IoT が拓く未来　　2022 年度
2020 年度採択研究代表者　　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

研究成果の概要

本年度は複製困難性を満たす共通鍵暗号技術の開発を実施した。複製困難性とは、仮に鍵やそれに相当する情報をデバイス上から盗まれたとしても，別デバイスでのプログラムの複製を困難にする技術である。具体的には、(1)鍵の情報を任意長に拡大するスペースハード暗号の設計と(2)それを用いて秘匿や認証等の機能を付加する暗号化モードの開発を行った。これらを用いることで、物理攻撃やサイドチャネル攻撃等で多くのデータを攻撃者に取得された場合でも安全性を保証する。

(1) スペースハード暗号の設計では、IoT 向けに特化した暗号として、Cortex-M をターゲットとした暗号 Cubicle を設計した[1]。Cubicle では、Cortex-M 向けの命令セットや RAM サイズに特化した構造を採用することで、既存技術の4倍以上の高速化に成功した。安全性に関しては、150KB 以下のメモリリークの場合安全性を保証可能である。一方通常の暗号であればたった 128 bit のリークで安全性が崩壊する。また、IoT 向けのスペースハード暗号の新しい攻撃モデル Hybrid Code Lifting モデルを考案し、既存の暗号である Yoroi や SPNbox の安全性を厳密に評価した[2]。本成果は、共通鍵暗号のトップジャーナル FSE2023 に採録され、Best Paper Award を受賞した。またプリミティブに対する安全性解析結果も Journal of Cryptology や ASIACRYPT に採択された[3,4]

(2) (1)で開発したブロック暗号プリミティブを拡張し、任意長のメッセージに対して秘匿や認証等の機能を付加するモードを開発した[5]。このモードでは、プリミティブの Hybrid Code Lifting の安全性をモードに拡張可能であり、サイドチャネル攻撃や物理攻撃で多くの秘密データを攻撃者に取得された場合でも秘匿性や認証などの安全性を数学的に保証する。さらにこのモードに特化した新しいプリミティブ SPACE256 を設計した。SPACE256 は、256 ビットのブロックサイズを持ち、この暗号をモードに組み込んだ場合は、数メガバイトの情報がリークした場合でも安全性を保証可能である。本成果は暗号のトップカンファレンス ASIACRYPT 2022 に採録された。

【代表的な原著論文情報】

1) Rentaro Shiba, Ravi Anand, Kazuhiko Minematsu and Takanori Isobe, "Cubicle: a family of space-hard ciphers for IoT", IET Information Security, 2023

2) Yosuke Todo and Takanori Isobe, "Hybrid Code Lifting on Space-Hard Block Ciphers", IACR Trans. Symmetric Cryptol (ToSC/FSE), 2022, issue 3, pp. 368-402, 2022.

3) Fukang Liu, Santanu Sarkar, Willi Meier and Takanori Isobe, "The Inverse of χ and Its Applications to Rasta-like Ciphers", Journal of Cryptology, vo.35, no.4, pp. 28-47, 2022.

4) Fukang Liu, Santanu Sarkar, Gaoli Wang, Willi Meier and Takanori Isobe, “Algebraic Meet-in-the-Middle Attack on LowMC”, ASIACRYPT 2022

5) Akinori Hosoyamada, Takanori Isobe, Kan Yasuda, Yosuke Todo, “A Modular Approach to the Incompressibility of Block-Cipher-Based AEADs”, ASIACRYPT 2022