On Generalized Huff's curves

Djiby SOW: Université de Cheikh Anta Diop de Dakar, Sénégal

Talk: Lens Jun 16-2011

joint paper with A. A. Ciss

Outline

Why new models of elliptic curves for cryptography

Classical model in Weirstrass form: $H(x,y) = y^2 + yh(x) - f(x) = 0$ with $h(x) = a_1x + a_3$ and $f(x) = x^3 + a_2x^2 + a_4x + a_6$
Problems: Not efficient, many attacks based on the curve agiants the cryptographic algorithms or protocols;

Basic notions on Elliptic curves cryptography

NB: In this talk, all fields are finite

Definition

A projective curve defined over a field K which is nonsingular and irreducible over the algebraic closure of $\overline{K}$, with geometric genus 1 and one distinguished K-rational point is called an elliptic curve over K.

Let us recall some elemantary definitions:

A projective curve $\mathcal{C}$ over K of dimension 1, admits a affine part wich can be represent as a polynomial $H(x, y)$ over $K[x, y]$ and then, the affine part of the curve become $H(x, y) = 0$.

(1) **smooth**: The curve $\mathcal{C}$ is nonsigular or smooth means that the system:

(1) $H(x, y) = 0$, (2) $\frac{dH(x,y)}{dx} = 0$ (3) $\frac{dH(x,y)}{dy} = 0$ has no solutions in $\overline{K}$.

(2) **Variety**: the curve $\mathcal{C}$ is irreducile means that the bivariete polynomial $H(x, y)$ is irreducible in $\overline{K}$; in this case the irreducible curve is called a variety.

(3) **Genus** Let $\mathcal{C}$ be a the projective smooth variety over a field K, with affine model given by the form:

$$H(x,y) = y^2 + yh(x) - f(x) = 0$$

where f, h are polynomes in $K[x]$, f is monic and $\deg(h) \leq \lfloor(\deg(f) - 1)/2\rfloor$, (where $\lfloor . \rfloor$ denote a floor function for some integer).
Note that if $\text{degree}(f) = 2g + 1$ or $\text{degree}(f) = 2g + 2$, then $\text{degree}(h) \leq g$.
The integer g is unique and is an invariant of the curve C [given by *Riemann-Roch theorem* in the general case] and is called the Genus of curve.
(for more detail of Riemann-Roch theorem see [page 66] of "Handbook of Hyperellitics" of Cohen and *al.*, or [page 37] of "Arithmetic of elliptic curves" of Silverman, and the given references on these books)
For elliptic curve, $h(x) = a_1x + a_3$ and $f(x) = x^3 + a_2x^2 + a_4x + a_6$ and thus the genus is $g = 1$.

(4) **Rational** The set of K-rational points of the elliptic curve $\mathcal{C}$ is defined by the set of points:

$$\mathcal{C}(K) = \{(x, y) \in K \times K, \ /H(x, y) = 0\} \cup S_\infty$$

where S_∞ is the set of infinite points.

Applications in cryptography (1)

$\Longrightarrow$ Elliptic curve cryptographic schemes: introduced by in 1985 by **Neal Koblitz** and **Victor Miller**.
$\Longrightarrow$ These schemes are the elliptic curve analogues of schemes based on the discrete logarithm problem where the underlying group is a cyclique subgroup of the group of points on an elliptic curve defined over a finite field.
$\Longrightarrow$ The security of all elliptic curve schemes and protocls s is based on the apparent intractability of the elliptic curve discrete logarithm problem (ECDLP).

Discret Logarithm problem

Let $\mathbb{G}$ be a a finite cycle group with a prime order p, g a generator of $\mathbb{G}$; select randomly $h \in \mathbb{G}$ and find x such that: $g^x = h$.
An algorithm $\mathcal{R}$ is said to $(\tau_{\mathcal{R}}, \varepsilon_{\mathcal{R}})$-solve the DLP problem, if in at most $\tau_{\mathcal{R}}$ operations, $Pr\{h \leftarrow \mathbb{G}, x \leftarrow \mathcal{R}(\mathbb{G}, g, h), g^x = h\} \geq \varepsilon_{\mathcal{R}}$, where the probability is taken over the distribution of (p, h) and over $\mathcal{R}$'s random tapes.

Applications in cryptography (2)

$\Longrightarrow$ **Computational Diffe Hellmann Problem** Let $\mathbb{G}$ be a a finite cycle group with a prime order p, g a generator of $\mathbb{G}$; select randomly $g^a, g^b \in \mathbb{G}$ and find g^{ab}.

An algorithm $\mathcal{R}$ is said to $(\tau_{\mathcal{R}}, \varepsilon_{\mathcal{R}})$-solve the CDH problem, if in at most $\tau_{\mathcal{R}}$ operations, $Pr\{g^a, g^b \leftarrow \mathbb{G}, g^{ab} \leftarrow \mathcal{R}(\mathbb{G}, g, g^a, g^b)\} \geq \varepsilon_{\mathcal{R}}$, where the probability is taken over the distribution of (p, g^a, g^b) and over $\mathcal{R}$'s random tapes.

Why one want to use elliptic curves in cryptography?

$\Longrightarrow$ There is no subexponential-time algorithm known for the ECDLP.

$\Longrightarrow$ Smaller parameters can be selected for elliptic curve schemes than for ordinary discrete logarithm schemes or for RSA, and achieve the same level of security.

$\Longrightarrow$ Smaller parameters can potentially result in significant performance benefits, especially for higher levels of security.

$\Longrightarrow$ many tools for cryptography and cryptanalysis can done via pairings on elliptic curves: by examples we have the following:

Applications in cryptography (3)

Elliptic curves have been used:

1. in integer factoring algorithms,
2. in primality proving algorithms,
3. for Diffe Hellmann Key exchange and key agreement protocol;
4. for designing public-key cryptosystems: encryption and signatures (for example El Gamal cryptosystem) ,
5. for randomness extraction to design cryptographically secure pseudorandom numbers generators
6. for designing cryptography's tools such as cryptanalyses technics or protocols via pairings on elliptic curves (Weil and Tate Pairing Attacks,.....).

Group law on elliptic curves

- The set of K-rational points on the Weirstrass model of an elliptic curve $\mathcal{C}$ by means of the **"chord-and-tangent process"** turns $\mathcal{C}(K)$ into an abelian group with an infinite point P_∞ as the neutral element. Reamark that, with different model, one can have an abelian group for elliptic curve without "chord-and-tangent process".
- Elliptic curve arithmetic
  - Addition formulas:
    - **Complexity**: the numbers of operations when adding two points: mutiplications and additions in the field;
    - **Unified**: addition law is unified if it can be used to double a point (and two add two distincts points),
    - **Completeness**: addition law in a subgroup is complete if it is always possible to add two arbitrary points in this subgroup.
  - Scalar multiplication: multiplication by a constant
  - The coordinate systems: affine coordonates, projective coordonates, Jacobian coordonates, Chudnovsky coordinates, mixed Jacobian-Chudnovsky coordinates, mixed Chudnovsky-affine coordinates, Inverted edwards coordonates,..

It is known that Elliptic curves can be represented in different forms. This different forms induces different arithmetic properties, to obtain faster scalar multiplications, various forms of elliptic curves have been extensively studied in the last two decades.

Some ellptic forms over a non binary field

1. There are many ways to represent an elliptic curve such as
   - Short Weierstrass: $y^2 = x^3 + ax + b$
   - Twisted Edwards: $ax^2 + y^2 = c^2[1 + dx^2y^2]$
   - Doche-Icart-Kohel: $y^2 = x^3 + 3a(x + 1)^2$
   - Jacobi intersection: $x^2 + y^2 = 1, ax^2 + z^2 = 1$
   - Jacobi quartic: $y^2 = x^4 + 2ax^2 + 1$
   - Legendre: $y^2 = x(x - 1)(x - \lambda)$
   - Montgomery: $by^2 = x^3 + ax^2 + x$
   - Hessian: $x^3 + y^3 + 1 = 3dxy$
2. Note that some of these curves have singular points on the projective closures but they have all, a geometric genus equal to 1.

Overview on Huff's models

Recently, Joye, Tibouchi and Vergnaud revisits for finite fields, a model for elliptic curves over $\mathbb{Q}$ introduced by Huff in 1948 in order to study a diophantine problem. Now, the list of Huff form elliptic curves are the following.

1) Huff in 1948:: A field K, $charc(K) \neq 2$, Curve: $ax(y^2-1) = by(x^2-1)$ with $a^2 - b^2 \neq 0$, with $a, b, \in K$
2) Joye, Tibouchi and Vergnaud in 2010: A field K, $charc(K) \neq 2$, Curve: $ax(y^2 - d) = by(x^2 - d)$ with $abd(a^2 - b^2) \neq 0$, with $a, b, d \in K$
3) Wu and Feng in 2011: A field K, $charc(K) \neq 2$, Curve: $x(ay^2 - 1) = y(bx^2 - 1)$ with $ab(a - b) \neq 0$, with $a, b, \in K$
4) Ciss and Sow in 2011 (presented here): A field K, $charc(K) \neq 2$, Curve: $ax(y^2 - c) = by(x^2 - c)$ with $abcd(a^2c - b^2d) \neq 0$, with $a, b, c, d \in K$
5) Joye, Tibouchi and Vergnaud 2010: A field K, $charc(K) = 2$, Curve: $ax(y^2 + y + 1) = by(x^2 + x + 1)$ with $abcd(a^2c - b^2d) \neq 0$.
6) Devigne and Joye 2011: A field K, $charc(K) = 2$, Curve: $ax(y^2 + fy + 1) = by(x^2 + fx + 1)$ with $abf(a - b) \neq 0$.

Our contributions

The main contribution of this paper is to prove that:
first: the new generalized Huff curves contains more elliptic curves than the previous Huff curves

Second: the new generalized Huff curves have all the good properties for arithmetics than the previous Huff curves

Third The technic for parrings known for the particular Huff curves studied by Joye, Tibouchi and Vergnaud in 2010 and by Wu and Feng in 2011, can be generalized this new Huff curves.(NOT GIVEN IN THIS TALK)

Basic properties for the Generalized Huff curves

Affine smooth variety

Proposition: variety

Let K be a field with $charc(K) \neq 2$ and a, b, c, d be in K. Define the Multivariate polynomial $H(x, y) = ax(y^2 - c) = by(x^2 - d)$ in $K[x, y]$. If $abcd(a^2c - b^2d) \neq 0$, then $H(x, y)$ is irreducible in $\overline{K}[x, y]$ where $\overline{K}$ is the algebraic closure of K.

Proposition:nonsingularity

Let K be a field $charc(K) \neq 2$ and a, b, c, d in K. The affine variety defined by $\mathcal{H}_{(a,b)}^{(c,d)}$: $ax(y^2 - c) = by(x^2 - d)$ with $abcd(a^2c - b^2d) \neq 0$, is smooth.

Projective closure

Homogenus polynomial

We denotes $[X : Y : Z]$ a point on the projective plan $\mathcal{P}^2(K)$, where $[X : Y : Z]$ is the equivalence class
$[X : Y : Z] = \{(\lambda X, \lambda Y, \lambda Z), \lambda \in \bar{K}\}$.
If we homogenizes the affine previous curve, on the projective plane $\mathcal{P}^2(K)$, we have the projective closure of $\mathcal{H}_{(a,b)}^{(c,d)}$:

$$\overline{\mathcal{H}}_{(a,b)}^{(c,d)} : \ aX(Y^2 - cZ^2) = bY(X^2 - dZ^2) \ \text{ with } \ abcd(a^2c - b^2d) \neq 0$$

The points at infinity are the points of $\overline{\mathcal{H}}_{(a,b)}^{(c,d)}$ which do not lie in $\mathcal{H}_{(a,b)}^{(c,d)}$, in other words the points at infinitive are all points $[X : Y : 0] \in \overline{\mathcal{H}}_{(a,b)}^{(c,d)}$. and $Z = 0$ yields that $aXY^2 = bYX^2$. hence we have three infinite points $[1 : 0 : 0]$, $[0 : 1 : 0]$ and $[a : b : 0]$. Moreover this three infinite points are not singulars.

Birrational equivalence

In affine coordonates

Let K be a field $charc(K) \neq 2$ and a, b, c, d in K. The affine smooth variety defined by
$\mathcal{H}_{(a,b)}^{(c,d)}$: $ax(y^2 - c) = by(x^2 - d)$ with $abcd(a^2c - b^2d) \neq 0$ is birrationnaly equivalent to the elliptic curve defined by
$\mathcal{E}_{(a,b)}^{(c,d)} : v^2 = u(a - bu)(acu - bd)$ with $abcd(a^2c - b^2d) \neq 0$ via the transformation:

$$\begin{cases} u = \dfrac{x}{y} \\ v = \dfrac{x}{y}(ay - bx) \end{cases} \Leftrightarrow \begin{cases} x = \dfrac{v}{a - bu} \\ y = \dfrac{v}{u(a - bu)} \end{cases}$$

NB This birrational equivalence is not line preserving nevertheless, the addition provides a chord-and-tangent group law on E.

Remarks

1. $\mathcal{O} = [0 : 0 : 1]$ is an inflection point of E and $(E; \mathcal{O})$ is an elliptic curve with $\mathcal{O}$ as neutral element. The addition provides a chord-and-tangent group law on E.
2. The inverse of $P_1 = [X_1 : Y_1 : Z_1]$ is $\ominus P_1 = [X_1 : Y_1 : -Z_1]$
3. $[1 : 0 : 0], [0 : 1 : 0]$ and $[a : b : 0]$ are 2-torsion points of E
4. If c and d are square, $(\pm\sqrt{c} : \pm\sqrt{d} : 1]$ are 4-torsion points; these points form a subgroup isomorphic to $\frac{\mathbb{Z}}{4\mathbb{Z}} \times \frac{\mathbb{Z}}{2\mathbb{Z}}$

Universality of the model

Proposition

Let $\mathcal{H}^{(c,d)}_{(a,b)}$: $ax(y^2-c) = by(x^2-d)$ with $abcd(a^2c-b^2d) \neq 0$ be a Generalized Huff curve.

1. Any elliptic curve $(E;O)$ over a perfect field K of characteristic $\neq 2$ such that $E(K)$ contains a subgroup G isomorphic to $\frac{\mathbb{Z}}{2\mathbb{Z}} \times \frac{\mathbb{Z}}{2\mathbb{Z}}$ is birationally equivalent over K to a New Generalized Huff curve forme $\mathcal{H}^{(\frac{1}{a},d)}_{(a,-1)}$ with $ad(a-d) \neq 0$.
2. Any elliptic curve $(E;O)$ over a perfect field K of characteristic $\neq 2$ such that $E(K)$ contains a subgroup G isomorphic to $\frac{\mathbb{Z}}{4\mathbb{Z}} \times \frac{\mathbb{Z}}{2\mathbb{Z}}$ is birationally equivalent over K to a New Generalized Huff curve of the particular forme $\mathcal{H}^{(1,1)}_{(a,b)}$ with $ab(a^2-b^2) \neq 0$.

Arithmetic on the Generalized Huff curves

Addition law

Let $y = \alpha x + \beta$ denote the line (P_1P_2) where $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ are in the curve $\mathcal{H}^{(c,d)}_{(a,b)}$. We define $P_1 + P_2 = P_3$ where $P_3 = (x_3, y_3)$ and $-P_3 = (-x_3, -y_3)$ is third intersection point between the line and the curve.

We have $ax[(y = \alpha x + \beta)^2 - c] - b(y = \alpha x + \beta)[x^2 - d] = 0$ thus $(a\alpha^2 - \alpha b)x^3 + (2a\alpha\beta - b\beta)x^2 + [a(\beta^2 - c) + \alpha bd]x - \beta db = 0$.

Thus $-x_3 + x_1 + x_2 = -\dfrac{(2a\alpha\beta - b\beta)}{(a\alpha^2 - \alpha b)}$.

After a **long and tedius calculation** we find:

$$x_3 = \frac{d(x_1 + x_2)(c + y_1y_2)}{(d + x_1x_2)(c - y_1y_2)}$$

$$y_3 = \frac{c(y_1 + y_2)(d + x_1x_2)}{(c + y_1y_2)(d - x_1x_2)}$$

Efficiency in Projective coordinates

In projective coordinates, we have:
$[X_1 : Y_1 : Z_1] + [X_2 : Y_2 : Z_2] = [X_3 : Y_3 : Z_3]$ with:

$$\begin{cases} X_3 = d(X_1Z_2 + X_2Z_1)(cZ_1Z_2 + Y_1Y_2)^2(dZ_1Z_2 - X_1X_2), \\ Y_3 = c(Y_1Z_2 + Y_2Z_1)(dZ_1Z_2 + X_1X_2)(cZ_1Z_2 - Y_1Y_2), \\ Z_3 = (d^2Z_1^2Z_2^2 - X_1^2X_2^2)(c^2Z_1^2Z_2^2 - Y_1^2Y_2^2) \end{cases}$$

Let M, S and C denote respectively multiplication, squaring and constant multiplication, then direct counting shows that one can perform addition in projective coordinates with $\mathbf{11M + 5S + 4C}$. But it is possible to reduce the number of multiplications and squaring as follows: let $M_1 = X_1X_2$, $M_2 = Y_1Y_2$, $M_3 = Z_1Z_2$, $C_1 = cM_3$ and $C_2 = dM_3$, then:

1. $M_4 = (X_1 + Z_1)(X_2 + Z_2) - M_1 - M_3$, $M_5 = (Y_1 + Z_1)(Y_2 + Z_2) - M_2 - M_3$
2. $M_6 = (C_1 + M_2)(C_2 - M_1)$, $\quad M_7 = (C_2 + M_1)(C_1 - M_2)$,
3. $M_8 = M_4(C_1 + M_2)$, $\quad M_9 = M_5(C_2 + M_1)$
4. thus $X_3 = dM_8M_6$, $\quad Y_3 = cM_9M_7$ and $Z_3 = M_6M_7$

Hence, we have $12M + 4C$ instead of $11M + 5S + 4C$.

Completeness of the addition law

Theorem

Let K be a field of characteristic $\neq 2$. Let $P_1 = [X_1 : Y_1 : Z_1]$ and $P_1 = [X_2 : Y_2 : Z_2]$ be two points on a the New Generalized Huff curve over K. Then the addition formula $P_1 \oplus P_2 = P_3$ given by

$$\begin{cases} X_3 = d(X_1Z_2 + X_2Z_1)(cZ_1Z_2 + Y_1Y_2)^2(dZ_1Z_2 - X_1X_2), \\ Y_3 = c(Y_1Z_2 + Y_2Z_1)(dZ_1Z_2 + X_1X_2)(cZ_1Z_2 - Y_1Y_2), \\ Z_3 = (d^2Z_1^2Z_2^2 - X_1^2X_2^2)(c^2Z_1^2Z_2^2 - Y_1^2Y_2^2) \end{cases}$$

where $P_3 = [X_3 : Y_3 : Z_3]$, is valid provided that $X_1X_2 \neq dZ_1Z_2$ and $Y_1Y_2 \neq cZ_1Z_2$.

Proposition

Let E be a New Generalized Huff curve over a field K of odd characteristic. Let also $P \in E(K)$ be a point of odd order. Then the addition law in the subgroup generated by P is complete.

THINK YOU

WELCOME TO

The 4th Internationale Conference in Cryptology and Information Security

Dakar in Senegal, in July: 5-7 (2011)

See the web site www.africacrypt2011.com