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

RISC-V と SubRISC+における LED 暗号の Bitslice 実装の評価
Implementation and Evaluation of Bit-sliced LED on RISC-V and SubRISC+

渡辺陸 * 楊 明宇 † 原 祐子 † 崎山 一男 * 李 陽 *
Riku Watanabe Mingyu Yang Yuko Hara-Azumi Kazuo Sakiyama Yang Li

キーワード SubRISC+, RISC-V, LED 暗号, Bitslice

あらまし

近年の IoT デバイス需要の高まりを受け、省電力下での暗号実装が求められている。IoT デバイスでの実行を考えた場合、回路面積が小さく消費電力が少ないものが望ましい。また、使用できる計算リソースやメモリ領域が少ないことを考慮する必要がある。以上のような条件を満たす環境として RISC-V アーキテクチャや SubRISC+プロセッサー [1] などが挙げられる。

RISC-V アーキテクチャとは UCBerkeley で開発された RISC(Reduced Instruction Set Computer) アーキテクチャである。一方 SubRISC+は東工大で開発された SNG4 という単一命令のアーキテクチャを発展させた RISC プロセッサーである。分岐処理を含む減算、論理和、シフト、メモリ読み書き、の 4 つの命令からなる SubRISC から更に発展させたアーキテクチャが SubRISC+である。これらの RISC アーキテクチャは構成する命令数が少なく想定する回路規模が小さいため、省電力下での実行が想定される IoT デバイスに適している。また、2 つのアーキテクチャはレジスタのビット数や設計思想などに類似性が見られるため RISC − V から SubRISC+への変換も考えられる。

続いて IoT デバイス上で評価する暗号実装について考える。軽量な暗号方式の一つとして LED 暗号 [2] が挙げられる。LED 暗号は AES 暗号を基に、軽量化されたブロック暗号である。また、LED 暗号には軽量化、並列化が見込める Bitslice 実装が存在する [3]。Bitslice とは命令のオペランドを任意の個数に分割し、処理を並列に走らせる実装手法であり、ブロック暗号に対する高速化が望める。また、Bitslice は 64bitCPU での評価が先行研究として存在する [4]。

以上を踏まえ、回路面積の小さい RISC-V において Bitslice を施した LED 暗号と通常の LED 暗号をエミュレータ上で実装し、その性能を評価した。また、RISC − V 命令から SubRISC+命令の実行コードを変換することで Bitslice を施した LED 暗号と通常の LED 暗号を SubRISC+エミュレータ上でも実装し、同様に性能の評価を行った。また、Bitslice 実装による高速化を定量的に評価するためスループット、レイテンシ、実行ステップ数を評価項目とした。本論文では SubRISC+という新しいアーキテクチャに対する完全でないコンパイル環境においての実装手法も紹介する。

参考文献

[1] K. Saso and Y. Hara-Azumi. Revisiting simple and energy efficient embedded processor designs toward the edge computing. *IEEE Embedded Systems Letters*, 12(2):45–49, 2020.

[2] Jian Guo, Thomas Peyrin, Axel Poschmann, and Matt Robshaw. The led block cipher. In *International workshop on cryptographic hardware and embedded systems*, pages 326–341. Springer, 2011.

[3] Zhenzhen Bao, Peng Luo, and Dongdai Lin. Bitsliced implementations of the prince, led and rectangle block ciphers on avr 8-bit microcontrollers. In *International Conference on Information and Communications Security*, pages 18–36. Springer, 2015.

[4] Eli Biham. A fast new des implementation in software. In *International Workshop on Fast Software Encryption*, pages 260–272. Springer, 1997.

* 電気通信大学, 東京都調布市調布ヶ丘 1-5-1,Faculty of Informatics and Engineering, The University of Electro-Communications, 1-5-1 Chofu-shi, Tokyo 182-8585, Japan, (riku.w@uec.ac.jp)
† 東京工業大学, 〒 152-8550 東京都目黒区大岡山２丁目１２－１, Faculty of Information and Communications Engineering, Tokyo Institute of Technology, 2-12-1 Ookayama, Meguro-ku, Tokyo 152-8550 Japan