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

SABER における数論変換のC言語実装
C Language Implementation of Number Theoretic Tranform in Saber

青木 大地 * 峯松 一彦 * 岡村 利彦 * 高木 剛 †
Daichi Aoki Kazuhiko Minematsu Toshihiko Okamura Tsuyoshi Takagi

キーワード 数論変換，格子暗号，Saber

あらまし

現在，米国標準技術研究所による耐量子計算機暗号の標準化計画が進められており複数の格子暗号が最終候補に残っている [1]．Saber [3] は最終候補のひとつであり，Module-LWR 問題の計算量的困難性に基づく格子暗号である．Saber のような多項式環を利用した格子暗号では多項式乗算の効率が重要となる．高速な多項式乗算アルゴリズムとしては Karatsuba 法，Toom-Cook 法，数論変換 (NTT) などが知られており，漸近的計算量としては NTT が最も小さい．Saber は 2 冪の整数を法とする剰余環を用いるため多項式乗算に NTT が使えずリファレンスでは Toom-Cook 法に基づき実装されている．しかし Chung らにより Saber に NTT を導入する手法が提案された [2]．Chung らはこの手法の Cortex-M4 におけるアセンブリ実装を公開しているが C 言語のみの実装は公開されていない．本研究では Chung らの手法を C 言語のみで実装し，Cortex-M3/M4，RISC-V マイコン上でリファレンス実装の Saber と比較しある程度の高速化を達成した（表 1）．

表 1　多項式乗算における数論変換と Toom-Cook 法の比較．多項式 $a, b \in (\mathbb{Z}/2^{13}\mathbb{Z})[x]/(x^{256}+1)$ の乗算にかかった CPU サイクル数 ($\times 10^3$) を示す．ただし a, b の係数の大きさはそれぞれ 13 ビット，3 ビットである．

	K210	F104RB	F411RE
my-NTT	143	219	184
ToomCook	184(+30%)	298(+36%)	212(+15%)

K210: 64bit RISC-V dual core/600MHz
F103RB: ARM Cortex-M3 32bit/72MHz
F411RE: ARM Cortex-M4 32bit/100MHz

参考文献

[1] Gorjan Alagic, Jacob Alperin-Sheriff, Daniel Apon, David Cooper, Quynh Dang, John Kelsey, Yi-Kai Liu, Carl Miller, Dustin Moody, Rene Peralta, et al. Status Report on the Second Round of the NIST Post-Quantum Cryptography Standardization Process. *NIST, Tech. Rep., July*, 2020.

[2] Chi-Ming Marvin Chung, Vincent Hwang, Matthias J. Kannwischer, Gregor Seiler, Cheng-Jhih Shih, and Bo-Yin Yang. NTT Multiplication for NTT-unfriendly Rings: New Speed Records for Saber and NTRU on Cortex-M4 and AVX2. *IACR Transactions on Cryptographic Hardware and Embedded Systems*, Vol. 2021, No. 2, pp. 159–188, Feb. 2021.

[3] Jan-Pieter D' Anvers, Angshuman Karmakar, Sujoy Sinha Roy, and Frederik Vercauteren. Saber: Module-LWR based key exchange, CPA-secure encryption and CCA-secure KEM. In *International Conference on Cryptology in Africa*, pp. 282–305. Springer, 2018.

* 日本電気セキュアシステム研究所, 〒211-8666 神奈川県川崎市中原区下沼部 1753, NEC Corporation, 1753 Shimonumabe,Nakahara-ku, Kawasaki, Kanagawa 211-8666, Japan
† 東京大学大学院情報理工学系研究科数理情報学専攻, 〒113-8656 東京都文京区本郷 7-3-1, Department of Mathematical Informatics, University of Tokyo, 7-3-1 Hongo, Bunkyo-ku, Tokyo 113-8656, Japan.