数理解析研究所講究録 1420 巻 2005 年 174-182

超楕円暗号の最近の話題

趙 晋輝

中央大学理工学部
情報工学科

1 はじめに

RSAの誕生後、十年足らずのうちに提案された楕円曲線上の離散対数問題を利用した暗号系(通称楕円暗号)は、今や、ポストRSAの公開鍵暗号の標準方式となりつつある。

最近、超楕円暗号をはじめ、楕円暗号の一般化の研究も盛んに行われている。

2 楕円曲線とその離散対数問題

K: 有限体
K 上の楕円曲線は、方程式(Weierstrass標準形)

$E/K : y^2+a_1xy+a_3y = x^3+a_2x^2+a_4x+a_6,\ \ a_1, a_3, a_2, a_4, a_6 \in K$

によって定義される、無限遠点$\mathcal{O} = (0, 1, 0)$をもつ非特異代数曲線である。

楕円曲線のK-有理点$E(K)$は

$E(K) = \{(x, y) \in K^2 \mid y^2+a_1xy+a_3y = x^3+a_2x^2+a_4x+a_6\} \cup \{O\}$

と定義される。
$E(K)$は、可換群をなすことが知られている。

群の演算則：Chord-tangent law

楕円曲線上の離散対数問題

Given $P, Q \in E(\mathbb{F}_q), P \in < Q >$

find $n \in \mathbb{Z}\ s.t.\ P = nQ.$

楕円曲線上の離散対数問題に基づいて、楕円ElGamal公開鍵暗号、楕円DSAディジタル署名などが提案されている。

3 楕円暗号の一般化

Abel 群 G 上の一般的な離散対数問題:

$$G =< g >, \forall y \in G, \text{find } x \in \mathbb{Z}_+,$$
$$\text{s.t. } g^x = y, \text{ or } x = \log_g y$$

群多様体はアフィン代数群とAbel多様体を考えればよい。
完備な群多様体はAbel多様体であり、群演算は可換となる。
楕円曲線は、種数1のAbel多様体である。

離散対数の発展歴史：
線形代数群を用いた離散対数問題は、
準指数時間
例えば RSA, ElGamal : 鍵長1024ビット

楕円曲線(種数1のAbel多様体)の離散対数問題は、
完全指数時間
例えば、楕円暗号: 鍵長160ビット

超楕円曲線（種数2以上のAbel多様体）
種数2-4:完全指数時間
種数$\rightsquigarrow \infty$: 準指数時間
例えば、超楕円暗号: 鍵長160ビット

4 楕円暗号の一般化を研究する意味

1. Hasse-Weil定理より、種数gのヤコビ多様体の位数は

$(q^{1/2}-1)^{2g} \leq \#\mathcal{J}(\mathbb{F}_q) \leq (q^{1/2}+1)^{2g}$

$\#\mathcal{J}(\mathbb{F}_q) = O(q^g)$

となるので、プロセッサの語長を種数分の1まで（ビット幅）小さくとることができる。g=2, 80bit, g=3, 56bit
(1). ハードウェア実現のメリト
(2). ソフトウェア実現のメリト
よって、廉価なプロセッサを利用する、コンパクト化或は処理、伝送速度の能率を高めることが可能である。

2. より豊かな曲線:
位数が$\#\mathcal{J}(\mathbb{F}_{p^m}) = O(N)$の種数$g$のヤコビ多様体の同種類の数は、$\#\{\mathcal{J}(\mathbb{F}_{p^m})\} = O(4gN^{1-\frac{1}{2g}})$である。

3. より一般的な枠組みの中で楕円暗号の安全性に対する系統的な検討と理解が可能 (e.g. Weil descent)

どんなAbel多様体がよいのか？計算の面で考えると、

代数曲線は、関数体のイデアル群によって因子群を表現することで、計算に有利 (Grobner基底を用いる演算)

Superelliptic curves

C_{ab}曲線

特に、超楕円曲線の場合は、二次代数体の高速算法を類似することで、イデアル操作なしで高速演算可能。

5 超楕円曲線

体K上で種数gの超楕円曲線H

$$H/K: \quad y^2+h(x)y=f(x)$$

ここで,$f(x)$はモニックで,$\deg f(x)=2g+1$,$\deg h(x)\le g$とする. また, Hは,特異点を持たないとする.

標数$\neq 2,3$の体Kの上で、種数gの超楕円曲線H

$$H: \quad Y^2=F(X)$$

ここで、$F(X)$は、$2g+1$或は$2g+2$次の重根を持たない多項式とする。

種数が2以上の場合に、Hの有理点$H(K)$は群ではないが、それのg次対称積から、ヤコビ多様体という因子群を作ることが出来る。

(Weil) 因子 divisors $\mathcal{D}$ on H :
$\mathcal{D}(H):=\left\{\sum_i m_iP_i,\ m_i\in\mathbb{Z},\ P_i\in H(K^{sep})\right\}$.

$$\begin{aligned}\deg &: \textstyle\sum_i m_iP_i\longmapsto\sum_i m_i\\ \mathrm{Ker}(\deg)&:=\mathcal{D}_0(H)\end{aligned}$$

Hの関数体

$$K(H):=\left\{p/q\,\middle|\,p,q\in K^{sep}[u,v],\ q\neq 0 \bmod v^2+vh(u)-f(u)\right\}$$

主因子群

$$\mathcal{D}_l(H):=\left\{(f)=\sum_P \nu_P(f)P\,\middle|\,f\in K(H)\right\}\subset\mathcal{D}_0(H)$$

H の Jacobian variety は

$$\mathcal{J}(H)=\mathcal{D}^0(H)/\mathcal{D}_l(H)$$

と定義される。

超楕円曲線のヤコビ多様体上の離散対数問題

Given $P,Q\in\mathcal{J}(H)$. find $n\in\mathbb{Z}$ $s.t.$ $P=nQ$.

Cantor algorithm

ヤコビ多様体の群演算は一般的には難しいが,超楕円曲線の関数体が二次関数体であるため, 二次数体において古くから知られているGaussの合成と還元アルゴリズムが利用できる.

超楕円曲線のヤコビ多様体の演算を二次数体の類群の演算へ帰着した,種数の多項式時間のアルゴリズムが提案されている. さらに標数2の場合まで拡張されている.

Cantorアルゴリズム : 計算量は$O(g^3\log p)$である.

被約因子

$\mathcal{D}^0(H)$の任意の因子は,次のような半被約因子と線形同値である.

$$D=\sum_{i=1}^{r}P_i-r\cdot\infty$$

但し、 $P_i\in\mathrm{Supp}\,(D)/\{1,\iota\}$,

ιは,超楕円対合$P\longmapsto -P=(ax,-y-h)$とする.

さらに, Riemann-Rochにより,$r\le g$となるDと線形同値な半被約因子が一意に存在する. これを被約因子という.

Mumfordによる因子の多項式表現

任意の半被約因子Dは,

$$(U,V),\qquad U,V\in\mathbb{F}_q[x]$$

となる多項式のペアで一意に表現できる.

$$D=\mathrm{div}(U,V):=\gcd(U,V-Y)$$

$$V^2+hV-F\equiv 0 \bmod U,\quad \deg V<\deg U$$

$$D=\sum_i m_i(x_i,y_i)\Longrightarrow U(X)=\prod_i(X-x_i)^{m_i},\quad y_i=V(x_i)$$

$$\deg U\le g \iff \mathrm{div}(U,V)\ \text{is a reduced divisor}$$

Cantor Algorithm

D_1 =div(a_1, b_1) と D_2 =div(a_2, b_2) との和 D =div(a, b) を求めるために

Step 1 (Composition):
まず以下の合成演算によって,Dの半被約因子表現(a, b)を求める.

$$d := \gcd(a_1, a_2, b_1 + b_2 - h) = s_1 a_1 + s_2 a_2 + s_3(b_1 + b_2 + h)$$

$$\begin{aligned} a &= a_1 a_2 / d^2 \\ b &= (s_1 a_1 b_2 + s_2 a_2 b_1 + s_3(b_1 b_2 + f))/d \mod a. \end{aligned}$$

Step 2 (Reduction): div(a, b)が被約でない,つまり
deg$(a) > g$の場合
以下の演算をdeg$(a') \leq g$になるまで繰り返せば,被約因子へ一意に還元できる.

$$\begin{aligned} a' &= (f - hb - b^2)/a \\ b' &= -h - b \mod a' \end{aligned}$$

Step 3 $D = (a', b')$を出力する。

しかし、楕円暗号に比べて、暗号化、復号化の速度は数倍遅い。

Harley algorithm

2000年 Gaudry,Harley(ANTS) " Computing points on Hyperelliptic curves over finite fields "

1. 楕円曲線における chord-tangent 法を HEC へ拡張
2. 入力 divisor の場合分けにより重複処理を省く
3. 中国人剰余定理、Newton iteration、Karatsuba 乗算による高速化

Cantor algorithm より高速
Genus 2 の HEC に特化

6 種数2の超楕円曲線の高速演算法

種数2の超楕円曲線

$$\begin{aligned} H/\mathbf{F}_q : \quad & Y^2 = F(X), \\ & F(X) = X^5 + f_4 X^4 + \cdots + f_0, \\ & f_i \in \mathbf{F}_q, \operatorname{disc}(F) \neq 0 \end{aligned}$$

$D_1 = (U_1, V_1), D_2 = (U_2, V_2)$ の足し算 $D_3 = D_1 + D_2$

$$\begin{aligned} D_1 &= P_{11} + P_{12} - 2\infty, \quad U_1(X) = (X - x_{11})(X - x_{12}), \\ D_2 &= P_{21} + P_{22} - 2\infty, \quad U_2(X) = (X - x_{21})(X - x_{22}), \end{aligned}$$

$\gcd(U_1, U_2) = 1$という典型的な場合を考える。

まず直接足し算すると、半被約因子

$$D = P_{11} + P_{12} + P_{21} + P_{22} - 4\infty = (U, V)$$

が得られて、$U = U_1 U_2$ となる。

また、$1 = h_1 U_1 + h_2 U_2$ とすると、 $F \equiv V^2 \bmod U$ と中国剰余定理により、Vが求まる.

$$V = h_2 U_2 V_1 + h_1 U_1 V_2 \bmod U_1 U_2$$

次に、Dと線形同値な被約因子を求める.

Dの4点 $P_{ij} = (x_{ij}, y_{ij}), i, j = 1, 2$を内挿する$V(X)$は3次多項式。
関数$(V - Y)$が定義する主因子は、曲線$(V - Y)$とHと交わる6点によって定まる

$$\begin{aligned} P_{11} + P_{12} + P_{21} + P_{22} + P_{31} + P_{32} - 6\infty &= (V - Y) \\ \text{つまり} \quad D_1 + D_2 + D' &= 0 \end{aligned}$$

となる。ここで、
$D_3 := -(P_{31} + P_{32} - 2\infty)$或いは、$D_3 := -((V - Y) - D)$
D_3は被約因子である.

$$\begin{aligned} U_3 &= (F - V^2)/U \\ V_3 &\equiv -V \bmod U_3 \end{aligned}$$

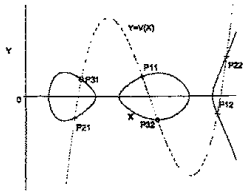


図 1: Y-V(X) による内挿とその主因子

	加算	2倍算	
Cantor	$70M+3I$	$76M+3I$	1987
Harley	$30M+2I$	$27M+2I$	2000
松尾,C.辻井	$23M+2I$	$25M+I$	
宮本,土居,松尾,C.,辻井	$26M+I$	$27M+I$	2002
高橋	$26M+I$	$27M+I$	2002
宮本, 土居, 松尾,C,辻井	$54M$	$53M$	
Lange	$50M$	$43M$	2002
Lange	$54M$	$41M$	2002
杉崎,松尾,C,辻井	$21M+2I$	$22M+2I$	2003
杉崎,松尾,C,辻井	$25M+I$	$26M+I$	2003
杉崎,松尾,C,辻井	$49M$	$44M$	2003

I: 定義体上の逆元計算時間, M: 乗算計算時間

標数2の場合への拡張

目的:
ハードウェア実装
高速乗算器を持たない安価なCPU
安全な曲線を高速に構成可能

	加算	2倍算	
杉崎,松尾,C,辻井	$25M+I$	$27M+I$	2002
Lange	$25M+I$	$27M+I$	2002

一般標数のの場合への拡張

目的:
Harleyアルゴリズムの研究に必要不可欠
数式処理システム上等への実装を考慮

	加算	2倍算	
杉崎,松尾,C,辻井	$29M+I$	$38M+I$	2002

楕円曲線暗号との比較

$\#E(\mathbb{F}_{q_E}) \approx q_E \qquad \#\mathcal{J}(\mathbb{F}_{q_H}) \approx q_H^2 \Longrightarrow q_H \approx \sqrt{q_E}$

乗算(classical)コスト: $M \approx 2(\log q)^2 \qquad M_K \approx 4M_H$

比較対象: IEEE P1363方式(Jacobian Projective)
加算: $16M$, 2倍算: $10M$

$I_H < 14M_H$

のとき, 超楕円曲線のほうが楕円曲線より高速!

超楕円曲線: Harley改
楕円曲線 : P1363

$\#J_C(\mathbb{F}_{q_H}) \approx \#E(\mathbb{F}_{q_E}) \approx 2^{186}$

使用言語 : C++
コンパイラ : gnu g++-2.95.2

	Genus two HEC	EC
加算	8.32μs.	11.6μs.
2倍算	8.74μs.	6.58μs.
整数倍算	1.98ms.	1.76ms.

on Pentium III 866MHz

7 種数3の超楕円曲線の高速算法

種数3の超楕円曲線の高速算法

p : 素数 $\neq 2, 7$. $q = p^n$

$C/\mathbb{F}_q$: $Y^2 = F(X)$
$F(X) = X^7 + f_5X^5 + f_4X^4 + \cdots + f_0 \in \mathbb{F}_q[X]$
$\mathrm{disc}\,(F) \neq 0$

Generic case
$D_1 = P_{11} + P_{12} + P_{13} - 3\infty$,
$U_1(X) = (X - x_{11})(X - x_{12})(X - x_{13})$,
$D_2 = P_{21} + P_{22} + P_{32} - 3\infty$,
$U_2(X) = (X - x_{21})(X - x_{22})(X - x_{33})$,

種数3超楕円曲線の暗号応用での利点

位数size≈種数×定義体size (Hasse-Weil range)

Thériaultによる Gaudry攻撃の改良を考慮しても
定義体size≥56bit ⇒ 160bit楕円曲線暗号と同等の安全性
64bit CPU上で多倍長演算を必要としないので，高速な実装が期待される。

種数3の超楕円曲線上の Harley algorithm及びその改良

Kuroki, Gonda, Matsuo, C, Tsujii(2002),
Pelzl-Wollinger-Guajardo-Paar(2003),
Gonda, Matsuo, Aoki, C, Tsujii(2004),

種数3の Harley algorithmの概略

1. 因子の分類
2. Composition
   - 多項式の中国人剰余定理（加算）
   - 多項式の Newton反復（倍算）
   - Karatsuba乗算
   - Montgomery逆元計算
3. Reduction（種数2と違って、2回必要）

因子の分類

- $\deg U$による場合分け
- 共通因子による場合分け

種数3では場合分けが約70通り必要

加算

1. $\deg U_1 = \deg U_2 = 3$,$\mathrm{res}(U_1, U_2) \neq 0$ (generic case)
   ⇒ Harley algorithm
2. それ以外の場合
   ⇒ Cantor algorithm : 確率 $\mathcal{O}(1/q)$ なので無視できる

2倍算

1. $\deg U_1 = 3$ and $\mathrm{res}(U_1, V_1) \neq 0$ (most frequent case)
   ⇒ Harley algorithm
2. それ以外の場合
   ⇒ Cantor algorithm : 確率 $\mathcal{O}(1/q)$ なので無視できる

改良の方針

1. Toom乗算の利用
2. Virtual polynomial multiplicationの利用

a, b : 定義体上の元
A : $a+b, -a, a-b, 2a, a/2$ の計算時間
M : ab, a^2の計算時間
I : $1/a$の計算時間

Toom乗算の利用

Toom乗算：高次多項式の効率的な乗算法
低次多項式においても特定の次数ならば効率的に計算可能
Toom乗算:$4M$ ←Karatsuba乗算:$5M$ ←Classical乗算:$6M$

入力: $R = r_2X^2 + r_1X + r_0$, $S = s_1X + s_0$
出力: $T = t_3X^3 + t_2X^2 + t_1X + t_0 = RS$

1: $w_1 = (r_2 + r_1 + r_0)(s_1 + s_0)$
2: $w_2 = (r_2 - r_1 + r_0)(-s_1 + s_0)$
3: $t_0 = r_0s_0$
4: $t_3 = r_2s_1$
5: $t_1 = (-2t_3 + w_1 - w_2)/2$
6: $t_2 = (-2t_0 + w_1 + w_2)/2$

Virtual polynomial multiplicationの利用

$$\cdots + s_1z_4 + \cdots,$$
$$\cdots + s_1z_3 + s_0z_4 + \cdots,$$
$$\cdots + s_0z_3 + \cdots,$$

を多項式乗算$(s_1X + s_0)(z_4X + z_3)$と見做し,Karatsuba乗算

$$s_1z_4$$
$$s_0z_3$$
$$(s_1 + s_0)(z_4 + z_3) - s_1z_4 - s_0z_3$$

を利用して$4M$から$3M$に削減

種数3の因子群演算の高速化

	Addition	Doubling
Kuroki,Gonda,Matsuo,C,Tsujii,02	$I + 81M + 125A$	$I + 74M + 125A$
Pelzl-W.G.P, 03	$I + 76M + 95A$	$I + 75M + 97A$
Gonda,Matsuo,Aoki,C,Tsujii, 04	$I + 70M + 113A$	$I + 71M + 107A$
Toom	$I + 70M + 113A$	$I + 71M + 107A$
Karatsuba	$I + 72M + 111A$	$I + 73M + 101A$
Classical	$I + 79M + 83A$	$I + 78M + 83A$

実装結果

定義体：素体$\mathbb{F}_p, p = 2^{61} - 1$

CPU：Alpha EV68CB 1.25GHz

Compiler：Compaq C++ with inline assembler

Cantor algorithmおよび整数倍算：NTL/GMPを利用

整数倍算：160bit乱数, signed sliding window method (window幅 5)

	Addition	Doubling	Scalar mul.
Toom	919ns	916ns	180μs
Karatsuba	920ns	897ns	177μs
Classical	888ns	875ns	172μs

Performance results on Alpha EV68 1.25GHz

Reference	CPU	Genus	Field	Scalar size	Scalar mul. (ms)
M.C.T 01	Pentium III@866MHz	2	186bit OEF	186	1.98
Miyamoto-Doi-M.C.T 02	Pentium III@866MHz	2	186bit OEF	186	1.69
Lange 02	Pentium IV@1.5GHz	2	$\mathbf{F}_{2^{80}}$	160	18.875
		2	$\mathbf{F}_{2^{160}}$	180	25.215
		2	$\mathbf{F}_p(\log_2 p = 160)$	160	5.663
		2	$\mathbf{F}_p(\log_2 p = 180)$	180	8.162
Pelzl et al. 03	ARM7TDMI@80MHz	2	$\mathbf{F}_{2^{80}}$	160	128
Kuroki-G.M.C.T 02	Alpha21264A@667MHz	3	$\mathbf{F}_{2^{61}-1}$	160	0.932
Pelzl et al. 03	ARM7TDMI@80MHz	3	$\mathbf{F}_{2^{80}}$	160	90
This Work	Alpha EV68CB@1.25GHz	3	$\mathbf{F}_{2^{61}-1}$	160	0.172

Timing of recent Harley algorithm implementations

8 Weil descent攻撃と安全性解析

Gehard Frey "How to disguis elliptic curves " ECC1998

$K/k, [K:k] = n$, e.g. $K = \mathbb{F}_{q^n}/k = \mathbb{F}_q$

X/K: AV

$\exists W_{K/k}/k$: n-D AV, s.t. $W_{K/k}(k) = X(K)$

$\exists \omega : W_{K/k}/K \longrightarrow X/K$: morphism

$\forall Y/K$: AV $\forall c : Y/K \longrightarrow X/K$: morphism

$$\begin{array}{ccc} & & \forall Y/K \\ & \overset{\exists !\iota}{\swarrow} & \downarrow \forall c \\ W/K & \xrightarrow{\omega} & X/K \end{array}$$

$\exists ! \iota : Y/K \longrightarrow W_{K/k}/K$: morphism s.t. $c = \omega \circ \iota$

Freyが注目した構造：

$X/k \Longrightarrow W_{K/k}(X) = X \times A$

A: irreducible $/k$, $\dim A = [K:k] - \dim X$

$W_{K/k}(X)$の構成法 (e.g.)

K/k: Galois, $G(K/k) = <\sigma>$, $\mathrm{ord}(\sigma) = l$: prime

$\mathbb{A}^n$のAffine coordinates $(X_1, ..., X_n)$からG-不変な関数:

$$W_{K/k}(\mathbb{A}^n) \times K \simeq \prod_{\sigma \in G(K/k)} (\sigma(X_1), ..., \sigma(X_n))$$

一般的な多様体：定義方程式からK/kの基底変換で求める。

Generic points of $W_{K/k}(X)$:

$(P, \sigma P, ..., \sigma^{l-1} P)$, P : a generic point of $X \times K$

Aはトレースゼロの部分多様体として定義される。

$$A = \left\{ (P', \sigma P', ..., \sigma^{l-1} P') \,\middle|\, \sum_i \sigma^i P' = 0 \right\}$$

例: K, k:有限体、$[K:k] = l$: prime, $X = E$: 楕円曲線

$$A(k) \supset \{ P \in E(K) | Tr_{K/k}(P) = 0 \}$$

A上の演算は、Xの演算から得られる。

特に$X = E$: elliptic curveのとき、Eの情報のみ与えて、実際にAを使って暗号を定義する。(disguise)(trapdoor)

この仕組みと構成は、結局攻撃法として生かされている。

Covering attack(Diem, Sholten 2003)

K/k

$c : C/K \longrightarrow H/K$ covering

$$\begin{array}{ccc} C/K & \xleftarrow{c^*} & H/K \\ {\scriptstyle N}\downarrow & \swarrow_{Noc^*} & \\ C/k & & \end{array}$$

$$\begin{array}{ccc} Cl^0(C/K) & \xleftarrow{c^*} & Cl^0(H/K) \\ {\scriptstyle N}\downarrow & \swarrow_{Noc^*} & \\ Cl^0(C/k) & & \end{array}$$

Covering attackが成り立つ条件：

1. Explicit C/K Weil restriction (GHS)
2. pullback c^* conorm (GHS)
3. $\ker N \circ c^*$: trivial ?(条件)
4. $g(C)$は大きすぎない ?? (評価)

条件1：Weil restrictionのfunctorial propertyよりこれをgeneral modelとして使ってよい。実際に、適当なhyperplane intersection (GHS cut)によって曲線を得る。

条件2：関数体のconormを利用する。

条件3：要検討：(素体や、素数次拡大体なら、安全)

条件4：具体的に評価が必要

$g(C) \geq ng(H)$

楕円・超楕円暗号に対する攻撃法

- Squared-root法 (BSGS, Pollard's lambda, rho法)
  一般有限アーベル群Gに適用可能$O(\sqrt{\#G})$
  $$C_P := O\left(g(K(C))^2 q^{\frac{g(K(C))n}{2}} (\log q^n)^2\right)$$
- ADH attack：種数の準指数時間攻撃
- Gaudry's variant：指数時間ではあるが、高速
  $$C_G := O\left(g(F)^3 q^2 (\log q)^2 + g(F)^2 (g(F)!) q (\log q)^2\right)$$
- Theriault's improvement

Square-root attackより早くなる種数の範囲: $5 \leq g \leq 9$

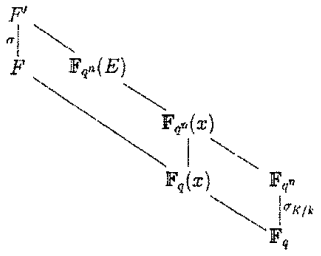
Time table

標数2の合成数次数の拡大体上の楕円曲線へ適用(GHS2000)
標数3の場合の楕円曲線への拡張(有田 2000)
標数2の超楕円曲線へ拡張(Galbraith, 2000)
実験的にGHSの得られた関数体の種数を評価(Menezes,Qu)
さらにGHSの攻撃実例(Jacobson,Menezes, Stein)
奇標数のhyperelliptic curves (Diem)
特殊なKummar extension (Theriault)
特殊なArtin-Schreier extension (Theriault)
一般的なArtin-Schreier curvesへ拡張(Hess)
cyclic Galois 拡大とsuperelliptic curves(飯島,志村,C,辻井)
偶数次、4次拡大体への攻撃(有田、長尾-有田-松尾-志村)

GHS Weil attack

$K = \mathbb{F}_{q^n}$, $k = \mathbf{F}_q$, $q = 2^l$

E/K: $Y^2 + XY = X^3 + \alpha X + \beta$



$G(K/k) \ni \sigma_{K/k} \quad \rightsquigarrow \quad \sigma \in G(K(x)/k(x))$

$F' := \prod_i \sigma^i\left(\mathbb{F}_{q^n}(E)\right)$: conjugate closure of $\mathbb{F}_{q^n}(E)$

Artin-Schreier拡大

定理 1. 条件† $\begin{cases} 1.\ n : odd \\ 2.\ m = n, \quad m := [F' : K(x)] \\ 3.\ Tr_{K/\mathbb{F}_2}(\alpha) = 0 \end{cases}$

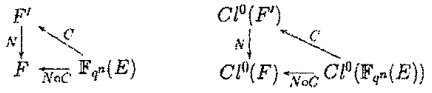
の一つでもを満たせば、$\Longrightarrow \exists \sigma \in G(F'/k),\ ord\,\sigma = n.$

In such case,

$F := (F')^\sigma$: *fixed field of* σ : *hyperelliptic*

$g(F) = 2^{m-1}, \quad or \quad 2^{m-1} - 1$

over the exact constant field k



攻撃が成り立つためには、$N = N_{F'/F}, C = Con_{F'/K(b)}$

$N_{F'/F} \circ Con_{F'/K(E)}$: $Cl^0(K(E)) \xrightarrow{Con_{F'/K(E)}} Cl^0(F') \xrightarrow{N_{F'/F}} Cl^0(F)$

は、離散対数を定義する巡回群を保存する必要がある。
つまり、自明なKernelを持つべき。

GHS

$\ker Con_{F'/K(E)} = \{$elts of orders 2 powers$\}$

Menezes, Quは、Fの種数を実験的に計算、
$q = 2, n$:prime $n \in \{160, 600\}$, 攻撃は無理

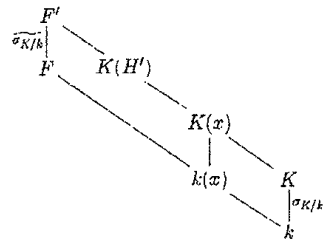
$n = 7, 31, 127, g(F) = n$となる楕円曲線がある。

しかし、IETF RFC 2412 1998では、$\mathbb{F}_{2^{155}}, \mathbb{F}_{2^{185}}$を推奨

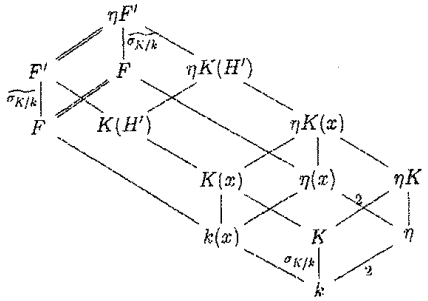
Jacobson, Menezes, Stein: $\mathbb{F}_{2^{155}}$を$\mathbb{F}_{2^5}$へdescent
2^{156}個の同型類のなかで2^{33}個へ攻撃可能。

Galbraithにより、同じisogeny classにある曲線へ攻撃範囲を広げる。

Diem 奇標数の超楕円曲線(Kummar拡大)
Theorem .
K/k: $[K : k] = \text{odd}$, H': a hyperelliptic K-curve
F': the Galois closure of $K(H')/K(x)$
If F'/K: regular, $\exists! F/k(x)$: regular subext of $F'/k(x)$,
s.t. $KF = F'$.



If F'/K:nonregular $\exists! \eta/k, [\eta : k] = 2$ s.t. $F'/\eta K$: regular,
$\exists! F/\eta(x)$: regular subext of $F'/\eta(x)$ s.t. F/η : regular,
$\eta KF = KF = F'$



以上の結論は、
Artin-Schreier拡大、(GHSを含む)
巡回Galois拡大体
へ拡張できる。

攻撃の条件(Artin-Schreier, 巡回拡大でも成り立つ)

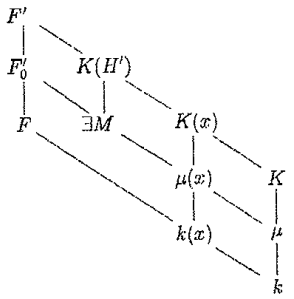
Proposition:

$k \subset \exists \mu \subsetneq K$ s.t. $K(H')/\mu(x)$: Galois
$\Longrightarrow \exists M/\mu$: regular , $KM = K(H')$ *s.t.*

$N \circ C$ factors through $N_{K(H')/M} : \mathrm{Cl}^0(K(H')) \to \mathrm{Cl}^0(M)$,
i.e. $\ker(N \circ C)$は、nontrivial.

By Hasse-Weil bound.

$\ker(N \circ C)$: trivial $\iff$ 中間体が存在しない



Diem：種数$g(F)$の上下界を計算

$\mathrm{char}K/k$=odd, $[K:k]=n=\prod p^{n_p}$: odd
H: hyperelliptic curve, $g(H)=g$

$$g(F)\le 2^{n-1}((g+1)n-1)+1$$

$k\subset \mathbb{F}_\mu \subsetneq K \Longrightarrow \ker N\circ C=\{$ elts of order 2 powers$\}$ and

$$g(F)\ge 2^{\lceil\frac{\sum_{p,n_p\neq 0}p^{n_p}}{2g+2}\rceil-2}\left(\sum_{p,n_p\neq 0}p^{n_p}-1\right)+1$$

$$g(F)\ge 2^{\phi_2(n)}-2(n-4)+1 \qquad n:\ \text{prime}$$

where $\forall n\in\mathbb{N},\quad \phi_2(n):=[\mathbb{F}_2[\xi_n],\mathbb{F}_2]$

楕円曲線に対する攻撃

素数拡大次数の場合

$n\ge 11\Longrightarrow \#Cl^0(F)\sim q^{g(F)}=2^{5000}$：安全
$n=5,7, g(F)=5$ *or* 7,,
F: hyperelliptic とは限らない。グレーゾン
$n=3$, F:種数3のhyperellitpic ：安全

Artin-Schreier 拡大に対する解析 (Hess)

$H/K: y^p-y=f(x),\quad K=\mathbb{F}_{q^n}, k=\mathbb{F}_q, q=p^r$
$E:=K(x),\quad \wp(x)=x^p-x$
$K(H):=E(\wp^{-1}(f))$: Artin-Schreier extension

$$\forall f\in E,\quad \Delta_f:=\left\{d^p-d+\sum_{i=0}^{n-1}\lambda_i\sigma^i(f)\middle| d\in E,\lambda_i\in\mathbb{F}_p\right\}$$

$$m_f(t):=\sum_{i=0}^{m}\lambda_i t^i\in\mathbb{F}_p[t]\ \ s.t.\ \ \sum_{i=0}^{m}\lambda_i\sigma^i(f)=d^p-d,\ \ \exists d\in E$$

となる最小次数のモニク多項式(unique)。

$$F'=E(\wp^{-1}(\Delta_f)),\qquad [F':E]=p^{\deg(m_f)}$$

定理 2. .
$\deg(m_f)\ge 2$,
$\Delta_f\cup K\subset \wp(E)$,
$E(\wp^{-1}(f,\sigma(f)))$ の種数は2以上

$$g(H)p^{\deg(m_f)-2}+1\le g(F)\le ng(H)\frac{p^{\deg(m_f)}-1}{p-1}$$

さらに、
$p=2, f=\gamma/x+\alpha+\beta x, \gamma,\alpha,\beta\in K, \gamma\beta\neq 0$
F'/E: regular, $F':=E(\wp^{-1}(\Delta_f))$

$$g(F')=2^{\deg(m_f)}-2^{\deg(m_f)\deg(m_\gamma)}-2^{\deg(m_f)-\deg(m_\beta)}+1$$

Superellitpic curvesに対する解析 (飯島, 志村, C, 辻井)

$$C/K: Y^r=f(X):=a_\delta X^\delta+\cdots+a_1X+a_0.$$

$r\mid q-1$, $\gcd(f(X),f'(X))=1$, $\gcd(r.\delta)=1$ or r.

$\alpha:=0$ *or* 1 if $\gcd(r,\delta)=r$ *or* 1

$$g(F)\le r^n\left\{\frac{n(\delta+\alpha)}{2}\left(1-\frac{1}{r}\right)-1\right\}+1$$

If $k\subset \mathbb{F}_\mu\subsetneq K$ s.t. $K(C)/\mu(x)$: Galois, $n:=\prod_{p|n}p^{n_p}$.

$$g(F)\ge\left(\prod_{i=1}^{\overline{m}}\overline{r}_i\right)\left[\frac{1}{2}\left\{\sum_{p,n_p\neq 0}p^{n_p}\left(1-\frac{1}{r}\right)\right\}-1\right]+1,$$

with $1\le {}^\exists\overline{m}\le n, {}^\exists\overline{r}_i\mid r,\ \overline{r}_i>1$.
If r is a prime number,

$$g(F)\ge r^{\left\lceil\frac{\sum_{p,n_p\neq 0}p^{n_p}}{\delta+\alpha}\right\rceil}\left[\frac{1}{2}\left\{\sum_{p,n_p\neq 0}p^{n_p}\left(1-\frac{1}{r}\right)\right\}-1\right]+1.$$

$\gcd(n,r)=1$とする。$\phi_r(n):=[\mathbb{F}_r[\zeta_n]:\mathbb{F}_r]$
Let n be a prime number. Then

$$g(F)\ge\ r^{\phi_r(n)}\left[\frac{1}{2}\left\{n\left(1-\frac{1}{r}\right)\right\}-1\right]+1.$$

$\gcd(n,r)=1$, r,n: primes $(n\ge 5)$,
C: superelliptic curve, non-hyperelliptic,
$g(K(C))\le 4$, $\log_2 q^{ng(C)}\le 560\qquad\Longrightarrow C_P<C_C$.

n	5	7	11	13	17
$g(F)\ge$	55	976	649	91	200884699

n: prime, $g(F)\ge 2107$ for $n\ge 17$. $g(F)\ge 55$ for $n\ge 5$

$\gcd(n,r)=1$, r,n : prime numbers $(n\ge 7)$,
C: superelliptic curve, non-hyperelliptic
$g(C)\le 4$, $q^{g(C)n}\ge 2^{160}$.
$\Longrightarrow q^{g(F)}\ge 2^{2360}$ except $n=13,\delta=4,5.6$

9 今後の課題

- 安全性の検討
- 暗号化・復号化用の高速算法の開発
- 安全な曲線を効率的な構成