数学アルゴリズム問題の研究調査

２００２年度

「数学アルゴリズム問題の研究調査」

1　はじめに

本文書は楕円暗号の安全性の根拠である楕円曲線離散対数問題について、公開鍵暗号の安全性評価の際の基礎資料として用いられることを前提とした調査報告書である。

本報告書に於いて「現在」とは 2002 年 8 月を指す。

記号：

p を素数、N を自然数とし、$q = p^N$ とおく。本稿に於いて p, q, N は常にこの関係を満たしているものとする。q 個の要素からなる有限体を $\mathbf{F}_q$ と書く。$\mathbf{F}_q$ 上定義された楕円曲線 E と $\mathbf{F}_q$ の有限次拡大体 k に対して E の k 有理点のなす群を $E(k)$ と書く。E の無限遠点を $\mathcal{O}$, 自己準同型環を $\mathrm{End}(E)$ により表す。E 上の X 座標関数、および Y 座標関数はそれぞれξ, η と書かれる。$n \in \mathbf{N}$ に対して p^n 乗 Frobenius 射を Fr_{p^n} と書く。n が N の倍数のとき（すなわち、p^n が q のベキとなるとき）は $\mathrm{Fr}_{p^n} \in \mathrm{End}(E)$ となる。

一般に、群 G と $g_1, \ldots, g_n \in G$ に対してそれらが生成する G の部分群を $\langle g_1, \ldots, g_n \rangle$ と書く。

2　楕円曲線離散対数問題

E を $\mathbf{F}_q$ 上定義された楕円曲線とする。**楕円曲線離散対数問題**とは一般の可換群に対する離散対数問題を $E(\mathbf{F}_q)$ に適用してできる問題であり、具体的に書くと

$B \in E(\mathbf{F}_q)$, $A \in \langle B \rangle$ が与えられたとき $A = mB$ となる整数 m $(0 \leq m < \nu)$ を求めよ

（ここで ν は base point B の位数。）となる。既に述べたように楕円曲線離散対数問題は一般的な離散対数問題のなかの一つの問題であるから一般的な離散対数問題の解法が適用できることはいうまでもない。特に Pohlig-Hellman の解法が適用できないために

(*) ν は大きな素数であり、ν^2 は $E(\mathbf{F}_q)$ を割らない

としてよい。ここでは楕円曲線離散対数問題に固有の解法について考察する。

楕円離散対数問題の解法（＝楕円曲線暗号・署名への攻撃）は以下のように大別される

(1) ほとんどすべての楕円曲線に適用できる。

(2) 特定の楕円曲線に適用できる、あるいは特定の楕円曲線の場合に特に効率良く楕円曲線離散対数問題を解くことができる。この場合さらに解法の適用対象となる楕円曲線に関して以下のような状況に分類される。

(A) 必要条件が分かっている。

(A+) 必要十分条件が分かっている。

(B) 必要条件は分かっていないが、十分条件は分かっている。

(C) 必要条件も十分条件も分かっていない。

このどの場合に該当するかで楕円曲線離散対数の困難性を維持するための方策が異る。現在までに、(1) 型の解法で、楕円曲線暗号に対して脅威となる方法は筆者の知る限り得られていない。(A) あるいは (A+) の場合、楕円曲線暗号の安全性という立場からは、必要条件を満たさない曲線を採ることでこの解法の適用を逃れることができる。(B) の場合、少なくとも十分条件に合致する楕円曲線は採用すべきではない。ただし、必要条件が分からない以上、十分条件に合致しないからといってこの解法が全く適用できないということにはならないことに注意を要する。(C) の場合、今後さらに研究が必要である。

2.1 乗法群への埋め込み

これは上記分類では (A+) 型である。$k := \min_{\nu|(q^n-1)} n$ とおいたとき $\langle B \rangle$ の離散対数を Weil pairing あるいは Tate pairing を用いて $\mathbf{F}_{q^k}$ の離散対数問題に帰着させる。後者には現時点で既に index calculus 法という「q^k に関して」準指数時間のアルゴリズムがある。Weil pairing を用いる方法は Menezes, Okamoto, Vanstone[24], Semaev[32] らにより、Tate pairing を用いる方法は Frey, Rueck[9] による。k の値が小さくなることが MOV reduction の必要条件であることが Balasubramanian, Koblitz[2] により証明されている。

k の値を求めることは一般には自明ではないが、k の値が少なくとも $O(\log q)$ ではないことは簡単に検証できる。超特異曲線に対しては常に $k \leq 6$ となる。ランダムに選んだ楕円曲線に対して k の値が有界な範囲に属する確率はおおよそ $O(1/\sqrt{q})$ である。

2.2 加法群への埋め込み

これは上記分類では (A+) 型であり、(条件 (*) の下で) 適用可能となる必要十分条件は$\nu = p$ である。$\mathrm{Tr}(\mathrm{Fr}_q) \equiv 1 \bmod p$ であるとき、$E(\mathbf{F}_q)$ は自明ではない p torsion 部分群を持つ。この p torsion 部分群に対する離散対数問題は $\mathbf{F}_q$ への多項式時間埋め込みを使って効率良く解くことができる。この埋め込みは現在のところ大きく分けて二つの方法がある。

(1) 代数幾何的方法 (Semaev[33])

(2) 数論的方法 (Smart[37], Satoh-Araki[28, 29])

後者の方が多少高速であるが、楕円曲線離散対数の困難性という観点からこの二つの方法の計算量の差は無視でき、いずれの方法でも、E 上の点の加法を $O(\log q)$ 回実行する時間で離散対数が解かれる。特に素体上の楕円曲線に対しては $\mathrm{Tr}\,\mathrm{Fr}_p = 1$ となるとき $\nu = p$ となり楕円離散対数は多項式時間で完全に解かれてしまう。このような楕円曲線は Mazur[22] に従って anomalous curve と呼ばれる。

解法の概要は以下のようなものである。E, B, A を p 進体 $\mathbf{Q}_p$ に持ち上げたものをそれぞれ$\tilde{E}$, $\tilde{B}$, $\tilde{A}$ とする。$p\tilde{B}$ に対応する local parameter $\tau_B := -\xi(p\tilde{B})/\eta(p\tilde{B})$ が $0 \bmod p^2$ なら別の持ち上げを取る。そうでなければ $\tau_A := -\xi(p\tilde{A})/\eta(p\tilde{A})$ も $0 \bmod p^2$ ではなく $m := \tau_A/\tau_B$ が $A = mB$ となる m を与える。この方法で正しい答が求まることを示すときに B の位数が p がであることが随所で使われ、そうでない場合に一般化するのは困難であろうと思われる。(そもそも、$\langle B\rangle$ から $\mathbf{F}_p$ への群準同型はすべて 0 写像となってしまう。) この解法を回避するため、$\nu = p$ すなわち $pB = \mathcal{O}$ となる E を用いてはならない。ランダムに選んだ $\mathbf{F}_p$ 上の楕円曲線が anomalous になる確率は $O(1/\sqrt{p})$ である。

2.3 自己同型写像による高速化

この方法は (B) 型である。可換群 $E(\mathbf{F}_q)$ の (可換群としての) 自己同型写像のなす群を A とする。(これは代数曲線 E の自己同型群 $\mathrm{Aut}(E)$ **ではない**。A は $\mathrm{Aut}(E)$ よりも遥かに大きな群であり、$\mathrm{Aut}(E)$ が小さいことと A が小さいことの間には何の関係もない。) A は $E(\mathbf{F}_q)$ に左から作用しているが、A の各元は $E(\mathbf{F}_q)$ の各点の位数を変えないから条件 (*) の基で $\langle B\rangle$ は A 不変、すなわち任意の $f \in A$ に対して $\lambda_f \in \mathbf{Z}$ で $f(B) = \lambda_f B$ となるものがある。

A の部分群 G で

(i) $\langle B\rangle$ の点が $G \setminus \langle B\rangle$ のどの軌道に入るかを判定する時間が E 上の加法に要する計算時間に比して無視できる

(ii) $f \in G$ に対して λ_f が既知である

というものがあれば、Pollard の ρ 法を $\langle B \rangle$ に適用したときの計算時間は一般の群に対する ρ 法の計算時間に比べて $1/\sqrt{\#G}$ になることが Wiener, Zuccherato[39], Gallant, Vanstone[12] により指摘されている。**どのような楕円曲線に対しても** $T := \langle -1 \rangle$ は上記条件を満たすことに注意する（このとき $\lambda_{-1} = -1$, $\#T = 2$ である）。ここでは、これを「自明な改良」と呼ぶことにする。

d が N の約数で E が $\mathbf{F}_{2^d}$ 上定義されている状況を考える。簡単のため、$\psi_d := \mathrm{Fr}_{2^d}$ とおく。$G := \langle -1, \psi_d \rangle$ は上記条件を満たす。このとき $\#G$ は A の元として $-1 \in \langle \psi_d \rangle$ なら N/d, そうでなければ $2N/d$ である。また d の値は $O(\log q)$ だから楕円曲線暗号に用いる N に対しては λ_{ψ_d} は全数探索などで簡単に求まる。この場合、自明な改良に比べて離散対数問題を最大限 $\sqrt{N/d}$ 倍速く解くことができる. （なお、ここでは自明な改良さえ用いない、一般の群に対する ρ 法を比較の対象とはしない。）この解法がもっとも良く機能するのが $d = 1$ となる Koblitz 曲線 [21] （anomalous binary curve, 略して ABC）の場合である。このような G による解法を回避するためには E の定義体が $\mathbf{F}_q$ の真の部分体とはならないようにすれば良い。また、何らかの事情により E の定義体が $\mathbf{F}_q$ の真の部分体となる場合は ν を一般の場合に安全と見込まれる値よりも $\sqrt{N}$ 倍以上大きく取ることが必要である（が、十分であるかどうかは分からない）。

また、efficient endomorphism を持つ楕円曲線については今後検討する必要がある。これは efficient endomorphism とは Gallant, Lambert, Vanstone[13] により提唱された概念で、少ない計算量で計算できる自己準同型のことを指す。このような自己準同型を持つ曲線では曲線上の整数倍演算が高速に行える。この結果は Park, Keong, Kim, Lim[27], Sica, Ciet, Quisquater[34] により厳密な証明がつけられ、なおかつ一段の高速化が計られているが、他方において自己同型写像による攻撃をも効率化する。Gallant, Lambert, Vanstone[13] は（証明・数値例をつけずに）「適用対象とならない」とだけ述べている。この点について、理論的な検証・数値実験等を行う必要があると思われる。

これ以外の場合に自己同型写像による方法の適用可能な場合を系統的に調べた文献を筆者は知らない。A は $\mathrm{Aut}(E)$ よりもだいぶ大きな群であるが、他方、あまり $\#G$ が大きくなると (i) のための計算時間が無視できなくなる可能性があり、今後この解法の適用範囲についてさらなる検討が必要と思われる。

2.4 Weil descent による方法

$\mathbf{F}_q$ 上の楕円曲線 E 上の離散対数問題を E を $\mathbf{F}_q$ 部分体に係数制限してできる Abel 多様体に含まれる超楕円曲線 の Jacobian 上の離散対数に帰着させ

るものである。基本的な枠組は Frey[8] により示され、Galbraith, Smart[10] により実行時間が準指数時間であることが示された。Gaudry, Hess, Smart[15] では具体的な一つのアルゴリズムが与えられた。これを 以下 GHS 法と呼ぶことにする。GHS 法を適用するための必要条件は Menezes, Qu[23] により明らかにされたが、Weil descent の枠組で論ぜられる一般のアルゴリズムがどの場合に適用できるかは現在のところ知られていない。GHS 法は (A) 型に分類されるが Weil descent 自体は (C) 型であるといえる。

以下、d を N の約数（$d \neq N$ とするが $d = 1$ は認める）とし、$n := N/d$, $k := \mathbf{F}_{2^d}$ とおく。楕円曲線 $E/\mathbf{F}_q$ に対して A を E の k への係数制限とする。A は n 次元の Abel 多様体である。このとき Gaudry, Hess, Smart[15] は n が偶数のときすべての E に対して、また n が奇数でおおよそ半分の E に対して A と（E に依存しない）$n-1$ 個の超平面との共通部分の既約成分が超楕円曲線 C になることを示し、しかも $E(\mathbf{F}_q)$ から C の Jacobi 多様体 $J_C(k)$ への計算可能な群準同型を与えた。もしこの準同型写像の $\langle B \rangle$ への制限が単射ならば $\langle B \rangle$ 上の離散対数を $J_C(k)$ の離散対数に帰着できる。このようにして作られた C の genus g は E に依存するが、もし $J_C(k)$ 上の離散対数問題が解けるのなら $\langle B \rangle$ 上の離散対数問題も解けてしまう。$J_C(k)$ 上の離散対数を解く方法には一般的な Pollard の ρ 法以外にも Adleman, DeMarrais, Huang[1] による準指数時間アルゴリズムや Gaudry[14] などの方法がある。上述のようにして構成された C に対して $J_C(k)$ の離散対数問題が解けるとは限らないが、$\langle B \rangle$ 上の離散対数を ρ 法を用いて解くよりは速くなる場合があり得る。Menezes, Qu[23] は GHS 法が適用できる場合を分析して、その適用対象は限定的であるとしている。たとえば n が素数の場合、$\mathbf{F}_n$ における 2 の位数が小さい（現在のところせいぜい 13 以下）ことが必要である。（もし、この値が大きければこの N に対して $\mathbf{F}_q$ 上の全ての楕円曲線が GHS 法の適用対象とならない。）ただし、これはあくまでも GHS 法そのまま適用した場合の結果であり Galbraith, Hess, Smart[11] らは GHS 法を拡張し、より多くの曲線が GHS 法の適用対象になりえることを示した。彼らによればランラムに選ばれた $\mathbf{F}_{2^{155}}$（注：$155 = 5 \times 31$）に対して元の GHS 法が適用可能となる確率は 2^{-122} だが拡張された GHS 法を用いたときのこの確率は 2^{-52} とのことである。

GHS 法を回避するだけならば N を素数でかつ $\mathbf{F}_N$ における 2 の位数が小さくならないようなものとすればよい。（160 から 600 までの素数はすべてこの条件を満たす。）しかし特定の拡大次数 N が Weil descent の一般的な枠組にたいしてその適用対象となり得るかということについては現在のところ知られていない。N の約数が多ければそれだけ適用パターンが増えることから N を素数とすることが考えられるが、これだけでは不十分（たとえば $N = 127$ は GHS 法に対して弱いと考えられている）である。また、Weil descent 法では最終的には超楕円曲線上の離散対数問題を解くことになるの

でその解析には楕円曲線のみならず超楕円曲線上の離散対数問題も合わせて考察することが必要である。

2.5 Xedni calculus

Xedni calculus は Silverman[35] と Kim, Cheon, Hahn[20] により独立に発見された確率的アルゴリズムである。いまのところ、この方法がどの曲線に対して適用できるかは知られていない。従って (C) 型に分類される。

Jacobson, Koblitz, Silverman, Stein, Teske[18] はある定数 C_0 があり、任意の $E/\mathbf{F}_p$ に対してこのアルゴリズムが成功する確率は C_0/p 以下であることを証明した。しかし、現在のところ C_0 の値は非常に大きく楕円曲線暗号で用いられる程度の p に対しては C_0/p は無視できるほど小さくはない（それどころか 1 より大きくなり得る）。[18] では各種の数値実験も行い暗号で用いられる p に対しても xedni calculus は適用できそうもないと結論しているが、これはあくまでも実験の結果に基づく経験則に過ぎない。他方、E が与えられたときに xedni calculus にとって都合のよい持ち上げが存在しないことを示す定理もアルゴリズムも知られていない。ところで [18] は素体上の楕円曲線についてのみ考察されている。小暮 [40] は Xedni calclus を標数 2 の体へ適用するための必要な変更を明らかにし、実装実験を行っている。この結果を見る限りでは Xedni calclus が標数 2 の大きな有限体上の楕円曲線に対して適用できる可能性は大きくはなさそうである。しかしながら、実験に用いられた曲線の数が少ないため、今後さらに詳細な分析が必要であると思われる。

3 楕円曲線の位数計算

E を $\mathbf{F}_q$ 上定義された楕円曲線とする。$\#E(\mathbf{F}_q)$ をできるだけ小さな計算量で求める方法について現在までに知られている方法は ℓ 進的方法と p 進的方法に大別される。前者はいわゆる SEA アルゴリズムであり、後者は標準持ち上げを用いるもの、算術幾何平均を用いるものなどがある。以下、多項式乗算あるいは多倍長整数乗算に Karatsuba 法を用いる場合は $\mu := \log_2 3$、素朴アルゴリズムを用いる場合は $\mu := 2$ とおく。特に断りのない限り、時間計算量は bit 演算の数を表し、領域計算量は必要とされるメモリーのサイズを表すものとする。

$f \in \mathrm{End}(E)$ に対して $\mathrm{End}(E)$ の元として $f^2 - cf + q = 0$ が成立するような $c \in \mathbf{Z}$ がただ一つ存在する。この c を f の trace といい $\mathrm{Tr}(f)$ により表す。このとき Hasse の関係式

$$\#E(\mathbf{F}_q) = 1 + q - \mathrm{Tr}(\mathrm{Fr}_q) \tag{3.1}$$

および Hasse の不等式

$$|\mathrm{Tr}(\mathrm{Fr}_q)| \leq 2\sqrt{q} \tag{3.2}$$

が成立する。

3.1 ℓ 進的方法

Schoof, Elkies, Atkin らによるアルゴリズムを総称して SEA アルゴリズムという。このアルゴリズムは N が $\log p$ ないしその数倍程度のときは適用できないが、楕円曲線暗号への応用に際しては p が大きく N は高々 10 以下、あるいは $p = 2$ で N が 100 以上なので問題は無い。時間計算量は経験的に $O((\log q)^{2\mu+2})$ と見積もられているがこのような評価を数学的に証明することはできそうに無い。しかしながら、この経験則は実験と良く合い、実際にいろいろな q の値に対して $\mathbf{F}_q$ 上の楕円曲線をランダムに発生させるとSEA アルゴリズムの所要時間の平均値は概ね $O((\log q)^{2\mu+2})$ 程度であることが観察される。他方、これはあくまでも平均値であり、最小値と最大値の開きが大きいので real time 系への応用など、最大時間を上から押えなければならない場合には注意を要する。

SEA アルゴリズムの基本は Schoof のアルゴリズム Schoof[31] である。M を $\prod_{\ell \leq M, \ell \neq p} \ell \geq 4\sqrt{q}$ となる最小の自然数とすると

$$M = O(\log q) \tag{3.3}$$

である (Chebyshev の定理 [3])。p と異る小さな素数 $\ell = 2, 3, 5, \ldots, M$ に対して $\mathrm{Tr}(\mathrm{Fr}_q) \bmod \ell$ を求めれば Chinese remainder theorem と Hasse の不等式 (3.2) より $\mathrm{Tr}(\mathrm{Fr}_q)$ が求まる。すると Hasse の関係式 (3.1) から $\#E(\mathbf{F}_q)$ が求まる。

$\mathrm{Tr}(\mathrm{Fr}_q) \bmod \ell$ を求めるには Fr_q の $E[\ell]$ への作用を調べれば良い。**素数** ℓ と $c \in \mathbf{Z}$ に対して $\mathrm{Fr}_q^2 - c\mathrm{Fr}_q + q$ の $E[\ell]$ への制限が零写像である（ℓ が素数だからこれは $P \in E[\ell]$ かつ $P \neq \mathcal{O}$ で $\mathrm{Fr}_q^2 P - c\mathrm{Fr}_q P + qP = \mathcal{O}$ となるものが存在することと同値になる。）ならば $c \equiv \mathrm{Tr}\,\mathrm{Fr}_q \bmod \ell$ である。ここで $\mathrm{Tr}\,\mathrm{Fr}_q \bmod \ell$ を得るのに位数 ℓ^2 の群 $E[\ell]$ が用いられていることに注意する。$\ell \neq p$ のときは $E[\ell]$ の点が Fr_q でどのように動くかは E の ℓ 等分多項式使い時間計算量 $O((\log q)^{\mu}\ell^{2\mu+1})$ で調べることができる。(3.3) より Schoof の方法のみを使って $\mathrm{Tr}(\mathrm{Fr}_q)$ を計算する場合の時間計算量は $O((\log q)^{3\mu+2})$ であることが示される。

Elkies の方法 [5] は $E[\ell]$ が $\mathbf{F}_q$ 上定義された位数 ℓ の部分群 V を持つときは $\mathrm{Tr}\,\mathrm{Fr}_q \bmod \ell$ が V から求まることに着目したものである。なお、E の部分集合 S は $\mathrm{Fr}_q S = S$ のとき $\mathbf{F}_q$ 上定義されているという。（これは S の各点 P に対して $\mathrm{Fr}_q P = P$ となることではない）このような V がある場合、ℓ を E に対する Elkies 素数という。$\mathrm{Tr}\,\mathrm{Fr}_q \bmod \ell$ を計算するアルゴリズム

の概要は以下のとおり：

Input: E, ℓ

Output: $E[\ell]$ が $\mathbf{F}_q$ 上定義された位数 ℓ の部分群を持つときは $\operatorname{Tr}\operatorname{Fr}_q \bmod \ell$

Procedure:

1: ℓ が E に対する Elkies 素数であるかどうか判定し、そうでなければ終了
2: E と ℓ-isogenus な楕円曲線 E' を求める。
3: E から E' への ℓ-isogey の核 V （これが $\mathbf{F}_q$ 不変な $E[\ell]$ の部分群となる）を求める。
4: $P \in V$, $P \neq \mathcal{O}$ に対して $\operatorname{Fr}_q P$ を求める。
5: $\operatorname{Fr}_q P = \lambda P$ となる $\lambda \in \mathbf{F}_\ell$ を求める。
6: $\lambda + q/\lambda$ を返して終了

V を定義する方程式の次数は $O(\ell)$ であり、$\operatorname{Tr}\operatorname{Fr}_q \bmod \ell$ を返すまでの上記アルゴリズムの実行時間は $O((\log q)^\mu \ell^{\mu+1})$ でありその dominant step は $\operatorname{Fr}_q P$ の計算である。λ を求める部分を高速化する Dewaghe[4] の方法が知られているが全体の時間計算量のオーダーを変えるものではない。Step 1 は具体的には ℓ 次 modular 多項式 Φ_ℓ を用いて$\Phi_\ell(j(E), X) = 0$ が $\mathbf{F}_q$ 内に解を持てば Elkies 素数であると判定する。ここで Φ_ℓ が必要であるが、Elkies のアルゴリズムの計算量を評価するときにΦ_ℓ を求めるための計算量は**含めない**。Φ_ℓ は個々の E や q には依存しない整数係数多項式であるからただ一度計算しておけば良い。

問題はこのアルゴリズムをどの範囲の ℓ に対して実行せねばならないかである。ℓ が E の Elkies 素数となるのは ℓ が $\operatorname{End}(E)$ の商体 K において分解するか分岐するときである。Δ_E を K の判別式とすると、mod Δ_E ではおおよそ半分の ℓ が Elkies 素数となる。しかし、一般には Δ_E は $O(q)$ であり、他方、ここで必要なのは適当な定数 c_1, c_2 に対して $\ell < c_1(\log q)^{c_2}$ の範囲にどの程度 Elkies 素数があるかということである。このような（q に比べて非常に）狭い範囲で素数がどのように振舞うかは今のところ良く分かっていない。E を止めたときに ℓ が Elkies 素数となるのがランダムに起こるのなら

$$\prod_{\ell:\text{Elkies prime},\ell<M'} \ell > 4\sqrt{q}$$

となる M' の最小値は $O(\log q)$ であることが期待され、位数計算全体の計算量は $O((\log q)^{2\mu+2})$ となることも期待される。

しかしながらこのような評価は証明できそうにない。これは一般化されたリーマン予想 (GRH) の下で以下のことが証明できるからである (Montgomery[25, Th 13.5])：ある定数 $c > 0$ があり、mod d での最小平方剰余が $c \log d \log\log d$ 以上となる虚二次体 $\mathbf{Q}(\sqrt{-d})$ が無限個存在する。（厳密にいうと Montgomery の結果は平方非剰余について述べたものだが、平方剰余についても全く同じ方法で証明される。）現在のところ GRH はあくまでも予想に過ぎないが、その成立は多くの数論研究者が確信しているものである。自

己同型環の商体がこのような体になってしまう楕円曲線に対しては後述する Elkies の方法が小さな素数 ℓ に対しては全く適用できず、$M' = O(\log q)$ とはなり得ない。

楕円曲線暗号で用いられる程度の q を止めて、ランダムに $\mathbf{F}_q$ 上の楕円曲線を生成し Elkies のアルゴリズムの時間計算量を計測すると概ね $O((\log q)^{2\mu+2})$ となることが観察される。しかし、特定の楕円曲線に対して（後述の Atkin のアルゴリズムを併用しても）実行時間は大きく変動することもあることには注意すべきである。なお、このことは Elkies のアルゴリズムが確率的アルゴリズムであることを**意味しない**。一旦入力となる楕円曲線 E が与えられた場合、その実行過程は（有限体上の多項式の因数分解を除き）deterministic である。

3.2 Atkin の方法

ℓ が Elkies 素数でないとき Elkies の方法では $\operatorname{Tr}\mathrm{Fr}_q \bmod \ell$ について何の情報も得ることができなかった。すなわち、$\operatorname{Tr}\mathrm{Fr}_q \bmod \ell$ がとり得る値は ℓ 個ある。Atkin はこのような場合でも $\operatorname{Tr}\mathrm{Fr}_q \bmod \ell$ の候補を得る方法を示した。Fr_q の固有方程式 $X^2 - (\operatorname{Tr}\mathrm{Fr}_q)X + q = 0$ の根 λ に対して r を $\lambda^r \in \mathbf{F}_l$ となる最小の自然数とする。このとき $\operatorname{Tr}\mathrm{Fr}_q$ の可能な値は $\varphi(r)/2$ 個（ここで φ は Euler 関数：$\varphi(r) = r\prod_d(1-d^{-1})$, d は r の素因数を渡る）である。異る Atkin 素数 $\ell_1, \ell_2, \ldots, \ell_m$ が得られたときに $\operatorname{Tr}\mathrm{Fr}_q \bmod \ell_1 \cdots \ell_m$ の可能な値の個数は m について指数関数的に増加するが、m がさほど大きくない場合はこれら候補の個数も計算機で扱えないほどではない。これにより $\operatorname{Tr}\mathrm{Fr}_q$ を決定するのに必要な Elkies 素数の数を減らすことができる。この方法の詳細は、Atkin 自身による論文は発表されていないようであるが、Müller[26] に詳しく解説されている。

3.3 p 進的方法

p を止めて $N \to \infty$ としたとき現在得られている p 進的方法による楕円曲線の位数計算の時間計算量は漸近的に $O(N^{2\mu+1})$（N にのみ依存する事前計算を認めれば $O(N^{2\mu+0.5})$, ONB が存在する場合だけでよければ $(N^{2\mu+1/(\mu+1)})$）であり、ℓ 進的方法よりも増大度が小さい。実用上は p はせいぜい数十程度が限度と見られ楕円曲線暗号への応用を考えたとき適用可能な場合は $p = 2$ に限られるが、$p = 2$ は p 進的方法が最も効果的に扱える場合でもある。

p 進的方法は有限体 $\mathbf{F}_q$ 上の楕円曲線 E を何らかの意味で剰余体が $\mathbf{F}_q$ になる完備離散的付値体 K に持ち上げる。現在知られている速い位数計算アルゴリズムでは K として p 進数体 $\mathbf{Q}_p$ の不分岐 N 次拡大体（同型を除いて一意に定まる）が用いられる。以下、K をそのようにとり R を K の付値

環とする。$K/\mathbf{Q}_p$ の Frobenius 置換（これは $\mathrm{Gal}(K/\mathbf{Q}_p)$ の生成元となる）はσ と記す。σ は K 上の等長写像であり特にすべての $m \in \mathbf{N}$ に対して環 R/p^m の自己同型を導く。この導かれた写像も同じ記号 σ により表す。また考える楕円曲線はすべて非超特異であるとする。

E の K への持ち上げは多数あるが、Fr_q も自己準同型として持ちあがるものは同型を除いて一意に定まる。これを E の標準持ち上げといい $E^{\uparrow}$ により表す。K 上の楕円曲線 E_1, E_2 に対して Abel 群として $\mathrm{Hom}(E_1, E_2) \cong \mathrm{Hom}(E_1^{\uparrow}, E_2^{\uparrow})$ であり左辺の元 f に対応する右辺の元を $f^{\uparrow}$ により表す。さらに環として

$$\mathrm{End}(E) \cong \mathrm{End}(E^{\uparrow}) \tag{3.4}$$

となる。

$\mathrm{End}(E)$ において $\mathrm{Fr}_q^2 - \mathrm{Tr}(\mathrm{Fr}_q)\mathrm{Fr}_q + q = 0$ が成立するが、(3.4) は同型だから $\mathrm{End}(E^{\uparrow})$ において $\mathrm{Fr}_q^{\uparrow 2} - \mathrm{Tr}(\mathrm{Fr}_q)\mathrm{Fr}_q^{\uparrow} + q = 0$ が成立する。これは $\mathrm{Tr}(\mathrm{Fr}_q) = \mathrm{Tr}(\mathrm{Fr}_q^{\uparrow})$ を意味する。$\mathrm{Fr}_q^{\uparrow}$ は標数 0 の体上の楕円曲線の自己準同型であり、$E^{\uparrow}$ の定義方程式は $\mathrm{Tr}(\mathrm{Fr}_q^{\uparrow})$ を計算するのに十分な情報を含んでいる、といのが p 進的方法の基本的なアイディアである。

3.4 算術幾何平均法

算術幾何平均は事前計算を認めず、すべての拡大次数に適用できるという条件の下で現在知られているアルゴリズムのうち最も高速なものである。これは Harley et al[16]. において発表された。なおこのアルゴリズムは ArgoTech 社が特許を保有している。

$a \equiv b \bmod 8$ を満たす $a, b \in R^{\times}$ に対して

$$\mathcal{M}(a,b) := \left(\frac{a+b}{2}, a\sqrt{\frac{b}{a}}\right)$$

（ここで平方根の符号は $\sqrt{b/a} \equiv 1 \bmod 4$ となるように定める）とおく。$\mathcal{M}(a,b)$ を a と b の算術幾何平均という。$E_{a,b}$ を $y^2 = x(x-a^2)(x-b^2)$ により定まる楕円曲線とする。このとき $E_{a,b}$ は $E_{\mathcal{M}(a,b)}$ と 2-isogenous であり、$j(E_{a,b}) \equiv j(E^{\uparrow}) \bmod 2^t$ ならば $j(E_{\mathcal{M}(a,b)}) \equiv j(\sigma(E)^{\uparrow}) \bmod 2^{t+1}$ となる。ゆえに a_0, b_0 を E_{a_0,b_0} が E の持ち上げになるように定め $(a_n, b_n) := \mathcal{M}(a_{n-1}, b_{n-1})$ により数列 $\{a_n\}_{n=1}^{\infty}$, $\{b_n\}_{n=1}^{\infty}$ を定めると

$$\lim_{n\to\infty} j(E_{a_n,b_n}) - j(\sigma^n(E)^{\uparrow}) = 0 \tag{3.5}$$

である。ここで a_0, b_0 を上のようにとると $a_0/b_0 \in 1 + 8R^{\times}$ となり、極限 $\lim_{n\to\infty} a_n$, $\lim_{n\to\infty} b_n$ は**存在しない**（これは Henniart, Mestre[17] の結果であるが、(3.5) において $\{j(\sigma^n(E)^{\uparrow})\}_{n=1}^{\infty}$ は明らかに収束しないことからも分かる。）ことに注意する。算術幾何平均法の概要は以下のようになる

Input: $E : y^2 + xy = x^3 + c$ $(c \in \mathbf{F}_q^\times)$
Output: $\mathrm{Tr}\,\mathrm{Fr}_q$
Procedure:
1: $a, b \in R^\times$ を $E_{a,b}$ が E の持ち上げになるようにとる
2: $M = [(N+1)/2] + 3$
3: 以下を M 回繰り返す
4: $\quad (a, b) = \mathcal{M}(a, b)$
5: $(c, d) = \mathcal{M}(a, b)$
6: $t \equiv N_{K/\mathbf{Q}_2}(a/c) \bmod 2^M$ かつ $|t| \leq 2\sqrt{q}$ となる整数 t を返す

このアルゴリズムの時間計算量は $O(N^{2\mu+1})$ であり、かつ O-constant は極めて小さい。領域計算量は $O(N^2)$ である。R の算術演算（加法、減法、乗法、および可逆元の逆元を求めること。当然のことながら実装にあたってはすべての計算は適切に定められた精度で行われる。）と Norm 計算がが既に使える（数式処理システム等にすでに組み込まれている、あるいは、C, C++ からリンクできるライブラリが使用可能である）ならば上のアルゴリズムを実装するのは容易である。

3.5 Norm 計算アルゴリズム

現在知られている標数 2 の有限体上楕円曲線の位数計算アルゴリズムではいずれのものも最終段階で $c \in 1 + 4R$, $c \bmod 2^M$ が与えられたときに $N_{K/\mathbf{Q}_2}(c) \bmod 2^M$ （ここで $M = N/2 + O(1)$）を計算する必要がある。Satoh, Skjernaa, Taguchi[30] は時間計算量 $O(N^{2\mu+0.5})$、領域計算量 $O(N^2)$ のアルゴリズムを与えた。従来法と異りこのアルゴリズムでは解析的手法を用いて計算する。

$$\exp(x) := \sum_{n=0}^{\infty} \frac{1}{n!} x^n$$

および

$$\log(y) := \sum_{n=1}^{\infty} \frac{(-1)^{n-1}}{n} (y-1)^n \tag{3.6}$$

とおくとこれらは $x \in 4R$, $y \in 1 + 2R$ のとき収束し、（考えている値が収束する限り）通常の指数関数、対数関数と同様な関係式を満たす。なお、上記無限級数の収束は K において考えているのであり、exp の収束半径は無限大ではない。また、σ は連続であり、$\frac{1}{n} \in \mathbf{Q} \subset \mathbf{Q}_2$ だから $\sigma(\log(y)) = \log \sigma(y)$ である。$c \in 1 + 4R$ という条件（これは以下に現れる級数の収束を保証する）の下で

$$N_{K/\mathbf{Q}_2}(c) = \prod_{j=0}^{N-1} \sigma^j(c) = \exp\left(\sum_{j=0}^{N-1} \log(\sigma^j(c)) \right) = \exp(\mathrm{Tr}_{K/\mathbf{Q}_2} \log(c))$$

となる。$\mathrm{Tr}_{K/\mathbf{Q}_2}$ の値は $\mathbf{Q}_2$ に属するので exp の計算量は無視できる。$\mathrm{Tr}_{K/\mathbf{Q}_2}$ の計算は、本質的には足し算であり、この計算量も無視できるほど小さい。このアルゴリズムの主要項は $\log(c)$ の計算であり、(3.6) をそのまま計算すると時間計算量 $O(N^{2\mu+1})$ となってしまう。

$c \equiv 1 \bmod 4$ を満たす $c \in R$ が $\bmod 2^M$ の精度で与えられているとき $t \geq 0$ に対して $c^{2^t} \equiv 1 \bmod 2^{2+t}$ かつ $c^{2^t} \bmod 2^{M+t}$ は well-defined である。したがって $\log(c^{2^t}) \bmod 2^{M+t}$ を計算するには (3.6) を $O((M+t)/(t+2))$ 項計算すれば良い。この値が求まれば $\log c \bmod 2^M$ は $2^{-t}\log(c^{2^t})$ として得られる。この計算量は $O(N^\mu M^\mu \max(t,(M+t)/(t+2)))$ であるから、$t = O(\sqrt{M})$ ととり時間計算量 $O(N^\mu M^{\mu+0.5})$、領域計算量 $O(NM)$ で $\log c \bmod 2^M$ が求まる。なお、この部分は time-space tradeoff が効き、領域計算量が $O(NM^{4/3})$ まで増大しても良いのなら時間計算量を $O(N^\mu M^{\mu+1/3})$ まで押えることができる。(これは R. Harley の注意による。)

楕円曲線の位数計算において norm 計算を行うときは $M = N/2 + O(1)$ であったので時間計算量 $O(N^{2\mu+0.5})$, 領域計算量 $O(N^{2)}$ で norm 計算は終了する。また、[30] では $\log \frac{1+x}{1-x} = 2\sum_{n=1}^{\infty} \frac{1}{2n-1}x^{2n-1}$ を用いてさらに若干の高速化が行われている。

3.6 事前計算を認める場合の高速計算

K は $\mathbf{Q}_p$ 上有限次拡大だから $K = \mathbf{Q}_p(\theta)$ となる$\theta \in R$ がある。θ の monic な $\mathbf{Q}_p$ 上の最小多項式を F とする。(実用上は θ は F のゼロでない係数の数ができるだけ小さくなるように選ばれる。) このとき$\psi \in R$ で $\psi^{q-1} = 1$ かつ $\psi \equiv \theta \bmod p$ を満たすものが一意的に存在して $R = \mathbf{Z}_p[\psi]$ となる。ψ は一の巾根だから σ は R に $\sigma(\psi) = \psi^p$ により作用している。よって $C_m(\psi) := \sigma^{-1}(\psi^m)$ とおくとσ^{-1} の R への作用は具体的に

$$\sigma^{-1}\left(\sum_{i=0}^{N-1} a_i\psi^i\right) = \sum_{m=0}^{p-1}\left(\sum_{0\leq pk+m<N} a_{pk+m}\psi^k\right)C_m(\psi)$$

と書ける。以下、ψ の monic な $\mathbf{Q}_p$ 上の最小多項式 G と $C_1, \ldots, C_{p-1}$ が事前計算されているものとする。これは N と θ にのみ依存する。なお、この事前計算は、$N \leq 600$ 程度に対しては容易に実行でき、現在楕円曲線暗号で用いられる楕円曲線に対しては問題とならない。$R = \mathbf{Z}_p[X]/\langle G\rangle$ であるが G は一般に密な多項式であり $\mathbf{Z}_p[X]/\langle G\rangle$ の乗算は $\mathbf{Z}_p[X]/\langle F\rangle$ の乗算に比べて 3 倍ほど遅いことに注意する。

楕円曲線 $E/\mathbf{F}_q$ が $j(E) \notin \mathbf{F}_{p^2}$ を満たしているとする。このとき、Vercauteren, Preneel, Vandewale[38] のアルゴリズムを多少修正して $j(E^{\uparrow}) \bmod p^M$ を時間計算量 $O(N^\mu M^{1+\mu})$, 領域計算量 $O(NM)$ で求めることができる。具体的手順は：

Input: $j(E)\mathbf{F}_q$, $M \in \mathbf{N}$,
Output: $j(E^{\uparrow}) \bmod p^M$
Procedure:
1: $x_1 :=$ any lift of a to R ;
2: for $(i = 1\ ;\ i < M\ ;\ ++i)$ {
3: $\Phi_p(b_i, x_i^p) = 0$ かつ $b_i^p \equiv x_i$ となる b_i を求める。
4: $x_{i+1} := \sigma^{-1}(b_i)$;
5: }
6: return x_M ;

ここで Step 4 で σ^{-1} を作用させた結果、$x_{i+1} \equiv x_i \bmod p^i$ が成立するから $d_{i+1} := x_{i+1} - x_i$ とおくと $d_i \in p^i R$ となる。よって

$$\partial_1\Phi_p(b_{i-1}, x_{i-1})\sigma(d_{i+1}) + \partial_2\Phi_p(b_{i-1}, x_{i-1})d_i \equiv 0 \bmod p \qquad (3.7)$$

となる。(∂_i は i 番目の変数に関する偏微分。) x_{i+1} は $\bmod p^{i+1}$ でしか意味を持たないから Koroecker relation を用いて x_{i+1} を求めるには $p^{-i}d_i \bmod p$ だけが本質的であることが分かる。従って (3.7) においてすべての計算を本質的に $\bmod p$ の精度で (すなわち $\mathbf{F}_q$ で) 済ませることができるので計算時間が短縮される。しかし、この考えをおし進めて $x_M = x_1 + d_2 + \cdots + d_M$ を用いて x_M を求めようとすると d_i 達は $\bmod p^M$ の精度で計算せねばならず、かえって計算量が増えてしまう。Satoh, Skjernaa, Taguchi[30] は適当な W をとり、$x_{(n+1)W}$ を x_{nW} から計算するのに d_{nW+1} のみを $\bmod p^{(n+1)W}$ で、d_{nW+2}, $\ldots$, $d_{(n+1)W}$ を $\bmod p^W$ で計算することによりこの問題を解決した。この W は理論上は時間計算量を最小にするように選択するべきであり、楕円曲線の位数計算においては $M = N/2 + O(1)$ であるから $W = O(N^{\mu/(\mu+1)})$ ととるべきである。$j(E^{\uparrow}) \bmod p^{M+O(1)}$ を求める時間計算量は $O(N^{2\mu+1/(\mu+1)})$ である。しかし、楕円曲線暗号で用いられる楕円曲線の位数計算においては W を N に関係なく CPU の語長 (の整数倍) ととるのが実際的である。

$j(E^{\uparrow})$ が求まったあと、$\mathrm{Fr}_p^{\uparrow}$ の双対同種写像 $V_p^{\uparrow}$ を局所パラメーターで展開したのときの 1 次の係数 c を求める必要がある。c が求まれば $\mathrm{Tr}\,\mathrm{Fr}_q$ は $t \equiv N_{K/\mathbf{Q}_p}(c) \bmod p^{N/2+O(1)}$ かつ $|t| \le 2\sqrt{q}$ を満たす整数である。c の計算は、特に $p = 2$ のとき、数学的には難しい問題であるが現在 Fouquet, Gaudry, Harley[6] による方法、Skjernaa[36] による方法が知られておりいずれも計算時間は $O(N^{2\mu})$ であり他の部分に比べて無視できるほど高速である。以上を総合して、事前計算を認める場合、位数計算の時間計算量は $O(N^{2\mu+0.5})$ となる。

3.7 特殊な拡大次数に対する高速計算

Kim et al.[19] は $\mathbf{F}_q/\mathbf{F}_p$ が Gauss 周期により生成される正規底 (この重要な一例が type I および type II の ONB である) を持つ場合に Satoh,

Skjernaa, Taguchi[30] で必要であった事前計算が不要となり、かつ norm 計算の時間計算量が $O(N^{\mu}\log N)$ で済むことを示した。彼らは $\mathbf{F}_q/\mathbf{F}_p$ が Gauss 周期により生成される正規底を持つとき $K/\mathbf{Q}_p$ も Gauss 周期により生成される正規底を持ち、正規底による表現と標準基底による表現の間を高速に変換することで R の算術演算を $O(N^{2\mu})$ で行えることを示した。この結果として得られる楕円曲線の位数計算アルゴリズムの時間計算量は $O(N^{2\mu+1/(\mu+1)})$ である。$\mu \geq 1$ だからこれは前節の方法よりも漸近的には高速である。しかし、実用上は R の乗算が前節で示した場合よりも 3 倍（type I のとき）あるいは 1.5 倍（type II のとき）速いことの寄与のほうが大きい。なお、type I の ONB を持つ場合、N は必ず合成数となる。しかし、type II の素数次 ONB を持つような体上の楕円曲線暗号への応用では有効である。

3.8 楕円曲線離散対数との関連

楕円曲線暗号にとって真に必要とされることは楕円曲線の位数を求めることではなく、楕円曲線暗号に適する曲線を求めることである。与えられた楕円曲線 E に対して位数計算により E 上の離散対数の解法のうち少なくとも Pohlig-Hellmann, 乗法的埋め込み、加法的埋め込みが適用できるかどうかを示すことはできるが、その他の攻撃に対しての安全性について何らかの見解を示すものではない。その意味で、E の位数を求めることは E 上の離散対数の困難性に対する必要条件ではあるが十分条件ではない。

ℓ 進的方法においては与えられた楕円曲線 E に対してアルゴリズムの実行途中で $\operatorname{Tr}\mathrm{Fr}_q \equiv 0 \bmod \ell$ となったならその時点で E は楕円曲線暗号に適さないと判断され、直ちにこの曲線を棄却することができる。この技法は early abort strategy と呼ばれる。p 進的方法はこのような性質を持たないが、それでも小さな ℓ に対して ℓ 進的方法を使って E の位数が ℓ で割れないことを確かめてから位数計算を行うほうが高速であることが Fouquet, Gaudry, Harley[7] により報告されている。この文献の表 3 および表 6 において同一の platform で ℓ 進的方法と p 進的方法を比較した結果が載っている。それによれば $p = 2$, $N = 155$ および $N = 197$ 対しては p 進的方法は ℓ 進的アルゴリズムよりもおおよそ 3 から 4 倍程度高速である。なお、この文献が書かれた当時から ℓ 進的方法はさほど進歩していないが本報告書で記載した p 進的アルゴリズムは当時よりも 4 から 6 倍程度速くなっている。従って、現在では標数 2 の有限体上で楕円曲線暗号に適する楕円曲線を選ぶ時間は大きな標数の素体上のそれに比して遥かに速いのであるが、他方において、素体上の楕円曲線と標数 2 の有限体上の楕円曲線に対する離散対数の困難性の比較に関する結果は現在のところ得られていない。

前述した 3 つの p 進的アルゴリズムを同一の platform （と同一の演算ライブラリ）を使って比較した結果は見当たらないが、Kim et al.[19, Table 1]

に各々のアルゴリズムの提案者による実装結果が platform と共にまとめられており、参考になる。

4 特殊なクラスの楕円曲線

特殊なクラスの楕円曲線を楕円曲線暗号に用いることの是非については様々な議論がある。超特異曲線、anomalous 曲線などはそれらが提案された当時はそれらの安全性は特に問題がないと思われていた。しかし、実際には**後になってから**それらの上の楕円離散対数問題が弱いことが判明した。特定の曲線に対してのみ適用できる攻撃法が発見される可能性はすべての楕円曲線に適用できる攻撃法が発見される可能性よりも遥かに大きい。これに対して、ランダムに楕円曲線を発生させる場合、その曲線が既存の攻撃法の適用対象ではないことを確かめてから使う必要があり、適切な曲線が見つかるまで少なくとも位数計算を繰り返す必要がある。また、「ランダムに選ばれた」とされる曲線が本当にランダムに選ばれているのかをどう検証するのか、本当に既存の攻撃に対する検討が済んでいるのかを誰が確認するのかという問題が残る。しかし、これは PKI の問題であり、特殊なクラスの楕円曲線を（いくつか固定して）使うことを支持する数学的理由は見当たらない。

なお、標数 2 の有限体上の楕円曲線の位数計算に関しては現在、実用上十分高速である。そのため、位数計算に伴うコストは以前と比べて非常に小さくなっている。ただ、素体上の楕円曲線と標数 2 の有限体上の楕円曲線に対する離散対数の困難性の比較に関する結果は現在のところ得られていないことを考慮するする必要がある。

Koblitz 曲線 [21] はもともとスカラー倍演算の高速化のために導入された曲線である。Menezes, Qu[23] によれば Koblitz 曲線には GHS 法が適用できない。しかし、$\mathbf{F}_2$ 上で定義されているため前節に見たように Wiener, Zuccherato[39], Gallant, Vanstone[12] の方法に対しては Koblitz 曲線は弱い。N ビットの一般的な楕円曲線を ρ 法により解くのと同程度の困難性を Koblitz 曲線に持たせるには $N + \log_2 N + 1$ ビット以上の体を用いることとなろうが、このとき他の攻撃法の対象とならないかどうか慎重に考慮する必要がある。小暮 [40] は Xedni calculus が一般の楕円曲線については適用できなくても Koblitz curve には適用できるかも知れないとの着想から実験を試みている。これによれば今のところ Koblitz curve が特に xedni calculus に対して脆弱であるという結果は得られていない。しかしながら [40] においては xedni calculus を標数 2 に適用するために修正する際 Koblitz curve の性質を用いてない。したがって Koblitz curve のみに適用できる xedni calculus がどのような性質を持つかということについては未だ明らかにはされていない。繰り返しになるが、現在知られているすべての攻撃法について考慮したとしても、将来 Koblitz 曲線に対する攻撃法が発見される可能性はランダム

に選ばれた楕円曲線に対する攻撃法が発見される確率よりも遥かに大きいことはいくら強調しても強調しすぎることはない。

参考文献

[1] Adleman, L., DeMarrais, J., Huang, M.-D.: A subexponential algorithm for discrete logarithms over the rational subgroup of the Jacobians of large genus hyperellipitc curves over finite fields, Algorithmic number thoery (Ithaca, NY, 1994), Lect. Notes in Comput. Sci., **877**, 28-40, Berlin: Springer, 1994.

[2] Balasubramanian, R., Koblitz, N.: The improbability that an elliptic curve has subexponential discrete log problem under the Menezes-Okamoto-Vanstone algorithm. *J. Cryptology* **11** (1998) 141-145.

[3] Chebyshev, P.L.: Mémoire sur les nombres premiers. *J. Math. Pures Appl.* **17** (1852) 366-390 (Œuvres, I-5).

[4] Dewaghe, L.: Remarks on the Schoof-Elkies-Atkin algorithm. *Math. Comp.* **67** (1998) 1247-1252.

[5] Elkies, N.D.: Elliptic and modular curves over finite fields and related computational issues, Computational perspectives on number theory (Chicago, IL, 1995), AMS/IP Stud. Adv. Math., **7**, 21-76, Providence, RI: AMS, 1998.

[6] Fouquet, M., Gaudry, P., Harley, R.: An extension of Satoh's algorithm and its implementation. *J. Ramanujan Math. Soc.* **15** (2000) 281-318.

[7] Fouquet, M., Gaudry, P., Harley, R.: Finding secure curves with the Satoh-FGH algorithm and an early-abort strategy, Advances in Cryptology - Eurocrypt 2001 (Innsbruck, Austria, May 2001), Lect. Notes in Comput. Sci., **2045**, 14-29, ed. Pfitzmann, B., Berlin, Heidelberg: Springer Verlag, 2001.

[8] Frey, G.: How to disguise an elliptic curve (Weil descent), (1998) Talk at ECC98 (available at http://www.cacr.math.uwaterloo.ca/conferences/1998/ecc98/slides.html).

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

[10] Galbraith, S., Smart, N.P.: A cryptographic application of Weil descent, Codes and Cryptography, Lect. Notes in Comput Sci., **1746**, 191-200, Berlin: Springer, 1999.

[11] Galbraith, S.D., Hess, F., Smart, H.P.: Extending the GHS Weil descent attack, Advances in cryptology – Eurocrypt 2002, Lect. Notes in Comput. Sci., **2332**, 29-44, Berlin: Springer, 2002.

[12] Gallant, R., Lambert, R., Vanstone, S.: Improving the parallelized Pollard lambda search on anomalous binary curves. *Math. Comp.* **69** (2000) 1699-1705.

[13] Gallant, R., Lambert, R., Vanstone, S.: Faster point multiplication on elliptic curves with efficient endomorphisms, Advances in cryptology - Proceedings of CRYPTO 2001, Lect. Notes in Comput. Sci., **2139**, 190-200, ed. Kilian, J., Berlin: Springer, 2001.

[14] Gaudry, P.: An algorithm for solving the discrete log problem on hyperellipitc curves, Advances in cryptology – Eurocrypt 2000, Lect. Notes in Comput. Sci., **1807**, 19-34, ed. Preneel, B., Berlin: Springer, 2000.

[15] Gaudry, P., Hess, F., Smart, N.P.: Constructive and destructive facets of Weil descent on elliptic curves. *J. Crypto.* **15** (2002) 19-46.

[16] Harley, R.: Counting points with the arithmetic-geometric mean (joint work with J.-F. Mestre and P. Gaudry), Eurocrypt 2001, Rump session, 2001.

[17] Henniart, G., Mestre, J.-F.: Moyenne arithmético-géométrique p-adique. *C.R. Acad. Sci. Paris Sér. I Math.* **308** (1989) 391-395.

[18] Jacobson, M.J., Koblitz, N., Silverman, J.H., Stein, A., Teske, E.: Analysis of the xedni calculus attack. *Des. Codes Cryptogr.* **20** (2000) 41-64.

[19] Kim, H., Park, J., Cheon, J., Park, J., Kim, J., Hahn, S.: Fast elliptic curve point counting using Gaussian normal basis, Algorithmic number theory (Sydney, Australia, July 2002), Lect. Notes in Cimput. Sci., **2369**, 292-307, ed. Fieker, C., Kohel, D., Berlin: Springer, 2002.

[20] Kim, H.J., Cheon, J.H., Hahn, S.G.: Elliptic curve lifting problem and its applications. *Proc. Japan Acad. Ser A Math. Sci.* **75** (1999) 166-169.

[21] Koblitz, N.: CM-curves with good cryptographic properties, Advances in cryptology—CRYPTO '91 (Santa Barbara, CA, 1991), Lecture Notes in Comput. Sci., **576**, 279-287, Berlin: Springer-Verlag, 1992.

[22] Mazur, B.: Rational points of Abelian varieties with values in towers of number fields. *Invent. Math.* **18** (1972) 183-266.

[23] Menezes, A., Qu, M.: Analysis of the Weil descent attack of Gaudry, Hess, and Smart, Topics in Cryptology - CT-RSA 2001, Lect. Notes in Comput. Sci., **2020**, 308-318, Berlin: Springer, 2001.

[24] Menezes, A. J., Okamoto, T., Vanstone, S. A.: Reducing elliptic curve logarithms to logarithms in a finite field. *IEEE Trans. Info. Theory* **39** (1993) 1639-1646.

[25] Montgomery, H.L.: "Topics in multiplicative number theory". Lect. Notes in Math., 227. Berlin, Heidelberg: Springer 1971.

[26] Müller, V.: Ein Algorithmus zur Bestimmung der Punktanzahl elliptischer Kurven über endlichen Körpern der Charakteristik grösser drei, (1995) Dissertation der Universität des Saarlandes.

[27] Park, Y.-H., Jeong, S., Kim, C., Lim, J.: An alternate decomposition of an integer for faster point multiplication on certain ellipitc curves, Proceedings of PKC 2002, Lect. Notes in Comput. Sci., **2274**, 323-334, ed. Naccache, D., Paillier, P., Berlin: Springer, 2002.

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

[29] Satoh, T., Araki, K.: Errata to the paper "Fermat Quotients and the Polynomial Time Discrete Log Algorithm for Anomalous Elliptic Curves". *Commentarii Math. Univ. St. Pauli.* **48** (1999) 211-213.

[30] Satoh, T., Skjernaa, B., Taguchi, Y.: Fast Computation of Canonical Lifts of Elliptic curves and its Application to Point Counting, (2001) preprint.

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

[32] Semaev, I. A.: On computing logarithms on elliptic curves. *Diskret. Mat.* **8** (1996) 65-71 (Russian, English translation in Discrete Math. Appl. 6(1996), 69-76).

[33] Semaev, I. A.: Evaluation of discrete logarithms in a group of p-torsion points of an elliptic curves in characteristic p. *Math. Comp.* **67** (1998) 353-356.

[34] Sica, F., Ciet, M., Quisquater, J.-J.: Analysis of the Gallant-Lambert-Vanstone method on efficient endomorphisms: elliptic and hyperelliptic curves, Proc. SAC 2002, 2002.

[35] Silverman, J.H.: The xedni calculus and the elliptic curve discrete logarithm problem. *Des. Codes Cryptogr.* **20** (2000) 5-40.

[36] Skjernaa, B.: Satoh's algorithm in characteristic 2, (2000) preprint, (to appear in Math. Comp.).

[37] Smart, N. P.: The discrete logarithm problem on elliptic curves of trace one. *J. Cryprology* **12** (1999) 193-196.

[38] Vercauteren, F., Preneel, B., Vandewalle, J.: A memory efficient version of Satoh's algorithm, Advances in Cryptology - Eurocrypt 2001 (Innsbruck, Austria, May 2001), Lect. Notes in Comput. Sci., **2045**, 1-13, ed. Pfitzmann, B., Berlin, Heidelberg: Springer Verlag, 2001.

[39] Wiener, M.J., Zuccherato, R.J.: Faster attacks on elliptic curve cryptosystems, Selected areas in cryptography (Kingston, ON, 1998), Lect. Notes in Comput. Sci., **1556**, 190-200, Berlin: Springer, 1999.

[40] 小暮淳: Xedni calculus method について（標数 2 の場合），「暗号理論とそれを支える代数曲線理論」（2002 年 8 月 27 日、中央大学）.

補遺

楕円曲線離散対数問題に関連したアルゴリズム：2002 年 8 月～2003 年 1 月末の新しい進展

以下、文献番号は報告書のもの

A. 楕円離散対数を求める効率の良い方法、あるいは既存の方法の改良
に関しては、知り得た限り、特に記述すべきものは見当たらない。

B. 有限体上の楕円曲線の位数を計算する方法については下記の進展があった。

B-1: P. Gaudry: A comparison and a combination of SST and AGM[AsiaCrypt 2002 で発表；報告集 Springer Lect. Notes in Comput. Sci. 2501]は Harley et al.[15] の算術幾何平均(AGM)法に Satoh, Skjernaa,Taguchi[28] による収束の加速法を組合せ位数計算をさらに高速にした。AGM 単独の場合に比べて 163bit で約 4 倍、239bit で約 5 倍の高速化が達成されている。適用可能な体のサイズに制限はないが、SST と同様の（暗号への応用では問題とならない）事前計算を必要とする。

B-2: R. Lercier と D. Lubciz は標準持ち上げを求める上で新たな加速法を提案した（preprint. Eurocrypt 2003 で発表予定）Newton の求根法は 2 乗収束であるが、微分可能な関数にしか適用できない。標準持ち上げを求めるためには $\Phi(x,\Sigma(x))=0$（ここで Φ は多項式、Σ は Frobenius 置換）という型の方程式の根を求めなければならないが、Σ は微分できないので Neweton 法を直接適用することはできなかった。彼らは $\Sigma(x)=ax+b$ （ここで a, b は適当な定数）という歪一次方程式が素早く解けるのなら、これを Newton 法に組み込み、収束を加速できることを示した。実際の漸近的計算量は Σ のベキの作用をどれだけ早く計算することに依存する。正規底が存在する場合には Σ のベキは O(1) で計算でき、 FFT が有効に効くサイズでは位数計算全体の時間計算量の増大度は bit 長の 2 乗である。一般の場合、理論上は bit 長の 2.69 乗でこれは SST の 2.5 乗よりも遅い。しかし、楕円暗号の応用においてはこの FFT を使うという仮定は妥当ではなく、また当該論文に納められている実装結果は 1000bit 以上の体に対するものである。従って、この方法については（特に、タイプが小さい正基底が存在しない場合に）今後実装を含めてさらに調査が必要であるものと思われる。

B-3: R. Harley は何らの事前計算を必要としない（正確にいうと事前計算の計算量が本計算の計算量よりも小さい）、すべての拡大次数に適用できる加速方法を発表した。（氏の学位論文に掲載予定；NMBRTHRY メーリングリストでアルゴリズムの詳細とともにアナウンスされた）FFT の元で時間計算量の増大度は bit 長の 2 乗であり、197bit での計算結果を見る限り、楕円暗号に用いられるサイズでも十分有効であると判断される。この方法は SST のように単一精度を用いて収束を加速するのではなく 2 乗収束させるよう細かく精度を制御して高速化を達成している。

楕円暗号に用いられるサイズで B-1 と B-3 の方法のいずれが速いかは実装依存である。（漸近的な速度は B-3 の方が bit 長の 0.5 乗だけ速く、その優位は明らかである。）

B-4: 下記の文献が出版された：
[28] Finite Fields and Their Appl. 9(2003)89-101
[33] Math. Comp. 72(2003) 477-487

以上