様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

令和　６ 年　 ６ 月 １２ 日現在

機関番号：８２６２６
研究種目：若手研究
研究期間：2022～2023
課題番号：２２Ｋ１７８９３

研究課題名（和文）クラウドFPGAにおける限界性能に達するセキュア高機能暗号回路の開発

研究課題名（英文）Development of Secure Advanced Cryptographic Circuits Pushing the Limit in Cloud FPGAs

研究代表者
坂本　純一（Sakamoto, Junichi）

国立研究開発法人産業技術総合研究所・情報・人間工学領域・研究員

研究者番号：７０９０９７１２

交付決定額（研究期間全体）：（直接経費）　　3,400,000円

研究成果の概要（和文）：本研究では、クラウドFPGAの最大性能を発揮する高機能暗号実装を行った。特にBN254及びBLS12_381曲線状のペアリング暗号の高速実装法を提案し、リソース利用率9割という極限環境であっても400MHz程度の高周波数を維持し、先行研究と比較して2～5倍のスループットを達成した。
研究成果は国内学会で発表し、また国際論文誌IEEE TVLSIに採択された。

研究成果の学術的意義や社会的意義
高機能暗号のFPGA実装の従来研究の多くにおいて，FPGA回路リソースの数%から数十%程度しか使用しておらず，回路リソースを全て消費した際の性能について評価した研究は少ない．また従来研究の多くは100～250MHz程度で動作する実装を提案しており，FPGAの最大動作周波数に迫る性能を発揮する実装も少ない。本研究は，これまでのコストパフォーマンス重視の研究の流れとは異なり，大規模FPGAにおける高機能暗号の性能限界を明らかにすることで，AWS (Amazon WebServices)などの巨大なFPGAをユーザーが利用できるクラウドサービスにおける高機能暗号の普及を促進させるという側面を持つ．

研究成果の概要（英文）：In this research, we have developed a high-performance cryptographic implementation that maximizes the performance of cloud FPGAs. In particular, we proposed a fast implementation method of BN254 and BLS12_381 curvilinear pairing ciphers, and achieved throughput 2 to 5 times higher than previous studies, maintaining a high frequency of about 400 MHz even in an extreme environment with 90% resource utilization.
The research results were presented at a national conference and accepted for publication in the international journal IEEE TVLSI.

研究分野：情報セキュリティ

キーワード：高機能暗号　ペアリング　BN254　BLS12

１．研究開始当初の背景

高機能暗号と呼ばれる最先端の暗号技術が，ビッグデータ時代の多くの課題を解決するものとして期待されている．高機能暗号とは，暗号化・署名などの基本的な機能に加えて何らかの付加機能を持った暗号技術のことであり，多くの有用な付加機能を持つ代わりに従来の暗号技術と比べて計算量が多いため，専用設計されたハードウェアを使った高速な実装による実用化が期待されている．高機能暗号は発展途上の段階であり効率的なプロトコルやパラメータが次々と更新されるため，製造時に機能が固定される ASIC（Application Specific Integrated Circuit）よりも運用中に機能の変更が可能な FPGA による実装が適しており，FPGA を用いた高機能暗号実装の研究が盛んである．

２．研究の目的

本研究の目的は，「クラウド FPGA の性能限界に迫る超高性能・耐タンパー高機能暗号回路アーキテクチャを開発する」ことである．従来の研究の多くは，回路リソース当たりの性能向上を目指したコストパフォーマンス重視の小規模回路アーキテクチャを提案しており，FPGA の性能を最大限活用できていない．

３．研究の方法

高機能暗号は基本的に素数体上の代数演算で構成されるため，剰余乗算及び剰余加算がプリミティブ演算となり高速化のターゲットである．剰余乗算のほうが多くの計算量を要することが一般的であるため，まず FPGA の限界性能を発揮する剰余乗算器を開発し，そののちに剰余加算他の必要な演算器を開発するアプローチをとった．

また一つの暗号演算器で膨大なクラウド FPGA の全リソースを消費することは困難であるため，演算器をマルチスレッド・マルチコア対応にすることで FPGA リソースを最大限利用した最大スループット性能を目指した．

４．研究成果

一つ目の成果として，クラウド FPGA 上の DSP 機能を最大限活用した剰余乗算器アーキテクチャ（図１）を開発し，先行研究と比較して 10~100 倍のスループットを達成した．回路規模当たりの性能で比較しても先行研究を数倍上回っている．本アーキテクチャのアイデアとしては、FPGA 上の LUT や FF 素子を極力排除して DSP だけで剰余乗算器を構成することである．これにより無駄な遅延が減少し，結果として 600MHz 級の高い動作速度を達成することができた．

二つ目の成果として，開発した剰余乗算器を使ったペアリング暗号アーキテクチャ（図２）を開発した．本アーキテクチャは、高機能暗号に頻出する２次拡大体演算を高速化するために剰余乗算器の前後に専用の剰余加算器を直接に接続した形になっている．高速化のポイントとして，我々は剰余乗算器をなるべく DSP だけで構築しているため，剰余加算器には大量のスライスリソースを割くことができる．FPGA の全リソースを消費することを考えた場合，使用量よりもむしろ割合が重要になるため，全リソースに対する割合が DSP に対するそれを越えなければ実質的にゼロコストである．そこで我々は剰余加算器部分にパイプラインと冗長加算器を積極的に利用し，動作周波数を向上させた．全体として 100 段程度の深い構成となるが，複数のトランザクションをインターリーブ実行する機能を搭載することで，スループット性能を向上させた．結果として先行研究の 2~5 倍のスループットを達成し，これらの結果を IEEE TVLSI で発表している．

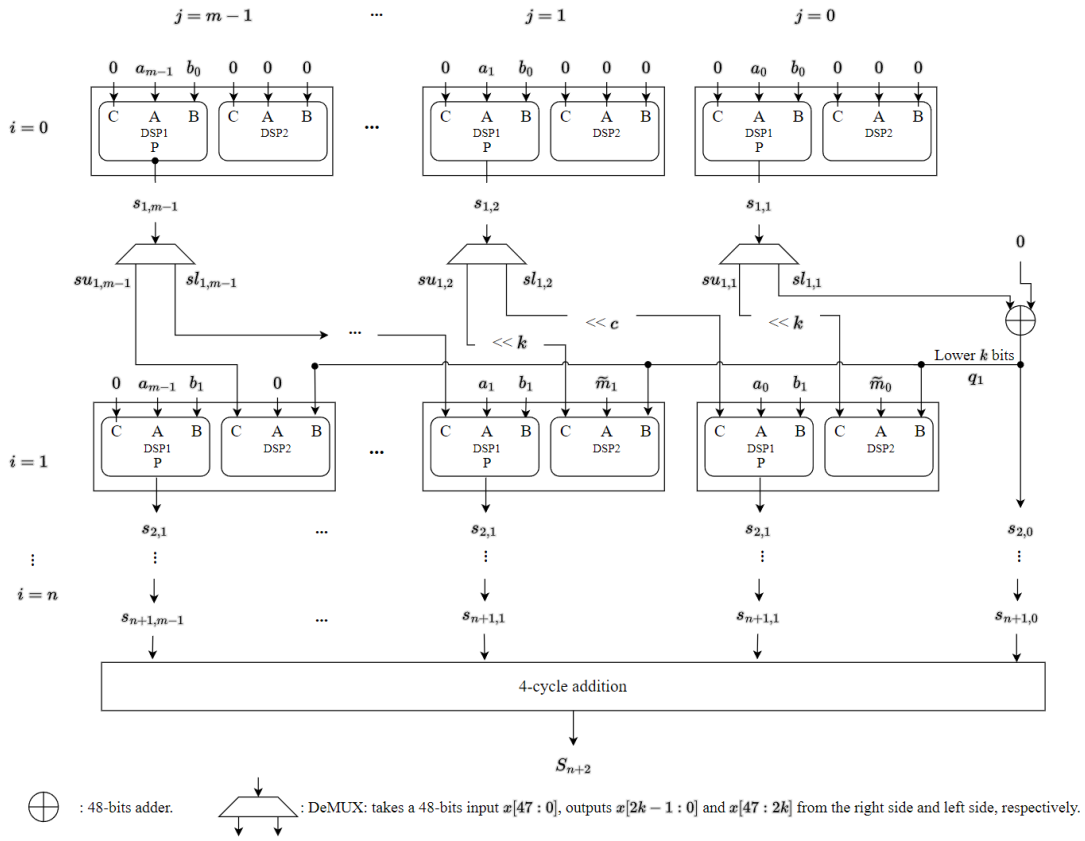

図 1 開発した高スループット剰余乗算器アーキテクチャ．DSP の機能を最大限利用することで，LUT, FF 利用による性能低下を防いでいる．

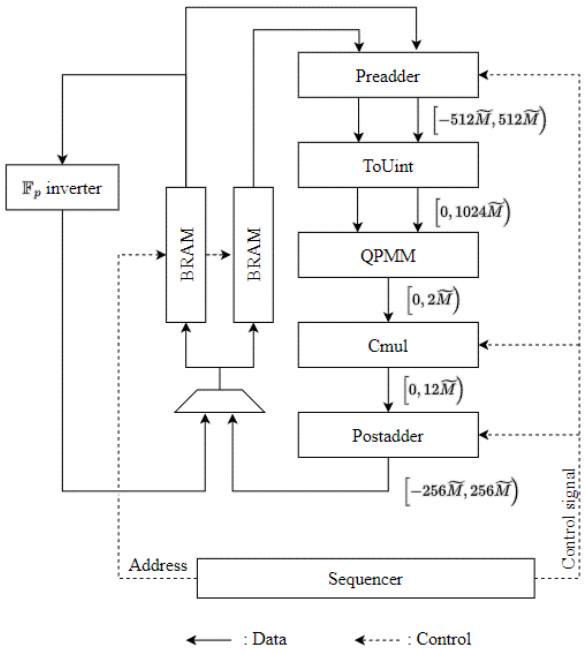

図 2 開発したペアリング演算アーキテクチャ．剰余加算器に大量の LUT, FF を利用することで最大限の性能を発揮している．

５．主な発表論文等

〔雑誌論文〕　計1件（うち査読付論文　1件／うち国際共著　0件／うちオープンアクセス　1件）

１．著者名 Sakamoto Junichi、Fujimoto Daisuke、Anzai Riku、Yoshida Naoki、Matsumoto Tsutomu	４．巻 -
２．論文標題 High-Throughput Bilinear Pairing Processor for Server-Side FPGA Applications	５．発行年 2024年
３．雑誌名 IEEE Transactions on Very Large Scale Integration (VLSI) Systems	６．最初と最後の頁 1～14
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/TVLSI.2024.3402164	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

〔学会発表〕　計1件（うち招待講演　0件／うち国際学会　0件）

１．発表者名 坂本 純一 、安西 陸、 吉田 直樹、松本 勉
２．発表標題 サーバーアプリケーション向け高スループット FPGA 剰余乗算器と そのペアリング暗号への応用
３．学会等名 2023年暗号と情報セキュリティシンポジウム
４．発表年 2023年

〔図書〕　計0件

〔産業財産権〕

〔その他〕

－

６．研究組織

	氏名 （ローマ字氏名） （研究者番号）	所属研究機関・部局・職 （機関番号）	備考

７．科研費を使用して開催した国際研究集会

〔国際研究集会〕　計0件

８．本研究に関連して実施した国際共同研究の実施状況

共同研究相手国	相手方研究機関