修士学位論文要約（令和４年３月）

格子暗号向け高効率数論変換ハードウェアに関する研究

板橋　由磨
指導教員：本間 尚文

Efficient Number Theoretic Transform Hardware for Lattice-Based Cryptography

Yuma ITABASHI
Supervisor: Naofumi HOMMA

This paper presents a hardware design that efficiently performs the number theoretic transform (NTT) for lattice-based cryptography. First, we propose an efficient modular multiplication method for lattice-based cryptography defined over Proth numbers. The proposed method is based on a K-RED technique specific to Proth numbers. In particular, we divide the intermediate result into the sign bit and the other absolute value bits and handles them separately to significantly reduce implementation costs. Then, we show a butterfly unit datapath of NTT and inverse INTT equipped with the proposed modular multiplier. We apply the proposed NTT accelerator to Crystals-Kyber, which is lattice-based cryptography, and evaluate its performance on Xilinx Artix-7. The results show that the proposed NTT accelerator is about 3.8 times more efficient in terms of area-time product (ATP) in LUT than existing methods.

1. はじめに

現在、秘匿通信や電子署名を実現するためにRSA 暗号や楕円曲線暗号などの公開鍵暗号が広く用いられている。これらの公開鍵暗号は大規模な量子計算機の実現により、危殆化が懸念されている。そのため、量子計算機を用いた暗号解読に対しても安全性を確保できる耐量子計算機暗号 (PQC: Post-Quantum Cryptography) への移行が強く推奨されている。PQC の代表例として格子暗号が挙げられる。その中でも LWE 暗号は計算時間と鍵長・通信量のバランスの良さから注目されており多くの方式が提案されている。本研究では Module-LWE 暗号の Crystals-Kyber に着目し、そのハードウェア実装の効率化を検討する。Module-LWE 暗号では数論変換が主要な演算となるため、数論変換 (NTT: Number Theoretic Transform) の効率化が重要となる。特に剰余演算の実装方法によって効率が大きく変化する。本研究では数論変換内の乗算に対する剰余演算として、低コストな剰余演算 K-RED[1] を応用した「符号テーブル参照型 2 重 K-RED」を提案する。

2. NTT を用いた剰余多項式環上の乗算

NTT は有限体上のフーリエ変換であり、格子暗号においては剰余多項式環上の乗算の計算量を減らすために用いられる。NTT を用いて 2 つの多項式を周波数領域上の表現に変換し、周波数領域で要素ごとの乗算 (PWM: Pointwise Multiplication) を行う。その後、逆数論変換 (Inverse NTT) を用いてもとの多項式表現に戻すことで乗算結果を得ることができる。通常の多項式乗算の計算量は $O(N^2)$ であるが、高速フーリエ変換と同様にバタフライ演算を用いた NTT を利用することで O(NlogN) まで抑えることができる。バタフライ演算内で行われる剰余演算の実装方法によって暗号全体の効率が大きく変化する。

3. 既存の剰余演算

加減算に対する剰余演算は簡単な分岐によって実装が可能である。一方、乗算に対する剰余演算は一度 2 倍に増えたビット幅を半分まで削減する必要があるため、分岐のみでの実装は難しい。Barrett Reduction や Montgomery Reduction といった既存の乗算に対する剰余演算のほとんどでは計算コストの大きい定数乗算が必要となる。剰余演算内で乗ずる定数が小さいほど、また定数乗算の回数が少ないほど効率的な剰余演算といえる。法素数がプロス数であるときにのみ利用可能な剰余演算 K-RED は定数乗算が小さい定数 k による乗算 1 回のみで済む低コストな剰余演算である。Kyber の法素数はプロス数であるため、K-RED の利用が可能である。しかし、K-RED はソフトウェア実装としての提案のため、乗算に対する剰余演算としてはビット削減が不十分であった。

4. 提案剰余演算 符号テーブル参照型 2 重 K-RED

本研究では乗算結果に対する剰余演算として K-RED を拡張した符号テーブル参照型 2 重 K-RED を提案する。図 1 に提案剰余乗算のブロック図を示す。提案手法では K-RED 1 回では不十分だった乗算結果へのビット幅削減を、再度の K-RED 適用により可能にする。ここで、2 回目の K-RED 適用の際は 1 回目の K-RED の出力が負となる可能性を考慮する

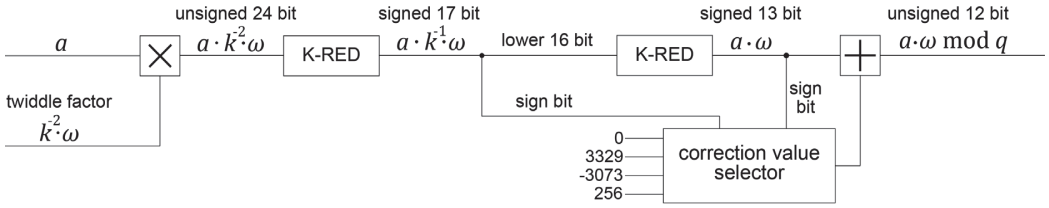

図 1　提案剰余演算 符号テーブル参照型 2 重 K-RED による剰余乗算

表 1　提案 NTT/INTT ハードウェアの性能評価

Work	NTT/INTT Cycles	Freq [MHz]	Time [μs]	Area / Area Time Products			
				LUTs	FFs	DSPs	BRAM
Yarman et al.[2]	904/904	190	3.18	948/4,512	352/1,676	1/4.76	2.5/11.90
This work (Radix-2 arch.)	902/902	208	4.34	274/1,190	181/786	1/4.34	1.5/6.51
This work (2xRadix-2 arch.)	455/455	216	2.11	538/1,133	417/879	2/4.21	2.5/5.27
This work (Radix-4 arch.)	268/268	216	1.24	904/1,122	811/1,006	4/4.96	2.5/3.10

必要がある。提案手法では 1 回目の K-RED 出力を符号ビットとその他のビットに分割し、再度それぞれに K-RED を適用する。符号付き整数の 2 の補数表現においては符号ビットのみが負の要素となるため、符号ビットに対する K-RED のみ別処理をすることで符号付き演算を回避できる。さらにこの際に符号ビットに対する K-RED の結果は事前計算して LUT に保存しておき、符号ビットの値によって結果を選択させることで計算コストの削減を図る。その後、それぞれの 2 回目の K-RED 出力を加算して、法素数 q の定数倍の加算による補正を行い、剰余演算を完了する。ここで、補正値は 2 回目の K-RED 出力の加算結果をもとに LUT を用いて選択されることに着目し、提案手法では同じく LUT を用いて行われる符号ビットへの K-RED 適用を補正値決定プロセスに統合することで 2 回目の K-RED 出力の加算を省略する。

5. 提案剰余演算による NTT/INTT ハードウェアの性能評価

表 1 に提案剰余演算を用いた NTT/INTT ハードウェアの実装結果を示す。実装対象は Xilinx 社の FPGA Artix-7 (XC7A100TFGG676-3) である。論理合成には Vivado 2020.2 を使用した。実装アーキテクチャは並列実行するバタフライ数によって、Radix-2 アーキテクチャ、2 並列 Radix-2 アーキテクチャ、Radix-4 アーキテクチャの 3 つに分けられる。表 1 には比較のために Yarman らの手法[2]の値を併記している。Yarman らの手法と比較すると提案手法は面積遅延積効率の点で LUT において 3.8 倍、FF において 2.1 倍、DSP において 1.1 倍、BRAM において 2.3 倍高効率である。これは、乗算に対する剰余演算のコストが Yarman らの手法では加減算 10 回であるのに対し、提案手法では加減算 7 回に抑えられていることによるものだと考えられる。

6. まとめ

低コストな剰余演算 K-RED を拡張した符号テーブル参照型 2 重 K-RED による格子暗号向け NTT/INTT ハードウェアを設計し、FPGA 上での評価により、提案手法の有効性を示した。面積遅延積の観点で提案手法は従来手法よりも最大 3.8 倍高効率であることを確認した。

文献

1) P. Longa and M. Naehrig, “Speeding up the Number Theoretic Transform for Faster Ideal Lattice-Based Cryptography,” in Cryptology and Network Security, S. Foresti and G. Persiano, Eds. Cham: Springer International Publishing, 2016, pp. 124–139.

2) F. Yarman, A. C. Mert, E. Ozt¨urk, and E. Sava¸s, “A Hardware Accelerator for ¨ Polynomial Multiplication Operation of CRYSTALS-KYBER PQC Scheme,” in 2021 Design, Automation Test in Europe Conference Exhibition (DATE), 2021, pp. 1020–1025.