【3】

氏名	四方順司（しかたじゅんじ）
博士の専攻分野の名称	博士（理学）
学位記番号	第 15135 号
学位授与年月日	平成12年3月24日
学位授与の要件	学位規則第4条第1項該当 理学研究科数学専攻
学位論文名	On the Reductions of the Elliptic Curve Discrete Logarithm Problem （楕円曲線上の離散対数問題について）
論文審査委員	（主査） 教授 藤木 明 （副査） 教授 山本 芳彦　教授 伊吹山知義　助教授 鈴木 譲 講師 藤原 彰夫

論文内容の要旨

楕円曲線上の離散対数問題を有限体の乗法部分群上の離散対数問題に帰着する方法として、現在までに、Menezes-Okamoto-Vanstone reduction（MOV reduction）（1991年）及びFrey-Rück reduction（FR reduction）（1994年）が知られている。ただし、ここで言う楕円曲線上の離散対数問題とは次のような問題である：F_qを標数pのq個の元からなる有限体とし、EをWeierstrass equationで与えられたF_q上定義された楕円曲線とする。位数lのF_q−有理点$P\in E(F_q)$及び$R\in\langle P\rangle$が与えられたとき、$R=nP$をみたす整数nを求めよ。（以下、Chinese Remainder Theorem及びPohlig-Hellman methodの適用によりlは奇素数と仮定して一般性を失わない。）

MOV reductionに関して、実際にMenezes, Okamoto, Vanstoneの論文の中で、計算量評価も含めて具体的なアルゴリズムとして実現されているのは、超特異楕円曲線に対してのみであった。本研究では、一般の楕円曲線上の離散対数問題に対してMOV reductionを適用するための最も弱い条件をアルゴリズムの立場から解析し、その条件の下、実際にMOV reductionを具体的なアルゴリズムとして実現した。これに関する本研究の結果は次の通りである。

定理1 $l\nmid q$, $l\nmid q-1$とし、またkは$l\mid q^k-1$をみたす最小の正整数とする。このとき、一般の楕円曲線に対して、MOV reductionを実現するk log qの確率的多項式時間アルゴリズムが存在する。より厳密に言えば、そのアルゴリズムの計算量は$O(k^3\log^3 q+\log^6 q)$ bit operationsであり、仮に$\#E(F_q)$を前もって知っている場合には$O(k^3\log^3 q)$ bit operationsである。

系1 前述の定理と同じ条件のもとで、$F_{q^k}^*$の離散対数問題がlog qの準指数時間で解けるならば、MOV reductionに対する提案アルゴリズムはlog qの確率的多項式時間で完了する。結果として、$F_{q^k}^*$の離散対数問題がlog qの準指数時間で解ける場合には、MOVアルゴリズム全体はlog qの確率的準指数時間で計算を終了する。

このことによりMOV reductionとFR reductionの厳密な差異をアルゴリズムの観点から明確にすることができる。特に、興味ある場合（$l\nmid q$かつ$l\nmid q-1$）の結果として次を得る。

定理2 $l\nmid q$かつ$l\nmid q-1$とする。このとき、MOV reduction（algorithm, resp.）とFR reduction（algorithm, resp.）は同じ計算量をもつ。

さらに、実際に暗号に用いられる規模のいくつかの楕円曲線に対して、MOV reduction及びFR reductionを実装し、その振る舞いを確認した。

論文審査の結果の要旨

一般の楕円曲線上の離散対数問題を、有限体の乗法群上のそれに帰着する方法である Menezes-Okamoto-Vanstone reduction について、これを適用するためのもっとも弱い条件をアルゴリズムの立場から解析し、その条件下に、実際に MOV reduction を具体的アルゴリズムとして実現した。また MOV reduction と Frey-Rück reduction の厳密な差異をアルゴリズムの観点から明確にした。

以上により、博士（理学）の学位論文として十分価値あるものと認める。