【184】

氏名（本籍）	照屋唯紀（てるや ただのり）（沖縄県）
学位の種類	博士（工学）
学位記番号	博甲第6059号
学位授与年月日	平成24年3月23日
学位授与の要件	学位規則第4条第1項該当
審査研究科	システム情報工学研究科
学位論文題目	**Efficient Software Implementation of Pairing Based Cryptography** （ペアリング暗号の高速なソフトウェア実装に関する研究）

主査	筑波大学教授	工学博士	岡本栄司
副査	筑波大学教授	博士（工学）	李頡
副査	筑波大学准教授	工学博士	片岸一起
副査	筑波大学助教	博士（工学）	金岡晃

論文の内容の要旨

ペアリング暗号を高速化するために、その主要な演算であるペアリングと楕円スカラー倍、二つの演算についての高速化の研究である。

ペアリングについては、x86-64命令セットアーキテクチャにおける126ビット安全性を持つ高速な非対称ペアリングのソフトウェア実装を行っている。具体的には、Barreto-Naehrig曲線上のoptimal ateペアリングを計算するためのソフトウェアライブラリを実装し、このペアリングを高速に計算できるような高速な有限体演算の実装手法を提案している。実装したライブラリはIntel Core i7-860（2.8GHz）のプロセッサの1つのコアのみを使用し、1回あたり約0.832ミリ秒でペアリングを計算できる。これは、マルチコアによるソフトウェア実装やハードウェア実装も含めて、世界で初めて1ミリ秒未満を達成した成果である。

楕円スカラー倍については、ペアリングの高速計算に適した楕円曲線における、楕円スカラー倍の高速計算手法を二つ提案している。提案手法はそれぞれate_iペアリングおよびoptimal ateペアリングというペアリングの高速計算手法に基づいた高速化である。従って、ある楕円曲線においてどちらかのペアリングが高速に実行できるならば、対応する提案手法もまた高速に実行できる。

審査の結果の要旨

新しい暗号のプリミティブとして研究が進みつつあるペアリング関数とそれに付随するスカラー倍演算についての研究である。それらは従来にない優れた性質を持つので、非常に応用が広く有望である。ただし、演算処理に時間がかかる欠点があった。本論文ではそれらを高速化し、世界トップの成果を上げた。そこで提案された手法はその後の多くの論文に引用・利用されている。

以上により、本論文は博士論文のレベルにあると判断できる。

平成24年1月24日、システム情報工学研究科において、学位論文審査委員の全員出席のもと、著者に論文について説明を求め、関連事項につき質疑応答を行った。この結果とリスク工学専攻における達成度評価

による結果に基づき、学位論文審査委員全員によって、合格と判定された。

上記の学位論文審査ならびに最終試験の結果に基づき、著者は博士（工学）の学位を受けるに十分な資格を有するものと認める。