99-01054

# 代数曲線暗号の安全性についての検討

代表研究者　鈴木　譲　大阪大学大学院理学研究科助教授
共同研究者　今井秀樹　東京大学生産技術研究所教授
共同研究者　藤原　融　大阪大学大学院基礎工学研究科教授
共同研究者　山本芳彦　大阪大学大学院理学研究科教授
共同研究者　小川裕之　大阪大学大学院理学研究科助手
共同研究者　Joseph H. Silverman　Brown 大学数学科教授
共同研究者　原澤隆一　日本学術振興会特別研究員

本研究では、楕円曲線上の離散対数問題について考察した。楕円曲線は、代数幾何や数論の分野で活発に研究されている。最近では素因数分解［11］、素数判定［３］に関するアルゴリズムや、公開鍵暗号の構成［14、9］などに使われている。特に、楕円曲線上の離散対数問題の困難さに安全性の根拠をおく楕円曲線暗号は、ここ数年注目されている。

$E/F_q$ を Weierstrass 方程式：

$$y^2+a_1xy+a^3y=x^3+a_2x^2+a_4x+a_6\ (a_1、a_2、a_3、a_4、a_6\in F_q) \qquad (1)$$

（ここで、$F_q$ は $q$ 個の元からなる有限体とし、$q=p^m$、$p$ は素数、$m\geqq 1$ とする）によって与えられる楕円曲線とする。$E/F_q$ 上の離散対数問題とは、$P\in E\ (F_q)$、$R\in <P>$が与えられた時、$R=lP:=\underbrace{P+P+\cdots+P}_{l}$ となる$0\leqq l\leqq n-1$ を見い

出す問題である。ここで $n$ は、有限巡回群$<P>$の位数とする。

本研究を通じ、$E/F_q$ および体 $K$ に対して、$E\ (K):=\{(x、y)\in K\times K|(x、y)$は(１)を満足する$\}\cup\{O\}$と定義する。また、$\bar{F}_q$を $F_q$ の代数的閉包とした時、$E:=E\ (\bar{F}_q)$ には $O$ を単位元とするようなアーベル群の構造が入ることが知られている［21］。

楕円曲線暗号が従来の方式に比べて受け入れられている主な理由は、$F^*_q$ 上の離散対数問題が高々 log $q$ の準指数時間で解かれるのに対し、$E/F_q$ 上の離散対数問題は一般に log $q$ の指数時間が必要であると信じられていることである（V. Miller［14］、J. Silverman、J. Suzuki［21］）。言い換えると、楕円曲線暗号は鍵の長さがより短くても従来のものと同程度の安全性をもつことができる。この性質は、カードシステムのような、メモリーや演算能力に制限があるような状況において応用上大変重要である。

しかしながら、いくつかの特別な場合に関しては、巡回群$<P>$から $F_q$ または $F^*_{q^k}$（$F_{q^k}$ は $F_q$ の適当な拡大体）へのlog $q$の多項式時間で実行可能な単射準同型を考えることにより、離散対数問題は有限体上のそれと同程度の困難さをもつことになる（超楕円曲線暗号に対する攻撃に関しては L. Adleman、J. DeMarrais、M. Huang が、ある仮定のもと次のようなヒューリスティックな結論を得ている。すなわち $\log p\leqq (2g+1)^{0.98}$ を満たす十分大きな種数 $g$ と奇素数 $p$ に対しては $F_p$ 上の超楕円曲線の Jacobian の有理点からなる群の離散対数問題が log $p$の準指数時間で解ける。詳細については［１］を参照されたい）。

加法群としての $F_q$ への帰着に関しては、anomalousな楕円曲線（すなわち $q=p$ で$\#E\ (F_p)=p$ となる）の場合もしくはその単純な一般化の場合が解決されている（［20］、［23］、［17］）。（位数 $n$ の巡回群 $G$ での離散対数問題を解くことは、本質的には $G$ と $Z_n$[1] の間の同型写像を計算することと同値である。）

他方 $F^*_{q^k}$ への帰着に関しては、A. Menezes、T. Okamoto、S. Vanstone［12］により超特異楕円曲線（すなわち $t:=q+1-\#E\ (F_q)$ とした時 $p\mid t$ となる）の場合に適用できる MOV 帰着[2] が提案された。言い換えると、超特異楕円曲線に対しては、$E/F_q$ での離散対数問題は、ある $k$ に対して $F^*_{q^k}$ での離散対数問題に帰着され、これは log $q$ の準指数時間で解くことができる（結果として、ここで得られた離散対数問題は $F^*_{q^k}$ 上のそれに相応し、入力サイ

1　本研究では、$Z/nZ$ を $Z_n$ と略記している。

2　本研究において、``MOV 帰着 '' で楕円曲線上の離散対数問題から有限体の乗法群上の離散対数問題までの変換部分を指す。また、``MOV アルゴリズム '' で変換部分、及び変換後の有限体上の離散対数問題を解くことを指す。

ズは $k$ 倍となる)。この場合、$k$ の値は $E[n]=\{T\in E \mid nT=O\}$ としたとき、$E[n]\subset E(F_{q^k})$ をみたす正整数となる。Menezes、Okamoto、Vanstone は 文献［12］の中で、もし $E/F_q$ が超特異楕円曲線ならばそのような $k$ は高々６を考えればよく、Weil pairing［21］$e_n(P,Q)$ が $F^*_{q^k}$ の位数 $n$ の元となるような $Q\in E[n]$ が log $q$の確率的多項式時間アルゴリズムで得られることを示した。

$F^*_{q^k}$ への帰着に関して MOV 帰着が提案された後、G. Frey と H. Rück［７］は Tate pairing を基にした単射準同型を提案した（FR 帰着[3])。すなわち、FR 帰着は $n \mid q-1$ の場合に適用でき、さらに $n \nmid q-1$ の場合にも定義体 $F_q$ を $F^*_{q^k}$ に拡大することによって適用できる。この場合の $k$ は $n \mid q^k-1$ を満たす最小の正整数を考えればよく、MOV と同様 離散対数問題の入力サイズは $k$ 倍となる。しかし、文献［７］では基本的概念の記述のみにとどまっている。

また、簡単な考察から、FR 帰着の適用条件が MOV 帰着の適用条件を含んでいることを示すことができる。実際 R. Schoof［18］によって、もし $p \nmid n$ ならば E［n］⊂E（$F^*_{q^k}$）であることと、$n \mid q^k-1$ および他２つの条件と同値であることが示されている（4.1 節)。

本研究では、$E[n]\subset E(F^*_{q^k})$（$k$ はある正整数）を満たすまで定義体を拡大し、ある種の非超特異楕円曲線に適用できるような MOV 帰着の具体的実現方法を提案する（２節)。現在まで、一般の非超特異楕円曲線に対しては、$e_n(P,Q)$ が 位数 $n$ の元となる $Q\in E[n]$ を効率的に見つけるアルゴリズムが提案されていないので、この内容は必ずしも自明ではなかった。

我々は、全ての非超特異楕円曲線とまではいかないが、ある条件のもとで、MOV 帰着を実現するための具体的なアルゴリズムを提案する。すなわち、

$$E(F_q)\cong Z_{n1}\oplus Z_{n2},\ E[n]\subset E(F_{q^k}),\ E(F_{q^k})\cong Z_{c1n}\oplus Z_{c2n}$$

（$n_2 \mid n_1$ かつ $c_2 \mid c_1$）としたとき、$c_2 n \mid c_1$ でない限り、MOV 帰着が成功する $Q\in E[n]$を容易に見い出せることを示す。

他方、最近 R. Balasubramanian、 N. Koblitz［５］によって、$n$ が素数で $n \nmid q$かつ $p \nmid n-1$ の場合には、$E[n]\subset E(F_{q^k})$ であることと $n \mid q^k-1$ は同値であることが示されている。

以上のことから、$n$ が素数の時、

1. $n \mid q-1$

以外に、

2. E［n］⊂E（$F_{q^k}$)、$c_2 n \mid c_1$

の場合にも FR 帰着が適用でき、MOV 帰着が適用できない可能性がある。

次に、FR 帰着の詳細なアルゴリズムを提案し、その計算量的な性質を解析する。また多数の実際規模にわたって、FR 帰着の実装を行う（３節)。 さらに、帰着の適用条件、 効率性に関して、MOV 帰着との比較を検討する（4節)。その結果、どのような場合においても FR 帰着はMOV 帰着より優れているという結論を得る。

本研究を通じ、議論を簡単にするために、以下の条件を仮定する：

１．$<P>$の位数 $n$ は素数

もし、$n=\Pi_i p_i^{e_i}$ が合成数であれば、問題は各 $i$ に対して $R=lP$ となる $l \bmod p_i$ を見つけることに帰着される。この時、 Pohlig‐Hellman のアルゴリズム［16］より全ての $i$ に対して、$l \bmod p_i^{e_i}$ を求めることができ、中国人剰余定理を用いて $l \bmod n$ が得られる。

さらに、一般性を失うことなく、以下の２条件を仮定する。

２．$p \nmid t$（非超特異性）

３．$n\neq p$（非 anomalous 性）

上記２条件が成立する場合に関しては、離散対数問題は log $q$ の多項式時間でそれぞれ $F^*_{q^k}$、$F_q$ 上の離散対数問題に帰着される。

## １　非超特異楕円曲線に対するMOV帰着の実現

(Weil pairing の定義と基本的な性質は、［21］、［12］、［13］を参照されたい。)

MOV アルゴリズムの概要は以下のように述べることができる(文献［12］または［13］の71ページ)。

3　本研究において、“ FR帰着 ”で楕円曲線上の離散対数問題から有限体の乗法群上の離散対数問題までの変換部分を指す。また、“ FRアルゴリズム ”で変換部分、及び変換後の有限体上の離散対数問題を解くことを指す。

**アルゴリズム1**
**Input**：位数 $n$ の元 $P \in E(F_q)$、 $R \in \langle P \rangle$
**Output**：$R = lP$ を満たす 整数 $l$
**Step 1**：$E[n] \subset E(F_{q^k})$ を満たす最小の正整数 $k$ を求める。
**Step 2**：$\alpha = e_n(P, Q)$ の位数が $n$ となる $Q \in E[n]$ を見い出す。
**Step 3**：$\beta = e_n(R, Q)$ を計算する。
**Step 4**：$F^*_{q^k}$ において、$\alpha$ を底とする $\beta$ の離散対数問題を解き、$l$ を求める。
(Weil pairing の計算過程については、[12]、[13] を参照されたい。)

着想は、$E[n] \subset E(F_{q^k})$ となる $k$ に対して、定義体 $F_q$ から $F_{q^k}$ に拡大することである。$\mu_n$ を 1 の $n$ 乗根からなる群、$e_n : E[n] \times E[n] \to \mu_n$ を Weil pairing ( [12]、[13]、[21]、$Q \in E[n]$ を $e_n(P, Q)$ が 1 の原始 $n$ 乗根となる元とする。この時、Weil pairing の性質より、$\mu_n \subset F^*_{q^k}$ が成り立つ。ゆえに、$S \mapsto e_n(S, Q)$ で定義された群の同型写像 $\langle P \rangle \to \mu_n$ は、単射準同型 $\langle P \rangle \to F^*_{q^k}$ を与える ([12]、[13])。

任意の $E/F_q$ に対して、$E(F_q) \cong Z_{n1} \oplus Z_{n2}$、$n_2 \mid n_1$ を満たす対 $(n_1, n_2)$ が存在することが知られている ([12]、[13])。 また、$E/F_q$ が 超特異ならば、$E[n_1] \subset E(F_{q^k})$ を満たす最小の $k$ まで定義体 $F_q$ を拡大したとき、

1. $k$ の値は高々 6 であり、
2. $E(F_{q^k}) \cong Z_{cn1} \oplus Z_{cn1}$ が成り立つ。

ここで、 $k$ 及び $c$ の値は後述するように、超特異楕円曲線に対する MOV アルゴリズムの具体的実現において大変重要である。さらに、文献 [12] では、超特異楕円曲線に関する次の事実を利用することで後述するアルゴリズム 1 ' を具体的に構成している。

1. 超特異楕円曲線は 6 個の類にわけられる。
2. $k$ と $c$ の値はその類によって一意的に決定される。そして、
3. その類は $E$ の $q$ 乗 Frobenius 写象のトレース $t = q + 1 - \#E(Fq)$ の値から計算される。

以上の事実から超特異楕円曲線に対しては、次のアルゴリズムが提案されている ([12]、[13])。

[**アルゴリズム 1 '**]
**Input**：位数 $n$ の元 $P \in E(F_q)$、$R \in \langle P \rangle$
**Output**：$R = lP$ を満たす 整数 $l$
**Step 1**：$E[n_1] \subset E(F_{q^k})$ を満たす最小の正整数 $k$ を求める (この $k$ は超特異楕円曲線の類により決定される)。
**Step 2**：$Q' \in E(F_{q^k})$ をランダムに選び、$Q = [c_{n1}/n]\, Q'$ とする (この $c$ は超特異楕円曲線の類により決定される)。
**Step 3**：$\alpha = e_n(P, Q)$ および $\beta = e_n(R, Q)$ を計算する。
**Step 4**：$F^*_{q^k}$ において、$\alpha$ を底とする $\beta$ の離散対数問題を解き、$l'$ を求める。
**Step 5**：$l' P = R$ が成り立つかどうか確認する。もし成り立てば、$l = l'$。 そうでなければ、Step 2 へ戻る。

ここで、アルゴリズム 1 'はアルゴリズム 1 と若干、形式は異なるが、本質的には同じ内容のものである。ただし、アルゴリズム 1 'のStep 2 では、$E[n] \subset E(F_{q^k})$ となる最小の $k$ ではなく、$E[n_1] \subset E(F_{q^k})$ を満たす最小の $k$ をとっている。(このとき、$n \mid n_1$ より $E[n] \subset E[n_1] \subset E(F_{q^k})$。) 一般に、後者の $k$ の方が前者のそれよりも大きくなるのが普通であるが、それでも上述したように $k$ は高々 6 でおさまる。むしろ、注目すべきは、$E[n]$ の元 $Q$ の求め方であり、アルゴリズム 1 'のStep 1～5 の後、確率 $1 - 1/n$ (もし $n$ が合成数ならば $\varphi(n)/n$) で正しい $l$ を得ることができる。$n$ は大きいので、平均試行回数は限りなく 1 に近い。

本研究では、非超特異楕円曲線を考察しているので、上記の方法を使うことはできない。まず、$E[n] \subset E(F_{q^k})$ をみたすまで定義体 $F_q$ を拡大する。具体的な $k$ の値に関しては、4.1節で詳しく述べる。ここでは、非超特異の場合の元 $Q \in E[n]$ の求め方を、超特異の場合にとられていた方法を基に次のように考えてみる。

$E(F_{q^k}) \cong Z_{c1n} \oplus Z_{c2n}$ ($c_2 \mid c_1$) と表したとき、$c_1/c_2 = n^e r$、$e \geqq 0$、$(n, r) = 1$ となる対 $(e, r)$ をとる。ただし、$c_1$、 $c_2$ の値は、一般の楕円曲線の場合には以下のようにして求めることができる。

1. Schoof のアルゴリズム [19] またはその改良法 (例えば [6、2]) を用いて、$\#E(F_q)$ を計算する。
2. Weil の定理 [12] [13] を用いて $\#E(F_q)$ から $\#E(F_{q^k})$ を計算する。
3. $\#E(F_{q^k})$ を因数分解する。
4. Miller のアルゴリズム [15] を用いて $E(F_{q^k}) \cong Z_{n'1} \oplus Z_{n'2}$ となる $n'_1$、$n'_2$ を見つける。
5. このとき、$c_1 = n'_1/n$、$c_2 = n'_2/n$

そして、非超特異楕円曲線に対して、アルゴリズム 1 のStep 2 の詳細として、以下の方法を提案する。

Step2 - 1：$Q' \in E(F_{q^k})$ をランダムに選ぶ。
Step2 - 2：$Q = [c_1 n / n^{e+1}]\, Q' \in E[n^{e+1}] \cap E(F_{q^k})$ とする。
Step2 - 3：もし $Q \notin E[n]$ (すなわち $nQ \neq O$) ならば、Step2 - 1に戻る。

Step2 - 4：α＝$e_n$（$P$、$Q$）を計算する。もしα＝1ならばStep2 - 1に戻る。

この方法での考え方は、超特異な場合の拡張になっていることに注意する。すなわち、$e$=0かつ $r$=1のときが超特異の場合に相当する。また、もし $e$=0ならば、Step2 - 3は省略できることにも注意する。実際には、計算量的観点から、この提案方法が有効に機能するのは、$e$=0のときに限ることが以下の定理からわかる。

**定理1** Step2 - 2で得られた $Q\in E$［$n^{e+1}$］$\cap E$（$F_{q^k}$）が、$Q\in E$［$n$］かつ $e_n$（$P$、$Q$）≠1となる確率は$\frac{1}{n^e}(1-\frac{1}{n})$である。

証明：次の写像を考える：

$$f: E(F_{q^k})\to E(F_{q^k}),\ f(Q)=[c_1 n/n^{e+1}]\ Q$$

この時、$E$（$F_{q^k}$）$\cong Z_{c1n}\oplus Z_{c2n}$ なので、$f$の像は $Z_{ne+1}\oplus Z_n$ と同型となる。Ωを $Q\in E_n$ かつ $e_n(P、Q)\neq 1$ となる $Q$ からなる集合とする。Weil pairing の性質から、$e_n(P、Q)=1$であることは、$Q\in<P>$であることと同値である（［12］、［13］）。ゆえに、$\#\Omega=n^2-n$ となる。

したがって、Step2 - 1で $Q'\in E$（$F_{q^k}$）がランダムに選ばれれば、成功する確率は、以下で得られる。

$$\frac{\#Kerf\times\#\Omega}{\#E(F_{q^k})}=\frac{\frac{c_1 n\times c_2 n}{n^{e+1}\times n}\times(n^2-n)}{c_1 n\times c_2 n}=\frac{1}{n^e}(1-\frac{1}{n})$$

**系1** アルゴリズム1のStep2 - 1で、$Q'\in E$（$F_{q^k}$）をランダムに選ぶ回数の期待値は$\frac{n^{e+1}}{n-1}\approx n^e$である。

証明：Kac の補題［8］より、期待値は定理1で得られた確率$\frac{1}{n^e}(1-\frac{1}{n})$の逆数である。

$n=O$（$q$）のとき、このことはもし e≧1ならば、Step2 - 3

$$1/[\frac{1}{n^e}(1-\frac{1}{n})]=\frac{n^{e+1}}{n-1}$$

は平均して log $q$ の指数時間かかることを意味する。

MOV 帰着が適用できるまで体を拡大した後、$c_2 n\mid c_1$ であるならば、この提案方式によるMOV 帰着はあきらめなければならない。そのような確率は小さいかもしれないし、また今後そのような場合でも別の方法で扱うことができるかもしれない。しかしながら、非超特異楕円曲線に対する MOV 帰着を実現するためには、更なる計算が必要である。すなわち、E［n］$\subset E$（$F_{q^k}$）、$c_2 n\nmid c_1$ の時でさえも Step2 - 3 における $c_1 n/n^{e+1}$ の値が必要であり、そのためには#E（$F_q$）の計算、$\#E$（$F_{q^k}$）の因数分解、および $E$（$F_{q^k}$）の群構造（$c_1 n$、$c_2 n$）の計算などが要求される。

## 2　FR 帰着の実装

FR 帰着の実現法を考察する。この章では、ある $k$ に対して $K=F_{q^k}$ とする。

### 2.1　FR 帰着の概要

$Div$（$E$）を $E$ の因子群、$D=\sum_{P\in E} n_P(P)\in Div(E)$ に対して $supp(D):=\{P\in E: n_P\neq 0\}$とする。この時、$E$ は $K$ 上定義されているので、Galois 群 $G_{\bar{K}/K}$ は $Div$（$E$）に以下のようにして作用する：$D=\Sigma_{P\in E} n_P(P)\in Div(E)$、$\sigma\in G_{\bar{K}/K}$ に対して、$D^\sigma=\sum_{P\in E} n_P(P^\sigma)$。もし全ての$\sigma\in G_{\bar{K}/K}$ に対して $D^\sigma=D$ を満たすならば、$D\in Div(E)$ は K 上定義されているといい、そのような元からなる集合を $Div_K(E)$と書くことにする。また、$\bar{K}(E)^*$で常には 0 でない $E$ 上の$\bar{K}$係数の有理関数体を表す。$E$ 上の有理関数 $f=f_1/f_2\in\bar{K}(E)^*(f_2\neq 0)$ に対する因子 $div(f)$ を

$$div(f)=\sum_{P\in E}(ord_P(f))(P)$$

で与え、主因子という。ここで、$ord_P(f)=ord_P(f_1)-ord_P(f_2)$ とし、$ord_P(f_1)$、$ord_P(f_2)$ はそれぞれ、$P\in E$ における $f_1$、$f_2$の零点の位数とする。そして、因子の次数を $deg(D):=\Sigma n_P$ で定義し、$Div^0(E):=\{D\in Div(E)\mid deg(D)=0\}$とするとこれは $Div(E)$ の部分群をなす。さらに、主因子からなる集合を $Prin(E)$と書くことにすると、これは $Div^0(E)$の部分群となる。ここで、次の全射準同型写像を定義する。

$Div^0(E) \to \mathrm{Pic}^0(E) := Div^0(E)/Prin(E)$、$D \mapsto \overline{D}$

そして、2因子 $D_1$、$D_2$のこの写像による像が同じならば（すなわち$\overline{D}_1 = \overline{D}_2$in $Pic^0(E)$）、$D_1 \sim D_2$と書く。さらに、$Pic_K^0(E)$ を $K$ 上定義された$\overline{D}$からなる $Pic^0(E)$ の部分群とし、$Pic_K^0(E)_n := \{\overline{D} \in Pic_K^0(E) \mid n\overline{D} = 0\}$ とする。

$A$ を、$\overline{A} \in Pic_K^0(E)_n$ となる因子とし、$B = \Sigma_i a_i (Q_i) \in Div_K^0(E)$ を $supp(A) \cap supp(B) = \phi$を満たすものとする。$nA \sim 0$なので $div(f_A) = nA$ となる $f_A \in \overline{K}(E)^*$が存在する［21］。このとき、$f_A(B)$ を $f_A(B) := \Pi_i f_A(Q_i)^{a_i}$ で定義する。

Frey-Rück［7］は、以下の結果を証明している。

**命題1**（［7］）もし $n \mid q^k - 1$ならば、$\{\overline{A}, \overline{B}\}_{0,n} := f_A(B)$は、非退化双一次形式

$$\{,\}_{0,n} : Pic_K^0(E)_n \times Pic_K^0(E)/nPic_K^0(E) \to K^*/(K^*)^n$$

を与える。

pairing$\{,\}_{0,n}$ は Tate pairing の変種であるということができる。（［7］、［24］）また、楕円曲線の場合は、［21］の278ページも参照されたい。 以降 pairing$\{,\}_{0,n}$ を FR pairing とよぶことにする。

**注意1** 本研究では、楕円曲線の場合を考えているため、同型写像

$$E(K) \to Pic_K^0(E),\ Q \mapsto \overline{(Q)-(O)}$$

によって（［21］）、$E(K)$ と$Pic_K^0(E)$ を同一視して考えることにし、$\overline{(Q)-(O)}$ を$\overline{Q}$と書くことにする。このとき、$Pic_K^0(E)_n$、$Pic_K^0(E)/nPic_K^0(E)$ はそれぞれ $E(K)[n] := E[n] \cap E(K)$、$E(K)/nE(K)$ と同一視することができる。

**注意2** $\mu_n$ を1の $n$ 乗根からなる $K^*$の部分群とする。このとき、$\alpha \mapsto \alpha^{\frac{q^k-1}{n}}$ によって定義された準同型写象 $K^* \to K^*$によって $K^*/(K^*)^n \cong \mu_n \subset K^*$ が得られる。また、pairing$\{,\}_{0,n}$ の非退化性より $\{\overline{P}, \overline{Q}\}_{0,}^{\frac{q^k-1}{n}}{}_n$が1の原始 $n$ 乗根となる $Q \in E(K)$ が存在する。ゆえに、$S \cong \{\overline{P}, \overline{Q}\}_{0,}^{\frac{q^k-1}{n}}{}_n$によって与えられる同型写象 $<P> \mapsto \mu_n$ は、単射準同型$<P> \to F_{q^k}^*$ を与える。

### 2.2 FR 帰着の実現方法

文献［7］の内容は、一般の曲線を扱っており、数学的でむしろ複雑である。それゆえ、実現に関する結果については報告がなされていない。ここでは、楕円曲線に限定しているので議論が簡潔になる。本研究では、楕円曲線の場合の実現を以下のように考える。ここで、FR pairingは $K = F_{q^k}$（ただし、$k$ は $n \mid q^k - 1$を満たす最小の正整数）上で実行される。

**アルゴリズム2**

**Input**：位数 $n$ の元 $P \in E(F_q)$、$R \in <P>$

**Output**：$R = lP$ を満たす整数 $l$

**Step1**：$n \mid q^k - 1$を満たす最小の正整数 $k$ を求める。このとき $K = F_{q^k}$ となる。

**Step2**：$S$、$T \in E(K)$ をランダムに選ぶ。[4]

**Step3**：$div(f) = n((P)-(O))$ となる $f \in K(E)^*$ を求め、$\alpha = f(S)/f(T)$ を計算する。

**Step4**：$\gamma = \alpha^{\frac{q^k-1}{n}}$ を計算する。 もし $\gamma = 1$ならば、$Step2$ へ戻る。

**Step5**：$div(g) = n((R)-(O))$ となる $g \in K(E)^*$ を求め、$\beta = g(S)/g(T)$、$\delta = \beta^{\frac{q^k-1}{n}}$ を計算する。

**Step6**：$F_{q^k}^*$ 上での離散対数問題 $\delta = \gamma^l$ を解く。

実現は、むしろ単純である。概念上の考察については［7］で述べられており、FR 帰着（アルゴリズム2の Steps 2 - 5）の計算量は $k \log q$ の確率的多項式時間であると見積もられている。以下では実際に提案されたアルゴリズムにおける各 Step（Steps 2 - 5）での計算量を評価すると共に、各 Step について多少補足する。ここで、計算量は通常の乗法を用いて評価を行う。つまり、2つの $N$ ビットの元の乗法に必要な計算量は $O(N^2)$ と仮定して考える。

Step 2については、$K$ の元 $x = a$ を選び（1）式に代入する。この時、$y$ についての2次方程式が $K$ で解をもつかを調べる。解をもつ確率は約1/2である。もし解をもてば、その2次方程式を解く。2次方程式を解くための計算量は、平均実行時間 $O((\log q^k)^3) = O(k^3 (\log q)^3)$ かかる（詳細については、例えば［4］、［10］を参照されたい）。

4 $T$ を $E(K)$ からランダムにとらず $kP$（$kP \neq O$、$P$、$R$）と決めてもよい。

Step 3 については、主因子から関数 $f \in \overline{K}(E)^*$を求める標準的方法がある（例えば文献［13］の63‐64ページ）。基本的には、以下の手順で行う。

1.$div(f)=\Sigma_i a_i((P_i)-(O))$ と表す。

2.各 $i$ に対して、以下を満たす $P_i' \in E$、$f_i \in \overline{K}(E)^*$を計算する。

$$a_i((P_i)-(O))=(P_i')-(O)+div(f_i)$$

3.全ての $i$ に対して、$(P_i')-(O)+div(f_i)$ を足し合わせる。

ここで、以下の方法により因子を足し合わせることができる。すなわち2因子 $D$、$D'$ が $P$、$P' \in E$、$f$、$f' \in \overline{K}(E)^*$を用いて

$$D=(P)-(O)+div(f)、D'=(P')-(O)+div(f')$$

と表せるとき、その和 $D+D'$ は

$$D+D'=(P+P')-(O)+div(ff'g)$$

と計算できる。ここで、$g=l/v$ で、$l$ を $P$、$P'$ を通る直線、$v$ を $P+P'$ を通る垂直線とした（特に、$P'=-P$ の時、$v \equiv 1$）。前述の $f$、$f$、$g$ に、$S$、$T$ をそれぞれ代入し、それをかけあわせることで$\alpha=f(S)/f(T)$が得られ、また、上記の因子の足し合わせは $F_{q^k}$ 上の演算を $O(\log n)$ 回行われることになる。したがって、この Step の計算量は、$O((\log q^k)^2)\times O(\log n)=O(k^2(\log q)^3)$ となる。また、$Q:=S-T \in E(K)$ としたとき、

$$(S)-(T)=(Q+T)-(T)\sim(Q)-(O)$$

より、この Step では $\{\overline{P}、\overline{Q}\}_0$、$n$ を計算することを意味している。

Step 4 については、まず $\gamma=\alpha^{\frac{q-1}{n}}$ の計算量は、$O(\log^{\frac{q-1}{n}})\times O((\log q^k)^2)=O(k^3(\log q)^3)$ となる。さらに全体のStep を計算する時間を調べるためには、Step 2 に戻る確率を評価しなければならない。つまり、Step 2 でランダムに選んだ $S$、$T$ に対して上述したように $Q=S-T \in E(K)$ としたとき[5]、$\{\overline{P}、\overline{Q}\}_0$、$n$ が $K^*/(K^*)^n$の生成元となる確率を評価する必要がある。そのために以下の定理を証明する。

**定理2** $k$ は $n \mid q^k-1$ を満たす最小の正整数とする。（この場合 $K=F_{q^k}$ となる。）このとき、Step 4 から Step 2 に戻る確率は $1/n$ である。

**証明：** $E(K) \cong Z_{n1} \oplus Z_{n2}$、$n_2 \mid n_1$、$E[n] \cong Z_n \oplus Z_n$と書ける。ゆえに、

$$E(K)[n] \cong \begin{cases} Z_n & (n \nmid n_2) \\ Z_n \oplus Z_n & (n \mid n_2) \end{cases}$$

また、FR pairingの非退化性より

$$E(K)/nE(K) \cong \begin{cases} Z_n & (n \nmid n_2) \\ Z_n \oplus Z_n & (n \mid n_2) \end{cases}$$

ここで、2つの場合に分けて考える。

1. $E[n] \not\subset E(K)$、すなわち $n \nmid n_2$ の場合。Q∈E（K）をランダムに選ぶとき、$\{\overline{P}、\overline{Q}\}_0$、$n \notin (K^*)^n$ となる確率は、

$$\frac{\#E(K)-\#nE(K)}{\#E(K)}=\frac{n_1n_2-n_1n_2/n}{n_1n_2}=1-1/n$$

となる。

2. $E[n] \subset E(K)$ すなわち $n \mid n_2$ の場合。$T:=\{Q \in E(K)/nE(K) \mid \{\overline{P}、\overline{Q}\}_0、n \notin (K^*)^n\}$ とおく。このとき、$\#T=n^2-n$ となる。写像$\psi: E(K) \to E(K)/nE(K)$ はアーベル群の準同型なので、$S \in E(K)$ をランダム

5 $S$、$T$をランダムに選んだとき、$Q=S-T$ も $E(K)$ からランダムに選んだことになるのは、簡単な確率計算で確認できる。

に選ぶとき、 $\{\overline{P}、\overline{Q}\}_0$、$n \notin (K^*)^n$ となる確率は、

$$\frac{\#\psi^{-1}(T)}{\#E(K)} = \frac{\#\mathrm{Ker}(\psi)\times\#T}{\#E(K)}$$
$$= \frac{(n_1n_2/n^2)(n^2-n)}{n_1n_2}$$
$$= 1-1/n$$

となる。

**注意3** 例えば条件 $n^2 \nmid \#E(F_q)$ のもとでは、$E(F_q)$ には位数 $n^2$ の元が存在しないので、$P \notin nE(F_q)$ となる。ゆえにもし $n \mid q-1$ ならば FR pairing の非退化性より、$\{\overline{P}、\overline{P}\}_0$、$n \notin (K^*)^n$ となる。したがって、この場合はランダムに $Q \in E(F_q)$ をとる必要はなく、$Q := P$ とすることで、確率1で FR 帰着が成功する。この場合、$S$、$T$ の取り方について言えば、アルゴリズム2のStep2において、ランダムに $T \in E(K)$（$T \neq P$、$-P$、$O$）を選び、$S$ に対しては、 $S := T+P$ とする。このとき、

$$(S)-(T) = (T+P)-(T) \sim (P)-(O)$$

より、$\overline{P} = (S)-(T)$ となる。

また、次の系は $n \nmid q-1$ならば $Q$ を $E(K)-E(F_q)$ から選ぶことで成功確率をもう少し良くできることを示している。

**系2** $n \nmid q-1$、$n \mid q^k-1$とする（この場合 $K = E(F_{q^k})$、$k \geqq 2$となる）。このとき、$Q$ を $E(K)-E(F_q)$ からランダムに選ぶとき、$\{\overline{P}、\overline{Q}\}_0$、$n \notin (K^*)^n$ となる確率は$\frac{\#E(K)}{\#E(K)-\#E(F_q)}(1-\frac{1}{n})(>1-\frac{1}{n})$ となる。特に、$\frac{\#E(K)}{\#E(F_q)} = n$のとき、確率は1となる。

**補題1** 記号の表記は系2と同様とする。もし $n \geqq 5$ならば、任意の $Q \in E(F_q)$ に対して $Q+kP \neq P$、$Q+kP \neq O$、$kP \neq P$、$kP \neq O$ を満たす $k$、$2 \leqq k \leqq n-1$が存在する。

証明： まず、任意の $k$（$2 \leqq k \leqq n-1$）に対して、$kP \neq O$、$P$ は明らか。

1.ある $k$ について $Q+kP = P$ とする。$k \leqq n-2$ならば、$k$ として $k+1$ を、また $k = n-1$ならば、$k$ として2をとることにより、題意を満たすことができる。

2.ある $k$ について $Q+kP = O$ とする。このとき、$Q+(k+1)P = P$ なので、$k \leqq n-2$ならば先の議論に帰着できる。また、$k = n-1$ならば、$k$ として2をとることにより、題意を満たすことができる。

系2の証明： まず、$div(f) = n((P)-(O))$ とする（$f \in F_q(E)$）。このとき、任意の $Q \in E(F_q)$ に対して、 $f(\overline{Q}) = \mathrm{T} \in K^*/(K^*)^n$ となる［証明：任意の $Q \in E(F_q)$ をとり固定する。このとき、補題1で $R = kP$ とおくと$\frac{f(Q+R)}{f(R)} \neq 0$、$\infty$を満たし、$f$、$Q$、$R$ の取り方より $f(Q+R)$、$f(R) \in F^*_q$。また、$n \mid q^k-1$、$n \nmid q-1$ より$n \mid \frac{q^k-1}{q-1}$となるので、$F^*_q \subset (K^*)^n$ が得られる。ゆえに、$\frac{f(Q+R)}{f(R)} \in F_q^* \subset (K^*)^n$ となる 。したがって、$f(\overline{Q})$ の定義より、$f(\overline{Q}) := \frac{f(Q+R)}{f(R)} = \mathrm{T} \in K^*/(K^*)^n$］。

ここで、$T$、$\psi$を定理2の証明で用いたものとする。このとき、前半の議論から$\psi^{-1}(T) \cap E(F_q) = \phi$より$\psi|: E(K)-E(F_q) \to T$ が全射である。従って $Q$ を $E(K)-E(F_q)$ からランダムに選ぶとき、$\{\overline{P}、\overline{Q}\}_0$、$n \notin (K^*)^n$となる確率は、

$$\frac{\#(\psi\ |\ )^{-1}(T)}{\#E(K)-\#E(F_q)} = \frac{\#\psi^{-1}(T)}{\#E(K)-\#E(F_q)}$$
$$= \frac{\#\mathrm{Ker}(\psi)\times\#T}{\#E(K)-\#E(F_q)} = \frac{(\#E(K)/n^2)(n^2-n)}{\#E(K)-\#E(F_q)}$$
$$= \frac{\#E(K)}{\#E(K)-\#E(F_q)}(1-\frac{1}{n})$$

特に、確率1となるのは、$\frac{\#E(K)}{\#E(K)-\#E(F_q)}(1-\frac{1}{n})^{-1}$ のときで、つまり$\frac{\#E(K)}{\#E(F_q)} = n$の場合である。

$n$ は、相当大きいと仮定しているので、Step4からStep2へ戻る確率は非常に少ないことが分かる。

Step５については、Step３、 Step４と同様の操作をおこなっているので、計算量は $O$（$k^3(\log q)^3$）となる。

以上の考察から、FR 帰着（アルゴリズム２のStep2‐5まで）の平均実行時間を計算すると、$O(k^3 \log^3 q)$ となる。以下では、現実の問題に際して、どの Step の計算に時間がかかるかを、大規模な実装データに基づいて考察する。

### 2.3 実装

本研究では、以下の４個の場合を含め、幾つかの実装に関する実験を行った。ハードウェアは Pentium 75MHz（SONY Quarter L、QL-50NX、the second cashe capacity：256kB）による。

例１、例２では、FR 帰着のアルゴリズムを特にトレース２の楕円曲線に対して実行する。

**例１（トレースが２の楕円曲線、すなわち＃$E(F_p)=p-1$）** 曲線 $E/F_p: y^2=x^3+ax+b$、位数が $n$ の生成元 $P=(x_0, y_0) \in E(F_p)$、$R=[l]P=(x_1, y_1)$ を以下で与える。

$p$＝23305425500899（２進表記で**45桁**、$p-1=2\times3^2\times1137869^2$）、$a$＝13079575536215、$b$＝951241857177、

$n$＝1137869、$x_0$＝17662927853004、$y_0$＝1766549410280、$x_1$＝2072411881257、$y_1$＝5560421985272

この時、以下の手順で FR 帰着を実行する。

１）$S$、$T \in E(F_p)$ をランダムに選ぶ。

$S=(x_2, y_2)$、$x_2$＝6547445868887、$y_2$＝15268497365638

$T=(x_3, y_3)$、$x_3$＝21607570403474、$y_3$＝17017092706263

計算時間：21sec

２）FR pairing を計算する。

$div(f)=n((P)-(O))$、$div(g)=n((R)-(O))$、$D=(S)-(T)$ としたとき、

$\{\overline{P}, \overline{D}\}_0$、$n=\frac{f(S)}{f(T)}$＝10524302872489

$\{\overline{R}, \overline{D}\}_0$、$n=\frac{g(S)}{g(T)}$＝20741597863959

$(\frac{f(S)}{f(T)})^{\frac{p-1}{n}}$＝6517708164097

$(\frac{g(S)}{g(T)})^{\frac{p-1}{n}}$＝14903993396317

計算時間：

$f(S)$ の計算：99 sec

$f(T)$ の計算：99 sec

$g(S)$ の計算：101 sec

$g(T)$ の計算：98 sec

$(\frac{f(S)}{f(T)})^{\frac{p-1}{n}}$ の計算：０sec

$(\frac{g(S)}{g(T)})^{\frac{p-1}{n}}$ の計算：０sec

３）$F^*_p$ 上の離散対数問題

$(6517708164097)^l=14903993396317$

を解き、$l$＝709658を得る。

**例２（トレースが２の楕円曲線、すなわち＃$E(F_p)=p-1$）** 曲線 $E/F_p: y^2=x^3+ax+b$、位数が $n$ の生成元 $P=(x_0, y_0) \in E(F_p)$、$R=[l]P=(x_1, y_1)$ を以下で与える。

$p$＝93340306032025588917032364977153

（２進表記で**107**桁 $p-1=2^{10}\times7^2\times163\times847321^2\times3986987^2$）、

$a$＝712354694036970210519026883668 16、

$b$＝474903129357980140346017922445 44、

$n$=3986987、

$x_0$＝103624099299650416143178356924 63、

$y_0$＝795290491914689056521723060355 73、

$x_1$＝154113495854233214689442210898 88、

$y_1$＝941605290788327808878233583003 3

この時、以下の手順でFR帰着を実行する。

１）$S$、$T \in E(F_p)$ をランダムに選ぶ。

$S=(x_2, y_2)$、$x_2$＝781831266536229655644442556815 46、

$y_2$＝785889451358545608004936721812 65

$T=(x_3, y_3)$、$x_3$＝587146588843218597063396580123 14、

$y_3$＝293523592943075483044814000791 14

計算時間：177 sec

2）FR pairing を計算する。

$div(f)=n((P)-(O))$、$div(g)=n((R)-(O))$、$D=(S)-(T)$ としたとき、

$\{\overline{P}、\overline{D}\}_0$、$n=\frac{f(S)}{f(T)}$ =280896737020849225791892103620 50

$\{\overline{R}、\overline{D}\}_0$、$n=\frac{g(S)}{g(T)}$ =545381056152818070323809147441 28

$(\frac{f(S)}{f(T)})^{\frac{p-1}{n}}$ =860485481197365375119399092795 95

$(\frac{g(S)}{g(T)})^{\frac{p-1}{n}}$ =441794237239751734273448931821 75

計算時間：

$f$（$S$）の計算：982 sec

$f$（$T$）の計算：996 sec

$g$（$S$）の計算：971 sec

$g$（$T$）の計算：968 sec

$(\frac{f(S)}{f(T)})^{\frac{p-1}{n}}$ の計算：５sec

$(\frac{g(S)}{g(T)})^{\frac{p-1}{n}}$ の計算：６sec

3）$F^*_p$ 上の離散対数問題

$(860485481197365375119399092795 95^l=441794237239751734273448931821 75$を解き、$l=764009$を得る。

例１、例２では拡大次数 $k=1$なので、3.2節の最後に考察したように、FR 帰着の各 Step の計算量はいずれも$O(\log^3 q)$となり、特に平方根を求める計算量も無視できないはずであった。ところが例１、例２の実際の実装データでは、pairing の計算量が全体の大部分をしめていることが分かる。

次の例３、例４では超特異楕円曲線に対して、FR 帰着および MOV 帰着を実行し、両者の実装データを比較してみる。

**例３（超特異楕円曲線）**曲線 $E/Fp: y^2=x^3+ax+b$、位数が $n$ の生成元 $P=(x_0、y_0)\in E(F_p)$、$R=[l]P=(x_1、y_1)$ を以下で与える。

$p$＝23305425500899（２進表記で**45**桁、$p+1=2^2\times5^2\times29\times1217\times6603413$）、

$a=1$、$b=0$、$n=6603413$、

$x_0=18414716422748$、$y_0=9607997424906$、

$x_1=22829488331658$、$y_1=15463570264423$

今、$E(F_p)\cong Z_{p+1}$、$E(F_p^2)\cong Z_{p+1}\oplus Z_{p+1}$なので［12］、２次拡大体 $F_p^2$上で、FR 帰着および MOV 帰着を実行する。ここで、$F_p^2\cong F_p[\alpha]/g(\alpha)$、$g(\alpha)=\alpha^2+1$とする。

**(FR帰着)：**１）$S$、$T\in E(F_p^2)$をランダムに選ぶ。

$S=(x_2、y_2)$、$x_2=2\alpha+1$、$y_2=5082265331371$

$T=(x_3、y_3)$、$x_3=12597365260456$、$y_3=7074814188341$

計算時間：53 sec

２）FR pairing を計算する。

$div(f)=n((P)-(O))$、$div(g)=n((R)-(O))$、$D=(S)-(T)$ としたとき、

$\{\overline{P}、\overline{D}\}_0$、$n=\frac{f(S)}{f(T)}$ =512914823171$\alpha$ +6345799643121

$\{\overline{R}、\overline{D}\}_0$、$n=\frac{g(S)}{g(T)}$ =2171013538342$\alpha$ +5170682846849

$(\frac{f(S)}{f(T)})^{\frac{p^2-1}{n}}$ =13658110482464$\alpha$ +9714164225724

$(\frac{g(S)}{g(T)})^{\frac{p^2-1}{n}}$ =6585153989459$\alpha$ +21359314672278

計算時間：

$f$（$S$）の計算：238 sec

$f$（$T$）の計算：231 sec

$g$（$S$）の計算：235 sec

$g$（$T$）の計算：233 sec

$(\frac{f(S)}{f(T)})^{\frac{p^2-1}{n}}$ の計算：４sec

$(\frac{g(S)}{g(T)})^{\frac{p^2-1}{n}}$ の計算：４sec

３）$F_{p^2}{}^*$上の離散対数問題

$(13658110482464\alpha+9714164225724)^l$

$=6585153989459\alpha+21359314672278$

を解き、$l=4500974$を得る。

**(MOV 帰着)：** $S$、$T$ は、FR 帰着の場合と同様とする。

1）位数 $n$ の元 $Q=(x_4、y_4)=[\frac{p+1}{n}]$ を計算する。

ここで、$x_4=19767140138478\alpha$、

$y_4=7558009608324\alpha+15747415892575$

計算時間：$Q$ の計算：69 sec

2）Weil pairing を計算する。

$div(f)=n((P+S)-(S))$、$div(g)=n((R+S)-(S))$、$div(h)=n((Q+T)-(T))$ としたとき、

$e_n(P、Q)=\frac{f(Q+T)}{f(T)}\times\frac{h(S)}{h(P+S)}$

$=9647315018435\alpha+9714164225724$

$e_n(R、Q)=\frac{g(Q+T)}{g(T)}\times\frac{h(S)}{h(R+S)}$

$=16720271511440\alpha+21359314672278$

計算時間：

$f(Q+T)$ の計算：250 sec

$f(T)$ の計算：251 sec

$h(S)$ の計算：255 sec

$h(P+S)$ の計算：256 sec

$g(Q+T)$ の計算：246 sec

$g(T)$ の計算：248 sec

$h(R+S)$ の計算：260 sec

3）$F_{p^2}{}^*$上の離散対数問題

$(9647315018435\alpha+9714164225724)^l$

$=16720271511440\alpha+21359314672278$

を解き、$l$=4500974を得る。

**例４（超特異楕円曲線）**曲線 $E/F_p：y^2=x^3+ax+b$、位数が $n$ の生成元 $P=(x_0、y_0)\in E(F_p)$、$R=[l]P=(x_1、y_1)$ を以下で与える。

$p=1020213065766829380286510327794694206930683196983$

（２進表記で**163**桁、$p+1=2^3\times3^3\times59\times113\times708445873377740404845389902584519528254884 7$）、

$a=-1$、$b=0$、

$n=70844587337774040484538990258451952825488 47$、

$x_0=6361408431660145018472734964469918949727993631117$、

$y_0=2224285726125163515264642109319596318772261492 91$、

$x_1=1791400202383882094094972648523798358242766050148$、

$y_1=6662282879825452479945554028296857282243572635001$

今、$E(F_p)\cong Z_{\frac{p+1}{2}}\oplus Z_2$、$E(F_{p^2})\cong Z_{p+1}\oplus Z_{p+1}$なので［12］、２次拡大体 $F_{p^2}$上で、FR 帰着および MOV 帰着を実行する。ここで、$F_{p^2}\cong F_p[\alpha]/g(\alpha)$、$g(\alpha)=\alpha^2+1$とする。

**(FR帰着)：** 1）$S$、$T$ $\in E(F_{p^2})$をランダムに選ぶ。

$S=(x_2、y_2)$、

$x_2=5$、$y_2=27852796410200185179475948855871584013745987522 49\alpha$

$T=(x_3、y_3)$、

$x_3=33853061138514517118689385450582211861725979374 36$、

$y_3=49867706544069535317451861847580269610486195989 92$

計算時間：2245 sec

2）FR pairing を計算する。

$div(f)=n((P)-(O))$、$div(g)=n((R)-(O))$、$D=(S)-(T)$ としたとき

$\{\overline{P}、\overline{D}\}_{0、n}=\frac{f(S)}{f(T)}$

$=3533166625479465632799073949081211397797456268974\alpha$

$+4001496656282493042880656119736166996221452751615$

$\{\overline{R}、\overline{D}\}_{0、n}=\frac{g(S)}{g(T)}$

$=7618053821224285687383466174720252396501663499416\alpha$

$+5910267516953452268669659762088222325143176074230$

$(\frac{f(S)}{f(T)})^{\frac{p^2-1}{n}}$

＝501035026731987279504884889683664624292006059759 2α

＋684597904528238743074511834101748764895625936788 9、

$(\frac{g(S)}{g(T)})^{\frac{p^2-1}{n}}$

＝135433531518182121168248536585921809875527887737 8α

＋865441031838417931745198119632221028739343235484 7、

計算時間：

$f(S)$ の計算：39667 sec

$f(T)$ の計算：40023 sec

$g(S)$ の計算：39634 sec

$g(T)$ の計算：39646 sec

$(\frac{f(S)}{f(T)})^{\frac{p^2-1}{n}}$ の計算：116 sec

$(\frac{g(S)}{g(T)})^{\frac{p^2-1}{n}}$ の計算：136 sec

3）$F_{p^2}{}^*$上の離散対数問題

（501035026731987279504884889683664624292006059759 2α

＋684597904528238743074511834101748764895625936788 9）$^l$

＝135433531518182121168248536585921809875527887737 8α

＋865441031838417931745198119632221028739343235484 7

を解き、$l$＝388267735689900037826187381399337 8を得る。

**（MOV帰着）：**$R$、$S$ は、FR 帰着の場合と同様とする。

1）位数 $n$ の元 $Q$＝($x_4$、$y_4$)＝$[\frac{p+1}{n}]S$ を計算する。ここで、

$x_4$＝268607399899856195293423320463290449641853638513 8、

$y_4$＝769368303013534155401573490515765808450022343909 5α

計算時間： $Q$ の計算：1203 sec

2）Weil pairing を計算する。

$div(f)$＝$n((P+S)-(S))$、$div(g)$＝$n((R+S)-(S))$、$div(h)$＝$n((Q+T)-(T))$としたとき、

$e_n(P、Q)=\frac{f(Q+T)}{f(T)}\times\frac{h(S)}{h(P+S)}$

＝519178039034842100781625438111029581801062259939 1α

＋684597904528238743074511834101748764895625936788 9

$e_n(R、Q)=\frac{g(Q+T)}{g(T)}\times\frac{h(S)}{h(R+S)}$

＝884779534248647259118261791208772396217540431960 5α

＋865441031838417931745198119632221028739343235484 7

計算時間：

$f(Q+T)$の計算：39972 sec

$f(T)$の計算：39720 sec

$h(S)$の計算：39626 sec

$h(P+S)$の計算：39850 sec

$g(Q+T)$の計算：39992 sec

$g(T)$の計算：39956 sec

$h(R+S)$の計算：39862 sec

3）$F_{p^2}{}^*$上の離散対数問題

（519178039034842100781625438111029581801062259939 1α

＋684597904528238743074511834101748764895625936788 9）$^l$

＝884779534248647259118261791208772396217540431960 5α

＋865441031838417931745198119632221028739343235484 7

を解き、$l$＝388267735689900037826187381399337 8を得る。

FR 帰着、MOV 帰着を上述のように実行するのに際して、ランダムな点はそれぞれ２個必要とされ、それを用いて FR 帰着、MOV 帰着の pairing に必要な関数値の個数はそれぞれ４個、７個であった。実際の計算時間について考察してみると、両者とも全体の計算のうち関数値の計算が大部分をしめていることがわかった。（表１）。

**表1　例1～例4の実行時間**

| タイプ | $\log q$ | $k$ | 実行時間 (sec) | |
|---|---|---|---|---|
| 例 1 | 46 | 1 | FR 帰着 | 419 |
| 例 2 | 108 | 1 | FR 帰着 | 4105 |
| 例 3 | 46 | 2 | FR 帰着 | 999 |
| | | | MOV 帰着 | 1872 |
| 例 4 | 164 | 2 | FR 帰着 | 161467 |
| | | | MOV 帰着 | 282426 |

$q$を定義体の大きさ、$k$を拡大次数とする。

実装データおよび上述の考察から、FR 帰着、MOV 帰着を実行するのに際して、理論的には $O(log^3 q)$かかる Step が他にあるにもかかわらず、実際には必要とする関数値の計算の負担が大きいことが分かる。したがって、FR、MOV 両帰着の全体の計算時間の比は、おおよそ必要な関数値の個数の比４：７になっていることがわかる。これは3.2節の解析だけからでは得られなかった発見である。

## 3　MOV帰着 と FR 帰着の比較

本研究では、ある種の非超特異楕円曲線に対する MOV 帰着の具体的な実現方法を提案した。また、FR 帰着を実現する具体的なアルゴリズムを考察し、その実装を行った。ここでは、その２つの帰着の比較を検討する。

### 3.1　拡大次数について

MOV 帰着に関して、一般には、R. Schoof［18］による以下の群構造に関する事実が知られている。

**命題２**（[19]）次の２つの条件は同値である。

1. $E[n] \subset E(F_{q^k})$
2. $n \mid q^k-1$, $n^2 \mid \#E(F_{q^k})$, かつ $\phi \in Z$ または$O\left(\frac{t_k^2-4q^k}{n^2}\right) \subset \mathrm{End}_{F_{q^k}}(E)$,

ここで、$\phi, t_k$ は、それぞれ $E$ の $q^k$ 乗 *Frobenius* 自己準同型写像とそのトレースとする。また、$O\left(\frac{t_k^2-4q^k}{n^2}\right)$、$\mathrm{End}_{F_{q^k}}(E)$をそれぞれ判別式が $\frac{t_k^2-4q^k}{n^2}$ である*order*、$F_{q^k}$ 上定義された同種写像からなる $E/F_{q^k}$ の自己準同型環とする。

これより、一般に $FR$ 帰着の適用条件が、 MOV 帰着のそれを含むことがわかる。ところが、ある条件のもとでは、FR 帰着と MOV 帰着の適用条件の差異(つまり、定義体の拡大次数 $k$ に関する条件)はそれほど大きくないことが知られている。実際、*R. Balasubramanian*, N. Koblitz［5］により以下のことが証明された。

**命題３**（[5]）$n$ は $n \neq p$ を満たす素数とする。もし $n \nmid q-1$ ならば、

$$E[n] \subset E(F_{q^k}) \Leftrightarrow n \mid q^k-1$$

また、命題３の証明［5］と同様にして、以下の事実を証明できる。この結果は、文献［5］から明らかであるが、MOV帰着とFR帰着の拡大次数を比較する上で重要なので、注意としてあげておく。

**注意４** $E[n] \subset E(F_q)$ とし、$n$は $p \neq n$ を満たす素数とする。もし $n \mid q-1$ ならば、

$$E[n] \subset E(F_{q^k}) \Leftrightarrow k = nj\ (j \geq 1)$$

証明: $q$乗 Frobenius 自己準同型写像 $\phi$ の $E[n]$ 上の行列表現が

$$M_\phi = \begin{pmatrix} 1 & a \\ 0 & q \end{pmatrix} = \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \in GL_2(Zn)$$

( $q \equiv 1 \bmod n$ であることに注意)で与えられるような $E[n]$ の基底 $\{P, T\}$ を選ぶ。この時、$\phi^k$ を表す行列 $M\,\phi^k$ は、$M\phi^k = (M\phi)^k = \begin{pmatrix} 1 & ka \\ 0 & 1 \end{pmatrix}$となる。ゆえに、

$$\phi^k(T) = T \Leftrightarrow ka \equiv 0 \mod n \Leftrightarrow k \equiv 0 \bmod n$$

ここで、$E[n] \not\subset E(F_q)$ なので、$a \not\equiv 0 \bmod n$ となることを用いた(もし $a \equiv 0 \bmod n$ ならば、$\phi$ の $E[n]$ 上の行列表現が

M $\phi = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$となり、これは $E[n] \subset E(F_q)$ を意味することになり、仮定に反する)。ゆえに、$k = nj, j \geq 1$ となる。

もし、$E[n] \not\subset E(F_q)$, $n|q$-1 ならば、注意4から拡大次数 $k$ は $n$ 未満にならないことがわかり、このことはさらに、拡大に対して指数的な計算量がMOV帰着で必要とされることを意味する。よって、MOV帰着の適用をあきらめなければならない。

### 3.2 帰着の効率性について

次に、 $n \not| q$-1 の場合における提案MOV帰着とFR 帰着の効率性の比較を行う。

ここで、楕円曲線上の離散対数問題からFR、MOV両帰着によってそれぞれ得られた有限体の乗法群上の離散対数問題が、本質的に同じ困難性をもつとする。このとき、比較すべきことは、それぞれの帰着の主要部分、すなわちアルゴリズム１のSteps２,３とアルゴリズム２のSteps ２-５である。

しかしながら、２節で考察したように、FR帰着と比較して我々の提案したMOV帰着では $E(F_q{}^k)$ の群構造を見つけることを必要としている。もっとも、それは一般に$k$ log $q$ の準指数時間以下で実行される。(変換後の有限体上の離散対数問題が log $q$ の準指数時間で解けるような $k$ に対しては、これも log $q$ の準指数時間以下で実行される。) さらに、本研究で提案したMOV帰着の適用については、定理 1 における$e$が 1以上の場合は、あきらめなければならない。また、実用上は、Weil pairing は FR pairing に比べて、計算機上ではおおよそ２倍の計算量が必要であることにも注目すべきである。

### 3.3 ２つの帰着の条件間の実際の差異について

本研究では、FR帰着とMOV帰着の適用範囲の差を明確にした。すなわち、現時点では

1. $n|q$-1、 または
2. $E[n] \subset E(F_q)$、$c_2 n | c_1$

の場合には、FR帰着が適用され、MOV帰着が実際上は適用が困難である(条件(2)が除外できるか否かは今後の課題でもある)。さらに、我々の提案したMOV帰着の実行の際には、$E(F_q{}^k)$ の群構造に関する情報が必要である。従って、それを計算するために、

3. $E(F_q{}^k)$の因数分解

が必要となってくる。(Millerのアルゴリズムは完全な因数分解を必要としない場合があるので、このことはすぐに解かれるかもしれない。)たとえ将来、上記(2)の場合が解決されたとしても、つまりMOV帰着が(2)の場合に具体的に実現されたとしても、実用上は$E[n]$ の元を求める計算過程がFR帰着に比べて余分に必要であるのに変わりはない。また計算機上では、Weil pairing の計算は、FR pairingのそれの約２倍の実行時間が必要となる。

以上の考察から、本研究では、いかなる場合においても、実用上、FR帰着がMOV帰着よりも同等以上に効率的であることがわかる。この意味でFR帰着はMOV帰着より優れているという結論を得る。

また、変換後の離散対数問題を含めた漸近的な計算量評価としては、条件(1)の場合はFRアルゴリズムがlog $q$の準指数時間で解けるのに対し、MOVアルゴリズムは log $q$ の指数時間かかる。それ以外の場合、FR、MOVアルゴリズムで必要な拡大次数は同じで、仮に変換後の離散対数問題が log $q$ の準指数時間で解けるとすると、FR、MOVアルゴリズムの差は前者が log $q$ の準指数時間で解けるのに対して、後者は条件(2)以外のときは我々の提案アルゴリズムによりlog $q$ の準指数時間で解けるが、条件(2)のときには log $q$ の指数時間かかる可能性がある。この意味でFRアルゴリズムはMOVアルゴリズムより優れているという結論を得る。

### 参考文献


[1] L. Adleman, J. DeMarrais, and M. Huang, *A subexponential algorithm for discrete logarithms over the rational subgroup of the Jacobians of large genus hyperelliptic curves over finite fields*, Algorithmic Number Theory, Lecture Notes in Computer Science, volume 877, Springer-Verlag, 1994, pp. 28-40.

[2] A. O. Atkin, *The number of points on an elliptic curve modulo a prime*, preprint, 1988.

[3] A. Atkin and F. Morain, *Elliptic curves and primality proving*, Mathematics of Computation 61 (1993), 29-68.

[4] E.Bach, *Algorithmic Number Theory,Volume I; Efficient Algorithms*, MIT Press, Cambridge, Massachusetts, 1996.

[5] R. Balasubramanian and N. Koblitz, *The improbability that an elliptic curve has subexponential discrete log*

*problem under the Menezes-Okamoto-Vanstone algorithm*, Journal of Cryptology 11 (1998), 141-145.

[6] N. Elkies, *Explicit isogenies*, preprint, 1991.

[7] G. Frey and H. Rück, *A remark concerning m-divisibility and the discrete logarithm in the divisor class group of curves*, Mathematics of Computation 62 (1994), 865-874.

[8] M. Kac, *On the notion of recurrence in discrete stochastic processes*, Ann. of Math. Statist., 53 (1947), 1002-1010.

[9] N. Koblitz, *Elliptic curve cryptosystems*, Mathematics of Computation 48 (1987), 203-209.

[10] N. Koblitz, *A Course in Number Theory and Cryptography*, Springer-Verlag, New York, 2nd edition, 1996.

[11] H. W. Lenstra, *Factoring integers with elliptic curves*. Annals of Mathematics, 126 (1987), 649-673.

[12] A. Menezes, T. Okamoto, and S. Vanstone, *Reducing elliptic curve logarithms to logarithms in a finite field*, IEEE Transactions on Information Theory 39 (1993), 1639-1646.

[13] A. Menezes, *Elliptic curve public key cryptosystems*, Kluwer Academic Publishes (1994).

[14] M V. S. Miller, *Use of elliptic curves in cryptography*, Advances in Cryptography CRYPTO ' 85 (Lecture Notes in Computer Science, vol 218), Springer-Verlag, 1986, pp. 417-426.

[15] V. Miller, *Short program for functions on curves*, unpublished manuscript, 1986.

[16] S.C.Pohlig and M.E.Hellman, *An improved algorithm for computing logarithms over GF(p) and its cryptographic significance*, IEEE Transactions on Information Theory, 24 (1978),pp 106-110.

[17] T. Satoh and K. Araki, *Fermat quotients and the polynomial time discrete log algorithm for anomalous elliptic curves*, Commentarii Math,Univ,Saniti Pauli, 47 ,1,pp 81 - 92 (1998).

[18] R. Schoof, *Nonsingular plane cubic curves over finite fields*, Journal of Combinatorial Theory, Vol. A. 46 (1987), 183-211.

[19] R. Schoof, Elliptic curves over finite fields and the computation of square roots modulo *p* Math. Comp. 44 (1985), 483-494.

[20] I. Semaev, *Evaluation of discrete logarithms in a group of p-tortion points of an elliptic curve in characteristic p*, Mathematics of Computation 67 (1998), 353-356.

[21] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Graduate Texts in Math., vol. 106, Springer-Verlag, Berlin and New York, 1994.

[22] J. H. Silverman, J. Suzuki, *Elliptic curve discrete logarithms and index calculus*, ASIACRYPT ' 98 (Lecture Notes in Computer Science,vol. 1514), Springer-Verlag, 1998 ,pp 110-125

[23] N. Smart, *The discrete logarithm problem on elliptic curves of trace*, preprint, 1997.

[24] J. Tate, *WC-groups over p-adic fields*, Ann. Sci. Ecole Norm. Sup. 2 (1969), 521-560

## ＜ 発　表　資　料 ＞

| 題　　名 | 掲載誌・学会名等 | 発表年月 |
|---|---|---|
| Fast Jacobean Group Arithmetic cheme for algebraic curve Cryptography | IEICE Trans. Form Damentals. | 2001年１月 |
| Fast Jacobean Group Arithmetic on Cab Curves | Int. Symp. on Algorithmic Number Theory (ANTS IV) | 2000年７月 |
| An Efficient Jacobean Group Arithmetic for Algebraic curve Cryptography | 電子情報通信学会情報セキュリティ研究会 | 2001年７月 |