奇標数有限体の素数次拡大体上GHS攻撃の対象となる楕円曲線に関する解析

Analysis on Elliptic Curves Subjected to GHS Attack over Prime Degree Extensions of Finite Fields with Odd Characteristic

情報工学専攻　細萱　隆之
Takayuki Hosogaya

1　はじめに

楕円曲線暗号とは有限体上の楕円曲線の有理点を用いた離散対数問題 (ECDLP) の困難性を利用した公開鍵暗号である．他の公開鍵暗号より鍵長を短く取れることで実装面などで優位性をもつ．特にソフトウェア実装においては, 奇標数有限体の拡大体上定義した楕円曲線を用いる高速化手法が知られている．

一方で拡大体上定義された楕円曲線に対する攻撃方法として GHS 攻撃が知られている．この攻撃は, 条件によっては鍵長を 160bit として設計された楕円曲線暗号系の安全性を鍵長が 107bit 程度のそれの安全性と同等にするなど現存暗号系に対して非常に強力に働く場合がある．この攻撃を受ける奇標数有限体上の楕円曲線の従来の分類はある条件下で行われたものであった．

そこで本研究では, 奇標数有限体の素数次拡大体上 GHS 攻撃を受けうる曲線の完全な分類を行い, それらの曲線に対して GHS 攻撃への耐性を考察する．

2　楕円曲線暗号と ECDLP

2.1　楕円曲線

p を 3 より大きい素数とし, 正整数 n をつかい $p^n = q$ とする．有限体 $\mathbb{F}_q = k$ 上の楕円曲線とは,

$$E : y^2 = x^3 + Ax + B \quad (A, B \in k)$$

で表される．このとき右辺は重根を持たない．

このとき E の k 上有理点に無限遠点 ∞ を加えた集合に, 楕円曲線暗号特有の加算を定義することでこの集合は有限アーベル群をなす．

2.2　ECDLP

E 上の**離散対数問題 (ECDLP)** とは, B を E 上の点として, 与えられた点 $P \in E$ について $xB = P$ なる整数 $x \in \mathbb{Z}$ が存在するとき, これを求める問題である．楕円曲線暗号は, x と B から P を求めるのは容易だが ,P と B から x を 求めるのは困難なことを利用しており, 楕円曲線暗号に対する攻撃はこの x を求めるためのものである．

3　GHS 攻撃

k_d を k の d 次拡大体とする．ここで, k_d/k のフロベニウス自己同型写像 $\sigma_{k_d/k}$ から拡張した, $k_d(x)$ の分離閉包での位数 d の自己同型 σ を仮定する．その様な写像の存在条件は [3] 等で与えられている．この仮定の下, $k_d(C_0)/k(x)$ のガロア閉包は $K := k_d(C_0) \cdot \sigma(k_d(C_0)) \cdots \sigma^{d-1}(k_d(C_0))$ であり, 自己同型写像 σ による固定体は $K' := \{\zeta \in K | \sigma(\zeta) = \zeta\} \simeq k(C)$ である．もともとの GHS 攻撃は, 標数 2 の楕円曲線に対し, 下記に示すような conorm-norm 写像の合成

$$N_{K/K'} \circ Con_{K/k_d(C_0)} : Cl^0(k_d(C_0)) \to Cl^0(K')$$

を使い, $Cl^0(k_d(C_0)) \simeq J(C_0)(k_d)$ 上 DLP を, $Cl^0(K') \simeq J(C)(k)$ 上 DLP へと写像する [1]．この攻撃は様々な種類の曲線へ拡張されており, Frey と Diem によって被覆攻撃へと一般化されている．

本論文では C_0 を標数が 3 より大きい奇標数有限体 k とその d 次拡大体 k_d 上定義されている超楕円曲線とする．C_0 が以下の形で与えられているとする．ここで, d は素数とする．

$$C_0/k_d \ : \ y^2 = c \cdot f(x) \tag{1}$$

ここで, $c \in k_d^{\times}$ かつ $f(x) \in k_d[x]$ はモニック多項式とする．すると C_0 は下記の様な k_d 上の 2 次の被覆写像を持っている．

$$C_0 \xrightarrow{2} \mathbb{P}^1(x) \tag{2}$$

これ以降, 被覆写像 $\pi/k_d : C \to \mathbb{P}^1(x)$ が存在すると仮定する．そのとき, $n \leq d$ で $\overbrace{(2, \cdots, 2)}^{n}$ 型の関数体の拡大 $k_d(x, y, {}^{\sigma}y, \cdots, {}^{\sigma^{n-1}}y) \simeq k_d(C)$ が得られ, $cov(C/\mathbb{P}^1) := Gal(k_d(C)/k_d(x)) \simeq \mathbb{F}_2^n$ となる．このとき, $d \geq 11$ の素数に関しては被覆曲線 C の種数 $g(C)$ が大きくなりすぎて GHS 攻撃がうまく働かないことが知られている．そこで本研究では, まず k 上 $d = 2, 3, 5, 7$ 次の奇標数拡大体 k_d に関して GHS 攻撃の対象となりうる被覆曲線 C を持つような楕円曲線 C_0 を完全に分類する．4 章では C_0 の分類とその分類方法について述べる．

4　GHS 攻撃を受けうる楕円曲線の分類

4.1　$cov(C/\mathbb{P}^1)$ 上のガロア表現の分類

下記のような次数 2 の被覆 $C_0/\mathbb{P}^1$ を伴う全ての $\overbrace{(2, \cdots, 2)}^{n}$ 被覆曲線 $C/\mathbb{P}^1$ の分類を考える．

$$\overbrace{\underbrace{C \to C_0 \to \mathbb{P}^1(x)}_{2}}^{\overbrace{(2, \cdots, 2)}^{n}} \tag{3}$$

そのために, $cov(C/\mathbb{P}^1) \simeq \mathbb{F}_2^n$ に作用している $Gal(k_d/k)$ の表現を考える．

$$Gal(k_d/k) \times cov(C/\mathbb{P}^1) \to cov(C/\mathbb{P}^1) \tag{4}$$

$$(\sigma_{k_d/k}^i, \phi) \mapsto {}^{\sigma^i}\phi := \sigma^i \phi \sigma^{-i} \tag{5}$$

簡単のため, 今後この $\sigma_{k_d/k}$ を σ と表記する. σ は $\mathbb{F}_2^n$ の間の対応を与えているため,

$$Gal(k_d/k) \hookrightarrow Aut(cov(C/\mathbb{P}^1)) \simeq GL_n(\mathbb{F}_2) \quad (6)$$

となる. 例として, $d=2, n=2$ の場合の σ の表現を以下に示す.

- $d=2, n=2$
  $\sigma = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in M_2(\mathbb{F}_2),\ F(x) = x^2+1$

また, σ の最小多項式 $F(x) \in \mathbb{F}_2[x]$ を用いて, C が k_d 上のモデルとなるための必要十分条件はガロア群 $Gal(k_d/k)$ の y に対する作用から以下のように導かれる.

$$\begin{aligned} &{}^{\forall}G(x)|F(x), G(x) \neq F(x) \text{ に対して,} \\ &{}^{F(\sigma)}y^2 \equiv 1 \mod (k_d(x)^\times)^2 \text{ かつ} \\ &{}^{G(\sigma)}y^2 \not\equiv 1 \mod (k_d(x)^\times)^2 \end{aligned} \quad (7)$$

続いて, (7) が成立していると仮定して $C_0 : y^2 = c \cdot f(x)$ を求めていく.

4.2 (2, ... ,2) 被覆を持つ楕円曲線の分類法

これ以降, $\hat{F}(x) \in \mathbb{F}_2[x]$ を以下の様な多項式として定義する.

$$x^d + 1 = F(x)\hat{F}(x) \in \mathbb{F}_2[x]$$

(7) のもとで, c が満たすべき条件として以下が知られている (Lemma 6.1[3]).

- $\hat{F}(1) = 0$ のとき, c$\in (k_d^\times)^2$
- $\hat{F}(1) = 1$ のとき, c$\in k_d^\times$

次に, (7) のもとで $f(x)$ を求めていく. まず, d, n, σ を与えて, $C_0/\mathbb{P}^1$ の分岐点の候補を求める. いま, $\Phi(x) := a(x)\hat{F}(x) = b_{d-1}x^{d-1} + \cdots + b_1 x + b_0$, $\mathbb{F}_2[x] \ni a(x)$, $\deg a(x) < \deg F(x)$, $(a(x), F(x)) = 1$, $N := \#\{(\mathbb{F}_2[x]/(F(x)))^\times\}/d$ と定義する.

1. $a(x) = 1$ とする. $\Phi(x) := \hat{F}(x)$ は, $C_0/\mathbb{P}^1$ の分岐点の候補の 1 つ $\{(\alpha^{q^i}, 0)|i = 0, \cdots, d-1 \text{ s.t. } b_i = 1\}$ を与えている. ここで, $\alpha \in k_d \setminus k_v, v|_{\neq d}$ or $\alpha \in k_{d\tau} \setminus k_v, v|_{\neq d\tau}, \tau \in \mathbb{N}_{>1}$ としてよい. ただし, 後者の場合, $f(x)$ が k_d 上 $\alpha^{q^i} \in k_{d\tau}$ の全ての共役元を含む必要がある. もし $N = 1$ ならば, 終了. $N \geq 2$ ならば, Step2 へ.
2. $(a(x), F(x)) = 1$ かつ $\deg a(x) < \deg F(x)$ となるような別の $a(x) \in \mathbb{F}_2[x]$ を選び, $\Phi(x) := a(x)\hat{F}(x)$ とする.
3. 今までに選んだ全ての $\Phi(x)$ が互いに異なるかどうかを調べる. ここで, 互いに異なった $\Phi(x)$ とは, その係数 $(b_0, b_1, \cdots, b_{d-1})$ が

   $$(b_j, \cdots, b_{d-1}, b_0, \cdots, b_{j-1})$$

   の様な巡回置換になっていない事を意味する. もし選んだ $\Phi(x)$ が互いに異なるならば, 分岐点の候補に $\{(\alpha^{q^i}, 0)|b_i = 1\}$ を加える. そうでないなら, その $\Phi(x)$ を捨てて Step2 へ.
4. N 個の候補が見つかったならば, 終了. そうでないならば, Step2 へ戻る.

S を $C/\mathbb{P}^1$ の分岐点の数, S_0 を $C_0/\mathbb{P}^1$ の分岐点の数とすると, Riemann-Hurwitz の genus formula より

$$S = 4 + \frac{d \cdot g(C_0) + e - 1}{2^{n-2}} \quad (8)$$

が得られる. また, Abhyankar's lemma により,

$$dS_0 \ \geq \ S \geq max\{d, 2g_0 + 3\} \quad (9)$$

となる. リストアップした分岐点を, 上記の S に関する制約条件の下で全ての組み合わせを試すことで $f(x)$ を見つけ, c を決定し C_0/k_d を求める. 例として, 再び $d=2, n=2$ の場合を述べる. この場合, 上記の方法により分岐点の候補が $(\alpha, 0)$ のみであることが分かる. また, 式 (8) と式 (9) より以下の不等式が成り立つ.

$$\begin{aligned} &8 \ \geq \ S = 4 + \frac{2 \cdot 1 + e - 1}{2^0} \geq 5 \\ &3 \ \geq \ e \ \geq \ 0 \end{aligned}$$

この例では, $e = 3$ の場合を取り上げる. (8) より $g(C_0) = 1$ なので $S = 8$ となり, 上記分岐点の候補を含むように $f(x)$ のすべての組み合わせを考慮すると $f(x) = (x-\alpha_1)(x-\alpha_2)(x-\alpha_3)(x-\alpha_4)$ しかないことが分かる. 最後に, $\hat{F}(1) = 1$ なので $c \in k_2^\times$ としてよい. 以上のことから, $d=2, n=2, e=3$ の場合の GHS 攻撃を受けうる被覆曲線 C を持つ楕円曲線 C_0 は

$$y^2 = c(x-\alpha_1)(x-\alpha_2)(x-\alpha_3)(x-\alpha_4) \quad (10)$$

である. $d = 2$ の場合, GHS 攻撃の対象となる, k 上被覆曲線 C を持つ C_0 と C の種数 $g(C)$ は表 1 の通りである. ただし, $C_0 : y^2 = f(x) = c \cdot h_d(x)h(x)$, $\deg(f(x)) = 4$, $h_d(x) \in k_d[x] \setminus k[x]$, $h(x) \in k[x]$ とする. c については, 平方元と非平方元どちらでも構わないため省略する. また, $\alpha_i \in k_2 \setminus k$, $\beta_i \in k$, $i \in \{1,2,3,4\}$ である. ただし Case 2, 3, 4 の曲線は, $\alpha_i \in k_2 \setminus k$ or

表 1 $d = 2$ の場合の k 上被覆曲線 C を持つ k_2 上楕円曲線 C_0

⟨Case⟩	$h_d(x)$
n , e , $g(C)$	deg$h[x]$
⟨1⟩	$(x-\alpha_1)$
2 , 0 , 2	3
⟨2⟩	$(x-\alpha_1)(x-\alpha_2)$
2 , 1 , 3	2
⟨3⟩	$(x-\alpha_1)(x-\alpha_2)(x-\alpha_3)$
2 , 2 , 4	1
⟨4⟩	$(x-\alpha_1)(x-\alpha_2)(x-\alpha_3)(x-\alpha_4)$
2 , 3 , 5	0
⟨sub⟩	-
-	4

$\alpha_i \in k_{2\tau} \setminus k_v$, $v|_{\neq 2\tau}, \tau \in \mathbb{N}_{>1}$ である．後者の場合は, $h_d(x)$ が k_d上 $\alpha^{q^i} \in k_{d\tau}$ の全ての共役元を含む．

本研究では, 上記の例を含め $g_0 = 1$, $S_0 = 4$ として $d = 2, 3, 5, 7$ について C を持つ楕円曲線 C_0/k_d に関する完全な分類をおこなった．5 章ではその分類された楕円曲線のうち, $d = 2$ の曲線に対して $\mathbb{P}^1(k_2)$ 上の $\mathrm{PGL}(2, k_2)$ により誘導される同型写像による軌道分解を求め, 各軌道における被覆曲線の種数全体を示す．

5 GHS 攻撃に対する耐性の考察

4 章では, 被覆曲線 C を持つ楕円曲線 C_0 を分類し, 各被覆曲線 C の種数を示した．以下では, $\mathbb{P}^1(k_d)$ 上の $\mathrm{PGL}(2, k_d)$ により誘導される k_d 上の楕円曲線 C_0 の同型写像

$$x \mapsto \frac{ax+b}{cx+d} \qquad (11)$$
$$a, b, c, d \in k_d \text{ かつ } ad - bc \neq 0$$

の作用について考察する．同型写像 (11) によって, 異なる種数の被覆曲線 C' を持つような楕円曲線 C_0' へと写像されることがある．そのため, C_0 の被覆曲線 C の種数 $g(C)$ に関する分類は, GHS 攻撃に対する安全性を保証するためには不十分である．よって (11) により移される $g(C')$ のとりうる値を示す必要がある．本章では, 4 章で分類した曲線のうち拡大次数 $d = 2$ の曲線に対し (11) の作用による軌道分解を求め, それぞれの軌道における全ての被覆曲線の種数を求める．

5.1 k_d 上の楕円曲線の分岐パターン

k_d 上定義されている 4 次楕円曲線 $C_0 : y^2 = f(x)$, $f(x) \in k_d[x]$ は, $f(x)$ の分岐の様子に合わせて表 2 の 5 つのパターンに分類できる．

表 2　$f(x)$ の分岐パターン

Pattern A	$(x-a_1)(x-a_2)(x-a_3)(x-a_4)$
Pattern B	$(x-a_1)(x-a_2)F_2(x)$
Pattern C	$(x-a_1)F_3(x)$
Pattern D	$F_2(x)\acute{F}_2(x)$
Pattern E	$F_4(x)$

$a_i \in k_d$, $i \in \{1, 2, 3, 4\}$, F_dは k_d 上 d 次既約多項式

この分岐パターンは, (11) の作用に対して不変である．

補題 1. $\mathrm{PGL}(2, k_d)$ により誘導される同型写像 (11) の作用によって, k_d 上楕円曲線の分岐パターンは不変である．

表 1 の各曲線は, (11) によって互いに移りあう場合があるが, (11) に対して楕円曲線の分岐パターンは補題 1 より不変である．つまり, 表 1 の各曲線の (11) による各軌道は, 同一の分岐パターンを持つ楕円曲線のみで構成されている．よって, 分岐パターンごとに表 1 の曲線の (11) による軌道を考察していく．そこで, 各分岐パターンに存在する表 1 の曲線とそのときの $f(x)$ の形をまとめたものが, 表 3 である．5 つの分岐パターンのうち, 3 次の $f(x)$ を持つ楕円曲線に (11) によって

表 3　$d = 2$ の場合の k_2 上の C_0 の分岐パターンが持つ Case

分岐パターン	⟨Case⟩	$f(x)$
Pattern A	⟨1⟩	$(x-\alpha_1)(x-\beta_1)(x-\beta_2)(x-\beta_3)$
		$(x-\alpha_1)(x-\alpha_2)(x-\alpha_2^q)(x-\beta_1)$
	⟨2⟩	$(x-\alpha_1)(x-\alpha_2)(x-\beta_1)(x-\beta_2)$
		$(x-\alpha_1)(x-\alpha_2)(x-\alpha_3)(x-\alpha_3^q)$
	⟨3⟩	$(x-\alpha_1)(x-\alpha_2)(x-\alpha_3)(x-\beta_1)$
	⟨4⟩	$(x-\alpha_1)(x-\alpha_2)(x-\alpha_3)(x-\alpha_4)$
	⟨*sub*⟩	$(x-\beta_1)(x-\beta_2)(x-\beta_3)(x-\beta_4)$
Pattern B	⟨2⟩	$F_2(x)(x-\beta_1)(x-\beta_2)$
		$F_2(x)(x-\alpha_1)(x-\alpha_1^q)$
	⟨3⟩	$F_2(x)(x-\alpha_1)(x-\beta_1)$
	⟨4⟩	$F_2(x)(x-\alpha_1)(x-\alpha_2)$
Pattern C	⟨1⟩	$G_3(x)(x-\alpha_1)$
	⟨3⟩	$F_3(x)(x-\beta_1)$
	⟨4⟩	$F_3(x)(x-\alpha_1)$
	⟨*sub*⟩	$G_3(x)(x-\beta_1)$
Pattern D	⟨4⟩	$F_2(x)F_2'(x)$
	⟨*sub*⟩	$G_2(x)G_2'(x)$
Pattern E	⟨4⟩	F_4

$\alpha_i \in k_2 \setminus k$, $\beta_i \in k$, $i \in \{1, 2, 3, 4\}$
$F_d(x)$ は k_2 上既約 d 次多項式, $G_d(x)$ は k 上既約 d 次多項式

変換可能なパターンは Pattern A, B, C である．それ以外の分岐パターンを持つ楕円曲線は, (11) によって 3 次の $f(x)$ へ変換できない．一般的に楕円曲線暗号に用いられる楕円曲線の $f(x)$ は 3 次であるため, 本研究では軌道の考察を Pattern A, B, C の $f(x)$ を持つ楕円曲線に限定して行った．

5.1.1 Pattern A の場合　(11) の性質として, $\mathbb{P}^1(k_d)$ 上の任意の相異なる 3 点の組 P_1, P_2, P_3 と Q_1, Q_2, Q_3 を選んだとき, これらの 3 点の対応を与える k_d 上の (11) がただ一つ存在することが知られている．この性質を利用し, 例えば Case 4 の楕円曲線の $k_2 \setminus k$ 上の分岐点 4 つのうち 3 つを Case 1 の楕円曲線の 3 つの k 上の分岐点へと対応させる (11) を取る．すると j 不変量が $k_2 \setminus k$ の値の場合は Case 4 から Case 1 の楕円曲線への同型写像となる．j 不変量が k の値の場合も

$$\frac{a\alpha_1 + b}{c\alpha_1 + d} \neq \frac{a^q\alpha_1^q + b^q}{c^q\alpha_1^q + d^q}$$

となるように a, b, c, d をとることによって得られる．その他の Case 間の同型写像も同様にして得られる．以上より, Pattern A の楕円曲線 Case 1, 2, 3, 4(j 不変量が k の元なら ⟨*sub*⟩ が含まれる場合がある) は, 全て同一の (11) による軌道に含まれ, この軌道の被覆曲線の種数は 2, 3, 4, 5 である．

5.1.2 Pattern B の場合　(11) によって $F_2(x)$ が一次式の積に分解されることはないため, 残りの 2 つの根の間の対応を考えればよい．(11) は相異なる 3 点の組同士の対応を与えるため, Pattern B の場合全て

の Case の間に同型写像が存在することは自明である. よって Pattern B の楕円曲線 Case 2, 3, 4 は全て同一の (11) による軌道に含まれ, この軌道の被覆曲線の種数は 3, 4, 5 である.

5.1.3 Pattern C の場合 Pattern C の場合, $f(x)$ は 3 次既約多項式と一次式の積であらわされる. 拡大次数 $d = 2$ の場合, 3 次既約多項式は k 上既約である $G_3(x)$ と $k_2 \setminus k$ 上既約である $F_3(x)$ が存在する. $G_3(x)$ の分解体は k_3 であり, k_3 上で

$$G_3(x) = (x-\gamma)(x-\gamma^q)(x-\gamma^{q^2}) \qquad \gamma \in k_3 \setminus k$$

と表される. $F_3(x)$ の分解体は k_6 であり, k_6 上で

$$F_3(x) = (x-\delta)(x-\delta^{q^2})(x-\delta^{q^4}) \qquad \delta \in k_6 \setminus \{k_2 \cup k_3\}$$

と表される. ある γ に対し,

$$^{\exists}A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}(2,k_2),\ s.t.\ \frac{a\gamma+b}{c\gamma+d} = \delta \quad (12)$$

となることが知られており, $\mathrm{PGL}(2,k_2)$ の作用によって $F_3(x)$ と $G_3(x)$ が対応する.

補題 2. $G_3(x)$ 同士の対応は $\mathrm{PGL}(2,k)$ の作用によって与えられる.

$\langle sub \rangle$ の一次式 $(x-\beta)$ と Case 1 の一次式 $(x-\alpha)$ の対応は $\alpha \in k_2 \setminus k$ より $\mathrm{PGL}(2,k_2)$ で与えられるため, $\langle sub \rangle$ と Case 1 の間に $\mathrm{PGL}(2,k_2)$ によって誘導される同型写像は存在しない. 次に, 残りの各ケース間同士に同型写像が存在するかを考察していく.

- $\langle sub \rangle$, Case 1 から Case 3, 4

この場合, $G_3(x)$ 同士の対応が $\mathrm{PGL}(2,k_2)$ ではつかないため, 一次式同士の対応を $\mathrm{PGL}(2,k_2)$ でとることで, 自然に $G_3(x)$ と $F_3(x)$ との対応が誘導される.

- Case 3, 4 から $\langle sub \rangle$, Case 1

$F_3(x)$ を $G_3(x)$ へ対応させる $\mathrm{PGL}(2,k_2)$ は (12) の逆写像である. $G_3(x)$ 同士の対応が $\mathrm{PGL}(2,k_2)$ ではつかないため, その $\mathrm{PGL}(2,k_2)$ によって Case 3, 4 の一次式は $k_2[x] \setminus k[x]$ の一次式のみか $k[x]$ の一次式のみに対応づけられる. Case 3, 4 の楕円曲線の j 不変量が $k_2 \setminus k$ 上の値の場合, 前者のみである.

- Case 3, 4 から Case 3, 4

Case 3 と Case 4 の間の対応は, Case 3, 4 から $\langle sub \rangle$, あるいは Case 1 への写像と, $\langle sub \rangle$, Case 1 から Case 3, 4 への写像の合成によって実現できる.

以上より, (11) に対する Pattern C の楕円曲線の (11) による軌道に含まれる楕円曲線は, j 不変量が $k_2 \setminus k$ の値の場合, Case 1, 3, 4 であり, その軌道の $g(C)$ は 2, 4, 5 である. j 不変量が k の値の場合, Case 1, 3, 4 または $\langle sub \rangle$ と Case 3, 4 であり, その軌道の $g(C)$ は 2, 4, 5 または 4, 5 である.

6 まとめ

4 章では, 奇標数の有限体 k の d 次拡大体 k_d のうち, $d = 2,3,5,7$ において GHS 攻撃を受けうる楕円曲線を求めた. 5 章では, 4 章でまとめた楕円曲線のうち, $d = 2$ の場合について k_2 上の同型写像の作用による軌道分解を求め, 各軌道のとりうる種数全体を示した (表 4). 表 4 より, 全ての軌道の $g(C)$ に 4 または 5 が含まれる. C 上の DLP を解く Index calculus algorithm 等は $g(C) > 3$ に対し作用し (3 にも一部有効ではあるが), 計算量は原則 $g(C)$ の値によって評価される. つまり, 上記軌道は全て GHS 攻撃の対象となる. また, 分岐パターン A, B, C を持つ任意の楕円曲線はいずれかの $\langle$Case$\rangle$ に該当している. つまり, それらの曲線は表 4 のいずれかの軌道に含まれていることとなる. よって $d = 2$ の場合 3 次に変換できる楕円曲線全てが GHS 攻撃の対象となり, 奇標数有限体の偶数次拡大体上定義された楕円曲線は GHS 攻撃により破れることが明らかとなった. これは, 楕円曲線暗号系の設計に新たな安全指標を与えることとなる.

表 4 $f(x)$ の分岐パターン毎の軌道とその $g(C)$

分岐パターン	軌道に含まれる曲線	$g(C)$
Pattern A	$\langle 1 \rangle, \langle 2 \rangle, \langle 3 \rangle, \langle 4 \rangle,$ と $\langle sub \rangle$	2, 3, 4, 5
Pattern B	$\langle 2 \rangle, \langle 3 \rangle, \langle 4 \rangle$	3, 4, 5
Pattern C	$\langle 1 \rangle, \langle 3 \rangle, \langle 4 \rangle$	2, 4, 5
	$\langle sub \rangle$ と $\langle 3 \rangle, \langle 4 \rangle$	4, 5

謝辞

本研究を進めるにあたり，適切な御指導, 御助言, 御検討を頂いた中央大学理工学部趙晋輝教授, 趙研究室共同研究員, 飯島努氏, 東海大学理学部情報数理学科, 志村真帆呂准教授に深く感謝いたします.

関連発表

- 細萱 隆之, 飯島 努, 志村 真帆呂, 趙 晋輝 "GHS 攻撃の対象となる奇標数素数次数拡大体上楕円曲線の完全分類", Proc of SCIS2014, IEICE Japan, 2014.
- 細萱 隆之, 飯島 努, 志村 真帆呂, 趙 晋輝 "GHS 攻撃の対象となる被覆曲線を持つ楕円曲線の同型類に関する考察", Technical Report of IEICE, 2015/03, to apper

参考文献

[1] P. Gaudry, F. Hess and N. Smart, "Constructive and destructive facets of Weil descent on elliptic curves," J. Cryptol, 15, pp.19–46, 2002.

[2] T. Iijima, F. Momose, and J. Chao "Classification of elliptic/ hyperelliptic curves with weak coverings against GHS attack without isogeny condition," Proc. of SCIS2010, IEICE Japan, 2010.

[3] T. Iijima, F. Momose, and J. Chao "Classification of Elliptic/hyperelliptic Curves with Weak Coverings against GHS Attack under an Isogeny Condition", preprint, 2013. Available from http://eprint.iacr.org/2013/487.