Efficient Algorithms for Identity-Based Encryption using Supersingular Elliptic Curves

富田, 琢巳

https://doi.org/10.15017/1441044

出版情報：九州大学, 2013, 博士（機能数理学）, 課程博士
バージョン：

氏　　名：富田　琢巳

論文題目：Efficient Algorithms for Identity-Based Encryption using Supersingular Elliptic Curves
（超特異楕円曲線を用いたIDベース暗号の効率的アルゴリズム）
区　　分：甲

論　文　内　容　の　要　旨

本論文では、楕円曲線上のペアリングに基づくIDベース暗号（Identity-Based Encryption、以下、IBE）の高速化について得られた結果を報告する。

近年、楕円曲線上のペアリングを用いた暗号化方式（以下、ペアリング暗号）が注目され、世界中で活発な研究が行われている。IBEは、ペアリング暗号の一種であり、従来の公開鍵暗号方式と比べ、ユーザ公開鍵の管理や配布の必要がないといったメリットをもつ新しいタイプの公開鍵暗号化方式である。一方、ペアリング暗号を含め、IBEの実用上の課題として計算速度の向上が求められている。特に、携帯電話やスマートフォンといった組込み系のデバイスは、CPUやメモリといった計算リソースが制限されることが多く、高速化のニーズは高い。本研究の目的は、IBEの高速化である。しかし実用上の観点を考慮し、既にユーザに利用されているアプリケーションへの影響を最小限にするという制限を設けることにした。即ち、高速化のアプローチとして、既に、実用上標準化されているIBEのアルゴリズムを変更せず、パラメータの最適化という高速化のアプローチを選択している。本論文の主結果は、2001年にボネ氏とフランクリン氏によって提案された、超楕円曲線上のペアリングに基づくIBE（以下、BF-IBE）の高速化に関するものである。BF-IBEは、IBEの最初の実用例であり、インターネットに関する技術の標準を定める団体であるIETFが正式に発行する文書（RFC5091）として標準化されている。以下、高速化のアイデアについて述べる。

BF-IBEでは、IDを楕円曲線の捻れ元へ埋込む処理がある（この処理はHashToPointと呼ばれる）。HashToPointは、BF-IBE全体の処理と比較し相対的に計算コストが高く、BF-IBEの不利な点と考えられていた。HashToPointの計算処理において支配的な部分は、コファクターと呼ばれ巨大な定数による楕円曲線上有理点のスカラー倍算である。セキュリティの観点より、BF-IBEでは512bitの素数p上の超楕円曲線と、160bitの素数lの捩れ群が利用される。この時、コファクターは352bit（512bitから160bitを引いた値）の定数となる。高速化のアイデアは、このコファクターによる、楕円曲線上の有理点のスカラー倍算の計算量を減らす為に、低Hamming重みのコファクターを利用する点である。統計的観点からは、素数定理を利用することにより、そのような低Hamming重みのコファクターの存在は期待できることが分かる。本研究の貢献は、そのようなコファクターを具体的にリストアップし、その効果を評価した点にある。実際、Hamming重みが2であるコファクターのリスト化に成功した。また、Hamming重みが2であるコファクターと、従来のようにHamming重みを意識せず、ランダムに生成したコファクターとを用いて、デスクトップPC上でHashToPointの計算時間の比較を実施した。計算時間の比較結果では、本論文で提案するコファクターを利用した場合、従来に比べHashToPointの計算時間が約30%短縮されることが確認でき、最終的にBF-IBEの高速化を実現する事ができた。