SCIS 2022 2022 Symposium on
Cryptography and Information Security
Osaka, Japan & Online, Jan. 18 – 21, 2022
The Institute of Electronics,
Information and Communication Engineers

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

Implementation and Evaluation of ARX-based Ciphers on a Simple Instruction-Set Embedded Processor

楊明宇 * 卯木あゆ美 * 李陽 † 﨑山一男 † 原祐子 *
Mingyu Yang Ayumi Uki Yang Li Kazuo Sakiyama Yuko Hara-Azumi

キーワード 共通鍵暗号 IoT

あらまし

近年、Internet of Things (IoT) 社会の発展により、IoT デバイス上の秘密情報の保護が注目されている。しかしながら、計算リソースが限られている IoT デバイスでは、複雑な暗号のリアルタイム処理は大きな課題である。本研究では、我々が既に開発した小型な組込みプロセッサ SubRISC+を、Add-Rotation-XOR (ARX) 型軽量暗号アルゴリズムを対象に拡張し、効率的な暗号処理の実現に向けたプロセッサの実装と最適化について検討する。具体的には、ARX 計算に基づくメッセージ認証符号に適した命令セットの定義、および、アーキテクチャ実装とその最適化を行う。実験では、ブロック暗号・ストリーム暗号の ARX 型アルゴリズムに対して RISC-V (Ibex) と提案プロセッサを比較評価し、提案アーキテクチャの有用性を示す。

* 東京工業大学, 東京都目黒区大岡山 2-12-1, Tokyo Institute of Technology, 2-12-1, Ookayama, Meguro-ku, Tokyo, Japan
† 電気通信大学, 東京都調布市調布ケ丘 1-5-1, The University of Electro-Communications, 1-5-1, Chofu-shi, Tokyo, Japan