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

BLS12-381 曲線上ペアリング計算の低レイテンシ FPGA 実装
Low-latency Hardware Implementation of BLS12-381 Pairing

安西 陸* 坂本 純一*† 宋 子豪* 吉田 直樹* 松本 勉*
Riku Anzai Junichi Sakamoto Zihao Song Naoki Yoshida Tsutomu Matsumoto

キーワード IoT ネットワーク，ペアリング，高機能暗号, FPGA 実装

あらまし

今後さらに複雑化すると見込まれる IoT(Internet of Things)ネットワークのセキュリティ要求に応えるため，暗号文のまま検索を行うことのできる検索可能暗号や複数の署名データをひとまとめに集約しデータ量を圧縮することのできる集約署名[1]などといった高機能暗号の活用が期待されている．高機能暗号は楕円曲線上の点のペアリングという複雑な演算を用いて構成されるものが多く，ペアリングの計算時間が高機能暗号実用化のための課題である．これまで，ソフトウェア・ハードウェアの両面からペアリング計算高速実装の研究が行われている．特にサーバでの高機能暗号の利用を考えると，専用ハードウェアが有用であり使用する回路規模は多いとしても高速な実装が必要になると考えられる．そのため本研究ではサーバサイドのアプリケーションに着目し，専用ハードウェアによる高速化を目指す．我々は高速なペアリング計算を，パイプライン型の剰余乗算器を用いることにより，FPGA 上で実装する手法を提案した[2, 3]．現在，BN12-254 曲線上の Optimal Ate ペアリングの FPGA 実装においては，報告[2]の実装を改良した我々の実装[3]が他手法と比べて計算時間が短く高速である．本報告では図 1 のようなペアリング計算器に用いられている 13 段パイプライン剰余乗算器を 2020 年に Ozturk[4]らが提案した冗長 2 進表現を用いた低遅延剰余乗算アルゴリズムを 13 段パイプライン化して構成した剰余乗算器に置き換えた際のペアリング計算器の FPGA 実装の性能を評価する．また，提案手法のペアリング計算器を BN12-254 曲線上の Optimal Ate ペアリングに利用した際の性能について評価し，さらに BN12-254 曲線上の Optimal Ate ペアリングの FPGA 実装を BLS12-381 曲線上のペアリングが行えるように計算単位を 384bit に変更した際の性能評価を行う．

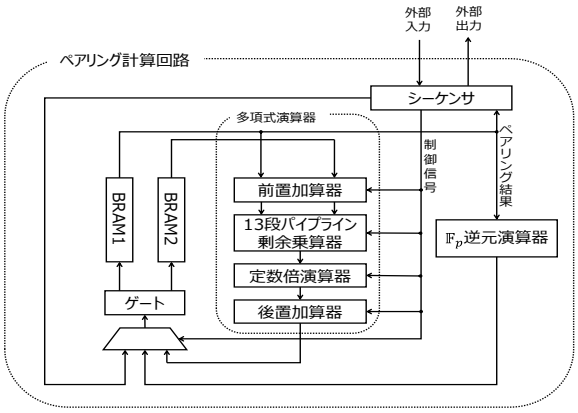

図 1. ペアリング計算回路の構成

* 横浜国立大学 〒240-8501 横浜市保土ヶ谷区常盤台 79-7
Yokohama National University, 79-7 Tokiwadai,, Hodogaya-ku, Yokohama 240-8501, Japan
† 国立開発法人産業総合研究所, 〒135-0064 東京都江東区青海 2-3-26
National Institute of Advanced Industrial Science and Technology, 2-3-26 Aomi, Koto-ku, Tokyo 1350-0064, Japan

本研究の一部は，内閣府が進める戦略的イノベーション創造プログラム（SIP）「IoT 社会に対応したサイバー・フィジカル・セキュリティ」（管理法人：NEDO）によって実施されたものである．

参考文献

[1] Aggregate and Verifiably Encrypted Signatures from Bilinear Maps. In Eli Biham, editor, Advances in Cryptology - EUROCRYPT 2003, volume 2656 of LNCS, pages 416–432. Springer, 2003.

[2] 藤本大介，坂本純一，奥秋陽太，吉田直樹，松本勉，“最先端暗号のハードウェア実装，”DA シンポジウム 2018，2018

[3] Sakamoto, Junichi, et al. "Low-latency pairing processor architecture using fully-unrolled quotient pipelining montgomery multiplier." 2019 Asian Hardware Oriented Security and Trust Symposium (AsianHOST). IEEE, 2019.

[4] Öztürk, Erdinç. "Design and implementation of a low-latency modular multiplication algorithm." IEEE Transactions on Circuits and Systems I: Regular Papers 67.6 (2020): 1902-1911.