Elliptic and hyperelliptic curves with weak coverings against Weil descent attack

Jinhui Chao

Joint work with Fumiyuki Momose

Dept. of Information & Sysytem Eng.
Chuo University,
Tokyo, Japan

Attacks to algebraic-curve-based cryptosystems:

1. The square-root Attacks

General attacks to a finite abelian group G,

$l := \#G$ the key length

e.g. Baby-step-giant-step attack or Pollard's rho-method or lambda-method, with complexities as $\tilde{O}(l^{1/2})$.

2. Index calculus to hyperelliptic curves

The double-large-prime variation is the most powerful attack for hyperelliptic curves(Gaudry-Theriault-Thome-Diem, Nagao).

For a hyperelliptic curve $H/\mathbb{F}_q$ of genus g, it costs $\tilde{O}(q^{2-\frac{2}{g}})$

e.g. a hyperelliptic curve of genus 3 over $\mathbb{F}_q$ is attacked with cost of $\tilde{O}(q^{\frac{4}{3}})$, a little faster than square-root attacks.

Presently, cryptosystems use elliptic curves and hyperelliptic curves of genus $2, 3$, with key length of 160 bits.

3. Index calculus to non-hyperelliptic curves

Diem's recent attack shown that non-hyperelliptic curves with low degrees are weaker than hyperelliptic curves.

For a nonhyperelliptic curve $C/\mathbb{F}_q$ of $g \geq 3$, $\deg C = d$, Diem's double-large-prime variation costs $\tilde{O}(q^{2-\frac{2}{d-2}})$.

When genus $g = d - 1$, $\tilde{O}(q^{2-\frac{2}{g-1}})$.

e.g. $g = 3$ non-hyperelliptic curves s.t. C_{34} curves can be attacked in $\tilde{O}(q)$.

4. Attacks to curves defined over extension fields

In implementation, there are always strong requests to use curves defined over certain extension of finite fields with good properties.

e.g., the extension fields which possess a normal basis.

or extension fields with small characteristics so Frobenius expansion can be used in fast addition.

On the other hand, such structures could also introduce properties which can be used in attacks.

Weil descent and GHS attack

Weil descent is introduced to cryptography by G. Frey in ECC1998.
This idea is realized by Gaudry-Hess-Smart 2000 (GHS attack)

$$\begin{tikzcd}[arrows=dash]
F' \arrow[d, "\sigma"'] \arrow[dr] & & & \\
F \arrow[ddrr] & \mathbb{F}_{q^d}(E) \arrow[dr] & & \\
 & & \mathbb{F}_{q^d}(x) \arrow[d] \arrow[dr] & \\
 & & \mathbb{F}_q(x) \arrow[dr] & \mathbb{F}_{q^d} \arrow[d, "\sigma_{K/k}"] \\
 & & & \mathbb{F}_q
\end{tikzcd}$$

$$K := \mathbb{F}_{q^d},\ k := \mathbb{F}_q,$$

$$F' := \prod_{i=0}^{d-1} \sigma^i\big(K(E)\big)$$

$$\begin{tikzcd}
Cl^0(F') \arrow[d, "N_{K/k}"'] & \\
Cl^0(F) & K(E) \arrow[ul, "Con_{K/k}"'] \arrow[l, "N_{K/k}\circ Con_{K/k}"]
\end{tikzcd}$$

The DL on E/K is mapped to $Cl^0(F/k)$ by the norm-conorm map

GHS as a covering attack(Frey, Diem)

$K/k, [K:k]=d$:

$$\pi/K : C \longrightarrow C_0 \quad \text{: a covering}$$

$$\begin{tikzcd} C/K \arrow[d] & C_0/K \arrow[l] \arrow[dl] \\ C/k & \end{tikzcd} \qquad \begin{tikzcd} J(C/K) \arrow[d, "N"'] & J(C_0/K) \arrow[l, "\pi^*"'] \arrow[dl, "N\circ\pi^*"] \\ J(C/k) & \end{tikzcd}$$

The DL on $J(C_0/K)$ is mapped to $J(C/k)$ by the norm-conorm map

$$N_{K/k} \circ Con_{K/k} : J(C_0/K) \longrightarrow J(C/k)$$

Researches on Weil descent attack

Frey “How to disguis elliptic curves “ ECC1998
GHS attack to elliptic curves over char=2 2000
GHS to genus 2 hyperelliptic curve in char=2, Galbraith
Evaluation the genera of F in GHS by Menezes, Qu
GHS attack implementation by Jacobson, Menezes, Stein
GHS to families of Kummar extensions by Theriault
GHS to families of Artin-Schreier extensions by Theriault
GHS to genearal Artin-Schreier curves by Hess
Using isogeny classes by Galbraith, Hess and Smart
GHS to hyperelliptic curves of arbitary characteristics by Diem
Cover attack by Frey, Diem
Weak fields by Menezes, Teske, Weng
......

Curves with weak coverings

If such coverings exist and DL on $J(C/k)$ can be solved faster than on $J(C_0/K)$, we call C_0 to be "with weak coverings".

Questions:

(1) what kind curves C_0 have weak coverings.
(2) how many of them
(3) how to construct such coverings

Classification and density analysis seemed nontrivial.

It is also believed that they are special therefore rare.

This research

(1) A classification of elliptic/hyperelliptic curves with $(2, ..., 2)$ coverings under a condition.

(2) We show that such weak curves do exists except for the case $(g_0, d) = (1, 2), (1, 3)$ (where C is hyperelliptic.)

(3) Density analysis of these curves are shown.

(4) Explicit defintion equations of such weak curves.

(5)Explicit construction of the coverings.

In fact, the number of these weak curves could be large.

e.g. for char$(k) \neq 2, g_0 = 1, d = 3$, a half of random elliptic curves E defined over k_3 in the Legendre form are weak.

A such curve with 160-bit key-length will have only strength of 107 bits under GHS attack.

Similar for $g_0 = 2, 3$.
Also in the cases of char$= 2, g_0 = 1, 2, 3$.

GHS attack considered in this research

Let q be a power of prime. $k := \mathbb{F}_q,\ K = k_d := \mathbb{F}_{q^d}$.

Let C_0/k_d be a hyperelliptic curve with $g(C_0) = 1, 2, 3$.

We assume $\exists C/k$: a curve s.t.

$$\pi/k_d : C \longrightarrow C_0$$

is a covering defined over k_d.

We consider that following curves.

$$C_0/k_d \; : \quad y^2 + g(x)y = f(x)$$

$g(x)$: monic if char$(k) = 2$, $g = 0$ if char$(k) \neq 2$, such that

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

is a degree 2 covering over k_d

Definition of a $(2, 2, \cdots, 2)$ covering

A n-tuple $(2, ..., 2)$ covering is a covering $\pi/K : C \longrightarrow \mathbb{P}^1$ s.t.

$$cov(C/\mathbb{P}^1) \simeq (\mathbb{Z}/2\mathbb{Z})^n$$

Here, $cov(C/\mathbb{P}^1) := Gal(K(C)/K(x))$.

$(2, 2, \cdots, 2)$ covering in GHS attack

Assume C_0 is a hyperelliptic curve,

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

is a $(2, 2, ..., 2)$ covering of degree 2^n

$$\begin{tikzcd}
 & & C \arrow[dll] \arrow[dl] \arrow[d] \arrow[drr] & & & C \arrow[dd, "2^n"] \\
C_0 \arrow[drr, "2"'] & {}^{\sigma}C_0 \arrow[dr, "2"] & {}^{\sigma^2}C_0 \arrow[d, "2"] & \cdots & {}^{\sigma^{d-1}}C_0 \arrow[dll, "2"] & \\
 & & \mathbb{P}^1 & & & \mathbb{P}^1
\end{tikzcd}$$

In language of function fields, the function field of C: $k_d(C)$ is the composite of $k_d({}^{\sigma^i}C_0), i = 0, ..., d-1$

$$k_d(C) = \prod_{i=0}^{d-1} k_d({}^{\sigma^i}C_0)$$

$$\begin{tikzcd}
 & & k_d(C) \arrow[dll] \arrow[dl] \arrow[d] \arrow[drr] & & \\
k_d(C_0) \arrow[drr, "2"'] & k_d({}^{\sigma}C_0) \arrow[dr, "2"] & k_d({}^{\sigma^2}C_0) \arrow[d, "2"] & \cdots & k_d({}^{\sigma^{d-1}}C_0) \arrow[dll, "2"] \\
 & & k_d(\mathbb{P}^1) & &
\end{tikzcd}
\qquad
\begin{tikzcd}
k_d(C) \arrow[d, "2^n"] \\
k(\mathbb{P}^1)
\end{tikzcd}$$

$$g_0 := g(C_0), \quad g := g(C)$$

Condition (C):

$$Res(\pi_*) : \quad J(C) \longrightarrow Res_{k_d/k}(J(C_0))$$

is an isogeny over k.

This implies $g = dg_0$, the smallest possible genus of C.

Lemma 1: Equivalent statement to the Condition (C):

$\exists H < cov(C/\mathbb{P}^1)$, a subgroup of index 2 such that the Tate module of $J(C)$ has the decomposition:

$$V_l(J(C)) = \oplus_{j=0}^{d-1} \quad V_l(J(C))^{\sigma^j H}$$

We will classify $(2, ..., 2)$ coverings of

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

satisfying the Condition (C).

Then analyze the density of curves with such coverings.

Show explicit definition equations of C_0 and C.

Approach:

Classification of representation of $G(k_d/k)$ on cov$(C/\mathbb{P}^1)$

$$G(k_d/k) =< \sigma > \ \curvearrowright \ cov(C/\mathbb{P}^1) \simeq \mathbb{F}_2^n$$
$$G(k_d/k) =< \sigma > \ \hookrightarrow \ GL_n(\mathbb{F}_2)$$

$$\begin{cases} \text{char}(k) \neq 2: & \text{Riemann-Hurwitz inequality} \\ \text{char}(k) = 2: & \begin{cases} \text{ordinary} & \begin{cases} \text{(R-H)} + \text{classification of} \\ \text{orders of ramification groups} \end{cases} \\ \text{non-ordinary} & \text{ramification theory} \end{cases} \end{cases}$$

Cases when $(2, 2, ..., 2)$ coverings exist:

$$
\left\{
\begin{array}{ll}
\text{Indecomposable} &
\left\{
\begin{array}{l}
2|d \left\{ \begin{array}{ll} \mathsf{char}(k) = 2: & (d,n) = (2,2), (4,3) \\ \mathsf{char}(k) \neq 2: & (d,n) = (2,2) \end{array} \right. \\
2 \nmid d \left\{ \begin{array}{l}
d \neq 2^n - 1 \left\{ \begin{array}{ll} \mathsf{char}(k) \neq 2: & (d,n) = (5,4) \\ \mathsf{char}(k) = 2: & \text{Not exist} \end{array} \right. \\
d = 2^n - 1 \left\{ \begin{array}{ll} \mathsf{char}(k) \neq 2: & \text{Exist} \\ \mathsf{char}(k) = 2: & \text{Exist} \end{array} \right.
\end{array} \right.
\end{array}
\right. \\
\text{Decomposable} &
\left\{
\begin{array}{ll}
\mathsf{char}(k) = 2: & g_0 = 1, d = (2^a - 1)(2^b - 1), n = a + b \\
\mathsf{char}(k) \neq 2: & g_0 = 1,\ (d,n) = (3,3)
\end{array}
\right.
\end{array}
\right.
$$

Weak curves in the char$(k) \neq 2$ cases:

d	n	hyper/nonhyper	g_0	$\#C_0$
2	2	hyper		$\Theta(q^{2g_0})$
3	2			$\Theta(q^{3g_0})$?(*)
		hyper	1	$\Theta(q^2)$
3	3	hyper	1	$\Theta(q^2)$
$2^n - 1$	≥ 3	nonhyper		$\Theta(q^{d\ell-3})$?(**)
5	4	nonhyper	1	$\Theta(q^2)$

(*) In the case $g_0 = 1$, this density is proved.
(**) $\ell \;\; s.t. \;\; g_0 + 1 = 2^{n-2}\ell$
Note: Here "?" means a conjectured density.

Weak curves in the char$(k) = 2$ case:

d	n	hyper/non	g_0	ordin/non	$\#C_0$
2	2	hyper			$\Theta(q^{2g_0})$
4	3	hyper			$\Theta(q^{2g_0+1})$
$2^n - 1$					$\Theta(q^{(n+1)(g_0+1)-3})$
	e.g. 2	hyper	1	ordin	$\Theta(q^n)$? $\Theta(q^2)$
$(2^{n_1} - 1)(2^{n_2} - 1)$ $2 \le n_1, n_2$ $(2^{n_1} - 1, 2^{n_2} - 1) = 1$	$n_1 + n_2$	nonhyper	1	ordin	$\Theta(q^{n_1+n_2-1})$?

Note: Here "?" means a conjectured density.

An important case: char$(k) \neq 2, g_0 = 1, d = 3$

Elliptic curves over extension fields are often desirable in practice for fast and low-cost implementation.

e.g. a fast and cheap way of implementation is to use an elliptic curve defined over degree 3 extension of a 64bit finite field, on a 64bit processor with single-decision-arithmetics.

In fact, we show that such a setting is dangeous.

Genus 3 hyperelliptic covering

The degree of the covering $C \longrightarrow \mathbb{P}^1(x)$ is 8.

$$\begin{aligned} E/k_3: \quad y^2 &= eg(x)(x-\alpha)(x-\alpha^q) \\ \text{here} \quad & \alpha \in k_3 \setminus k, \quad e \in k_3^\times \\ & g(x) \in k[x], \quad \deg g(x) = 1 \text{ or } 2, \end{aligned}$$

This equation has been also obtained by Theriault.

$$\#\{k_3 - \text{Isomorphic classes of } E\} = \Theta(q^2)$$

C/k can be explicitly constructed.

Genus 3 non-hyperelliptic covering

The degree of the covering $\pi : C \longrightarrow \mathbb{P}^1(x)$ is 4.

$C_0 = E/k_3$ can be separated into the following two types:

Type 1: $E:$

$$y^2 = (x-\alpha)(x-\alpha^q)(x-\beta)(x-\beta^q)$$

$$\alpha, \beta \in k_3 \setminus k, \quad \#\{\alpha, \alpha^q, \beta, \beta^q\} = 4$$

Type 2: $E:$

$$y^2 = (x-\alpha)\left(x-\alpha^{q^3}\right)(x-\alpha^q)\left(x-\alpha^{q^4}\right)$$

$$\alpha \in k_6 \setminus \{k_2 \cup k_3\}$$

The Type I curve has been also obtained by Diem.

Sufficient and necessary condition that C is hyperelliptic

(For Type II, $\beta := \alpha^{q^3}$)

$$C: \text{ hyperelliptic} \quad \Longleftrightarrow \left\{ \begin{array}{l} \exists A \in GL_2(k) \\ s.t.\ Tr(A) = 0 \\ \text{and } \beta = A \cdot \alpha \end{array} \right.$$

which reduces to the former case, hereafter we will consider only non-hyper cases.

$PGL_2(k)$-action:

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in PGL_2(k),, \alpha \in k_3 \qquad A \cdot \alpha := \frac{a\alpha + b}{c\alpha + d}$$

Type I curves:

E is k_3-isomorphic to the following Legendre canonical form.

$$E \underset{/k_3}{\simeq} y^2 = x(x-1)(x-\lambda)$$

$$\lambda = \frac{(\beta-\alpha^q)(\beta^q-\alpha)}{(\beta-\alpha)(\beta^q-\alpha^q)}$$

The action of $PGL_2(k)$ on $k_3\backslash k$ induces an action on $\{(\alpha,\beta)\}$:

$$\{(\alpha,\beta)\} \longrightarrow \{(A\cdot\alpha, A\cdot\beta)\}, \qquad \forall A \in GL_2(k)$$

Under which, E is mapped into

$$E' : y^2 = (x - A\cdot\alpha)(x - A\cdot\alpha^q)(x - A\cdot\beta)(x - A\cdot\beta^q)$$

$$\lambda' := \frac{(A\cdot\beta - A\cdot\alpha^q)(A\cdot\beta^q - A\cdot\alpha)}{(A\cdot\beta - A\cdot\alpha)(A\cdot\beta^q - A\cdot\alpha^q)}$$

$$\lambda = \lambda'$$

or the Legendre forms are invariant under this action.

Therefore, by transitivity of the action of $PGL_2(k)$ on $k_3 \backslash k$, the α in the pair (α, β) can be fixed to an $\epsilon \in k_3 \setminus k$.

Thus, we hereafter consider only the pairs $\{(\epsilon, \beta)\}$

From now we assume the Type I curves to be

$$E: \; y^2 = (x - \epsilon)(x - \epsilon^q)(x - \beta)(x - \beta^q)$$
$$\epsilon, \beta \in k_3 \setminus k, \quad \#\{\epsilon, \epsilon^q, \beta, \beta^q\} = 4$$
$$\lambda = \tfrac{\beta - \epsilon^q}{\beta - \epsilon} \cdot \tfrac{\beta^q - \epsilon}{\beta^q - \epsilon^q}$$

To count the number of isomorphic classes of Type I elliptic curves, we first count the number of λ.

$$\mu := \begin{pmatrix} \epsilon^q & -\epsilon \\ 1 & -1 \end{pmatrix} \cdot \lambda$$

Since $\lambda \neq 0, 1, \infty$, $\mu \neq \epsilon, \epsilon^q, \infty$.

Define

$$A =: \begin{pmatrix} -\mu + \epsilon + \epsilon^q & -\epsilon^{1+q} \\ 1 & -\mu \end{pmatrix}$$

and

$$B :={}^{\sigma^2}A\ {}^{\sigma}A\ A.$$

Lemma 2:

1. Given a λ, there exists a β or E is Type I iff

$$A \cdot \beta = \beta^q$$

2. The above condition is equivalent to

$$B \cdot \beta = \beta.$$

   Then one can find β from λ as solutions of a quadratic equation,hence find E which have the covering C.

Thus, it is easy to test if an elliptic curve is of Type I.

3. When such a β exists or E is of Type I,

$$B \not\equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \mod k_3^\times$$

i.e., the quadratic equation will not degenerate into a linear one.

4. Let the discriminant $D := (TrB)^2 - 4(\det B) \quad (\in k)$ then there exists such a β given an λ iff $D \in (k)^2$;

5. $$D = 0 \Longrightarrow \begin{cases} \exists C \in GL_2(k),\ C^2 \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \mod k^\times \\ \beta = C \cdot \epsilon \end{cases}$$

Density of Type I curves

Corollary 1

For the Type I E defined by having the covering C or defined by λ,

$$\#\{\lambda\} \approx \frac{1}{2}q^3.$$

Type II curves:

Type II elliptice curve E are k_3-isomorphic to

$$E \underset{/k_3}{\simeq} \; y^2 = x(x-1)(x-\lambda)$$

$$\lambda = \left(\frac{\alpha^q - \alpha^{q^3}}{\alpha^q - \alpha}\right)^{1+q^3}$$

Density of Type II curves

Lemma 3: For Type II elliptic curves defined by λ,

$$\#\{\lambda\} = \Theta(q^3)$$

Explicit construction of the covering $C \longrightarrow E$

$q = 9007199254741813$, (17 digits), q^3: 168bit
$k = \mathbb{F}_{9007199254741813}$,
$k_3 = \mathbb{F}_{9007199254741813^3} = k[x]/\langle x^3 - 2\rangle$.

Consider a Type I curve :

$$C_0/k_3 :\ y^2 = (x-\alpha)(x-\alpha^q)(x-\beta)(x-\beta^q)$$

${}^\exists \epsilon \in k_3$ s.t. $\epsilon^3 = 2,\ \alpha = \epsilon + 1,\ \beta = \alpha^2$.

$$\begin{aligned} \#(C_0(k_3)) &= 730750818665651281401256783079976841670686577776 \\ &= 2^4 * 45671926166603205087578548942498552604417911111 \end{aligned}$$

Definition equation of C

One can construct the $g = 3$ non-hyperelliptic covering C of C_0 over k as a degree 4 canonical curve :

$$
\begin{aligned}
C/k \quad : \quad & 5749228520209069X^3Y + 3918009341123426X^3Z + 4705833439190178X^2Y^2 \\
+ \quad & 1000799917193535X^2YZ + 271497561211062X^2Z^2 + 5003999585967674XY^3 \\
+ \quad & 6835218765053317XY^2Z + 787824098066752XYZ^2 + 2501999792983837XZ^3 \\
+ \quad & 271497561211062Y^4 + 1959004670561713Y^3Z + 5754599523862825Y^2Z^2 \\
+ \quad & 8192706571108627YZ^3 + 1860526658303369Z^4 = 0
\end{aligned}
$$