isobe, ″Efficient constructions for large-state

block ciphers based on AES-NI" , IET Information Security, vol. 16, No.3, pages 145-160, 2022.