Arithmetic of an Edwards model of elliptic curves defined over any field

Emmanuel FOUOTSA and Oumar DIAO

Université de Yaoundé 1-Cameroun
Université de Rennes 1 (IRMAR)-France

Journées C2 : Codage et Cryptographie
Dinard, 7-12 Octobre 2012
France

Outline

- Motivation
- Theta Functions in dimension 1
- Arithmetic of the level 4 theta model
- Arithmetic of the Edwards model
- Differential addition
- Work in progress

Motivation : The history of Edwards model

- [Edw. 07] introduces $x^2 + y^2 = a^2(1 + x^2y^2)$ of Elliptic curve
  - $(+)$ addition law is unified : also valid for doubling.
  - $(-)$ one can not add (x, y) and $(1/x, 1/y)$.

- [*Ber*.& Lan. 08] fill this gap with $x^2 + y^2 = c^2(1 + dx^2y^2)$.
  - $(+)$ BL model comes from Edw. model (unified addition)
  - $(+)$ Addition in BL model is also complete if d is not a square
  - $(-)$ BL model is not valid over binary fields.

- [Ber. Lan. & Far. 08] gave binary Edwards model (B.E.M) $a(x + y) + b(x^2 + y^2) = xy + xy(x + y) + x^2y^2$.
  - $(+)$ Complete & unified addition law.
  - $(-)$ relation between BLF & Edw. models is ?.

- [Wu.Tang. & Feng. 10] gave a new B.E.M $x^2y + xy^2 + x + y = axy$ with *complete, unified* & *fast* addition law.

- [Diao. 10] gave a "new" B.E.M $1 + x^2 + y^2 + x^2y^2 = axy$.
  - $(+)$ Diao B.E.M. comes from Edwards model
  - $(-)$ Addition law on Diao model is *slow* & *not unified*.

Goal : Give an Edwards model which is valid over any fields and have **complete, unified & competitive** addition law.

Method : Use theory of theta functions.

- **unified** : to protect against *Side Channel Attacks* [KJJ99]
- **complete** : to avoid *Exceptional Procedure Attacks* [IT02]

Theta Functions in dimension 1

An analogy to well understand

$$cos(x) = \sum_{n=0}^{+\infty}(-1)^n \frac{x^{2n}}{(2n)!} \text{ and } sin(x) = \sum_{n=0}^{+\infty}(-1)^n \frac{x^{2n+1}}{(2n+1)!} \qquad (1)$$

cos and *sin* satisfy the algebraic relations :

$$\begin{array}{rcl} cos^2(x) + sin^2(x) & = & 1 \\ cos(x_1 + x_2) & = & cos(x_1)cos(x_2) - sin(x_1)sin(x_2) \\ sin(x_1 + x_2) & = & sin(x_1)cos(x_2) + cos(x_1)sin(x_2) \end{array} \qquad (2)$$

The functions *cos* and *sin* enable to :

- parametrize the circle : $x^2 + y^2 = 1$
- add two points : $(x_1, y_1) + (x_2, y_2) = (x_1x_2 - y_1y_2, y_1x_2 + x_1y_2)$

Let $\omega \in \mathbb{C}$ s.t. $\mathcal{I}m(\omega) > 0$. Let $\Lambda_\omega := \omega\mathbb{Z} + \mathbb{Z}$ be a lattice of $\mathbb{C}$.

- The theta functions are analytics functions defined by :

$$\theta_{a,b}(z,\omega) = \sum_{n \in \mathbb{Z}} \exp\left(i\pi(n+a)^2\omega + 2i\pi(n+a)(z+b)\right). \tag{3}$$

Pseudo-periodicity

$$\theta_{a,b}(z + \omega m + n, \omega) = e^{-i\pi m(m\omega+2z)+2i\pi(an-bm)}\theta_{a,b}(z,\omega) \tag{4}$$

- [Mumford] The theta functions enable to :
  - parametrize points of an elliptic curve E ($\equiv \mathbb{C}/\Lambda_\omega$).
  - give addition law on E (Riemann relations).
- Each point of E can be represented by ℓ theta functions for $\ell \geq 3$.
- [Lefschetz principle] is used to valid algebraic formulas over any fields.

Def. A function $f \in \mathbb{C}$ is $\Lambda_\omega-$pseudo-periodic of level $\ell \in \mathbb{N}$ if

$$f(z + \omega m + n) = \exp\left(-i\ell\pi m^2\omega - 2\ell i\pi mz\right) f(z). \quad (5)$$

$\mathcal{R}_{\ell,\omega}$: set of $\Lambda_\omega-$quasi-periodic functions of level ℓ

Riemann theta functions

- $\mathcal{R}_{\ell,\omega}$ is a $\mathbb{C}-$vector space of dimension ℓ, for $\ell \geq 3$ [Mumford]
- For $\ell = 4$, two basis of $\mathcal{R}_{4,\omega}$ are :
  $\left\{\theta_{0,b}(z, \frac{1}{4}\omega), b \in \frac{1}{4}\mathbb{Z}/\mathbb{Z}\right\}$ & $\left\{\theta_{a,b}(2z, \omega), a, b \in \frac{1}{2}\mathbb{Z}/\mathbb{Z}\right\}$.
- [Koizumy] formula give relation between $\mathcal{B}_4$ and $\mathcal{B}_{(2,2)}$:

$$\theta_{0,b}(z, 4^{-1}\omega) = \sum_{\alpha \in \frac{1}{2}\mathbb{Z}/\mathbb{Z}} \theta_{\alpha,2b}(2z, \omega). \quad (6)$$

Riemann theta functions

Riemann theta relations

Let z_1 and z_2 be elements in $\mathbb{C}$. Then Riemann theta relations are :

$$\sum_{\eta \in \frac{1}{2}\mathbb{Z}/\mathbb{Z}} \theta_{i+\eta}(z_1 + z_2)\theta_{j+\eta}(z_1 - z_2)\theta_{k+\eta}(0)\theta_{l+\eta}(0) = \sum_{\eta \in \frac{1}{2}\mathbb{Z}/\mathbb{Z}} \theta_{i'+\eta}(z_1)\theta_{j'+\eta}(z_1)\theta_{k'+\eta}(z_2)\theta_{l'+\eta}(z_2). \tag{7}$$

- Lefschetz principle $\Rightarrow$ Riemann theta relations are valid over any field

Level 4 theta model

Taking $z_2 = 0$ in formula (7), we have :

$$E_{\lambda_1,\lambda_2} : \begin{cases} X_0^2 + X_2^2 = (c_0^2 + 4c_2^2)X_1X_3 \\ X_1^2 + X_3^2 = \frac{1}{c_0 c_2} X_0 X_2 \end{cases}, X_i = \theta_i(z_1);$$

Level 4 theta model

$$[X_0 : X_1 : X_2 : X_3] + [Y_0 : Y_1 : Y_2 : Y_3] = [Z_0 : Z_1 : Z_2 : Z_3]$$

Unified addition in odd characteristic

$$\begin{array}{rcl} Z_0 & = & (X_0^2 Y_0^2 + X_2^2 Y_2^2) - 4(c_2/c_0) X_1 X_3 Y_1 Y_3 \\ Z_1 & = & c_0(X_0 X_1 Y_0 Y_1 + X_2 X_3 Y_2 Y_3) - 2c_2(X_2 X_3 Y_0 Y_1 + X_0 X_1 Y_2 Y_3) \\ Z_2 & = & (X_1^2 Y_1^2 + X_3^2 Y_3^2) - 4(c_2/c_0) X_0 X_2 Y_0 Y_2 \\ Z_3 & = & c_0(X_0 X_3 Y_0 Y_3 + X_1 X_2 Y_1 Y_2) - 2c_2(X_0 X_3 Y_1 Y_2 + X_1 X_2 Y_0 Y_3) \end{array} . \quad (8)$$

Unified addition in characteristic 2

$$\begin{array}{rcl} Z_0 & = & (X_0 Y_0 + X_2 Y_2)^2 \\ Z_1 & = & c_0(X_0 X_1 Y_0 Y_1 + X_2 X_3 Y_2 Y_3) \\ Z_2 & = & (X_1 Y_1 + X_3 Y_3)^2 \\ Z_3 & = & c_0(X_0 X_3 Y_0 Y_3 + X_1 X_2 Y_1 Y_2) \end{array} . \quad (9)$$

$O_0 = [c_0 : 1 : 2c_2 : 1]$ and $-[X_0 : X_1 : X_2 : X_3] = [X_0 : X_3 : X_2 : X_1]$.

Smoothness and complete group law

Set $\lambda_1 = c_0^2 + 4c_2^2$; $\lambda_2 = \frac{1}{c_0 c_2}$

- $\lambda_1\lambda_2 \neq 0$ ensures that the level 4 theta model E_{λ_1,λ_2} is not singular.
- If one of the conditions hold in $\mathbb{K}$:
  1. -1 not a square in $\mathbb{K}$
  2. $\sqrt{-1}\lambda_1$ not a square in $\mathbb{K}$

  then the group law on E_{λ_1,λ_2} is complete. Indeed otherwise $[0 : 1 : \pm\sqrt{\pm\varepsilon\lambda_1} : \varepsilon] + [\pm c_0\varepsilon : 1 : \pm 2c_2\varepsilon : \pm 1]$ is not possible.

An Edwards model defined over any field

The Edwards model

Let $\mathbb{K}$ be a field of characteristic $p \geq 0$. The level 4-theta model E_{λ_1,λ_2} gives a normal form with equation : $\mathcal{E}_\lambda : 1 + x^2 + y^2 + x^2y^2 = \lambda xy$, where $\lambda = \lambda_1\lambda_2 \in \mathbb{K}^\star$.

Proof

$[X_0 : X_1 : X_2 : X_3] \longmapsto (x, y) = (X_2/X_0, X_3/X_1)$, then we have :

$$1 + x^2 = \lambda_1 \frac{X_1X_3}{X_0^2} \quad \text{and} \quad 1 + y^2 = \lambda_2 \frac{X_0X_2}{X_1^2}.$$

$(1 + x^2)(1 + y^2) = \lambda_1\lambda_2 xy$ equivalently $1 + x^2 + y^2 + x^2y^2 = \lambda_1\lambda_2 xy$.
neutral element $O_0 := (2c_2/c_0, 1)$.

An Edwards model defined over any field

Properties

- Isomorphic to the well known Edwards model in odd characteristic : $Ed_c : x^2 + y^2 = c^2(1 + x^2y^2)$ with $c^2 = \frac{\theta_{00}^2(0)}{\theta_{10}^2(0)}$.
- Smooth : $c^4 \neq 1 \Leftrightarrow (c_0 - 2c_2)^4 \neq (c_0 + 2c_2)^4 \Leftrightarrow c_0 c_2(c_0^2 + 4c_2^2) \neq 0$: Jacobi relation
- $\mathcal{E}_\lambda : 1 + x^2 + y^2 + x^2y^2 = \lambda xy$ is ordinary in binary fields.
- Birationally equivalent to an Weierstrass model.

An Edwards model defined over any field

$$(x_1, y_1) + (x_2, y_2) = (x_3, y_3)$$

Unified addition in odd characteristic

$$\begin{aligned} x_3 &= \frac{c_0(x_2 + x_1y_1y_2) - 2c_2(y_2 + x_1y_1x_2)}{c_0(y_1 + x_1x_2y_2) - 2c_2(x_1 + y_1x_2y_2)} \\ y_3 &= \frac{c_0(x_1y_1 + x_2y_2) - 2c_2(1 + x_1y_1x_2y_2)}{c_0(x_1y_2 + y_1x_2) - 2c_2(x_1x_2 + y_1y_2)} \end{aligned} \tag{10}$$

Unified addition in characteristic 2

$$(x_3, y_3) = \left(\frac{x_1 + y_1x_2y_2}{y_2 + x_1y_1x_2}, \frac{x_1x_2 + y_1y_2}{1 + x_1y_1x_2y_2}\right) \tag{11}$$

$-(x_1, y_1) = (x_1, 1/y_1)$ and the neutral element is $O_0 := (2c_2/c_0, 1)$.

Comparison with other models

In characteristic 2

Table: Comparisons of the points operations over binary fields

Models	Doubling	Addition
Weierstraß	$7M + 3S$	$14M + 1S$
Binary Edwards of [Ber,Lan,Far 08]	$4M + 4S + 1m$	$16M + 1S + 4m$
Hessian	$6M + 3S$	$12M + 6S$
Huff of [Dev,Joy 11]	$6M + 5S + 2m$	$13M + 2S + 2m$
Edwards model of [Wu,Tang,Feng 10]	$3M + 3S + 1m$	$12M + 4S + 2m$
Level 4 theta model	$3M + 6S + 2m$	$7M + 2S + 2m$
Our Edwards model	$7M + 3S$	$12M + 3S$

- (+) is not efficient in odd characteristic but we provide efficient differential addition.

$-[X_0 : X_1 : X_2 : X_3] = [X_0 : X_3 : X_2 : X_1]$. Then
$\mathcal{K}_{E_{\lambda_1,\lambda_2}} : W^2 = \frac{2}{\lambda_1}(X_0^2 + X_2^2) + \lambda_2 X_0 X_2$,
Given $P = [X_0 : X_1 : X_2 : X_3]$, $Q = [Y_0 : Y_1 : Y_2 : Y_3]$,
$S = P - Q = [T_0 : T_1 : T_2 : T_3]$. Let $R = P + Q = [Z_0 : Z_1 : Z_2 : Z_3]$ and
$U = [U_0 : U_1 : U_2 : U_3] = 2P$. The coordinates $Z_0, Z_2, Z_1 + Z_3$,
$U_0, U_2, U_1 + U_3$ are :

$$\left\{\begin{array}{lcl} Z_0 & = & T_0 \\ Z_2 & = & \frac{2a_0^2 - 2c_2^2}{c_0 c_2} X_0 Y_0 \cdot X_2 Y_2 - T_2 \\ W_3 & = & W_1 \cdot W_2 \cdot \Big(c_0(X_0 \cdot Y_0 + X_2 \cdot Y_2) - 2c_2(X_0 Y_2 + X_2 Y_0)\Big) - W_4 \end{array}\right. \quad (12),$$

$$\left\{\begin{array}{lcl} U_0 & = & \frac{c_0^2}{c_0^2 + 4c_2^2}(X_0^2 + X_2^2)^2 - 2X_0^2 X_2^2 \\ U_2 & = & (c_2/c_0) X_0^2 \cdot X_2^2 - 2\frac{c_0}{c_0^2 + 4c_2^2} c_2 (X_0^2 + X_2^2)^2 \\ W_5 & = & \frac{c_0}{c_0^2 + 4c_2^2}(a_0^2 - 4c_2^2)(X_0^2 + X_2^2) \cdot (W_1^2 - 2c_0 c_2 (X_0^2 + X_2^2)) \end{array}\right. \quad ,(13)$$

Differential addition on the Edwards model

The first coordinate of (x, y) is invariant under the opposite action.
$(x_3, y_3) = (x_1, y_1) + (x_2, y_2), (x_4, y_4) = (x_1, y_1) - (x_2, y_2)$ and
$(x_5, y_5) = 2(x_1, y_1)$.

$$x_3 = \frac{(c_0^2 - 4c_2^2)x_1 x_2}{c_0 c_2(1 + x_1^2 x_2^2)} - x_4 \tag{14}$$

$$x_5 = \frac{(c_2/c_0)x_1^2 - 2\mu c_2(1 + x_1^2)^2}{\mu c_0(1 + x_1^2)^2 - 2x_1^2} \mu = c_0/(c_0^2 + 4c_2^2). \tag{15}$$

Comparison of differential arithmetic in odd characteristic

Table: Comparisons of differential addition over non-binary fields

model	differential arithmetic
Montgomerry	$5M + 4S + 1m$
Weierstraß	$10M + 5S + 4m$
[Gau-Lub09]	$3M + 6S + 3m$
Level 4-theta model	$\mathbf{4M + 3S + 4m}$
Our Edwards model	$5M + 5S + 2m$

- if $M = S = m$, we save one multiplication

Comparison of differential arithmetic in characteristic 2

Table: Comparisons of differential addition over binary fields

model	differential arithmetic
Weierstraß [Stam03]	$5M + 4S + 1m$
Binary Edwards [Ber.Lan.Far 08]	$5M + 4S + 2m$
Huff of [DevJoy 11]	$5M + 5S + 1m$
New Edwards model[Wu,Tang,Feng 10]	$5M + 6S + 1m$
[Gaud-Lub 09]	$5M + 5S + 1m$
Level 4 theta model	$\mathbf{4M + 3S + 2m}$
Our Edwards model	$5M + 4S + 2m$

Conclusion

- Improve addition in odd characteristic.
- Pairing in characteristic 2 with theta functions.
- Factorisation
- Supersingular Edwards models
- Genus 2 Edwards model

A complete version of this work is avalaible here :

eprint.iacr.org/2012/346.pdf

Thanks for your attention ! !