ペアリング演算の安全性およびハードウェア実装コストの自動設計手法による見積もり評価

Estimating Pairing Security and Hardware Implementation Cost by Design Automation Technique

東大工[1]，○福田桃子[1]，池田誠[1]
The Univ. of Tokyo.[1], ○Momoko Fukuda[1], Makoto Ikeda[2]
E-mail: fukuda@silicon.t.u-tokyo.ac.jp

【はじめに】ペアリング暗号は，楕円曲線暗号を発展させた公開鍵暗号の一種であり，RSA よりも高速かつ高機能な暗号方式であり，近年注目を集めている．しかし，ペアリング演算のアルゴリズムは現在研究途上にあり，どの楕円曲線を用いるのが適切なのかは未だ標準化されていない．また，ペアリング演算はソフトウェアで実装するには計算コストが高いことも問題である．そこで本研究では，ペアリング演算の楕円曲線ごとの ASIC 実装を自動化し，レイテンシ・面積・電力などの性能指標の正確な値を示す．

【提案手法】自動設計の具体的な流れは以下の通りである．まず，曲線の固有パラメータ u を入力し，ペアリング演算に必要な標数 p，位数 r などのパラメータを Sagemath[1] によって計算する．得られたパラメータから必要な演算の数・依存関係を取得し，Pyschedule[2] を用いた自動スケジューリングで演算の順序・並列性を最適化する．最後に，スケジューリング結果から演算器の制御を行うシーケンサの RTL を生成し，アーキテクチャのテンプレートと組み合わせて出力する．図 1 に，BLS12-381 曲線に提案手法を適用した場合のアーキテクチャを示す．また，曲線ごとのペアリング演算の安全性は離散対数問題と楕円曲線離散対数問題を解く際の計算コストによって決まり，固有パラメータ u から見積もりが可能である．

【結果】以上の議論から，いくつかの BLS12, BLS24 曲線について提案手法を用いて設計し，論理合成で得られた結果をプロットして対数近似により外挿した．図 2 に BLS12 と BLS24 についての安全性とハードウェアコストの関係を示す．現在実装の中心となっている 128bit，192bit セキュリティでは BLS12，それより高いセキュリティが必要な場合は BLS24 を利用するとレイテンシ・電力を少なく出来ると言える．一方，BLS24 は同じセキュリティを満たすために必要となる標数 p が小さくて済むため，今回の設計では演算器の bit 幅が小さくなり，面積を抑えることが出来ると分かる．

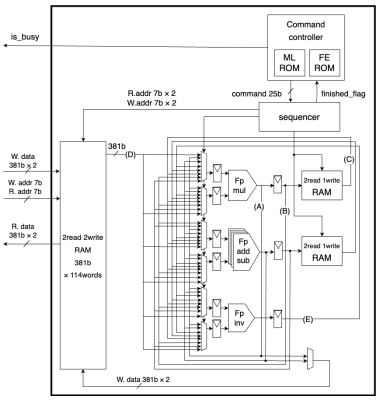

図 1. An example pairing processor architecture for BLS12-381.

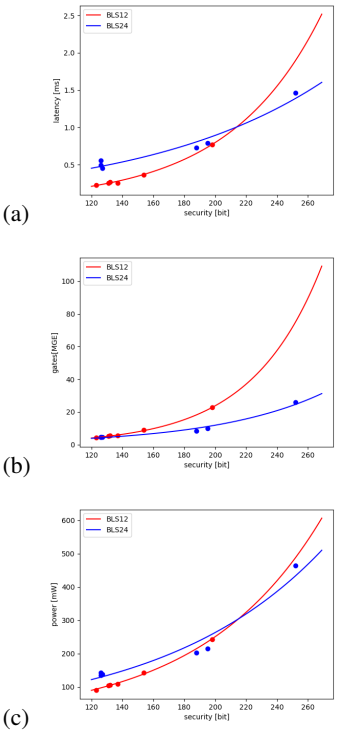

図 2. Balance estimation between pairing security and (a) latency, (b) gates (c) power

[1] The Sage Developers, ”SageMath, the Sage Mathematics Software System (Version 10.0)”, 2024, https://www.sagemath.org.
[2] T. Nonner, ”pyschedule”, 2021, https://github.com/timnon/pyschedule.