楕円暗号と認証システムに関する研究

研究代表者　趙　晋輝　研究員

The GHS attack is known to map the discrete logarithm problem (DLP) in the Jacobian of a curve C_0 defined over the d degree extension of a finite field k to the DLP in the Jacobian of a new curve over k which is a covering curve of C_0 . This attack is very powerful. e.g., in the case of d=3, security of ECC with 160-bit key length is reduced to security of 107-bits. In this research, we show a complete classification of all elliptic curves subjected to the GHS attack over prime degree extensions of finite fields with odd characteristic. Furthermore, we present a detailed analysis on k-isomorphic classes of these curves. In particular, we show orbit-decomposition of them under action of PGL(2, k) in case of d= 2 and evaluate genera of C over k among each PGL-orbits.

1. はじめに

楕円曲線暗号(ECC)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，ECCの安全性を160-bitから107-bitとするなど現存暗号系に対して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全ての曲線を網羅しているわけではない．そこで本研究では，以下を目的とする．

1. 奇標数有限体の素数次拡大体上被覆曲線C を持つ(＝GHS 攻撃を受けうる)楕円曲線C_0の完全な分類
2. それらの曲線に対してGHS 攻撃への耐性の考察

2. GHS攻撃

k_d上の楕円曲線C_0のECDLPを上の被覆曲線CのDLPへ変換

$$C/k \longrightarrow E/k_d$$

被覆曲線 C が存在する場合

$E(k_d)$ 上DLP　→(変換)→　$J(C)(k)$ 上DLP

k_d →(下の体へ)→ k

$g(E) \leq g(C)$

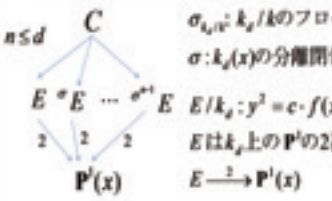
計算量Down

計算量Up

全体として計算量が削減されれば攻撃は成功

3.GHS攻撃を受けうる楕円曲線の分類

Cの存在を仮定した場合の被覆の様子は



$\sigma_{k_d/k}$: k_d/kのフロベニウス自己同型写像

σ : $k_d(x)$の分離閉包における $\sigma_{k_d/k}$の位数 dの拡張

$E/k_d : y^2 = c\cdot f(x), c \in k_d^*, f(x)(\in k_d[x])$:モニック

Eはk_d上の$\mathbf{P}^1$の2次のCovering

$E \xrightarrow{2} \mathbf{P}^1(x)$

よって $\mathrm{cov}(C/\mathbf{P}^1) \cong \mathbf{F}_2^*$, ここにσが作用しているので σ を線形写像の行列表現ととらえ分類

その後、

1. $E/k_d : y^2 = c\cdot f(x)$の$c \in k_d^*$ の決定
2. $E/\mathbf{P}^1$ の分岐点の候補の導出
3. E/k_d の方程式 $f(x)$の導出

を行うことによって，被覆曲線 Cを持つ楕円曲線 C_0 を分類した

例) $d=2$ の場合の分類

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

$f(x) = h_d(x)\cdot h(x), h_d(x) \in k_d[x] \setminus k[x], h(x) \in k[x]$

4.GHS攻撃に対する耐性の考察

$$\phi : x \mapsto \frac{ax+b}{cx+d}$$
$$ad-bc \neq 0$$
$$a,b,c,d \in k_d$$

Pattern A	$(x-\alpha_1)(x-\alpha_2)(x-\alpha_3)(x-\alpha_4)$
Pattern B	$(x-\alpha_1)(x-\alpha_2)F_2(x)$
Pattern C	$(x-\alpha_1)F_3(x)$
Pattern D	$F_2(x)F_2(x)$
Pattern E	$F_4(x)$

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

k_d上の同型写像

$g(C) \overset{?}{=} g(C')$

C — ϕ → C_0 ,　C' — ϕ → C_0'

k_d上の$f(x)$の分岐パターン

ϕ によって $g(C)$ は変化する可能性がある．

しかし，ϕ によって分岐パターンは変化しないため，分岐パターン毎に ϕ の作用による軌道分解を求めた．

※ D,E は3次への同型がないため除外

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

全軌道が $g(C)=4,5$ を含む．

C上DLPの計算量は $g(C)>3$ に対し $g(C)$ で評価

→ **$d=2$ の場合GHS攻撃を受ける**