修士学位論文要約（令和２年３月）

同種写像暗号のハードウェア実装に関する研究

船越　秀隼
指導教員：本間　尚文

Hardware Architecture for Isogeny Based Cryptography

Shuto FUNAKOSHI
Supervisor: Naofumi HOMMA

Currently, public key cryptography such as RSA and elliptic curve cryptography (ECC) are widely used. These conventional cryptography are based on difficult problems such as prime factorization problems and (elliptic) discrete logarithm problems. On the other hand, quantum computers have been rapidly developed, and in 1994, a quantum algorithm called Shor's algorithm that can calculate prime factorization problems in polynomial time was discovered. Along with this, attention has been focused on post-quantum cryptography (PQC), which is difficult to break even with quantum computers. Isogeny-based cryptography has been applied for NIST standardization. Isogeny-based Cryptography is a PQC with a relatively short key length, and a method to further shorten the key length by compressing the public key has been reported. Isogeny-based cryptography has a problem that it requires more computation (execution time) than other PQC. This paper proposes a low-latency and efficient hardware architecture for isogeny-based cryptography, and shows its effectiveness by implementation evaluation.

1. はじめに

現在一般的に利用されている公開鍵暗号は，素因数分解問題や離散対数問題を安全性の根拠としている．近年，量子計算機の開発が活発に行われており，公開鍵暗号への影響が懸念されている．米国の NIST (National Institute of Standards and Technology) により，2030 年までに従来の暗号を解読できる規模の量子計算機が実現する可能性が指摘されており，耐量子計算機暗号 (PQC: Post-Quantum Cryptography) の研究が急務となっている．PQC は耐量子性を持つ一方で，その暗号方式の多くは鍵長が従来よりも非常に長くなるという欠点を持っている．IoT や組込み機器では暗号処理よりも通信の際に電力を消費するため，鍵長が短く，通信量の小さい暗号方式が必要とされている．PQC の中で最も鍵長の短い暗号方式として同種写像暗号が提案されているが，一方で処理が重く実行時間が長いという側面もあり高速化が必要となっている．ハードウェア実装は既存研究で報告されているが，同種写像暗号へ適したアーキテクチャとは言えず，最適化も十分ではない．そこで，本研究では同種写像暗号へ最適化したハードウェアアーキテクチャを提案する．

2. 同種写像暗号

同種写像暗号はいくつか暗号方式が提案されている．SIDH (Supersingular Isogeny Diffie-Hellman) 鍵交換や SIKE (Supersingular Isogeny Key Encapsulation)，また電子署名などが提案されている [1]．同種写像暗号では，同種写像と呼ばれる写像を次々とランダムに適用し，その写像の経路を暗号の秘密情報とする．同種写像暗号の処理では二次拡大体での有限体演算を利用する．また，有限体の標数が従来の暗号方式よりも大きいため，暗号処理の 8 割以上を有限体乗算が占めている．そのため，剰余乗算の効率化が必要である．既存研究ではシストリックアレイ型などの乗算器を並列実装することで高速化を図っている．しかし，同種写像暗号は演算の依存関係が非常に強いという特徴があるため，シストリックアレイ型の並列実装は適しているとは言えない．そのため，1 回あたりの乗算を低遅延に行うことのできる乗算器が求められている．

3. 剰余数系を利用したハードウェアアーキテクチャ

剰余数系 (RNS: Residue Number System) は整数の表現方法の一つであり，剰余乗算器の効率化手法として利用される．RNS では互いに疎な整数の組で割った余りで数を表現する．互いに疎な整数の組のことを基底と呼ぶ．RNS を用いると小さいビットの組で整数を表現できるため，演算器のビット幅を小さくすることができ，ハードウェアの動作周波数が向上する．RNS で剰余を直接行うのはコストが大きいため，一般的にはモンゴメリ乗算を利用して剰余乗算を実現する．RNS 上でのモンゴメリ乗算には効率化手法が多数提案されており，2018 年には Q-RNS と呼ばれる，現在最も効率的な手法が報告された．Q-RNS を利用した

表 1 提案ハードウェアの実装評価

Work	基底数	並列度	#LUTs	#DSPs	動作周波数 [MHz]	乗算時間 [ns]	SIDH 実行時間 [ms]
Koziel et al. [2]	-	-	23,483	256	202.5	642	15.2
This Work	9	2	23,886	225	334.0	200	(17.5)
	10	2	24,543	250	327.4	211	11.5 (18.2)
		3	29,911	370	250.1	211	(19.5)
		6	45,660	730	248.7	165	(16.4)
		11	73,937	1,330	303.5	131	(13.1)

ハードウェアは今まで報告されていないため，本研究で Q-RNS のハードウェアアーキテクチャを提案する．

提案ハードウェアは Cox-Rower アーキテクチャと呼ばれる構造で，概略図を図 1 に示す．Cox はモンゴメリ乗算の際に利用するもので，Rower ではチャネル毎に並列に演算を行う．次に，Rower の最適化について述べる．Rower のブロック図を図 2 に示す．同種写像暗号では二次拡大体乗算を多用し，その効率化手法として Karatsuba 法が知られている．PreAdder や Acc，ConstMul は Karatsuba 法をハードウェアで効率的に計算するためのモジュールである．また，RNS では基底毎による剰余を低コストで行うために，基底として疑似メルセンヌ数を用いる．疑似メルセンヌ数による剰余演算は効率的に行う方法が知られており，2 つの段階に分けられる．その 2 つの段階がそれぞれ L1mod と L2mod に対応する．BaseExt は基底拡張と呼ばれる計算を行うモジュールである．基底拡張は基底数の数だけ乗算を行う必要がありクロックサイクル数が増大するため，BaseExt の乗算器をスケーラブルに並列化する仕様とすることで，低面積実装から高速実装まで実装することができる．

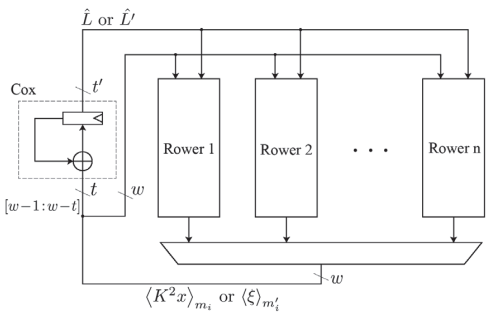

図 1　提案ハードウェアアーキテクチャの概略図

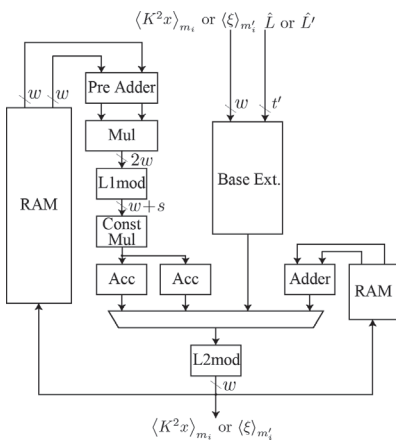

図 2　Rower のブロック図

4. 実装評価

Xilinx 社の FPGA である Kintex Ultrascale+に提案ハードウェアを実装し，既存手法との比較を行った．その結果を表 1 に示す．乗算時間は二次拡大体乗算に掛かる時間を表し，SIDH 実行時間は SIDH 鍵交換の計算に掛かる時間を表している．提案ハードウェアは基底数 10，並列度 2 の場合のみ SIDH 全体の実装ができているため，その他については見積もり（実行時間の上限値）を括弧で示している．二次拡大体乗算においては，どの基底数や並列度でも既存手法より乗算時間が改善するという結果が得られた．また，SIDH 全体においては，基底数 10，並列度 2 の場合は既存手法と同程度の面積で実行時間が改善するという結果が得ら，提案ハードウェアの有効性が示された．

5. まとめ

本研究では，同種写像暗号向けの高効率なハードウェア実装について，剰余数系を利用したアーキテクチャの提案を行った．また，既存手法との実装比較を行い，その有効性を確認した．今後，提案ハードウェアの耐タンパ性の評価を行うことが考えられる．

文献

1) David Jao et al., “Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies,” In International Workshop on Post-Quantum Cryptography, pp. 19-34, 2011.
2) Brian Koziel et al., “A high performance and scalable hardware architecture for isogeny-based cryptography,” IEEE Transactions on Computers, Vol. 67, No. 11, pp. 1594-1609, 2018.