

# Generating Genus two Hyperelliptic Curves over Large Characteristic Finite Fields



Takakazu Satoh  
Graduate school of Mathematics  
Tokyo Institute of Technology

佐藤 孝和  
大学院数学専攻  
東京工業大学

ECC 2009, Calgary, 26 Aug

# Outline

---

- Backgrounds
  - Elliptic vs. hyperelliptic curves
  - Curve generation
  - Explicit splitting
- Our algorithm
- Implementation, numerical examples
- Security consideration
- after"math"

This part is a joint work with David Mandell Freeman.

  - primitive varieties
  - pairing friendly hyperelliptic curves

## Genus 2 Hyperelliptic Curves

---

$p$ : a large prime ( $p \geq 7$ ),  $q$ : a power of a prime

$\mathbf{F}_q$ : the finite fields with  $q$  elements

A hyperelliptic curve  $H$  of genus two defined over  $\mathbf{F}_q$ :

$$H : Y^2 = X^5 + a_4X^4 + a_3X^3 + a_2X^2 + a_1X + a_0 \quad (a_4 \sim a_0 \in \mathbf{F}_q)$$

The polynomial in the right hand side is square free.

Property :  $H$  does **not** have a natural group structure.

$J$ : the Jacobian of  $H$

- A set of unordered pairs of two points on  $H$
- An Abelian group (in fact, a 2-dim **Abelian variety**)

Elliptic curve: genus one curve, 1-dim Abelian variety.

## Elliptic vs. Genus 2

(proj.) Weierstrass model EC 11M+3S vs. genus 2 47M+4S

Non Weierstrass models:

- EC: Hisil et al., "Twisted Edwards curves revisited", Asiacrypt 2008: 8M
- genus 2: P. Gaudry, "Fast genus two arithmetic based on Theta functions", J. Math. crypt. 1(2007).

$J[2] \subset J(\mathbf{F}_q) \Rightarrow 16M+9S/1$  step of the Montgomery ladder

If group order is  $\approx 2^{160}$ :

$$\text{EC} \quad (\sqrt{p} - 1)^2 \leq \#E(\mathbf{F}_p) \leq (\sqrt{p} + 1)^2 \Rightarrow p \approx 2^{160}$$

$$\text{genus 2} \quad (\sqrt{p} - 1)^4 \leq \#J(\mathbf{F}_p) \leq (\sqrt{p} + 1)^4 \Rightarrow p \approx 2^{80}$$

$\Rightarrow$  The smaller  $p$  is, the faster field operations are.

## Curve Generation: Former Methods

---

- generate random curves until we find a good curve.

EC/ $\mathbf{F}_q$  : SEA 1~20 min for  $q \cong 2^{160}$  with a modern CPU

HEC: in theory  $P$ -time but unrealistic for crypto size

Gaudry-Schoof: details in their ECC 2008 slides

2.4GHz Operon, 8GB,  $p = 2^{127} - 1$ , ca. 4 CPU·wk/curve

(2004 2.66GHz Xeon, 2GB,  $p \approx 2^{82}$ , ca. 1 CPU·wk/curve)

prime density: around  $2^{160} \approx \frac{1}{110}$ , around  $2^{256} \approx \frac{1}{176}$ .

- Explicit order formulae for  $Y^2 = X^5 + aX$ ,  $Y^2 = X^5 + a$ :

(Furukawa, Haneda, Kawazoe, Takahashi).

The curves are very special: try many  $p$  until we find a good curve.

## Curve Generation: Our Method

---

Generate  $u, v \in \mathbf{F}_p$  randomly until  $Y^2 = X^5 + uX^3 + vX$  is suitable for cryptographic use.

- still in a special form
- not so special as binomials

Our method can compute its group order quickly **only if the order is a product of small number and a large prime.**

If not, our method aborts quickly.

It does not matter for us because we are looking for a curve for cryptographic use.

## Explicit Splitting(1)

$H : Y^2 = X^5 + uX^3 + vX$ , with  $u \in \mathbf{F}_p$  and  $v \in \mathbf{F}_p^\times$ .

- Frey, Kani: Progress in Math., **89**(1991) 153-176.
- Leprévost, Morain: J. Number Theory, **64**(1997), 165-182.

There exist  $\alpha, \beta \in \mathbf{F}_{p^4}^\times$  such that

$$X^5 + uX^3 + vX = X(X^2 - \alpha^2)(X^2 - \beta^2).$$

Choose and fix  $s \in \mathbf{F}_{p^8}^\times$  such that  $s^2 = \alpha\beta$ .

Actually,  $s \in \mathbf{F}_{p^4}^\times$  because  $s^4 = \alpha^2\beta^2 = v \in \mathbf{F}_p^\times$ .

$$\begin{aligned} X^4 + uX^2 + v &= (X^2 - \alpha^2)(X^2 - \beta^2) = (X + \alpha)(X + \beta)(X - \alpha)(X - \beta) \\ &= AB \left( (X + s)^4 + \left( \frac{B}{A} + \frac{A}{B} \right) (X + s)^2 (X - s)^2 + (X - s)^4 \right). \end{aligned}$$

where  $A := \frac{1}{2} \left( 1 + \frac{\alpha + \beta}{2s} \right)$ ,  $B := \frac{1}{2} \left( 1 - \frac{\alpha + \beta}{2s} \right)$ .

## Explicit Splitting(2)

Since  $X = \frac{1}{4s} \left( (X+s)^2 - (X-s)^2 \right)$ ,  $H$  is given by

$$Y^2 = \frac{AB}{4s} \left( (X+s)^2 - (X-s)^2 \right) \times \left( (X+s)^4 + \left( \frac{B}{A} + \frac{A}{B} \right) (X+s)^2 (X-s)^2 + (X-s)^4 \right).$$

i.e.  $\left( \frac{Y}{(X-s)^3} \right)^2 = \frac{AB}{4s} \left( \left( \frac{X+s}{X-s} \right)^2 - 1 \right) \left( \left( \frac{X+s}{X-s} \right)^4 + \left( \frac{B}{A} + \frac{A}{B} \right) \left( \frac{X+s}{X-s} \right)^2 + 1 \right)$

We have a map  $\varphi_1 : H \rightarrow E_1 : Y^2 = \delta(X-1)(X^2 - \gamma X + 1)$  defined by

$$\varphi_1(x, y) := \left( \left( \frac{x+s}{x-s} \right)^2, \frac{y}{(x-s)^3} \right)$$

where  $\delta := \frac{AB}{4s}$  and  $\gamma := -\left( \frac{B}{A} + \frac{A}{B} \right)$ .

## Explicit Splitting(3)

---

$$\varphi_1(x, y) := \left( \left( \frac{x+s}{x-s} \right)^2, \frac{y}{(x-s)^3} \right) \quad H \rightarrow E_1: Y^2 = \delta(X-1)(X^2 - \gamma X + 1)$$

$$\varphi_2(x, y) := \left( \left( \frac{x-s}{x+s} \right)^2, \frac{y}{(x+s)^3} \right) \quad H \rightarrow E_2: Y^2 = -\delta(X-1)(X^2 - \gamma X + 1)$$

The maps  $\varphi_1$  and  $\varphi_2$  are defined over  $\mathbf{F}_{p^4}$ .

They induce  $\mathbf{F}_{p^4}$  rational maps

$$\varphi_i^* : \text{Div}(E_i) \rightarrow \text{Div}(H) \quad \varphi_i^*([Q]) = \sum_{P \in \varphi_i^{-1}(\{Q\})} e_{\varphi_i}(P)[P],$$

$$\varphi_{i*} : \text{Div}(H) \rightarrow \text{Div}(E_i) \quad \varphi_{i*}([P]) = [\varphi_i(P)].$$

They again induce maps

$$\varphi_i^* : \text{Pic}^0(E_i) \rightarrow \text{Pic}^0(H) (\cong J) \quad \text{and} \quad \varphi_{i*} : J \rightarrow E_i.$$

## Explicit Splitting(4)

---

We can show

$$\begin{aligned}\varphi_{1*} \circ \varphi_1^* &= 2_{E_1}, & \varphi_{2*} \circ \varphi_1^* &= 0, \\ \varphi_{1*} \circ \varphi_2^* &= 0, & \varphi_{2*} \circ \varphi_2^* &= 2_{E_2}.\end{aligned}$$

$\text{Ker}((\varphi_{1*}, \varphi_{2*}): J \rightarrow E_1 \times E_2)$  is finite.

(Because  $(\varphi_{1*}, \varphi_{2*}) \circ (\varphi_1^* \circ \pi_1 + \varphi_2^* \circ \pi_2) = 2_{E_1 \times E_2}$ , which is finite).

Therefore  $J$  is isogenous to  $E_1 \times E_2$  over  $\mathbf{F}_{p^4}$ .

Both  $E_1$  and  $E_2$  are isomorphic to

$$E/\mathbf{F}_{p^4}: Y^2 = X^3 - \frac{(\gamma-2)(\gamma+1)}{3} \delta^2 X - \frac{(\gamma-2)^2(2\gamma+5)}{27} \delta^3.$$

over  $\mathbf{F}_{p^4}$ , i.e.,  $J$  is isogenous to  $E^2$ .

## Why can we Have an Efficient Algorithm?

If  $H$  is  $Y^2 = X^5 + uX^3 + vX/\mathbf{F}_p$ , then its Jacobian  $J$  is  $\mathbf{F}_{p^4}$ -isogenous to  $E \times E$  with some EC  $E/\mathbf{F}_{p^2}$ .

Tool:  $Z_A(T, \mathbf{F}_q) \in \mathbf{Z}[T]$ : 1-dim part of  $\zeta$  ft. of an A.V.  $A/\mathbf{F}_q$

- (1) Compute  $Z_E(T, \mathbf{F}_{p^2})$  by SEA, then compute  $Z_E(T, \mathbf{F}_{p^4})$
- (2) If  $A$  is  $\mathbf{F}_q$ -isog. to  $U \times V$ ,  $Z_A(T, \mathbf{F}_q) = Z_U(T, \mathbf{F}_q)Z_V(T, \mathbf{F}_q)$   
 $Z_J(T, \mathbf{F}_{p^4}) := Z_E(T, \mathbf{F}_{p^4})^2$
- (3)  $\#A(\mathbf{F}_q) = Z_A(1, \mathbf{F}_q)$ .  $Z_A(T, \mathbf{F}_{q^n}) = \prod (T - \alpha_i^n)$  if  $Z_A(T, \mathbf{F}_q) = \prod (T - \alpha_i)$   
 Obtain at most 26 candidates of  $Z_J(T, \mathbf{F}_p)$  and  $\#J(\mathbf{F}_p)$
- (4) If an order is not a product of small number and a large prime, it is never suitable for cryptographic use.
- (5) Take random points to determine the correct order.

## Implementation (1)

---

Our curves are still in the special form.

Can we find crypto oriented curve of the form?

For 10 primes  $p$  ( $\approx 2^{86}$ ), random 200 pairs of  $(u, v)$  for each  $p$  are generated.

Among 2000 curves, the order of 13 curves is  $2 \times \text{prime}$ .

Example:  $p = 97254360139138202069000909$

$$Y^2 = X^5 + 93589879629357849667104247X^3 + 2243510914087562678935813X$$

order:  $2 \times 172$  bit prime

$2 \times 4729205283037531066627852907078079919137325850534317$

3~20 min/curve: no assembly code, no Atkin primes used.

almost all time is spent for EC point counting.

## SEA for non Prime Fields

---

In most references:  $\tilde{O}((\log q)^{2\mu+2})$  bit ops., typically.

$\mu$ : exponent of multiplication (naive: 2, Karatsuba: 1.59)

Use BSGS for eigenvalue search.

The dominant step is computation of  $a(t)^q \bmod b(t)$  for  $a(t)$ ,  $b(t) \in \mathbf{F}_q[T]$ ,  $\deg b = O(\log q)$ .

- Shift-and-multiply:  $\tilde{O}((\log q)^{2\mu+1})$  bit ops.
- Modular polynomial composition with  $p$ -th power map:

Compensate the action of  $p$ -th power on  $\mathbf{F}_q$ .

$$\Rightarrow \tilde{O}((\log \log q)(\log q)^{3/2+\mu} + (\log p)(\log q)^{2\mu}).$$

F. Vercautern: preprint(2000) for  $p=2$ .

In my program(only Elkies primes are used) overall computation runs 20% faster (even only the case  $q=p^2$  is used).

## Implementation(2)

---

$J[2] \subset J(\mathbf{F}_p)$ : fast Montgomery ladder due to Gaudry

$p = 2^{87} - 67$ : Among 400 random pairs  $(\alpha, \beta) \in \mathbf{F}_p^2$  such that  $\alpha \neq \pm\beta$  and that  $\alpha\beta$  is not square in  $\mathbf{F}_p$ , two pairs attained that the order of Jacobian of

$$Y^2 = X(X^2 - \alpha^2)(X^2 - \beta^2)$$

is  $16 \times \text{prime}$  (best possible since  $J[2] \subset J(\mathbf{F}_p)$ ).

$$\begin{aligned} \text{Example: } Y^2 = X^5 &+ 143809213492221778144040547X^3 \\ &+ 131138969142842659104031301X \end{aligned}$$

Order:

$$16 \times 1496577676626844588240571984812022411283373002097969$$

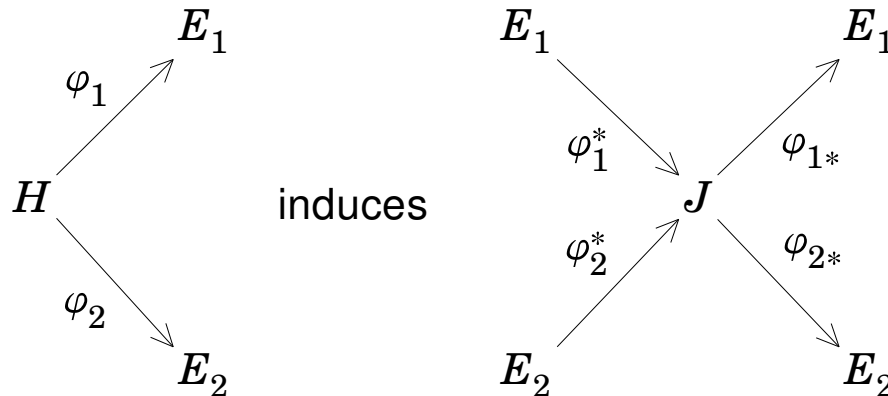
## Security Considerations(1)

---

Our curve is still in the special form  $Y^2 = X^5 + uX^3 + vX$

Are they weaker than generic genus two curves?

It the special form which enables us DLP hardness comparison



DLP on  $J(\mathbf{F}_q) = \text{ECDLP on } E_i$  over some extension.

Still, it might happen that both DLP are easy.

## Security Considerations(2)

---

Large automorphism group: probably effect is limited

$G$ : any group acting on  $J(\mathbf{F}_p)$  from left,

$N := \#J(\mathbf{F}_p)$ ,  $M := \#(G \setminus J(\mathbf{F}_p))$ ,

$T$ : time to proceed one step on  $J(\mathbf{F}_p)$ .

**Assumption:** time to find a  $G$ -orbit representative is greater than  $t \times (\text{avg number of points in the orbits}) = tM/N > 0$ .

avg. steps of random walk on  $J(\mathbf{F}_p)$ :  $c\sqrt{N}$ ,  $c > 0$ .

avg. steps of random walk on  $G \setminus J(\mathbf{F}_p)$ :  $c\sqrt{M}$

$$\frac{c\sqrt{M}\left(t\frac{N}{M} + T\right)}{cT\sqrt{N}} \geq \sqrt{\frac{M}{N}} + \frac{t}{T}\sqrt{\frac{N}{M}} \geq 2\sqrt{\frac{t}{T}}$$

In reality, we can perhaps assume that  $t/T \geq 2^{-10}$ .

## Security Consideration(3)

---

Gaudry's variant of index calculus:

DLP on  $J(\mathbf{F}_p)$  is reduced to DLP on a subgp. of  $E(\mathbf{F}_{p^4})$  or  $E(\mathbf{F}_{p^2})$ .

- running time of index calculus type algorithm is dominated not by the base point order but by the whole group size
- a square root algorithm is faster

## After'math'

37:20 1:20

$$H : Y^2 = X^5 + uX^3 + vX, \quad \varphi_1 : H \rightarrow E_1, \quad v \in \mathbf{F}_p^2 - \mathbf{F}_p^4.$$

Let  $E/\mathbf{F}_p$  be the quadratic twist of  $E_1$ .

Assume: (\*)  $E$  is ordinary, and  $\text{End}(E) \otimes_{\mathbf{Z}} \mathbf{Q} \neq \mathbf{Q}(i)$ .

$$\Rightarrow Z_J(T, \mathbf{F}_p) = Z_E(iT, \mathbf{F}_p)Z_E(-iT, \mathbf{F}_p).$$

- No search for the correct zeta function
- In terms of the primitive variety,  $J = P_4(E)$ .  
C.Diem: Thesis,  $P_4(E)$  is simple under (\*).
- Application to pairing friendly curve generation.
- Possible application to point compression??, more security consideration?? (the Weil restriction attack????)

There are at least three ways to prove the Zeta relation.

## Application to Pairing Friendly Curves

---

Joint work with David Mandell Freeman is in progress.

Former genus 2 records:

absolutely simple:  $q=4$ , binomials  $q=3$

The relation

$$Z_J(T, \mathbf{F}_p) = Z_E(iT, \mathbf{F}_p)Z_E(-iT, \mathbf{F}_p)$$

allows us to construct pairing friendly hyperelliptic curves of genus two from **non-pairing friendly** elliptic curves.

Similar construction with  $P_6$  also applies to  $Y^2 = X^6 + aX^3 + b$ .

Good: curves of  $q \cong 2.22$  for embedding degree 27.

Bad: An analogue to the MNT curves (i.e. embedding deg = 3, 4, 6):  $\liminf q \geq 2$ .

## The Weil Restriction

---

$K$ : perfect (for simplicity),  $L$ : finite ext. field,  $A$ :  $L$ -scheme

$\exists A_{L/K}$ :  $K$ -scheme s.t.  $A_{L/K}(B) = A(L \otimes_K B)$  for  $K$ -algebra  $B$ .

For an Abelian scheme  $A$ :  $V_l(A_{L/K}) = \text{Ind}_{G_L}^{G_K} V_l(A)$

( $l$ : prime,  $\neq \text{char}(K)$ ,  $V_l(A) := \mathbf{Q}_l \otimes_{\mathbf{Z}_l} T_l(A)$ ,  $G_L := \text{Gal}(\bar{K}/L)$  etc.)

Example: Assume  $L = K(\omega)$ ,  $[L:K] = n$  and  $A$  is an affine variety defined by  $F(X_1, \dots, X_m) = 0$  with  $F \in L[X_1, \dots, X_m]$ .

$$F \left( \sum_{t=0}^{n-1} X_{1,t} \omega^t, \dots, \sum_{t=0}^{n-1} X_{m,t} \omega^t \right) = \sum_{t=0}^{n-1} f_t(X_{1,0}, \dots, X_{1,n-1}, \dots, X_{m,n-1}) \omega^t$$

where  $f_t \in K[X_{1,0}, \dots, X_{m,n-1}]$ .

Then  $A_{L/K}$  is the common zero set of  $f_1, \dots, f_{n-1}$ .

## Primitive Varieties(1)

Ref: Rubin, Silverberg: J. Crypto, **22**(2009), 330-374.

$L/K$ : cyclic, degree  $n$ ,  $A$ : Abelian variety/ $K$ .

The group ring  $\mathbf{Q}[G_K/G_L] = \mathbf{Q}[\text{Gal}(L/K)] \cong \mathbf{Q}[\mathbf{Z}/n\mathbf{Z}]$  decomposes as  $\bigoplus_{d|n} M_d$ , where  $M_d$  corresponds to the irreducible representation over  $\mathbf{Q}$  whose kernel is the unique subgroup of  $\text{Gal}(L/K)$  with index  $d$ .

$$\Rightarrow V_l(A_{L/K}) = \bigoplus_{d|n} M_d \otimes_{\mathbf{Q}} V_l(A)$$

$$\exists \text{ A.V. } P_d(A)/K \text{ s.t. } V_l(P_d(A)) = M_d \otimes_{\mathbf{Q}} V_l(A), \quad A_{L/K} \sim \bigoplus_{d|n} P_d(A).$$

This is an A.V. analogue of  $T^n - 1 = \prod_{d|n} \Phi_d(T)$

Example:  $P_1(A) = A$ ,  $P_2(A)$  is the quadratic twist of  $A$ .

If  $d$  is a prime,  $P_d(A)$  is the trace zero variety of  $A/L$ .

## Primitive Varieties(2)

---

We use the Weierstrass model in the affine  $X$ - $Z$  plane:

$$E : F(X, Z) := Z - (X^3 + a_2 X^2 Z + a_4 X Z^2 + a_6 Z^3) = 0.$$

- $E[l^n]$  is contained in a single affine piece for  $l > 2$ .
- The identity elt. of the Weil restriction is non-singular.

Let  $d := 2^n$

If  $\mathbf{F}_{pd} = \mathbf{F}_p(\omega)$  with  $\omega^d \in \mathbf{F}_p$ , then  $P_d(E)$  is defined by the coefficients of odd powers of  $\omega$  in

$$F(X_1\omega + X_3\omega^3 + \cdots + X_{d-1}\omega^{d-1}, Z_1\omega + Z_3\omega^3 + \cdots + Z_{d-1}\omega^{d-1})$$

A similar construction applies to the case  $d = 3 \cdot 2^n$  (in particular  $d = 6$ ).

## Explicit Isogeny

$$H : Y^2 = X^5 + uX^3 + vX, \quad E/\mathbf{F}_p : Y^2 = \delta\omega^{-2}(X-1)(X^2 - \gamma X + 1),$$

$$\varphi : H \rightarrow E, \quad \varphi(x, y) := \left( \left( \frac{x+s}{x-s} \right)^2, \frac{y/\omega}{(x-s)^3} \right), \quad s = v^{1/4}$$

On the  $X$ - $Z$  plane of  $E$ , it looks

$$\varphi(x, y) = \left( \frac{\omega(x^3 + sx^2 - s^2x - s^3)}{y}, \frac{\omega(x-s)^3}{y} \right).$$

The following map sends  $H$  to  $P_4(E)$ , which induces an isogeny  $P_4(E) \rightarrow J$ , i.e.  $Z_E(-iT, \mathbf{F}_p)Z_E(iT, \mathbf{F}_p) = Z_J(T, \mathbf{F}_p)$ .

$$(x, y) \rightarrow \left( \begin{array}{ll} X_1 := \frac{x^3 - s^2x}{y} & X_3 := r \frac{x^2 - s^2}{y} \\ Z_1 := \frac{x^3 + 3s^2x}{y} & Z_3 := -r \frac{3x^2 + s^2}{y} \end{array} \right) \quad (r := s\omega^{-2} \in \mathbf{F}_p^\times)$$

## Conclusion

---

- We considered HEC  $Y^2 = X^5 + uX^3 + vX$ .
- an algorithm that gives an order (and its large prime factor) if its Jacobian is suitable for HEC cryptography.
  - construction of a verifiably random curve in terms of  $u$  and  $v$ .
- pairing friendly hyperelliptic construction

Open problem:

- more security consideration

Thank you for your attention!