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

NIST 軽量暗号最終候補におけるソフトウェア実装性能の評価
Performance Evaluation of Software Implementation for the NIST Lightweight Cryptography Finalists

北原 知明 * 日良 僚太 * 原 祐子 † 宮原 大輝 * 李 陽 *
Tomoaki Kitahara Ryota Hira Yuko Hara-Azumi Daiki Miyahara Yang Li
崎山 一男 *
Kazuo Sakiyama

キーワード 軽量暗号，認証付き暗号，ブロック長，レイテンシ，スタック，スループット

あらまし

今日，Internet of Things（IoT）化が進み，様々な電子機器がネットワークに接続されるようになった．そのため，暗号に使用できる回路サイズやメモリサイズに制限がある環境で動く，安全で実装性の高い軽量暗号アルゴリズムがセキュリティ対策において重要である．軽量暗号は従来の共通鍵暗号 AES 暗号と同等の安全性を保ち，レイテンシやメモリサイズなど特定の性能指標で優位になるように設計される [1]．したがって，軽量暗号は使用されるデバイスやシナリオに合わせた性能の暗号を選定することで効率よく利用できる．本研究では使用するシナリオやデバイスに適した軽量暗号を選定するために，NIST で選定中の最終 10 候補 [2] についてレイテンシとメモリサイズ（RAM）の観点から性能比較ならびに特徴分析を行う．

最終 10 候補の暗号アルゴリズムに対してソフトウェア実装を行い，レイテンシとスタック/ヒープを測定した．各候補の測定結果は，NIST に提出された仕様書とサンプルコードをもとに性能に影響を与える要因を調査した．

測定の結果，レイテンシは入力データ長に比例して増加する傾向があった．他方，スタック使用量に関しては入力データ長と関連なくほぼ一定であった．スタック使用量とレイテンシの散布図は図 1 のようになり，弱い正の相関関係が見られた．調査の結果，ステート長をはじめとするパラメータの長さよりも他の変数やコーディングによる差の方がスタック使用量に大きな影響を与えていることが分かった．

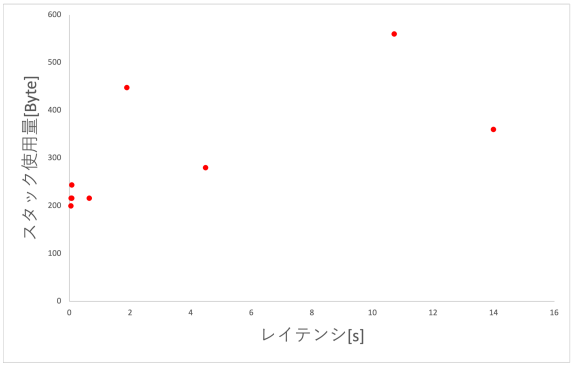

図 1: レイテンシとスタック使用量の関係

参考文献

[1] “暗号技術技術調査．WG（軽量暗号）報告書,” https://www.cryptrec.go.jp/exreport/cryptrec-ex-2406-2014.pdf，CRYPTREC，Mar. 2015

[2] “Submission Requirements and Evaluation Criteria for the Lightweight Cryptography Standardization Process,” https://csrc.nist.gov/CSRC/media/Projects/Lightweight-Cryptography/documents/final-lwc-submission-requirements-august2018.pdf，NIST，Aug. 2018

* 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.
† 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， Tokyo 152-8552， Japan.