SCIS 2010 The 2010 Symposium on Cryptography and Information Security
Takamatsu, Japan, Jan. 19-22, 2010
The Institute of Electronics, Information and Communication Engineers

ECDLP への Generalized Weil Descent Dttack の評価
Estimation of Generalized Weil Descent Attack for ECDLP

齋藤　恆和 * 小林　鉄太郎 † 山本　剛 † 金子　昌信 ‡
Tsunekazu Saito Tetsutaro Kobayashi Go Yamamoto Masanobu Kaneko

あらまし Gaudry は有限体の n 次拡大上の楕円離散対数問題への decomposition algorithm と指数計算法による攻撃を考え出した．この方法は基礎体の位数を q とし，$O(q^{2-\frac{2}{n}}\log q)$ の時間がかかる．しかし，この攻撃は q が十分に大きい時のみに実装され，とりわけ現段階では実装するに困難である．これに対して，Diem は一般の q に対して，同じ攻撃方法の詳細なアルゴリズムを与え $q > n!2^{n(n-1)}$ ならば q の多項式時間で攻撃できることを示した．本論文では Diem のアルゴリズムの改良と時間の評価を詳細に行い，実用的な範囲の拡大次数と有限体の位数毎に ρ 法との比較をした．

キーワード Decomposition algorithm, ECDLP, Index calculus, OEF, Semaev summation polynomial

1 Introduction

2 と 3 以外の素数の冪を q とし，q 元体 $\mathbf{F}_q$ の n 次拡大体 $\mathbf{F}_{q^n}$ を一つ固定する．この体 $\mathbf{F}_{q^n}$ 上の楕円曲線 $E : y^2 - x^3 - ax - b = 0$ を与える．この楕円曲線の $\mathbf{F}_{q^n}$ 有理点のなす群 $E(\mathbf{F}_{q^n})$ 上の二点 P, $A \in \langle P\rangle$ に対して離散対数問題つまり $A = lP$ として $\log_P A = l$ を求めることを考察する．Frey の提唱のもと Gaudry は因子基底を

$$\mathfrak{F} = \{P \in E(\mathbf{F}_{q^n}) \mid x(P) \in \mathbf{F}_q\}$$

と定め，指数計算法で離散対数問題に対する解法を与えた [4]．ここで楕円曲線上の点 $P \in E$ に対して affine 平面上の x 座標を $x(P)$ で記す．また指数計算法において，この因子基底から関係式を作る際には Semaev の与えた decomposition algorithm を用いている．この decomposition algorithm とは点 $P \in E(\mathbf{F}_{q^n})$ に対して，$P_1, \ldots, P_n \in E(\mathbf{F}_{q^n})$ が存在し，$P = \sum_{i=1}^{n} P_i$ となるかを判定する algorithm であり，その判定は $n+1$ 次 Semaev summation 多項式を用いて行われる．ただし指数計算法において Gaudry は q が十分大きいことを仮定し，この仮定のもと $\mathfrak{F}$ が非特異代数多様体の構造を持つことを示し，指数計算法の計算時間が $O(q^{2-\frac{2}{n}}\log q)$ で与えられることを示した [4].

これに対して Diem は一般の q に対して $\mathfrak{F}$ の代数幾何的な構造を調べて decomposition algorithm の詳細な algorithm を明記し計算時間と成功確率を求め，任意の q と拡大次数 n に対して，$q > n!2^{n(n-1)}$ ならば有限体 $\mathbf{F}_{q^n}$ 上で定義された楕円曲線上の有理点 $E(\mathbf{F}_{q^n})$ に関する離散対数問題は q の多項式時間によって解けることを示した [3].

本論文では，この Diem の定めた algorithm を Semaev 多項式の対称性を使い改良することで攻撃の適用範囲を $q > n!(\frac{2^{n-1}}{n})^n$ まで広げた．また，改良された decomposition algorithm の成功確率を無視した計算時間 R を具体的に評価をした．

Theorem 1.1 素数の冪 q と拡大次数 $n \geq 3$ について，$q > n!(\frac{2^{n-1}}{n})^n$ のとき

$$R \leq \begin{cases} O\Big((n!(\frac{2^{n-1}}{n})^n)^2 n^{2.81}\sum_{i=2}^{n-1}(i!(\frac{2^{n-1}}{n})^i)^{2.81}\log q \\ \quad +(n!(\frac{2^{n-1}}{n})^n)^2\log\left(n!(\frac{2^{n-1}}{n})^n\right)(\log q)^3\Big),\ (q \gg 1), \\ O\Big((n!(\frac{2^{n-1}}{n})^n)^2 n^{2.81}\sum_{i=2}^{n-1}(i!(\frac{2^{n-1}}{n})^i)^{2.81}\log q \\ \quad +q(n!(\frac{2^{n-1}}{n})^n)^3\Big),\ (otherwise). \end{cases}$$

この評価と Diem による成功確率

$$Prob(\mathfrak{F}^n) \geq \frac{q^n - n^3 2^{2n^2-n}(q+1)^{n-1} - n2^{n+3} + 2^{n+1} + 2^2 n - 1}{n!2^{n^2}\#E(\mathbf{F}_{q^n})}$$

* 九州大学数理学府 〒 819-0395 福岡市西区元岡 744. Graduate School of Mathematics Kyushu university, 744, Motooka, Nishi-ku, Fukuoka, 819-0395 Japan t-saito@math.kyushu-u.ac.jp
† 日本電信電話株式会社 〒 180-8585, 東京都武蔵野市緑町 3-9-11. Nippon telegraph and telephone corporation, 3-9-11, Midori-cho Musashino-shi, Tokyo 180-8585 Japan
‡ 九州大学大学院数理学研究院 〒 819-0395 福岡市西区元岡 744. Faculty of Mathematics Kyushu university, 744, Motooka, Nishi-ku, Fukuoka, 819-0395 Japan

の評価をあわせれば，改良した攻撃の十分な計算時間 $O(\#\mathfrak{F}\cdot R\cdot Prob(\mathfrak{F}^n)^{-1})$ が評価できる．

また 5 章において，この評価のもとに楕円曲線暗号としての実用的な範囲での素数の値の大きさと拡大次数の値で，ρ 法との計算時間の比較を表にまとめた．

Remark 1.2 本論文では以下のことを仮定する．単に楕円曲線と述べるときは，滑らかであることを認める．また楕円曲線上の点 $P\in E(\mathbf{F}_{q^n})$ を定め，$\langle P\rangle$ において離散対数問題を考察する際に $\mathrm{ord}P$ は *Pohlig-Hellman* 単純化により十分に大きな素数，即ち $\langle P\rangle$ は非自明な部分群を持たないものとする．

2 指数計算法

楕円曲線の有理点のなす群 $E(\mathbf{F}_{q^n})$ 上の離散対数問題に関して因子基底を $\mathfrak{F}=\{p\in E(\mathbf{F}_{q^n})|x(P)\in Fq\}$, $(\#\mathfrak{F}=\delta)$ として指数計算法を適用する．楕円曲線上の有理点 $P\in E(\mathbf{F}_{q^n})$ を位数 $\mathrm{ord}P$ が十分大きな素数 p となるようにとり固定し，$A\in\langle P\rangle$ を任意にとる．この A に対して以下に $\log_P A$ を求める algorithm を述べる．$\alpha_i,\beta_i\in\mathbf{F}_p$ をランダムに選び後に述べる decomposition algorithm により次の関係式を求める，

$$\alpha_i A+\beta_i P=\sum_{j=1}^{\delta} f_{ij}F_j.$$

これを δ 回繰り返し，ベクトルの関係式を得る，

$$\underline{\alpha}A+\underline{\beta}P=(f_{ij})\underline{F},$$

ここで，

$$\underline{\alpha}={}^t(\alpha_1,\ldots,\alpha_\delta),\underline{\beta}={}^t(\beta_1,\ldots,\beta_\delta),\underline{F}={}^t(F_1,\ldots,F_\delta)$$

である．後に述べるが因子基底の個数は $\delta\sim q$ であり，decomposition algorithm により行列 (f_{ij}) の非零要素は高々n 個である．ゆえに $q\gg n$ なので $\mathrm{rank}(f_{ij})<\delta$ としてよい．得られた、ベクトルの関係式を基本変形によって

$$\underline{\alpha}^*A+\underline{\beta}^*P=(f_{ij})^*\underline{F}$$

とする．ただし (f_{ij}) の一番下の行はすべて 0 である．そして $\alpha_\delta^*A+\beta_\delta^*P=0$ を解けばよい．

以上のことから楕円曲線 E 上の $\mathbf{F}_{q^n}$ 有理点 P と $A\in\langle P\rangle$ に対して，次のような algorithm を与えることができる．

Algorithm 1 指数計算法

入力：$P\in E(\mathbf{F}_{q^n})$, $\mathrm{ord}P=p$ (p は十分大きい素数), $\mathfrak{F}=\{P\in E(\mathbf{F}_{q^n})\mid x(P)\in\mathbf{F}_q\}=\{F_1,\ldots,F_\delta\}$, $A\in\langle P\rangle$.

出力：$\log_P A$.

1： $i=1,\ldots,\delta$ に対してランダムに $\alpha_i,\beta_i\in\mathbf{F}_p$ を選択し，decomposition algorithm により $\alpha_iA+\beta_iP=\sum_{j=1}^{\delta}f_{ij}F_j$ を求める．

2： 得られた行列の関係式を基本変形 $\underline{\alpha}^*A+\underline{\beta}^*P=(f_{ij})^*\underline{F}$ をして，$f_{\delta j}=0$ とする．

3： $\alpha_\delta^*A+\beta_\delta^*P=0$ を解く．

Step1 に関しては decomposition algorithm を δ 回行うことで $O(\delta\cdot R\cdot Prob(\mathfrak{F}^n)^{-1})$ の時間がかかる．ここで R は decomposition algorithm の成功確率を無視した時間であり，$Prod(\mathfrak{F}^n)$ は decomposition algorithm の成功確率である．Step2 に関しては行列の基本変形なので LUP 分解によって $O(\delta^{2.81}\log q)$ の時間がかかる [1].

3 Decomposition Algorithm

この節では，上の指数計算法において関係式を得るためにおこなった decomposition algorithm の詳細を述べる．

3.1 Decomposition Problem

Definition 3.1 (Decomposition problem) 任意の体 K 上定義された楕円曲線 E と楕円曲線上の点 $P\in E(\overline{K})$ に対して，$P_1,\ldots,P_m\in E(\overline{K})$ が存在し

$$P=\sum_{i=1}^{m}P_i$$

が成立するのか．もし成立するのであれば，その $P_1,\ldots,P_m$ を具体的に求めよ．

Semaev は楕円曲線上の点の和の x 座標を表記する多項式に注目し，この decomposition problem に対しある多項式による特徴付を示した．

Theorem 3.2 (Semaev) 自然数 $m\in\mathbf{N}_{\geq 2}$ と任意の体 $K(ch(K)\neq 2,3)$ 上定義された楕円曲線 E に対して，次のような多項式 $S_m(X_1,\ldots,X_m)\in K[X_1,\ldots,X_m]$ が唯一に定まる．任意の m 個の楕円曲線の K 有理点 $P_1,\ldots,P_m\in E(K)$ に対して $S_m(x(P_1),\ldots,x(P_m))=0$ が成立することは $\delta_i=\pm 1$ が存在し $\sum_{i=1}^{m}\delta_iP_i=0$ が必要十分である．

Definition 3.3 自然数 m に対して，S_m を m 次 *Semaev summation* 多項式という．

Proposition 3.4 (Semaev) 楕円曲線 $E/K: y^2-x^3-ax-b=0$ の m 次 *Semaev summation* 多項式に対して次が成立する．

(1) $\deg S_m(X_1,\ldots,X_m)=(2^{m-2},\ldots,2^{m-2})$.

(2) Semaev summation 多項式は次のように具体的に与えられる．

$S_2(X_1, X_2) = X_1 - X_2$,

$S_3(X_1, X_2, X_3) = (X_1 - X_2)^2 X_3^2 - 2((X_1+X_2)(X_1X_2+a)+2b)X_3 + ((X_1X_2 - a)^2 - 4b(X_1 + X_2))$,

$S_m(X_1, \ldots, X_m) = \mathrm{Res}_X(S_{m-k}(X_1, \ldots, X_{m-k-1}, X), S_{k+2}(X_{m-k}, \ldots, X_m, X))$ $(n \geq 4, and\ 1 \leq k \leq n-3)$.

(3) $m \geq 3$ のとき $S_m(X_1, \ldots, X_m)$ は対称式である．

上で定めた $n+1$ 次 Semaev summation 多項式に対して，有理点 $P \in E(\mathbf{F}_{q^n})$ を固定すると n 変数多項式 $S_{n+1}(X_1, \ldots, X_n, x(P)) \in \mathbf{F}_{q^n}[X_1, \ldots X_n]$ が得られる．体の拡大 $\mathbf{F}_{q^n}/\mathbf{F}_q$ の基底の一つを $\{b_1, \ldots, b_n\}$ とし，

$$S_{n+1}(X_1, \ldots, X_n, x(P)) = \sum_{i=1}^{n} s^{(i)}(X_1, \ldots, X_n) b_i,$$

$s^{(i)}(X_1, \ldots, X_n) \in \mathbf{F}_q[X_1, \ldots, X_n]$ と基礎体において分解する．ここで，$s^{(i)}$ は $deg = (2^{n-1}, \ldots, 2^{n-1})$ 次の多項式である．この分解を踏まえ theorem3.2 から $Q_1, \ldots, Q_n \in \mathbf{F}_q$ に対して次の同値が従う，

- $P_1, \ldots, P_n \in E(\mathbf{F}_{q^n}), \delta_1, \ldots, \delta_n = \pm 1$ が存在して，$x(P_i) = Q_i$ であり，$\sum_{i=1}^{n} \delta_i P_i = P$.
- $S_{n+1}(Q_1, \ldots, Q_n, x(P)) = 0$.
- $(Q_1, \ldots, Q_n)$ は $V(s^{(1)}, \ldots, s^{(n)})$ の $\mathbf{F}_q$ 有理点である．

この同値から拡大体上で定義された楕円曲線の点を $\mathfrak{F}$ の点で分解できるかどうか，またその分解を与えるためには $\mathbf{F}_q$ 有理点の集合 $V(s^{(1)}, \ldots, s^{(n)})(\mathbf{F}_q)$ のリストを与え，総当りで分解に現れる点を求めればよいことがわかる．

3.2 Semaev Summation 多項式の対称性による改良

$\mathbf{F}_q$ 有理点の集合 $V(s^{(1)}, \ldots, s^{(n)})(\mathbf{F}_q)$ を与えるアルゴリズムの計算時間と適用範囲は後に述べるが，多項式の各変数の次数の積に依存する．ゆえに我々は Semaev summation 多項式 $S_{n+1}(X_1, \ldots, X_n, x(P))$ の次数 $\deg = (2^{n-1}, \ldots, 2^{n-1})$ の積 $2^{n(n-1)}$ を下げるために，以下のように対称式で置換した．その結果，次数の積を $\leq (\frac{2^{n-1}}{n})^n$ とすことができる．Propsition3.4 により $m \geq 3$ に対して m 次 Semaev summation 多項式は対称式であり，基本対称式 $e_1 = X_1 + \cdots + X_m, \ldots, e_m = X_1 \cdots X_m$ を用いて

$$S_m(X_1, \ldots, X_m) = S_m(e_1, \ldots, e_m)$$

と変換できる．変換後の次数を

$$\deg_{(e_1, \ldots, e_n)} S_m(e_1, \ldots, e_m) = (\epsilon_1, \ldots, \epsilon_m)$$

とすれば

$$\epsilon_1 + \cdots + \epsilon_m = 2^{m-2}$$

となり，相加相乗平均の評価を考えれば

$$\epsilon_1 \cdots \epsilon_m \leq (\frac{2^{m-2}}{m})^m.$$

また，この変換における計算時間は n のに関しての多項式時間で解け，以下の多重終結式における時間が n に関して指数時間であるので無視できる．

3.3 多重終結式による有理点を求める Algorithm

2 つの多項式に対して共通零点を求めるのに終結式を計算することは周知のことである．ここでは、[2] に従って一般の個数の多項式への拡張された多重終結式を定義し，多項式の共通零点の存在性との関りを示す．また，この多重終結式をある行列の行列式で表し，これによって多重終結式を求める計算時間の評価を調べる．また，この多重終結式から共通零点を求める algorithm とその計算時間の評価を述べる．

任意の体 K を係数体とする多項式環 $K[X_1, \ldots, X_n]$ に対して，各変数の次数が $\underline{d} = (d_1, \ldots, d_n)$ 次以下の単項式のなす集合を $M_{\underline{d}} = \{X_1^{i_1} \cdots X_n{}^{i_n} | i_1 \leq d_1, \ldots, i_n \leq d_n\}$ とし，$\underline{d}$ 以下の次数の多項式のなす集合を $S_{\underline{d}}$ とする．このとき $S_{\underline{d}}$ は $M_{\underline{d}}$ の元の一次結合によってかけることは明らかである．$n+1$ 個のベクトル $\underline{d}_1, \ldots, \underline{d}_{n+1} \in \mathbf{N}^n$ を固定し j と $m \in M_{\underline{d}_j}$ に対して不定元 $u_{j,m}$ を定め，多項式環 $K[\{u_{j,m}\} \mid j = 1, \ldots, n+1, m \in M_{\underline{d}_j}]$ を得る．$\underline{d}_j$ 次の多項式 $F_j = \sum_{m \in M_{\underline{d}_j}} c_{j,m} m \in K[X_1, \ldots, X_n]$ と $\Phi = \sum_{j,m} \sum_{t_{j,m}} \alpha_{j,m,t_{j,m}} u_{j,m}^{t_{j,m}} \in K[u_{j,m}]$ に対して $\Phi(F_1, \ldots, F_n) = \sum_{j,m} \sum_{t_{j,m}} \alpha_{j,m,t_{j,m}} c_{j,m}^{t_{j,m}} \in K$ として定める．この際に次の命題が成立する．

Proposition 3.5 ([2]) $\underline{d}_1, \ldots, \underline{d}_{n+1} \in \mathbf{N}^n$ に対して，次 *(1), (2)* の条件を満足する多項式 $Res \in K[u_{j,m}]$ が唯一に存在する．

(1) 任意の $\underline{d}_j$ 次の多項式 $F_j \in K[X_1, \ldots, X_n]$ に対して

$$V(F_1, \ldots, F_{n+1}) \neq \emptyset \Longleftrightarrow Res(F_1, \ldots, F_n) = 0.$$

(2) Res は既約である．

Definition 3.6 任意の $\underline{d}_j$ 次の多項式 $F_j \in K[X_1, \ldots, X_n]$ に対して，$Res(F_1, \ldots, F_{n+1})$ を $F_1, \ldots, F_{n+1}$ の多重終結式という．

また，次数がすべて等しいとき即ちすべての j に対して $\underline{d}_j = \underline{d} = (d_1, \ldots, d_n)$ の場合,Res は線形写像

$$\begin{array}{ccc} Syl{:}S^{n+1}_{(d_1+1,d_2+1,\ldots,nd_n+1)} & \longrightarrow & S_{(2d_1+1,3d_2+1,\ldots,(n+1)d_n+1)} \\ (g_1,\ldots,g_{n+1}) & \longmapsto & \sum_{j=1}^{n+1} g_j F_j \end{array}$$

を用いて $Res(F_1, \ldots, F_{n+1}) = \det(Syl)$ となる [8]．線形写像 Syl は次元が $(n+1)!d_1 \cdots d_n$ の空間の間の線形写像なので，行列式の計算を LUP 分解により $Res(F_1, \ldots, F_{n+1})$ の計算は

$$O(((n+1)!d_1 \cdots d_n)^{2.81} \log q)$$

の時間で十分である [1]．

この多重終結式の計算をもとにして，$K = \mathbf{F}_q$ とし，$f_1, \ldots, f_n \in \mathbf{F}_q[X_1, \ldots, X_n]$ に対して多様体 $V(f_1, \ldots, f_n)$ の $\mathbf{F}_q$ 有理点のリストを求めるには以下のようにする（ただし，$\dim V(f_1, \ldots, f_n) = 0$ のときのみである）．各変数 X_i に対して $Res_{\check{X}_i}(f_1, \ldots, f_n)$ を X_i を除く変数に対する多重終結式とする．即ち係数環を $K = \mathbf{F}_q[X_i]$ とし,$f_1, \ldots, f_n \in \mathbf{F}_q[X_i][X_1, \ldots, X_{i-1}, X_{i+1}, \ldots, X_n]$ としての多重終結式であり，$n!d_1 \cdots d_n$ 次の $\mathbf{F}_q[X_i]$ の元である．この X_i としての多項式 $Res_{\check{X}_i}(f_1, \ldots, f_n) = 0$ の $\mathbf{F}_q$ 値の根を Berlekamp's algorithm により求める．この際に，この $\mathbf{F}_q$ 値の根は多様体 $V(f_1, \ldots, f_n)$ の $\mathbf{F}_q$ 有理点の i 番目の射影 $V^{(i)}(f_1, \ldots, f_n) \subset \mathbf{F}_q$ を与えている．この時に，$Res_{\check{X}_i}(f_1, \ldots, f_n)$ が多項式として消えているならば $V^{(i)}(f_1, \ldots, f_n) = \mathbf{F}_q$ であり，次元を持つこととなる．故に代数閉包 $\overline{\mathbf{F}_q}$ において，少なくとも $n!d_1 \cdots d_n$ 個の元を持つこと即ち $q \geq n!d_1 \ldots d_n$ が必要になる．ここで，R_i を $Res_{\check{X}_i}(f_1, \ldots, f_n) = 0$ の $\mathbf{F}_q$ 値の根全体とし，$S_1 = R_1$ とする．さらに 1 番目から i 番目までの射影 $V^{(1,\ldots,i)}(f_1, \ldots, f_n) \subset k^i$ の $\mathbf{F}_q$ 有理点のリスト S_i を帰納的に以下のように定める．$P = (P_1, \ldots, P_{i-1}) \in S_{i-1}$ と $Q \in R_i$ に対して，$X_1, \ldots, X_{i-1}$ を P とし，X_i を Q と置換し．このとき，$f_1, \ldots, f_n \in \mathbf{F}_q[X_{i+1}, \ldots, X_n]$ について $\overline{\mathbf{F}_q}^{n-i} \supset V(f_1, \ldots, f_n) \neq \emptyset$ であれば $(P, Q) \in S_i$ とする．最後 S_n が求める $V(f_1, \ldots, f_n)$ の $\mathbf{F}_q$ 有理点のリストとなる．以上により以下の algorithm によって多様体リストは具体的にもとまる．

Algorithm 2 $\mathbf{F}_q$ 有理点の algorithm

入力:$f_1, \ldots, f_n \in \mathbf{F}_q[X_1, \ldots, X_n], \deg f_i = (d_1, \ldots, d_n)$, $q \geq n!d_1 \cdots d_n, \dim_{\mathbf{F}_q} V(f_1, \ldots, f_n) = 0$

出力：$V(f_1, \ldots, f_n)(\mathbf{F}_q)$ のリスト.

1： $Res_{\check{X}_i}(f_1, \ldots, f_n)$ を求める.

2： $Res_{\check{X}_i}(f_1, \ldots, f_n) = 0$ を解き，$\mathbf{F}_q$ 値の根のリストを R_i とする.

3： $S_1 \longleftarrow R_1$

4： $i = 2, \ldots, n$ に対して S_i のリストを以下のように定める．$P = (P_1, \ldots, P_{i-1}) \in S_{i-1}$ と $Q \in R_i$ に対して，$X_1, \ldots, X_{i-1}$ を P とし，$X_i = Q$ と置換し．このとき，$f_1, \ldots, f_n \in \mathbf{F}_q[X_{i+1}, \ldots, X_n]$ について共通な零点が $\overline{F_q}^{n-i}$ にあれば $(P, Q) \in S_i$ とする

上の algorithm でかかる時間を評価する．Step1 では $O(n(n!d_1 \cdots d_n)^{2.81} \log q)$ の時間がかかる．Step2 では Berlekamp's algorithm を使えば，q に依存するが以下の時間で解ける.

Proposition 3.7 (Berlekamp, [6]) *Monic* な多項式 $F(X)$
$\in \mathbf{F}_q[X], \deg F = d$ に対して

$$F(X) = p_1(X)^{e_1} \cdots p_r(X)^{e_r}$$

と既約かつ *monic* な相異なる多項式 $p_1(X), \ldots, p_r(X)$ を用いて因数分解するのにかかる時間は以下で十分である.

$$\begin{cases} O(d^2 (\log q)^3 \log r), & (q \gg 1), \\ O(d^3 + qrd^2), & (otherwise). \end{cases}$$

この命題によって，step2 の計算時間は次のようになる，

$$\begin{cases} O((n!d_1 \cdots d_n)^2 (\log q)^3 \log r), & (q \gg 1), \\ O((n!d_1 \cdots d_n)^3 + qr(n!d_1 \cdots d_n)^2), & (otherwise). \end{cases}$$

ここで，$q \geq n!d_1 \cdots d_n$ に注意すれば,

$$O((n!d_1 \cdots d_n)^3 + qr(n!d_1 \cdots d_n)^2) = O(qr(n!d_1 \cdots d_n)^2).$$

である．Step4 では次の定理によって計算時間が調べられる.

Proposition 3.8 ([2]) 2 つの整数 $n > m$ と多項式 $F_1, \ldots, F_n \in \mathbf{F}_q[X_1, \ldots, X_m]$ $(\deg F_i = (d_1, \ldots, d_m))$ に対して
$V(F_1, \ldots, F_n)$ が空集合であるのは，線形写像

$$\begin{array}{ccc} \Phi{:}S^n_{(2d_1-1,2d_2-1,\ldots,md_m-1)} & \longrightarrow & S_{(2d_1-1,3d_2-1,\ldots,(m+1)d_m-1)} \\ (g_1,\ldots,g_n) & \longmapsto & \sum_{i=1}^{n} g_i F_i \end{array}$$

に対して，$rank\Phi = \dim S_{(2d_1-1,3d_2-1,\ldots,(m+1)d_m-1)}$ となることが必要十分である.

$rank\Phi$ の計算は線形写像 Φ の表現行列が $nm!d_1 \cdots d_m \times (m+1)!d_1 \cdots d_m$ であるので LUP 分解の計算によって $O((nm!d_1 \cdots d_m)^{2.81} \log q)$ で計算できる．ゆえに Step4 の計算は

$$O\left(\sum_{i=2}^{n-1} \#R_i \#S_{i-1} \cdot (ni!d_1 \cdots d_i)^{2.81} \log q\right)$$

の時間を要する．各 $\#S_i \leq n!d_1\cdots d_n$ と $R_i \leq n!d_1\cdots d_n$ であることに注意すれば，上の時間は次のようになる，

$$O\left((n!d_1\cdots d_n)^2\sum_{i=2}^{n-1}(ni!d_1\cdots d_i)^{2.81}\log q\right).$$

以上から成功確率を無視し $V(f_1,\ldots,f_n)(\mathbf{F}_{q^n})$ のリストを求めるにかかる時間は Step2 と Step4 の時間が主要な計算部分となり，以下で与えられる．

$$\begin{cases} O((n!d_1\cdots d_n)^2\sum_{i=2}^{n-1}(ni!d_1\cdots d_i)^{2.81}\log q \\ \qquad +(n!d_1\cdots d_n)^2(\log q)^3\log r),(q\gg 1), \\ O((n!d_1\cdots d_n)^2\sum_{i=2}^{n-1}(ni!d_1\cdots d_i)^{2.81}\log q \\ \qquad +qr(n!d_1\cdots d_n)^2),(otherwise). \end{cases}$$

これを $n+1$ 次 Semaev summation 多項式から得られる $s^{(1)}(e_1,\ldots,e_n),\ldots,s^{(n)}(e_1,\ldots,e_n)$ に適用すれば decomposition algorithm の成功確率を無視した計算時間 R は以下のようになる．

Theorem 3.9 素数の冪 q と拡大次数 $n\geq 3$ について，$q > n!(\frac{2^{n-1}}{n})^n$ のとき，

$$R\leq\begin{cases} O\Big((n!(\frac{2^{n-1}}{n})^n)^2 n^{2.81}\sum_{i=2}^{n-1}(i!(\frac{2^{n-1}}{n})^i)^{2.81}\log q \\ \quad +(n!(\frac{2^{n-1}}{n})^n)^2\log(n!(\frac{2^{n-1}}{n})^n)(\log q)^3\Big),\ (q\gg 1), \\ O\Big((n!(\frac{2^{n-1}}{n})^n)^2 n^{2.81}\sum_{i=2}^{n-1}(i!(\frac{2^{n-1}}{n})^i)^{2.81}\log q \\ \qquad +q(n!(\frac{2^{n-1}}{n})^n)^3\Big),\ (otherwise). \end{cases}$$

4 因子基底と Decomposition Algorithm の成功確率

この節では上の decomposition algoritm が成功する確率を [3] に従って述べる．拡大体上定義されている楕円曲線 $E/\mathbf{F}_{q^n}$ に関して因子基底を次のように定める，

$$\mathfrak{F}=\{P\in E(\mathbf{F}_{q^n})\mid x(P)\in\mathbf{F}_q\}.$$

この基底因子はよって代数多様体の構造を持ち，種数と特異点の個数が調べられている [3].

Proposition 4.1 因子基底 $\mathfrak{F}=\{P\in E(\mathbf{F}_{q^n})\mid x(P)\in\mathbf{F}_q\}$ に関して次が成立する．

(1) $\mathfrak{F}$ を種数 $g(\mathfrak{F})$ とすると $g(\mathfrak{F})\leq(2n-1)(2^n-1)$.

(2) $\mathfrak{F}$ の特異点の個数は高々$n2^{n+2}$ 個である．

上の proposition より，特異点解消と Weil conjecture から因子基底の位数が次のように評価される．

Theorem 4.2 因子基底 $\mathfrak{F}$ の個数は次のように評価される，

$$|\#\mathfrak{F}-(q^n+1)+(n2^{n+2})|\leq 2(2n-1)(2^n-1)\sqrt{q^n}.$$

この評価のもとに Decomposition algrithm が成功する確率は以下のように計算されている．

Theorem 4.3 (Diem) M を $\mathfrak{F}^n$ の部分集合とする．P を任意に定めたときに *decomposition algorithm* が成功し，非自明な $P_1,\ldots,P_n\in M$ が存在して $\sum_{i=1}^n P_i=P$ が成功する確率 $Prob(M)$ は次のように評価される，

$$Prob(M)\geq\frac{\#M-n^3 2^{2n^2-n}(q+1)^{n-1}}{n!2^{n^2}\#E(\mathbf{F}_{q^n})}.$$

特に，$M=\mathfrak{F}^n$ としたとき次の評価が従う，

$$Prob(\mathfrak{F}^n)\geq$$

$$\frac{q^n-n^3 2^{2n^2-n}(q+1)^{n-1}-n2^{n+3}+2^{n+1}+2^2 n-1}{n!2^{n^2}\#E(\mathbf{F}_{q^n})}.$$

5 計算時間の評価

以上により，素数のビット数と拡大次数によって改良された攻撃の時間 $O(\#\mathfrak{F}\cdot R\cdot Prob(\mathfrak{F}^n)^{-1})$ の $\log_2$ の値を表 1 にまとめた．表 1 において横の数値 m が素数のビット数，縦の数値 n が拡大次数であり，改良された攻撃のほうが ρ 法より速く実装する場合は太字にした．また n は拡大次数，m は素数のビット数即ち $q\sim 2^m$ とした．ただし Berlekamp's algorithm に関する計算時間は短いほうを用いるものとする．

6 まとめ

本論文では Gaudry によって構築された指数計算法による楕円離散対数問題の攻撃について以下のことを行った．まず，関係式を得るための decomposition algorithm を用いる際に，Semaev summation 多項式 S_{n+1} から得られる多項式の $s^{(1)},\ldots,s^{(n)}$ の零点集合を調べる必要がある．よって Diem が与えた有限体上の n 変数の n 個の多項式の有理点を求めるアルゴリズムの評価を詳細にした．次に，このアルゴリズムを Semaev summation 多項式に適用する際に対称性を利用し高速化を図った．また，具体的数値で改良された攻撃の評価をした．

参考文献

[1] A. V. Aho, J. E. Hopcroft, J. D. Ullman, "The Design and Analysis of Computer Algorithms". Addison-Wesley, 1974.

[2] D. Cox, J. Little, and D. O 'Shea, "Using Algebraic Geometry". Springer, 2005.

[3] C. Diem. "On the discrete logrithm problem in elliptic curves". Preprint, Aug. 2009.

	10	20	30	40	50	60	70	80	90	100	110	120	130	140	150	160
3	∞	53	64	75	86	97	107	**118**	**129**	**139**	**149**	**160**	**170**	**180**	**191**	**201**
4	∞	∞	∞	104	114	124	**135**	**145**	**155**	**165**	**175**	**185**	**195**	**206**	**216**	**226**
5	∞	∞	∞	∞	∞	166	176	**186**	**197**	**207**	**217**	**227**	**237**	**247**	**257**	**267**
6	∞	∞	∞	∞	∞	∞	∞	240	**250**	**260**	**270**	**280**	**290**	**300**	**311**	**321**
7	∞	∞	∞	∞	∞	∞	∞	∞	∞	**325**	**335**	**345**	**355**	**365**	**375**	**385**
8	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	**432**	**442**	**452**	**462**
9	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞
10	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞

表 1: 改良された攻撃にかかる時間 $O(\#\mathfrak{F} \cdot R \cdot Prob(\mathfrak{F}^n)^{-1})$ の $\log_2$ の値.

[4] P. Gaudry, “Index calculus for abelian varieties of small dimension and the elliptic curve discrete logarithm problem” J. Symbolic Computation, 2009, In press.

[5] P. Gaudry, F.Hess and N.P.Smart, “Constructive and destructive facets of Weil descent on elliptic curves”. J.Cryptol, vol.15, pp.19-46, 2002.

[6] D. Knuth “Seminumerical Algorithms. Volume 2 of The Art of Computer Programming. 3rd edition”. Reading, MA: Addison-Wesley , 1981.

[7] I. Semaev, “Summation polynomials and the discrete logarithm problem on elliptic curves”. Available under http://eprint.iacr.org/2004/031, Feb. 2004.

[8] B. Sturmfels and A. Zelevinsky, “Multigraded Resultants of Sylvester Type”. J. Algebra, 163:115-127, 1994.

[9] K. Yamahoka, S. Kozaki and K. Matsuo, “On index calculus algorithm for ECDLPs on extension fields (in japanese)”. Available under http://lab.iisec.ac.jp/ matsuo_lab/pub/pdf/yamahoka_jsiam0803.pdf, March 2008.