Constant-time encoding points on elliptic curve of different forms over finite fields

Tammam Alasha
work with
Serge Vlăduţ , Pascal Véron

C2 2012

October 9, 2012

Institut de Mathématiques de Luminy
IML

Elliptic curve cryptography

1. $\mathbb{F}_q$ finite field of characteristic > 3
2. Recall that an elliptic curve over $\mathbb{F}_q$ is the set of points $(x, y) \in \mathbb{F}_q^2$ such that :

   $$E_{W,a,b} : y^2 = x^3 + ax + b$$

   (with $a, b \in \mathbb{F}_q$ fixed parameters), together with a point at infinity $\mathcal{O}$.
3. This set of points forms an abelian group where the Discrete Logarithm Problem and Diffie-Hellman-type problems are believed to be hard.

Overview on elliptic curves formes

1. Short Weierstrass: $y^2 = x^3 + ax + b$
2. Montgomery: $by^2 = x^3 + ax^2 + x$
3. Legendre: $y^2 = x(x-1)(x-\lambda)$
4. Doche-Icart-Kohel: $y^2 = x^3 + 3a(x+1)^2$
5. Hessian: $x^3 + y^3 + 1 = 3dxy$
6. Jacobi intersection: $x^2 + y^2 = 1$, $ax^2 + z^2 = 1$
7. Jacobi quartic: $y^2 = x^4 + 2bx^2 + 1$
8. Huff: $ax(y^2-1) = by(x^2-1)$
9. Edwards: $x^2 + y^2 = 1 + dx^2y^2$

MOTIVATION

1. The classical problem of deterministic encoding into algebraic, in particular, elliptic curves over finite fields.
2. Numerous cryptographic protocols or schemes based on elliptic curve need efficient hashing of finite field elements into points on a given elliptic curve (IBE,HIBE,SPAKE,PAK,e-passports)
3. The recent study of models of elliptic curves suitable for cryptographic applications.

HASHING INTO ELLIPTIC CURVES

1. Hashing into elliptic curves in deterministic polynomial time is much harder than hashing into finite field
2. It requires a deterministic function from the base field to the curve
3. The classical point generation algorithm is a probabilistic

CLASSICAL TECHNIQUES

Try and Increment

Input: $E_{W,a,b}$, u an integer. We can take $u = H(m)$
Output: Q, a point of $E_{a,b}(\mathbb{F}_q)$.

1. For $i = 0$ to $k - 1$
   1.1 Set $x = u + i$
   1.2 If $x^3 + ax + b$ a quadratic residue in $\mathbb{F}_q$ then return $Q = (x, (x^3 + ax + b)^{1/2})$
2. end for
3. Return $\perp$

The running time depends on u. This leads to partition attacks.

DETERMINISTIC HASHING INTO ELLIPTIC CURVES

Supersingular Elliptic Curve

Definition: a curve $E_{0,b}$:$X^3 + b = Y^2 \bmod p$ with $p = 2 \bmod 3$ has $p + 1$ points and is supersingular.

1. The function $u \longmapsto ((u^2 - b)^{(1/3)}, u)$ is bijection from $\mathbb{F}_q$ to $E_{0,b}$
2. Because of the MOV attacks, large p should be used.

DETERMINISTIC HASHING INTO ELLIPTIC CURVES

Hashing into Ordinary Curves

1. First deterministic point construction algorithm on ordinary elliptic curves due to Shallue and Woestijne (ANTS 2006).
2. Later generalized and simplified by Ulas (2007).
3. In 2009 Thomas icart proposed a deterministic algorithm for hashing into the Weierstrass form of an elliptic curve over finite field.

WHAT WE DO WANT ?

Properties of f

1. It only requires the elliptic curves parameters
2. f requires a constant number of finite field operations
3. f^{-1} can be computed in polynomial time

Fact

1. Over field such that $p = 2 \bmod 3$, the map $x \longmapsto x^3$ is a bijection.
2. In particular: $x^{\frac{1}{3}} = x^{\frac{2p-1}{3}}$
3. This operation can be computed in a constant numbers of operations for a constant p

Icart Function (CRYPTO 2009)

$$E_{W,a,b} : y^2 = x^3 + ax + b \bmod p \text{ with } p = 2 \bmod 3$$

$$\begin{aligned} f_{a,b} : \mathbb{F}_q &\longmapsto E_{W,a,b} \\ u &\longmapsto (x, y) \end{aligned}$$

$$\begin{aligned} x &= (v^2 - b - \frac{u^6}{27})^{\frac{1}{3}} + \frac{u^2}{3} \\ y &= ux + v \\ v &= \frac{3a - u^4}{6u} \end{aligned}$$

Properties of Icart function

Let $P = (x, y)$ be a point on the curve $E_{W,a,b}$.

Lemma

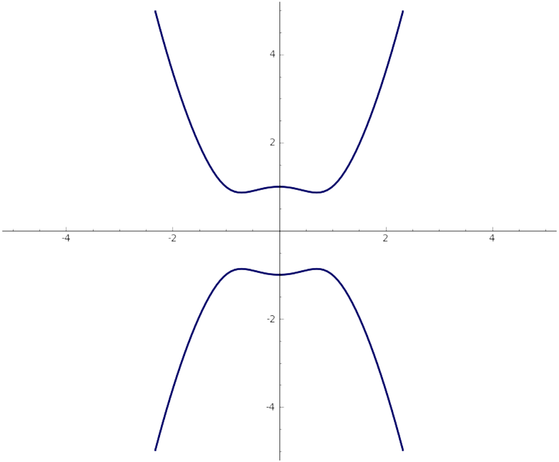
The soulutions u_s of $f_{a,b}(u_s) = P$ are the solutions of the equation:

$$u^4 - 6u^2x + 6uy - 3a = 0$$

This implies that

1. $f_{a,b}^{-1}(P)$ is computable in polynomial time.
2. $|f_{a,b}^{-1}(P)| \leq 4$, for all $P \in E_{a,b}$
3. $|im(f_{a,b})| \; > p/4$

JACOBI QUARTIC CURVE OVER ℝ



$$y^2 = x^4 + 2bx^2 + 1$$

OVERVIEW ON JACOBI QURATIC MODELS

Jacobi Quratic ellptic forms over a non binary field $\mathbb{F}_q$, $a, b, c \in \mathbb{F}_q$

1. Jacobi 1829 : $y^2 = (1 - x^2)(1 - a^2x^2)$, $a \neq 0, \pm 1$
2. Chudnovsky 1986 : $y^2 = x^4 + 2bx^2 + 1$, $b \neq \pm 1$
3. Billet 2003 : $y^2 = ax^4 + 2bx^2 + 1$, $(b^2 - a)^2 \neq 0$
4. Wang 2010: $y^2 = ax^4 + 2bc^2x^2 + c^4$, $a \neq b^2, c^2, c^4 \in \mathbb{F}_q$

New encoding for Jacobi Quratic

Let $E_{J,a,b}/\mathbb{F}_q$ be a twisted Jacobi quartic curve over a finite field, defined by the equation

$$y^2 = ax^4 + 2bx^2 + 1.$$

We consider the map

$$\begin{aligned} f_J : \mathbb{F}_q &\longrightarrow E_{J,a,b}(\mathbb{F}_q) \\ u &\longmapsto \left(\frac{2(b-s)}{us+v}, \frac{s^2-2bs+a}{a-s^2} \right) \end{aligned}$$

where (v, s) is given by the output of algorithm 1.

Algorithm 1

Input : a, b and $u \in \mathbb{F}_q$. We can take $u = H(m)$

Output : A point $Q = (x, y)$ on $E_{J,a,b}(\mathbb{F}_q)$

1. If $\{u = 0\}$ then return $\mathcal{O}$
2. $m := \frac{u^2 - 2b}{6}$
3. $v := \frac{3m^2 - a}{u}$
4. $s := \left(m^3 - v^2 + 2ab\right)^{1/3} - m$
5. If $s^2 = \{a\}$ then return $\mathcal{O}$
6. $y := \frac{s^2 - 2bs + a}{a - s^2}$
7. If $s = \{-v/u\}$ then return $\mathcal{O}$
8. $x := \frac{2(b-s)}{us+v}$
9. Return (x, y)

WHY IT WORKS

1. $E_{J,a,b} : y^2 = ax^4 + 2bx^2 + 1$
2. We suppose $x^2 = X$,$y = Y$, this yields the conic

$$\mathcal{C} : Y^2 = aX^2 + 2bX + 1$$

3. By inspection $(X, Y) = (0, 1)$ lies on the $\mathcal{C}$
4. We can use this point to parametrize all rational points on the conic $\mathcal{C}$

$$(X, Y) = (\frac{2(b-s)}{s^2-a}, -\frac{s^2-2bs+a}{s^2-a})$$

5. We get $x^2 = \dfrac{2(b-s)}{s^2-a}$, $y = -\dfrac{s^2-2bs+a}{s^2-a}$

Why it works

1. Then x will be rational provided that
$$\mathcal{E}_{\mathcal{W}} : t^2 = 2(b-s)(s^2-a)$$
2. Then we can use Icart method for $\mathcal{E}_{\mathcal{W}}$
3. $(s,t) = \left(\left(m^3 - v^2 + 2ab\right)^{1/3} - m, us + v\right)$ where
$$m = \frac{u^2 - 2b}{6}$$
$$v = \frac{3m^2 - a}{u}$$
4. We get $x = \dfrac{2(b-s)}{us+v}$

Algorithm 1.1

Input : a, b and $u \in \mathbb{F}_q$. We can take $u = H(m)$
Output : A point $Q = (x, y)$ on $E_{J,a,b}(\mathbb{F}_q)$

1. If $\{u = 0\}$ then return $\mathcal{O}$
2. $m := \frac{u^2-2b}{6}$
3. $v := \frac{3m^2-a}{u}$
4. $s := \left(m^3 - v^2 + 2ab\right)^{1/3} - m$
5. If $s^2 = \{a\}$ or $s = -v/u$ then then return $\mathcal{O}$
6. $\delta := \frac{1}{(a-s^2)(us+v)}$
7. $y := (s^2 - 2bs + a)(us + v)\delta$
8. $x := 2(b - s)(a - s^2)\delta$
9. Return (x, y)

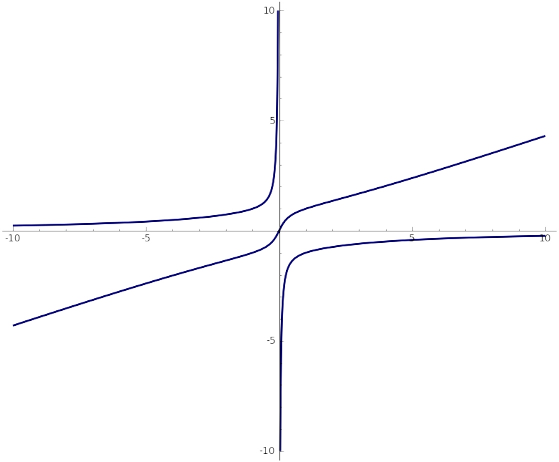
Algorithm 1.1.1

Input : a, b and $u \in \mathbb{F}_q$. We can take $u = H(m)$
Output : A point $Q = (x, y)$ on $E_{J,a,b}(\mathbb{F}_q)$

1. If $\{u = 0\}$ then return $\mathcal{O}$
2. $m := -2u^2 + b$
3. $v := m^2 + 3a$
4. $s := \left(u(-8u^2m^3 - 3v^2 - 216abu^2)\right)^{1/3} + 2um$
5. If $s^2 = \{36au^2\}$ or $s = -v/2u$ then return $\mathcal{O}$
6. $\delta := \dfrac{1}{(2us + v)(36au^2 - s^2)}$
7. $y := (s^2 - 12bus + 36au^2)(2us + v)\delta$
8. $x := 2(s - 6ub)(36au^2 - s^2)\delta$
9. Return (x, y)

(16 M, 1 I)

Huff Elliptic curve over $\mathbb{R}$



$$ax(y^2-1) = by(x^2-1)$$

OVERVIEW ON HUFF'S MODELS

Huff ellptic forms over a non binary field $\mathbb{F}_q, a, b, c \in \mathbb{F}_q$

1. Huff 1948 : $ax(y^2-1) = by(x^2-1), a^2-b^2 \neq 0$
2. M. Joye 2010 : $ax(y^2-c) = by(x^2-c), abc(a^2-b^2) \neq 0$
3. Feng 2011: $x(ay^2-1) = y(bx^2-1), ab(a^2-b^2) \neq 0$

NEW ENCODING FOR HUFF CURVE

Let $E_{H,a,b}/\mathbb{F}_q$ be a Huff curve over a finite field, defined by the equation

$$x(ay^2 - 1) = y(bx^2 - 1)$$

We consider the map

$$\begin{aligned} f_H : \mathbb{F}_q &\longrightarrow E_{H,a,b}(\mathbb{F}_q) \\ u &\longmapsto \left(\frac{12us + v}{2b(12au - s)}, \frac{2(12au - 24ub + s)}{12us + v} \right) \end{aligned}$$

where (v, s) is given by the output of algorithm 2.

Algorithm 2

Input : a, b and $u \in \mathbb{F}_q$. We can take $u = H(m)$

Output : A point $Q = (x, y)$ on $E_{H,a,b}(\mathbb{F}_q)$

1. $m := 72u^2 + a - 2b$
2. $v := m^2/3 + a^2$
3. $s := \left(64u^3m^3 - 6u(-576u^2a^2b + 288u^2a^3 - v^2)\right)^{1/3} - 4um$
4. If $s = \{12au\}$ then return $\mathcal{O}$
5. $x := \frac{12us+v}{2b(12au-s)}$
6. If $s = \{\pm - v/12u\}$ then return $\mathcal{O}$
7. $y := \frac{2(12au-24ub+s)}{12us+v}$
8. Return (x, y)

SUMMARY

1. Hashing and encoding to elliptic curves are problems worth looking into.
2. Our method enables to deterministically generate points into different forms of elliptic curves.
3. In the future work we plan to investigate the images of these encodings.
4. We can use our method for encoding points on hyperelliptic curves(under work)
5. Develop some new encodings into elliptic curves using geometric setting different from the rationality of conics.

Thank you for your attention!

Questions