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

耐量子計算機署名 Mod Falcon の Toom-Cook 法及び Radix4 FFT による高速化
Fast Implementation of Post Quantum Signature Mod Falcon with Toom-Cook Method and Radix4 FFT

福原 大毅 * Daiki Fukuhara
高橋 雄人 † Yuto Takahashi
山村 和輝 ‡ Kazuki Yamamura
齋藤 恆和 ‡ Tsunekazu Saito
横山 俊一 † Shunichi Yokoyama

キーワード 格子暗号, ModFalcon, Toom-Cook 法, Radix4 FFT

あらまし

耐量子計算機署名として Chuengsatiansup らによって Mod Falcon[1] が提案されている. Mod Falcon は, 現在 NIST のコンペティションの最終ラウンドに残っている Falcon をベースとしており, module 格子を組み込むことで, 署名サイズを小さくすることができる. しかし,Mod Falcon はスクリプト実装での評価のみで, 実環境での評価がされていない. また, スクリプト実装での評価では, 多項式乗算を Karatsuba 法や FFT による基本的な実装のみで, 高速化を検討していない. そこで本稿では, 高速な多項式乗算を実現する,Toom-Cook 法や Radix4 FFT を組み込んだ Mod Falcon の実環境での評価を行った.

参考文献

[1] Chitchanok Chuengsatiansup, Thomas Prest, Damien Stehlé, Alexandre Wallet,and Keita Xagawa, “ModFalcon: compact signature based on NTRU lattices”,ASIA CCS’20: The 15th ACM Asia Conference on Computer and Communications Security, pages 853–, october 2020

* 東京都立大学 〒 192–0397 東京都八王子市南大沢 1–1. Tokyo Metropolitan University, 1–1 Minamiosawa, Hachioji, Tokyo, 192-0397,Japan. fukuhara-daiki@ed.tmu.ac.jp
† 東京都立大学 〒 192–0397 東京都八王子市南大沢 1–1. Tokyo Metropolitan University, 1–1 Minamiosawa, Hachioji, Tokyo, 192-0397, Japan.
‡ NTT 社会情報研究所 〒 180–8585 東京都武蔵野市緑町 3–9–11. NTT Social Informatics Laboratories, 3–9–11 Midoricho,Musashino,Tokyo,180-8585,Japan.