離散対数問題の困難性に関する計算量についての調査・研究報告書

2007 年 1 月

1　はじめに

ここでは, 暗号技術の基礎となる数学的なアルゴリズムが持つ困難性, 特に有限体上の離散対数問題及び有限体上の楕円曲線上の離散対数問題の困難性について, 最近の研究について調査した結果について報告する。本レポートの構成は次の通りである：第 2 節では, 有限体上の離散対数問題について述べる. 次に, 第 3 節では, 有限体上の楕円曲線上の離散対数問題について述べる.

2　有限体上の離散対数問題

素因数分解問題と有限体上の離散対数問題は, 古くから知られている代表的な計算量的に困難な問題である. 素因数分解問題とは, 合成数 N が与えられた時, その非自明な約数 d $(d \mid N,\ 1 < d < N)$ を求める問題である. （一般的には, N を素数の冪積で表示することを言うが, 非自明な約数が存在すればそれを求める問題に効率よく帰着されること, さらに, 2 つの素数の積の合成数の場合を考える事が多いため, こう定義される事が多い.）また, 有限体上の離散対数問題とは, 有限体の乗法群 $\mathbb{F}_q^{\times}$ の二つの要素 t, u が与えられた時, $u = t^x$ なる整数 x が存在すれば, それを求める問題である. ここで, 整数 x は t の位数を法として一意に定まり, $\log_t u$ などと表され, t を底とした u の離散対数と呼ばれる. 有限素体上の場合に, 従来は指数と呼ばれていたものである. 1976 年に, Diffie と Hellman により公開鍵暗号の概念が提案され, その実現例として, 有限体上の離散対数問題の困難さに基づく Diffie-Hellman 鍵交換方式が提案された. 続く翌年の 1977 年には, Rivest, Shamir と Adleman により素因数分解問題の困難さに基づく公開鍵暗号である RSA 暗号が提案され, 上記 2 つの問題に対する高速なアルゴリズムを見つけるという研究は, 直接的に, これらの問題に基づく公開鍵暗号方式の安全性の研究を意味することとなった. こういった背景や, 計算機の能力の飛躍的な向上も追い風となり, これらのアルゴリズムについては, 実用的な公開鍵暗号方式の安全性の研究と密接な関係を保ちながら活発な研究がなされてきた.

本節では, 有限体上の離散対数問題に対する, 現在までのところ漸近的に最高速なアルゴリズムである, 数体ふるい法について, 最近の結果まで含めて概説する.

本節の構成は次の通りである. まず 2.1 節で, Schirokauer による有限体上の離散対数問題に対する数体ふるい法の概説を行う. 2.2 節では, NFS の詳しい解説, 2.3 節では拡大体上の場合について簡単にふれ, 2.4 節では計算量評価について述べる. 次に, 2.5 節では, 現在までに行われている有限体上の離散対数問題に対する数値実験について述べる. 最後に, 2.6 節で安全な鍵サイズについて考察する.

以下では, p を素数, n を自然数とし, $q = p^n$ とする.

2.1 数体ふるい法 (NFS)

ここでは, [26] に従って, 有限体上の離散対数問題への数体ふるい法の解説を行う.

数体ふるい法 (Number Field Sieve. 以下, NFS と略す.) は, Pollard によってアイデアが提案され [23], Lenstra 兄弟, Manasse 等によって, $N = r^e \pm s$ (r, s は小さな自然数) の形をした合成数に対する素因数分解アルゴリズムとして提案されたものである [18]. その後さらなる改良が加えられ, 一般の合成数に対しても有効なものとなった. 前者を特殊数体ふるい法 (SNFS), 後者を一般数体ふるい法 (GNFS) と呼ぶことが多い.

この NFS は, 1920 年代に Kraitchik によって導入された指数計算法 (Index Calculus Method) と呼ばれるアルゴリズムのクラスに属すものである. NFS 以前の指数計算法に属すアルゴリズムとしては, Pomerance による 2 次ふるい法 [25] が漸近的に高速な代表的なものであった. 素因数分解アルゴリズムとしては, NFS が漸近的に最速である. また, 計算時間は, 準指数時間アルゴリズムと呼ばれるクラスに属するものであって, 多項式時間アルゴリズムと指数時間アルゴリズムの中間的なものである. NFS を用いた合成数 N の素因数分解の計算量は, 次で与えられる：

$$L_N[1/3, (64/9)^{1/3}],$$

但し, $L_N[s, c]$ は, $L_N[s, c] = \exp((c + o(1))(\log N)^s(\log\log N)^{1-s})$ で定義されるもので (s, c は正の実数. s は $0 \leq s \leq 1$ を満たし, $o(1)$ は N が十分大きいとき 0 に収束するものである.), L 表示などと呼ばれる. (上記のものは GNFS の計算量であって, SNFS の場合は, $L_N[1/3, (32/9)^{1/3}]$ で与えられる.)

素因数分解と離散対数問題それぞれへの NFS の概略を述べると, 以下のようになる：今, N を分解したい大きな合成数とする. 何らかの方法で代数体とその整環 $\mathcal{O}$ (必ずしも極大とは限らない) を選び, 環準同型写像 $\phi : \mathcal{O} \to \mathbb{Z}/N\mathbb{Z}$ が存在するとする. このとき smoothness と呼ばれる (後で定義する) 性質を持つ $\mathcal{O}$ の要素を “ふるい” にかけて十分たくさん集め, 何らかの方法で代数体 $K = \mathbb{Q}(\alpha)$(α の $\mathbb{Q}$ 上の最小多項式を f とする. 但し, ある整数 m があって, $f(m) \equiv 0 \pmod{N}$ とする.) を選び, その整環 $\mathcal{O} = \mathbb{Z}[\alpha]$ から $\mathbb{Z}/N\mathbb{Z}$ への環準同型写像 $\phi : \mathcal{O} \ni a - b\alpha \mapsto a - bm \bmod N \in \mathbb{Z}/N\mathbb{Z}$ が構成できる. この時, smoothness とよばれる性質 (整数であれば, その素因子が小さい. また, 代数的整数であれば, そのノルムの素因子が小さい.) を持つ $\mathcal{O}$ の要素である $a - b\alpha, a - bm$ たちをたくさん集め, それらを用いて $\mathcal{O}$ の要素 δ^2, γ^2 ($\delta, \gamma \in \mathcal{O}$) で, $\phi(\delta^2) \equiv \phi(\gamma^2) \bmod N$ なるものを構成する. 集められた smoothness な $\mathcal{O}$ の要素たちの間の乗法的な性質をうまく使い, Gaußの消去法などの行列演算を用いて, このような平方数が構成出来る. この時, $\phi(\delta) \not\equiv \pm\phi(\gamma) \bmod N$ であれば, $\mathrm{GCD}(\phi(\delta) - \phi(\gamma), N)$ は N の非自明な約数とな

り, 素因数分解が成功する. (素因数分解に関する NFS の詳しい解説については, Lenstra 兄弟による [17] を参照.)

一方, $\mathbb{F}_q$ 上の離散対数問題の場合を考える. 素因数分解と同様に, 何らかの方法で代数体の整環 $\mathcal{O}$ と環準同型写像 $\phi : \mathcal{O} \to \mathbb{F}_q$ が与えられているとき, smoothness という性質を持つ $\mathcal{O}$ の要素をたくさん集め, それらを用いて $\mathcal{O}$ の要素 δ^l, γ^l $(\delta, \gamma \in \mathcal{O})$ で, ある整数 x が存在して $\phi(\delta^l) = ut^x \cdot \phi(\gamma^l)$ なるものを構成する. 但し, l は $q-1$ の素因子とする. この時, $x \equiv -\log_t u \pmod{l}$ となり, $x \bmod l$ が求まる. 一般的には, $x \bmod l^\nu$ $(l^\nu \mid (q-1))$ を求めることに離散対数問題を解く事は帰着される. このように見ると, 素因数分解の場合と離散対数問題の場合の NFS の適用方法は, 本質的にはほとんど同じで, 違いは, 整環 $\mathcal{O}$ の中で “平方数” を構成し, それを “開平” する必要があるか, “l 乗の要素” を構成する必要があるか, であると言えよう. また, 有限素体 $\mathbb{F}_p$ 上の離散対数問題を NFS を使って解く計算量は, サイズが p と同じ合成数の素因数分解と同じで $L_p[1/3, (64/9)^{1/3}]$ で与えられる. 一般の有限体の場合は, $q(= p^n)$ を十分大きくとるとき, n が p のサイズと比較して小さい場合 $(n < (\log p)^{1/2})$ は, 素体の場合と同じで $L_q[1/3, (64/9)^{1/3}]$ で与えられるが, 何の条件もない場合は, $L_q[1/2, c_1]$ (c_1 は定数) となるものしか知られていない [28].

2.2 有限体上の離散対数問題への NFS

有限体上の離散対数問題への NFS は, Gordon [8] によって最初提案され, Schirokauer [26] によって改良された. ここでは, Schirokauer のアルゴリズムの解説を行う. まず, いくつか用語を準備する. 正の実数 B に対して, 有理整数 a が B-smooth であるとは, a の素因子が全て B 以下であるときに言う. 同様に, 代数体 K, K の整数環 $\mathcal{O}_K$ の要素 γ が B-smooth であるとは, そのノルムの値 $N_{K/\mathbb{Q}}(\gamma)$ が B-smooth であるときに言う.

$\mathbb{F}_q$ 上の離散対数問題を考えるとき, その答えは一般には $\bmod (q-1)$ で一意に求まるが, $q-1$ の全ての素因子 l について, $\bmod l^{\nu_l(q-1)}$(ν_l は l 進付値) で答えが求められれば, 中国人剰余定理を用いて $\bmod (q-1)$ での答えを求めることが出来る. 以下では, 簡単のために l は奇素数で $\nu_l(q-1) = 1$ の場合, つまり, $\bmod l$ で求めればよい場合を考える. この節での解説は簡単のため $n = 1$ とし ($\mathbb{F}_q = \mathbb{F}_p$ の場合. $n > 1$ の場合は 2.3 節で簡単に触れる.), 離散対数問題のパラメータ $t, u \in \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ は共にアルゴリズムの中で定める smoothness bound に関して smooth な要素だとしておく. より一般の場合は, 原論文 [26, 27] を参照.

Step 1. 多項式の選択

NFS を行うためには, 代数体 $K = \mathbb{Q}(\alpha)$ を選ぶ, すなわち K を生成する多項式を選ぶ必要がある. 一般的に良く知られている方法は以下である：

自然数 d (どの程度の大きさのものを選べば良いかなどについては, 2.4 節で述べる.) を取り, $m = [p^{1/d}]$ とおき,

$$p = \sum_{i=0}^{d} a_i m^i$$

と p を m で展開する. これにより, d 次の多項式 $f(X) = \sum_{i=0}^{d} a_i X^i \in \mathbb{Z}[X]$ を得る. この多項式 f は, $\mathbb{Q}$ 上既約であることが示せる [2]. この f の根 $\alpha \in \mathbb{C}$ を用いて, $K = \mathbb{Q}(\alpha)$, 整環 $\mathcal{O} = \mathbb{Z}[\alpha]$ と取る. このとき, 一般に, $\mathcal{O}$ は K の整数環 $\mathcal{O}_K$ とは一致しない. また, $\phi : \mathbb{Z}[\alpha] \ni g(\alpha) \mapsto g(m) \bmod p \in \mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$ (但し, $g(X) \in \mathbb{Z}[X]$) で定義される ϕ は, 環準同型写像となる.

この多項式 f は以下の条件を満足している：
(i) f の各係数は $p^{1/d}$ 程度の大きさである.
(ii) $f \bmod p$ の根は高々 $p^{1/d}$ 程度の大きさである.

さらに, ここでは
(iii) f は monic である.
(iv) l は f の判別式を割らない.

という条件も加えておく. 条件 (i), (ii) は, NFS の計算量評価に影響を与えるが, (iii), (iv) は必要なものではなく [26, 27], 説明を簡単にするためのものである.

Step 2. ふるい (Sieve)

Smoothness bound と呼ばれる正の実数 B, ふるい (sieve) にかける代数的整数の探索範囲を決めるパラメータとなる正の実数 C を取る. (選び方などは, 2.4 節で述べる)

$|a|, |b| \leq C$ である互いに素な有理整数の組 $(a, b) \in \mathbb{Z} \times \mathbb{Z}$ で, $a - bm$, $a - b\alpha$ が B-smooth なものをたくさん集める. このような (a, b) の組の全体を S とする.

ここで, $|a - bm|$, $|N(a - b\alpha)|$ の大きさは

$$|a - bm| \leq C(1 + p^{1/d}),\ |N(a - b\alpha)| = |b^d f(a/b)| \leq (1 + d)C^d p^{1/d} \qquad (1)$$

と評価出来る. これら, ふるいにかける代数的整数のサイズが小さいことが, 他の指数計算法に属すアルゴリズムと比較して NFS が高速である主な理由である. 具体的なふるいの方法については, [17] などを参照.

Step 3. 指数ベクトルの計算

ここでは, Step 2 で集めた smooth な代数的整数たちの間の乗法的な関係式を見つけるための準備をする. B 以下の素数の個数を $\pi(B)$, B 以下の素数 $q_1, \ldots, q_{\pi(B)}$ の全体を $\mathcal{B}_{\mathbb{Q}}$ で表す. 同様に, B 以下のノルムを持つ $\mathcal{O}_K$ の 1 次の素イデアル,

及び $[\mathcal{O}_K : \mathcal{O}]$ の素因子の上にある $\mathcal{O}_K$ の素イデアルの個数を $\Pi(B)$, これらを $\mathfrak{q}_1, \ldots, \mathfrak{q}_{\Pi(B)}$ で表し, その全体を $\mathcal{B}_K$ とする. $\mathcal{B}_{\mathbb{Q}} \cup \mathcal{B}_K$ の要素は, 因子基底とも呼ばれる. さらに, 素イデアル $\mathfrak{q} \subset \mathcal{O}_K$ に対して, $\nu_{\mathfrak{q}}$ で $\mathfrak{q}$ 進付値を表すものとする.

このとき, 各 $(a, b) \in S$ について, $\mathbb{Z}^{\pi(B)+\Pi(B)+d}$ の要素となるベクトル $V_{a,b}$ を次で計算する：

最初の $\pi(B)$ 番目までは

$$\nu_{q_1}(a - bm), \ldots, \nu_{q_{\pi(B)}}(a - bm)$$

これに続く $\Pi(B)$ 個は

$$\nu_{\mathfrak{q}_1}(a - b\alpha), \ldots, \nu_{\mathfrak{q}_{\Pi(B)}}(a - b\alpha)$$

で与えられるものとする. ここで, イデアル $(a - b\alpha)\mathcal{O}_K$ を割る素イデアルは $\mathcal{B}_K$ の要素しか出てこないことに注意しておく ([6] の Lemma 10.5.1). 各 $\mathfrak{q} \in \mathcal{B}_K$ について, $\mathfrak{q}$ が 1 次の素イデアルの場合の $\nu_{\mathfrak{q}}(a - b\alpha)$ の値は, $N(\mathfrak{q}) = q'$ とすると, $\nu_{q'}(N(a - b\alpha))$ で与えられる. $[\mathcal{O}_K : \mathcal{O}]$ の素因子を割る $\mathcal{O}_K$ の素イデアルの場合の計算については [6] の 10.5 章に詳しい解説がある.

最後に, 残りの d 個の成分の計算については, Schirokauer によって提案された指標 λ を用いる [26].

$$\Gamma = \{\gamma \in \mathcal{O}_K \mid N(\gamma) \not\equiv 0 \bmod l\}$$

なる $\mathcal{O}_K$ の部分集合を考える. ℓ が l を割る $\mathcal{O}_K$ の素イデアルの全体を動くとして, ϵ を $\#(\mathcal{O}_K/\ell)^\times$ たちの最小公倍数とする. 今, l は f の判別式の約数ではなく, 即ち, K で不分岐であるので, 任意の $\gamma \in \Gamma$ に対して

$$\gamma^\epsilon \equiv 1 \bmod l$$

が言える. このとき, $\lambda : \Gamma \to l\mathcal{O}_K/l^2\mathcal{O}_K$ を $\lambda(\gamma) = (\gamma^\epsilon - 1) + l^2\mathcal{O}_K$ で定める. $l\mathcal{O}_K/l^2\mathcal{O}_K$ の基底を $\{b_j l + l^2\mathcal{O}_K\}_{1 \le j \le d}$ とすれば

$$\gamma^\epsilon - 1 \equiv \sum_{j=1}^{d} \lambda_j(\gamma) b_j l \bmod l^2$$

と書けるので, λ を d 個の成分で表せる. 各 $\lambda_j : \Gamma \to \mathbb{Z}/l\mathbb{Z}$ と λ は, 任意の $\gamma, \gamma' \in \Gamma$ に対して, 定義より明らかに $\lambda(\gamma\gamma') = \lambda(\gamma) + \lambda(\gamma')$, $\lambda_j(\gamma\gamma') = \lambda_j(\gamma) + \lambda_j(\gamma')$ なる準同型性を持つ. (この指標 λ は, 本質的に Fermat 商と呼ばれるものであり, l 進対数関数の近似を与えている.)

この指標を用いて, 残る d 個の成分は

$$\lambda_1(a-b\alpha),\dots,\lambda_d(a-b\alpha)$$

と定める.

ここで, 上で定めたベクトル $V_{a,b}$ の以降での役割について簡単に見ておく. まず,

$$a-bm=\pm\Pi_{q\in\mathcal{B}_{\mathbb{Q}}}q^{\nu_q(a-bm)}, \tag{2}$$

$$(a-b\alpha)\mathcal{O}_K=\Pi_{\mathfrak{q}\in\mathcal{B}_K}\mathfrak{q}^{\nu_{\mathfrak{q}}(a-b\alpha)} \tag{3}$$

が成り立っている事に注意しておく. 2 節の冒頭でも簡単に述べたが, このような関係式が Step 2 で十分たくさん集められており, これらを利用して $\mathcal{O}_K$ の要素の l 乗を構成することになる. すなわち, $\mathcal{O}_k$ の二つの要素 δ, γ, 整数 $x, e_{a,b}$ で

$$ut^x\cdot\prod_{(a,b)\in S}(a-bm)^{e_{a,b}}=\delta^l, \tag{4}$$

$$\prod_{(a,b)\in S}(a-b\alpha)^{e_{a,b}}=\gamma^l \tag{5}$$

を満たすものが発見できたとする.

このとき,

$$\phi(\delta)^l=ut^x\cdot\phi(\gamma)^l \tag{6}$$

が成り立ち, $x\equiv-\log_t u \bmod l$ が求まる.

具体的には, Step 4 で説明する Gauß の消去法などを用いた行列の計算で求められるのであるが, (5) の左辺のような代数的整数が, 正確に, ある $\mathcal{O}_K$ の要素の l 乗であるということを見るには $V_{a,b}$ の最初の $\pi(b)+\Pi(B)$ 個の成分だけでは情報が十分でない. 一般的には, イデアルとしての l 乗しか構成出来ない. 仮にそれが単項イデアルであったとしても, 単数倍は無視できず不確定さが残る. この問題は, Schirokauer によって導入された上述の指標 λ を用いれば解決できる.

実際, 次が成り立つ：

定理 1 (Schirokauer [26]). 代数体 K, その整数環 $\mathcal{O}_K$, 素数 l は K で不分岐とする. λ,Γ などは上述のものとすると, $\gamma\in\Gamma$ が
(i) 任意の素イデアル $\mathfrak{p}\subset\mathcal{O}_K$ について $\nu_{\mathfrak{p}}(\gamma)\equiv 0 \bmod l$,
(ii) $\lambda(\gamma)=0$(全ての $\lambda_j(\gamma)=0$)
を満たすとする. このとき, 素数 l が代数体 K の類数と互いに素であり, かつ $\mathcal{O}_K$ の単数で l^2 を法として 1 と合同なものは全て $\mathcal{O}_K$ の要素の l 乗となるか, 又は Leopoldt 予想が正しいと仮定すると, γ は $\mathcal{O}_K$ のある要素の l 乗である.

有限体上の離散対数問題を考える場合, 一般に, l は十分大きな素数であると考えてよいので, K の類数と l は互いに素だと期待され, 単数に関する条件も heuristic には満たしていると期待されるので [26], この定理を用いれば, 最初の $\pi(b)+\Pi(B)$ 個の成分を使ってイデアルとして l 乗のものを構成し, かつ残りの d 個の成分が全部 0 になるような関係式を求めれば (上述の集合 S, $x, e_{a,b} \in \mathbb{Z}/l\mathbb{Z}$ を求める事), 要素としての l 乗が構成出来る.

ここで注意として, 一般に, 上述の δ, γ は $\mathbb{Z}[\alpha]$ の要素とならない場合も考えられる. しかしながら, $f'(\alpha)\mathcal{O}_K \subset \mathbb{Z}[\alpha]$ が成り立つので, (4), (5) の両辺に $f'(\alpha)^l$ を乗じて

$$\phi(f'(\alpha)\delta)^l = ut^x \cdot \phi(f'(\alpha)\gamma)^l$$

を得る.

Step 4. 連立方程式の解法

ここでは, Step 3 で求めた各 $(a,b) \in S$ に対するベクトル $V_{a,b}$ を使って, 実際に代数的整数の l 乗を構成し, $\log_t u$ を求める. まず, 離散対数問題のパラメータ t, u に対しても $\mathbb{Z}^{\pi(B)+\Pi(B)+d}$ のベクトルを定義しておく. V_t は, 最初の $\pi(B)$ 個の成分が $\nu_{q_1}(t), \ldots, \nu_{q_{\pi(B)}}(t)$ で, 残りは全て 0 となるものとする. V_u も同様で, 最初の $\pi(B)$ 個の成分が $\nu_{q_1}(u), \ldots, \nu_{q_{\pi(B)}}(u)$ で, 残りは全て 0 となるものとする. 今, A を, 最初の 1 列が V_t, 他の列は $V_{a,b}$ として得られる $(\pi(B)+\Pi(B)+d) \times (\#S+1)$ 型の行列とする. $A = (a_{i,j})$ とする. 但し, S は $\#S+1 \geq \pi(B)+\Pi(B)+d$ を満たすとする. このとき次の連立方程式を考える：

$$AX \equiv -V_u \bmod l \tag{7}$$

この線形方程式が解けるためには, $\mathbb{Z}/l\mathbb{Z}$ 上の行列 $A \bmod l = (a_{i,j} \bmod l)$ のランクが $\pi(B)+\Pi(B)+d$ となればよく, ランクがこれより小さければ S の要素をさらに増やすか, Step 2 で定めたパラメータ C を大きく取り直すなどする必要がある.

この解を $(x, \ldots, e_{a,b}, \ldots)$ とすれば, Step 3 で考察した関係式 (4), (5) が得られることが簡単に分かる.

ここで, 連立方程式の解法に用いるアルゴリズムであるが, 一般によく知られているものは Gaußの消去法と呼ばれるものである. これは, 行列のサイズの 3 乗のオーダの計算量である事が知られているが, 現在の NFS の実装サイズでは大きすぎて実装には向いていないと考えられている. 行列が疎であるような場合は, conjugate gradient method や Lanczos 法と呼ばれるアルゴリズムが実用的であることが知られている. また, Wiedemann による coordinate recurrence method は理論的には高速で, 行列のサイズの $2+o(1)$ 乗のオーダの計算量である [22, 30].

2.3 $\mathbb{F}_{p^n}$ $(n > 1)$ 上の離散対数問題への NFS

この節では, 素体上でない場合の離散対数問題への NFS について簡単に説明する. 詳しくは [27] を参照. まずは, $\mathbb{F}_q = \mathbb{F}_{p^n}$ の構成から. r を, $r \equiv 1 \bmod n$ となる素数の中で, n と $(r-1)/e$ (e は $p \bmod r$ の位数) が互いに素となる最小のものとする. ζ_r を 1 の原始 r 乗根とし, $\mathbb{Q}(\zeta_r)$ の部分体で $\mathbb{Q}$ 上 n 次のものを F とする. p は F で惰性するので

$$\mathcal{O}_F/p\mathcal{O}_F \simeq \mathbb{F}_q$$

が成立する. t_1 を $T_{F/\mathbb{Q}}(\zeta_r)$ (ζ_r のトレース), $t_2, \ldots, t_n$ を t_1 の共役元とする. このとき, $t_1, \ldots, t_n$ は $\mathcal{O}_F$ の整数基底となる [3]. $\mathbb{F}_q$ は $\{\sum_{j=1}^{n} a_j t_j \mid 0 \le a_j < p\}$ と同一視することにする. 一般 Riemann 予想 (ERH) を仮定すれば, 上の素数 r は $r \le (\log q)^{c_3}$ (c_3 は定数) を満たすものが取れる [4].

この数体 F を用いて, 素体と同様に NFS を適用することが出来る. 多項式の選択も $m = [p^{1/d}]$ とおいて p を m で展開する方法で行い, $F(\alpha)$ が F の d 次拡大体だとする. Smooth な要素も, $a - bm, a - b\alpha$ $(a, b \in \mathcal{O}_F)$ たちを集めることになる.

2.4 NFS の漸近的な計算量評価

ここでは, 前節で見た Schirokauer のアルゴリズムの計算量評価を与える. アルゴリズムの中で出てきていたパラメータ d, B, C なども最適な値を求める. Step 2 で集められる smooth な要素の大きさの評価は (1) から $|(a - bm)N(a - b\alpha)| \le C(p^{1/d} + 1)(1 + d)C^d p^{2/d} \le 2dC^{d+1}p^{2/d}$ で与えられる. この最右辺の値を x とする. 次に, Step 4 での行列のサイズについて, $\#S + 1$ は $\pi(B) + \Pi(B) + d$ 以上である必要があり, $\pi(B) + \Pi(B) + d$ は $(d+1)B + d$ で上から押さえられるので, もし拡大次数 d が $d = B^{o(1)}$ とおけるならば $N = \#S$ は, $N = B^{1+o(1)}$ とおける. これは行列のサイズも与えている.

$\psi(x, B)$ で, x 以下の B-smooth な自然数の個数を表すことにする. すると, smooth な組 (a, b) を N 個集めるためには ($|(a - bm)N(a - b\alpha)|$ の値が, 一様に x 以下の自然数を動くと仮定して) $xN/\psi(x, B)$ 回 smoothness テストを繰り返せば良いと期待される. これから C の値を最適化することが出来るが, それには次の定理が有効である.

定理 2 ([17]). 任意の $y \ge 2$ で定義された関数 $g(y) = y^{1+o(1)}$*(*y が十分大きいとき $o(1)$ は 0 に近づく*)* に対して*,* x が十分大きいとき

$$\frac{xg(y)}{\psi(x, y)} \ge L_x[1/2, \sqrt{2}]$$

が成立する. さらに, この式で等号が成立するための必要十分条件は, $y = L_x[1/2, 1/\sqrt{2}]$ のときである.

この定理を用いると, $N = B^{1+o(1)}$ であれば, $C^2 \geq xN/\psi(x, B)$ は必要であるから

$$C^2 \geq L_x[1/2, \sqrt{2}]. \tag{8}$$

これから d, B, C の値を最適化すると [27]

$$C = L_p[1/3, (8/9)^{1/3}],\ d = (\frac{(3+o(1))\log p}{\log\log p})^{1/3},\ B = L_p[1/3, (8/9)^{1/3}]. \tag{9}$$

従って, smoothness テストにかかる計算量は $C^2 = L_p[1/3, (64/9)^{1/3}]$, 行列の計算は $B^{2+o(1)} = L_p[1/3, (64/9)^{1/3}]$ となり, 最終的な計算量は $L_p[1/3, (64/9)^{1/3}]$ で与えられる.

2.5 有限素体上の離散対数問題の数値実験

ここでは, 有限素体上の離散対数問題の数値実験について述べる. 有限素体上の離散対数問題の数値実験は, 素因数分解の数値実験ほど注目されておらず数も多くはないが, いくつかの数値実験が報告されている. 主なものは, 1998 年に Weber 等は [29], 129 桁の特殊な形の素数

$$p = \frac{740 \cdot 7^{149} - 737}{3}$$

位数の有限素体上の離散対数問題を, 本稿で説明した Schirokauer のアルゴリズムを実装して解いたものである. p が特殊な形なので SNFS を用いている. これは, この p を標数とする有限素体上の Diffie-Hellman 鍵交換方式を解くという McCurley によるチャレンジ問題 [20] の解でもある. 同じ年に, Joux 等 は, 90 桁 [11], 1999 年には 100 桁 [12], 2001 年には 110 桁と 120 桁 [14] のサイズの有限素体上の離散対数問題に対する離散対数問題に対する数値実験を行い成功している. さらに, 2005 年にも彼等 [16] は, 130 桁のサイズの有限素体上の離散対数問題を解いている. 同様に GNFS の数値実験である. 実装には [15] の改良などを用いている. 130 桁は, 2006 年 12 月現在でのチャンピオンレコードである.

形が特殊ではない素数を標数とする有限素体上の離散対数問題の年代ごとの桁数の記録を, 以下の表 1 に, 素因数分解と並べてまとめておく. 但し, 離散対数問題の方には, GNFS ではなく Gaussian Integer Method と呼ばれる手法を使ったものも含まれており（以下の表では, * を記している）, 素因数分解の方には MPQS（複数多項式 2 次ふるい）と呼ばれるものの記録も含まれる（以下の表では, + を記している） [13]. ：

年	DLP	IFP
1990		116+
1991	58*	
1992		
1993		120+
1994		129+
1995	65	
1996	85*	130
1997		
1998	90	
1999	100	155
1900		
2001	120	
2002		158
2003		174
2004		
2005	130	200

表 1

2.6 公開鍵暗号への安全な鍵サイズ

ここでは, 有限素体上の離散対数問題の困難性に安全性の根拠をおく公開鍵暗号の安全性を考える場合の鍵サイズについて考察する. すでに述べたように, 有限素体上の離散対数問題を解く場合に, 漸近的に最も高速なアルゴリズムは NFS であり, ここでは, NFS を用いた攻撃に対する安全性についてのみ考えることにする. 素因数分解アルゴリズムに対する NFS と有限素体上の離散対数問題に対する NFS は, そのサイズ（素因数分解の場合は合成数全体のサイズ, 有限体上の離散対数問題の場合は有限体のサイズ）の準指数時間アルゴリズムとしてオーダは同じである. 現在までの有限素体上の離散対数問題の数値実験例が素因数分解のそれと比べてあまり多くないため, 単純な比較は難しいが, 少なくとも素因数分解問題が困難になるサイズを取っておくことは必要である. 漸近的な計算量評価に関しては, 上述のように素因数分解も離散対数問題の場合もオーダは同じであり, さらなる数値実験によって具体的な差が出ることは期待出来なくはないが, 実用的な観点からの改良 [15] などを考慮しても, 計算量的にはほぼ同じであると考えてよいと思われる. 公開鍵暗号に関する安全な鍵サイズの予測に関しては, [1] 及び [19] 等が代表的である.

3　有限体上の楕円曲線上の離散対数問題

本節では, 有限体上の楕円曲線の有理点のなす有限アーベル群上の離散対数問題の困難性について述べる. 有限体 $\mathbb{F}_q$ 上定義された楕円曲線 E とは

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

という形の非特異３次曲線の事である. 但し, 各 $a_i \in \mathbb{F}_q$ である.

このとき, よく知られているように E の $\mathbb{F}_q$ 有理点の全体のなす集合 $E(\mathbb{F}_q)$ には, 無限遠点を単位元とする群構造を定義する事が出来, 有限アーベル群となる. 群演算は, 点を表す成分の有理関数で表すことが出来, 効率的に計算できる.

たとえば, 有限体 $\mathbb{F}_q$ の標数が奇素数で, 5 以上の場合, 定義方程式は

$$y^2 = x^3 + a_4x + a_6$$

で与えられ, その上の２つの点 $P = (x_1, y_1), Q = (x_2, y_2)$（$P \neq -Q = (x_2, -y_2)$）に対してその “和” $P + Q = (x_3, y_3)$ は次で計算できる：

$$x_3 = \lambda^2 - x_1 - x_2,$$

$$y_3 = \lambda(x_1 - x_2) - y_2$$

但し, $\lambda = (y_2 - y_1)/(x_2 - x_1)$（$P \neq Q$ の場合）, $= (3x_1^2 + a_4)/(2y_1)$（$P = Q$ の場合）

楕円曲線上の離散対数問題（ECDLP）とは, 有限体 $\mathbb{F}_q$ 上の楕円曲線 E とその上の２つの $\mathbb{F}_q$ 有理点 P, Q が与えられたとき, $Q = mP$ なる自然数 m が存在すれば, それを求める問題である. 有限体上の離散対数問題と同様に, 点 P の位数を l とすれば, m は $\bmod l$ で一意に定まる.

ECDLP への解法アルゴリズム研究は, 1990 年代に入って盛んになり, 特殊な曲線に対しては準指数時間となるものや（確率的）多項式時間で動くアルゴリズムも提案されている. 提案されている. 典型的な例は 超特異と呼ばれる曲線に対するアルゴリズムでこれは, 定義体の拡大体の乗法群に効率よく埋め込む写像が Weil 対や Tate 対と呼ばれる関数を用いて定義出来る事を用いている. 一般には, ランダムな曲線を選んだ場合は, その埋め込む際の拡大次数が入力サイズに対して指数的となるため, 有効でないことが知られている. また, 有限素体上定義され定義体を同じ位数を持つ楕円曲線に対しては楕円曲線上の Fermat 商, もしくは “対数微分商” を効率よく計算する事により離散対数問題を（確率的）多項式時間で解くアルゴリズムが存在することが知られている. 素体ではない有限体（単に拡大体と呼ぶことにする）上定義された ECDLP で, その拡大体の素体からの拡大次数が合成数

の場合に有効となる Weil descent なる手法も提案されているが, いずれも効果的に適用できるのは特殊な曲線に限られる. 他にも, ECDLP に対して, 有限体上の曲線を代数体上の曲線に “持ち上げ” て, 指数計算法が直接適用出来るかどうかの研究などもあるが, 現在のところ直接的に適用することは難しいと考えられている. [9]. 一方, 最近, Huang と Raskind によって, “Signature Calculas” [10] と呼ばれる, 有限体上の離散対数問題や ECDLP を統一的に扱おうという非常に興味深い研究も現れてきているが, 現段階では, 実用的ではなく, 純粋に理論的なものである. 代数曲線を用いた公開鍵暗号全般に関するサーベイとして [7] を挙げておく.

一般的な曲線を選んだ場合は, Pollard による Rho 法と呼ばれるものが最も有効である. ここでは, 一般的な ECDLP に対して, その計算量的困難さを, Rho 法を用いた場合に述べる.

本節の構成は次の通りである. まず 3.1 節で, Pollard の Rho 法やいくつかの ECDLP へのアルゴリズムについて説明する. 最後に 3.2 節では, 現在までに行われている ECDLP の数値実験について述べる. 最後に, 安全な鍵サイズについて簡単に考察する.

3.1 Pollard の Rho 法

ここでは, 簡単に Pollard の Rho 法について解説する. Rho 法は, ECDLP に限らず, 一般の有限アベール群上の離散対数問題に対して適用できるアルゴリズムである.

以下, 一般的な状況で述べる. G を位数 l の有限巡回群とし, 問題を $g, h \in G$ が与えられたとき, $h = g^m$ なる m を求める問題としておく. 群 G における演算は乗法的に記すことにする.

まず, G を, 3 つの部分集合にランダムに分割しておく: それぞれ, S_1, S_2, S_3 とおく. 次に, $x_0 = h$ とおく. このとき, G 自身の上への写像 f を次で定め G 内の要素の列 $\{x_k\}$ を $x_{k+1} = f(x_k)$ で定義する：

$$f(x) = \begin{cases} gx & x \in S_1 \\ hx & x \in S_2 \\ x^2 & x \in S_3 \end{cases}$$

このとき, $x_k = x_j$ と衝突が起きれば $x_k = g^{b_k m + c_k}$ などと書けるので $b_k m + c_k \equiv b_j m + c_j \pmod{l}$ となり, $m \equiv (c_k - c_j)/(b_k - b_j) \pmod{l}$ が得られる.

f が理想的にランダム写像とすると, この衝突が起きるのに必要な計算量は $O(\sqrt{l})$ である事が知られている. Rho 法は, 並列処理も可能であるので n 台のマシーンで行った場合は $\sqrt{n}$ 倍高速となる.

また, 最近, Miller と Venkatessan によって Rho 法の詳しい計算量評価も与えられている [21]

3.2 楕円離散対数問題の数値実験

ECDLP の数値実験については, カナダの Ceticom 社による 1997 年に始まった ECC challenge が有名であるので, ここでは 2006 年 12 月現在の ECC challenge のチャンピオンレコードについて簡単に述べる.

問題は大きく 2 つに分類されている（Koblitz 曲線と呼ばれるものも含まれているので, それも含めると 3 つ）, 定義体の標数が 2 の場合は奇素数の場合である. それぞれの問題（曲線と言っても良いが）ECC2-**, ECC2K-** や ECCp-** などと記される. 但し, ** にはビットサイズが入る.

2006 年 12 月現在の ECC challenge のチャンピオンレコードはどちらも 109 ビットで, つまり, ECC2-109, ECCp-109 である.

ECCp-109 は, 2002 年 11 月に解かれたもので, 約 10000 人のメンバーが参加し, 549 日かけて解いた.

ECC2-109 は, 2004 年 4 月に解かれたもので, 並列化された Rho 法を用いている. 2002 年の開始以来, 2000 人近いメンバーが参加し 17ヶ月かかっている.

以下の表 2 に, 現在までの ECC challenge の結果を抜き出しておく. 詳しくは Ceticom の web ページを参照されたい. [5]

年	ECC2	ECC2K	ECCp
1997	79		79
1998	97	95	97
1999			
2000		108	
2001			
2002			109
2003			
2004	109		

表 2

3.3 公開鍵暗号への安全な鍵サイズ

ECDLP については, 一般的な楕円曲線を用いる限りは, Rho 法が最も有効で, サイズはほぼ半分となるが, いわゆる総当り攻撃しかない. 計算量は $\frac{\sqrt{\pi 2^k}}{2}$（ECDLP

のビット長が k）に比例すると評価されるので, ECDLP の定義に現れる群位数 l のサイズが 160 ビット程度あれば, 現時点では, 十分安全であると考えられる. ちなみに, Lenstra 等による見積もり [19] では解法アルゴリズムの進歩がある場合には, 160 ビットのサイズの ECDLP が安全なのは, 2010 年頃までで, ない場合には 2020 年頃までとなっている.

参考文献

[1] R. Brent, "Recent Progress and prospects for integer factorisations algorithms," Proc. of COCOON, LNCS1858, pp.3–22, Springer-Verlag, 2000.

[2] J. Brillhart, M. Filaseta and A. Odlyzko, "On an irreducibility theorem on A. Cohn," Can. J. Math., vol.33, no.5, pp.1055–1059, 1981.

[3] E. Bach and J. Shallit, "Factoring with cyclotimic polynomials," Math. Comp., vol.52, no.185, pp.201–219, 1989.

[4] J.H. Buchmann and V. Shoup, "Constructing nonresidues in finite fields and the extended Riemann hypothesis," Math. Comp., vol.65, pp.1311–1326, 1996.

[5] http://www.certicom.com

[6] H. Cohen, *A Course in Computational Algebraic Number Theory*, GTM 138, Springer-Verlag, 1995.

[7] S. Galbraith and A. Menezes, "Algebraic Curves and Cryptography," Finite Fields and Their Applications, 11, pp.533-544, 2006.

[8] D. Gordon, "Discrete logarithms using the number field sieve," SIAM J. Discrete Math., vol.6, pp.124–138, 1993.

[9] M.-D. A. Huang, K.L. Kueh and K.-S. Tan, "Lifting elliptic curves and solving the elliptic discrete logarithm problem," Proc. of ANTS2000, LNCS1838, Springer-Verlag, 2000.

[10] M-D. A. Huang and W. Raskind, "Signature Calculus and Discrete Logarithm Problems," Proc. of ANTS2006, LNCS4076, pp.558–572, Springer-Verlag, 2006.

[11] A. Joux and R. Lercier, "Discrete logarithms in $GF(p)$ – 90 digits," May 1998, NMBRTHRY Maling List, Available at http://www.medics.polytechnique.fr/~lercier.

[12] A. Joux and R. Lercier, "Discrete logarithms in $GF(p)$ – 100 digits," Nov. 1999, Available at http://www.medics.polytechnique.fr/~lercier.

[13] R. Lercier, "State-of-the art in implementing algorithms for the (ordinary) discrete logarithm problem," slide from the talk at ECC99, Available at http://www.cacr.math.uwaterloo.ca/conferences/1999/ecc99/slides.html

[14] A. Joux and R. Lercier, "Discrete logarithms in $GF(p)$ – 120 digits," Apr. 17 2001, NMBRTHRY Maling List, Available at http://www.medics.polytechnique.fr/~lercier.

[15] A. Joux and R. Lercier, "Improvement to the general number field sieve for the discrete logarithms in prime finite fields," Math. Comp. 72, 242, pp.953–967, 2003

[16] A. Joux and R. Lercier, "Discrete logarithms in $GF(p)$ – 130 digits," June 18 2005, NMBRTHRY Maling List, Available at http://www.medics.polytechnique.fr/~lercier.

[17] A.K. Lenstra and H.W. Lenstra, Jr., *The Development of the Number Field Sieve*, LNM 1554, Springer-Verlag, 1993.

[18] A.K. Lenstra, H.W. Lenstra, Jr., M.S. Manasse and J.M. Pollard, "The Number Field Sieve," Proc. of STOC90, pp.564–572, 1990.

[19] A.K. Lenstra and E. Verheul, "Selecting cryptographic key sizes," Proc. PKC2000, LNCS1751, pp.446–465, Springer-Verlag, 2000.

[20] K. McCurley, "The discrete logarithm problem," in Cryptology and Computational Number Theory, Proc. of Sympos. Appl. Math., vol.42, AMS, pp.49–74, 1990.

[21] S.D. Miller and R. Venkatessan, "Spectral Analysis of Pollard Rho Collision," Proc. of ANTS2006, LNCS4076, pp.573–581, 2006.

[22] A.M. Odlyzko, "Discrete logarithms: the past and the future," Des. Codes Crypt., vol.19, pp.129–145, 2000.

[23] J. Pollard, Factoring with cubic integers, pp.4–10, in [17].

[24] J. Pollard, The lattice sieve, pp.43–49, in [17].

[25] C. Pomernace, "The Quadratic Sieve Factoring Algorithm," Proc. of Eurocrypt'84, LNCS 209, Springer-Verlag, pp.169–182, 1984.

[26] O. Schirokauer, "Discrete logarithms and local units," Theory and applications of numbers without large prime factors (R.C. Vaughan, ed.), Philos. Trans. Roy. Soc. London Ser. A, vol.345, Royal Society, London, pp.409–424, 1993.

[27] O. Schirokauer, "Using number fields to compute logarithms in finite fields," Math. Comp., vol.69, pp.1267–1283, 2000.

[28] O. Schirokauer, D. Weber and T. Denny, "Discrete logarithms – the effectiveness of the index calculus method," Proc. of ANTS-II, LNCS 1122, Springer-Verlag, pp.337–361, 1996.

[29] D. Weber and T. Denny, "The solution of McCurley's discrete log challenge," Proc. of Crypto'98, LNCS 1462, Springer-Verlag, pp.458–471, 1998.

[30] D.H. Wiedemann, "Solving sparse linear equations over finite fields," IEEE Trans. Inform. Theory, vol.32, pp.54–62, 1986.