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

STM32 上の AES コプロセッサを用いた OCB の高性能ソフトウェア実装
Software Implementation of OCB Using AES Coprocessor on STM32 Microcontroller

金 剛山 * 菅原 健 *
Kangsan Kim Takeshi Sugawara

キーワード OCB，認証暗号，AES，STM32，暗号コプロセッサ，暗号ハードウェア，暗号実装

あらまし

組込機器をネットワークに接続する応用が増加しつつあり，計算能力に乏しいマイコン上での効率的な暗号実装が求められている．その中で，チップベンダは，汎用のマイコンにも暗号コプロセッサを搭載しつつある．それを受けて，コプロセッサを積極的に利用した暗号利用モードの研究などが進められている [1].

暗号コプロセッサを効率的に利用するには，その性能の詳細を知る必要がある．そこで著者らは，先行研究において，複数のマイクロコントローラを対象に，性能評価を行った [2]．その結果，コプロセッサの呼び出しの初期コストが大きく，その性能を高めるには，大量の AES 暗号化を一度に呼び出す必要があることが分かった．

本研究はそのような暗号コプロセッサの特性を利用して，OCB (Offset Code Book) [3] の高性能実装を行う．OCB はブロック暗号をベースとした認証付き暗号のスキームの一種であり，各メッセージブロックが隣接ブロックとは独立に加工及び暗号化される仕組みになっている．メッセージ間の依存関係が無く，AES コールを並列化可能であるため，前述の暗号コプロセッサの性質に適している．すなわち，AES コプロセッサを用いて OCB を実装した場合，AES 呼び出し 1 回あたりの処理ブロック数を大きくするほど，OCB 全体の性能向上が期待される．

本研究では AES コプロセッサを用いて OCB を実装し，サイクル数による性能評価を行う．評価プラットフォームは，ARMv8-M プロセッサをコアとするマイコンであり, AES コプロセッサを搭載する STM32L562 [4] とする．並列度を変化させながら，それに応じた性能向上を検証する．また，最先端のソフトウェア実装技法である Fixslicing [5] を用いた OCB 実装との性能比較を行う．

* 電気通信大学，東京都調布市調布ヶ丘 1-5-1，The University of Electro-Communications, 1-5-1 Chofugaoka, Chofu, Tokyo 182-8585, Japan

参考文献

[1] Y. Naito, U. Sasaki, and T. Sugawara, ”AES-LBBB: AES Mode for Lightweight and BBB-Secure Authenticated Encryption,” TCHES, vol. 2021(3): pp. 298-333, 2021.

[2] 金剛山, 菅原健, ”ARMv8-M マイクロコントローラにおける AES コプロセッサの性能評価,” IEICE 2021 年ソサイエティ大会, 2021.

[3] T. Krovetz, P. Rogaway, ”The OCB Authenticated-Encryption Algorithm,” RFC7253, 2014.

[4] STMicroelectronics, ”Datasheet - STM32L562xx - Ultra-low-power ARM Cortex-M33 32-bit MCU+TrustZone+FPU, 165DMIPS, up to 512KB Flash, 256KB SRAM, SMPS, AES+PKA (DS12736),” `https://www.st.com/resource/en/datasheet/stm321562re.pdf`, 2020.

[5] A. Adomnicai, T. Peyrin, ”Fixslicing AES-like Ciphers: New Bitsliced AES Speed Records on ARM-Cortex M and RISC-V,” TCHES, vol. 2021(1), pp. 402-425, 2020.