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：

論文審査の結果の要旨

本博士論文では、超特異楕円曲線上で構成されるペアリング暗号において、暗号演算の高速化を目的としたアルゴリズムを考察している。ペアリング暗号は、大きな標数 p の有限体 $GF(p)$上の超特異楕円曲線 E_p におけるアルゴリズムにより構成される。ここで、ペアリング暗号を実用的に利用するためには、(1)有限体 $GF(p)$上の乗算、(2)楕円曲線 E_p 上の Tate ペアリングの演算、(3)楕円曲線上の点を生成する HashToPoint を実装できるアルゴリズムが必要となる。本博士論文では、超特異楕円曲線を利用したペアリング暗号の世界標準となる ID ベース暗号 RFC 5091: Identity-Based Cryptography Standard (IBCS) #1 に注目し、HashToPoint アルゴリズムを研究する。特に、ID ベース暗号では、受信端末の ID に対応した楕円曲線 E_p 上の点を HashToPoint により高速に計算できることが要求されている。

1985 年に Miller は楕円曲線 E_p 上のペアリングを標数 p の多項式時間で計算できるアルゴリズムを発表した。CRYPTO 2001 において Barreto らは、楕円曲線 E_p 上の Miller のアルゴリズムの高速化法として、因子計算の分母を消去する方法、楕円曲線の位数で割れる最大素数のハミング重みを下げる方法、Tate ペアリングの最終冪にフロベニウス写像を利用する方法を提案した。これらの高速化アルゴリズムは 2007 年に発表された ID ベース暗号の世界標準となる RFC 5091 に採用されている。その後、IWSEC 2010 において Nakajima らは、楕円曲線 E_p の標数 p のハミング重みを下げ、有限体 $GF(p)$の乗算で用いられるモンゴメリ乗算の高速化を発表している。

本博士論文では、楕円曲線上 E_p を ID ベース暗号の世界標準 RFC 5091 で利用されている有限体 $GF(p)$上の超特異楕円曲線 $y^2=x^3+x$ に特化した HashToPoint の高速化を考察する。超特異楕円曲線 $y^2=x^3+1$ は位数が $p+1$ であり、暗号方式では $p+1=cr$ が大きな素数 r を持つように生成する必要がある。特に、安全性と効率性のトレードオフの関係から、RFC 5091 では、p は 512 ビット、r は 160 ビットとして選ばれ、352 ビットの $c=(p+1)/r$ は Cofactor と言われている。今回の高速化対象となる HashToPoint は、次のように計算される。受信端末の ID に対して、$\mathrm{ID}+i$ $(i=0,1,2,\ldots)$が楕円曲線上の x 座標となる最小の非負整数 i を求めて、$Q_{\mathrm{ID}}=(\mathrm{ID}+i,((\mathrm{ID}+i)^3+(\mathrm{ID}+i))^{1/2})$とし、$Q_{\mathrm{ID}}$ の c 倍となる cQ_{ID} を計算することにより位数 r の楕円曲線上の点を求める。352 ビットの Cofactor c に対してスカラー倍算 cQ_{ID} を計算する必要があり、ID ベース暗号における他の演算と比較して計算量が多いアルゴリズムとなる。

本博士論文では、素数 r と p が関係式 $p+1=cr$ を満たす場合に c のハミング重みを最小にする問題を考察し、上記のパラメータサイズに対して素数(p,r)のリストを与えた。RFC 5091 では、素数 r が $r=2^{159}\pm 2^a\pm 1$ $(a=1,2,\ldots,158)$の Solinas 素数と言われる形で選ばれる。初期実験から c のハミング重みが 1 の場合は素数ペア(p,r)が存在しなかったため、Cofactor が $c=2^{352}\pm 2^b$ $(b=1,2,\ldots,351)$の形を満たす素数ペアを対象とした。素数の分布定理から、このような素数ペア(p,r)は 10 個程度のオーダーで存在すると予想されたが、計算整数論ソフトウェア Pari/GP を用いた計算機実験により 23 個の素数ペアが見つかった。

更に本博士論文では、これらの素数ペア (p,r) をパラメータとするIDベース暗号RFC 5091を標準的なPCおいて実装し暗号演算の性能を評価した。実装では、$r=2^{159}+2^{135}+1$, $c=2^{352}+2^{31}$, に対して標数 p = 0x 80000000 00000000 00000000 08000000 00000001 00000000 00000000 40000000 00000000 00000000 04000000 00000000 7fffffff ffffffff ffffffff ffffffff の有限体 $GF(p)$ 上の超特異楕円曲線 $y^2=x^3+x$ を用いて、Tateペアリングの計算、スカラー倍算、HashToPointの演算などのIDベース暗号で利用される暗号演算の実行時間に関する実験を行った。その結果、上記の素数ペア (p,r) を利用したHashToPointは、RFC 5091で利用された素数ペアと比較して30%の高速化を実現した。また、これらの高速化率を、最も計算時間を占める有限体上の乗算回数として理論的に評価したところ、実験結果と同程度の31%の高速化率の見積もりを得た。また、RFC 5091のIDベース暗号で用いられる他の暗号演算の計算時間は提案した素数ペア (p,r) を用いても大きく変化しておらず、HashToPointだけを高速化することに成功している。

本博士論文の結果は、2013年3月に日本応用数理学会「数論アルゴリズムとその応用」研究部会(JANT)で発表し、論文誌JSIAM Lettersに採録され公表予定である。この成果は、素数の分布を調べることによりペアリング暗号の高速化手法を詳細に考察し、実用的に利用される計算機環境で高速化も実証している。暗号理論の分野において学術的に高く評価できる研究業績であり、本研究者は博士（機能数理学）の学位を受ける資格があるものと認める。