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

格子暗号におけるノイズの数論変換の実装について
On Implementation of the Number Theoretic Transform for Noise in Lattice-based Cryptography

米村 智子 * 秋山 浩一郎 *
Tomoko Yonemura Koichiro Akiyama

キーワード 耐量子計算機暗号、ポスト量子暗号、格子暗号、格子署名、数論変換、事前計算、高速化

あらまし

有望な耐量子計算機暗号のひとつに格子暗号がある。格子暗号は実行サイクル数と鍵サイズのバランスの取れた方式であるが、普及に向けた課題のひとつにソフトウェア実装における更なる高速化がある。格子暗号の実行サイクル数において大きな割合を占めるのは数論変換および数論逆変換と呼ばれる多項式の演算とハッシュ関数計算である。本稿では数論変換に着目する。RLWE 問題および MLWE 問題に基づく格子暗号では、秘密鍵とノイズに数論変換を行い、その後の多項式乗算を高速に実行し、最後に数論逆変換を行って公開鍵と暗号文を得る。数論変換の入力は秘密鍵とノイズという制約された多項式である。そこで、制約を用いて数論変換における多項式の係数の剰余乗算を事前計算することを提案する。数論逆変換の入力は任意の多項式なので、数論逆変換には提案手法は適用できない。提案手法により数論変換を高速化し、格子暗号における鍵生成と暗号化、および KEM における、鍵生成、鍵カプセル化、鍵デカプセル化を高速化する。

* 株式会社東芝 研究開発センター サイバーセキュリティ技術センター, 212-8582 川崎市幸区小向東芝町 1. Toshiba Corporation Corporate Research & Development Center Cyber Security Technology Center, 1 Komukai-Toshiba-cho, Saiwai-ku, Kawasaki, 212-8582, Japan. tomoko.yonemura@toshiba.co.jp