A New Model of Binary Elliptic Curves

Rongquan Feng
School of Mathematical Sciences, Peking University, Beijing, China

Joint work with Hongfeng Wu and Chunming Tang.

December 11, 2012

1. Elliptic curve
2. New curve: $S_t : x^2y + xy^2 + txy + x + y = 0$
3. Differential Addition

Elliptic curve

Definition

A nonsingular absolutely irreducible projective curve defined over a field $\mathbb{F}$ of genus 1 with at least one F-rational point is called an elliptic curve over $\mathbb{F}$.

Elliptic curve

Definition

A nonsingular absolutely irreducible projective curve defined over a field $\mathbb{F}$ of genus 1 with at least one F-rational point is called an elliptic curve over $\mathbb{F}$.

- An elliptic curve E over $\mathbb{F}$ can be given by the so-called Weierstrass equation

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

where the coefficients $a_1, a_2, a_3, a_4, a_6 \in \mathbb{F}$.

Elliptic curve

Definition

A nonsingular absolutely irreducible projective curve defined over a field $\mathbb{F}$ of genus 1 with at least one F-rational point is called an elliptic curve over $\mathbb{F}$.

- An elliptic curve E over $\mathbb{F}$ can be given by the so-called Weierstrass equation

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

  where the coefficients $a_1, a_2, a_3, a_4, a_6 \in \mathbb{F}$.
- We note that E has to be nonsingular.

Elliptic curve

- The set of $\mathbb{F}$-rational points on E is defined by the set of points

$$E(\mathbb{F}) = \{(x, y) \in \mathbb{F} \times \mathbb{F} : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6\} \cup \{\mathcal{O}\},$$

where $\mathcal{O}$ is the point at infinity.

Elliptic curve

- The set of $\mathbb{F}$-rational points on E is defined by the set of points

$$E(\mathbb{F}) = \{(x, y) \in \mathbb{F} \times \mathbb{F} : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6\} \cup \{\mathcal{O}\},$$

  where $\mathcal{O}$ is the point at infinity.
- The set of $\mathbb{F}$-rational points on E by means of the chord-tangent process turns $E(\mathbb{F})$ into an abelian group with $\mathcal{O}$ as the neutral element.

Elliptic curve

- The set of $\mathbb{F}$-rational points on E is defined by the set of points

$$E(\mathbb{F}) = \{(x, y) \in \mathbb{F} \times \mathbb{F} : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6\} \cup \{\mathcal{O}\},$$

  where $\mathcal{O}$ is the point at infinity.
- The set of $\mathbb{F}$-rational points on E by means of the chord-tangent process turns $E(\mathbb{F})$ into an abelian group with $\mathcal{O}$ as the neutral element.
- If $\mathbb{F}$ be a finite field then $E(\mathbb{F})$ is a finite abelian group.

Elliptic Curve Cryptography

- ECC: elliptic-curve cryptography proposed by Miller 1984 (published 1985) and independently by Koblitz 1984 (published 1987).

Elliptic Curve Cryptography

- ECC: elliptic-curve cryptography proposed by Miller 1984 (published 1985) and independently by Koblitz 1984 (published 1987).
- Elliptic curves over finite fields are used for cryptosystems based on the Discrete Logarithm problem.

Elliptic Curve Cryptography

- ECC: elliptic-curve cryptography proposed by Miller 1984 (published 1985) and independently by Koblitz 1984 (published 1987).
- Elliptic curves over finite fields are used for cryptosystems based on the Discrete Logarithm problem.
- The use of elliptic curves in public-key cryptography can offer improved efficiency and bandwidth.

Arithmetic on ECC

- Finite fileds arithmetic (odd and even characteristic)

Arithmetic on ECC

- Finite fileds arithmetic (odd and even characteristic)
- Elliptic curve arithmetic

Arithmetic on ECC

- Finite fileds arithmetic (odd and even characteristic)
- Elliptic curve arithmetic
  - The shape of the curve

Arithmetic on ECC

- Finite fileds arithmetic (odd and even characteristic)
- Elliptic curve arithmetic
  - The shape of the curve
  - The coordinate systems

Arithmetic on ECC

- Finite fileds arithmetic (odd and even characteristic)
- Elliptic curve arithmetic
  - The shape of the curve
  - The coordinate systems
    - The addition(doubling) formulas:

Arithmetic on ECC

- Finite fileds arithmetic (odd and even characteristic)
- Elliptic curve arithmetic
  - The shape of the curve
  - The coordinate systems
    - The addition(doubling) formulas:
    - What is the cost?

Arithmetic on ECC

- Finite fileds arithmetic (odd and even characteristic)
- Elliptic curve arithmetic
  - The shape of the curve
  - The coordinate systems
    - The addition(doubling) formulas:
    - What is the cost?
    - Is it unified?

Arithmetic on ECC

- Finite fileds arithmetic (odd and even characteristic)
- Elliptic curve arithmetic
  - The shape of the curve
  - The coordinate systems
    - The addition(doubling) formulas:
    - What is the cost?
    - Is it unified?
    - Is it complete?

Arithmetic on ECC

- Finite fileds arithmetic (odd and even characteristic)
- Elliptic curve arithmetic
  - The shape of the curve
  - The coordinate systems
    - The addition(doubling) formulas:
    - What is the cost?
    - Is it unified?
    - Is it complete?
    - The differential addition and doubling formulas

Arithmetic on ECC

- Finite fileds arithmetic (odd and even characteristic)
- Elliptic curve arithmetic
  - The shape of the curve
  - The coordinate systems
    - The addition(doubling) formulas:
    - What is the cost?
    - Is it unified?
    - Is it complete?
    - The differential addition and doubling formulas
  - Scalar multiplication

Some forms of elliptic curves

There are many other ways to represent an elliptic curve such as:

- Long Weierstrass: $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$.

Some forms of elliptic curves

There are many other ways to represent an elliptic curve such as:

- Long Weierstrass: $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$.
- Short Weierstrass: $y^2 = x^3 + ax + b$.

Some forms of elliptic curves

There are many other ways to represent an elliptic curve such as:

- Long Weierstrass: $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$.
- Short Weierstrass: $y^2 = x^3 + ax + b$.
- Legendre: $y^2 = x(x-1)(x-\lambda)$.

Some forms of elliptic curves

There are many other ways to represent an elliptic curve such as:

- Long Weierstrass: $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$.
- Short Weierstrass: $y^2 = x^3 + ax + b$.
- Legendre: $y^2 = x(x-1)(x-\lambda)$.
- Montgomery: $by^2 = x^3 + ax^2 + x$.

Some forms of elliptic curves

There are many other ways to represent an elliptic curve such as:

- Long Weierstrass: $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$.
- Short Weierstrass: $y^2 = x^3 + ax + b$.
- Legendre: $y^2 = x(x-1)(x-\lambda)$.
- Montgomery: $by^2 = x^3 + ax^2 + x$.
- Jacobi intersection: $x^2 + y^2 = 1, ax^2 + z^2 = 1$.

Some forms of elliptic curves

There are many other ways to represent an elliptic curve such as:

- Long Weierstrass: $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$.
- Short Weierstrass: $y^2 = x^3 + ax + b$.
- Legendre: $y^2 = x(x-1)(x-\lambda)$.
- Montgomery: $by^2 = x^3 + ax^2 + x$.
- Jacobi intersection: $x^2 + y^2 = 1, ax^2 + z^2 = 1$.
- Jacobi quartic: $y^2 = x^4 + 2ax^2 + 1$.

Some forms of elliptic curves

There are many other ways to represent an elliptic curve such as:

- Long Weierstrass: $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$.
- Short Weierstrass: $y^2 = x^3 + ax + b$.
- Legendre: $y^2 = x(x-1)(x-\lambda)$.
- Montgomery: $by^2 = x^3 + ax^2 + x$.
- Jacobi intersection: $x^2 + y^2 = 1, ax^2 + z^2 = 1$.
- Jacobi quartic: $y^2 = x^4 + 2ax^2 + 1$.
- Hessian: $x^3 + y^3 + 1 = dxy$.

Some forms of elliptic curves

There are many other ways to represent an elliptic curve such as:

- Long Weierstrass: $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$.
- Short Weierstrass: $y^2 = x^3 + ax + b$.
- Legendre: $y^2 = x(x-1)(x-\lambda)$.
- Montgomery: $by^2 = x^3 + ax^2 + x$.
- Jacobi intersection: $x^2 + y^2 = 1, ax^2 + z^2 = 1$.
- Jacobi quartic: $y^2 = x^4 + 2ax^2 + 1$.
- Hessian: $x^3 + y^3 + 1 = dxy$.
- Twisted Edwards: $ax^2 + y^2 = 1 + dx^2y^2$.

Some forms of elliptic curves over fields of char 2

There are several ways to represent an elliptic curve over a field of characteristic 2 such as:

- Weierstrass: $y^2 + xy = x^3 + ax + b$.

Some forms of elliptic curves over fields of char 2

There are several ways to represent an elliptic curve over a field of characteristic 2 such as:

- Weierstrass: $y^2 + xy = x^3 + ax + b$.
- Binary Edwards: $d_1(x+y) + d_2(x^2+y^2) = xy + xy(x+y) + x^2y^2$.

Some forms of elliptic curves over fields of char 2

There are several ways to represent an elliptic curve over a field of characteristic 2 such as:

- Weierstrass: $y^2 + xy = x^3 + ax + b$.
- Binary Edwards: $d_1(x+y) + d_2(x^2+y^2) = xy + xy(x+y) + x^2y^2$.
- Binary Huff: $ax(y^2 + y + 1) = by(x^2 + x + 1)$.

Some forms of elliptic curves over fields of char 2

There are several ways to represent an elliptic curve over a field of characteristic 2 such as:

- Weierstrass: $y^2 + xy = x^3 + ax + b$.
- Binary Edwards: $d_1(x+y) + d_2(x^2+y^2) = xy + xy(x+y) + x^2y^2$.
- Binary Huff: $ax(y^2 + y + 1) = by(x^2 + x + 1)$.
- Hessian curve: $x^3 + y^3 + 1 = dxy$.

A new model of elliptic curves over Char 2

- A new model of elliptic curves

$$S_t : x^2y + xy^2 + txy + x + y = 0$$

over $\mathbb{F}_{2^m}$, where $t \in \mathbb{F}_{2^m}$ and $t \neq 0$.

A new model of elliptic curves over Char 2

- A new model of elliptic curves

$$S_t : x^2y + xy^2 + txy + x + y = 0$$

over $\mathbb{F}_{2^m}$, where $t \in \mathbb{F}_{2^m}$ and $t \neq 0$.

- Projective equation

$$S_t : X^2Y + XY^2 + tXYZ + XZ^2 + YZ^2 = 0.$$

A new model of elliptic curves over Char 2

- A new model of elliptic curves

$$S_t : x^2y + xy^2 + txy + x + y = 0$$

  over $\mathbb{F}_{2^m}$, where $t \in \mathbb{F}_{2^m}$ and $t \neq 0$.

- Projective equation

$$S_t : X^2Y + XY^2 + tXYZ + XZ^2 + YZ^2 = 0.$$

- with three points at infinity: $(1:0:0), (0:1:0)$ and $(1:1:0)$.

A new model of elliptic curves over Char 2

- A new model of elliptic curves

$$S_t : x^2y + xy^2 + txy + x + y = 0$$

over $\mathbb{F}_{2^m}$, where $t \in \mathbb{F}_{2^m}$ and $t \neq 0$.

- Projective equation

$$S_t : X^2Y + XY^2 + tXYZ + XZ^2 + YZ^2 = 0.$$

- with three points at infinity: $(1:0:0), (0:1:0)$ and $(1:1:0)$.
- isomorphic to the Weierstrass form

$$V^2W + UVW = U^3 + (1/t^8)W^3$$

with
$(U:V:W) = (t^2(X+Y) : X+Y+t^2X+tZ : t^4(X+Y+tZ)$.

New curve: $S_t : x^2y + xy^2 + txy + x + y = 0$

- two variant form:

$$x^2y + xy^2 + axy + b(x + y) = 0$$

is isomorphic to

$$x^2y + xy^2 + txy + (x + y) = 0$$

via $(x, y) \to (ax/\sqrt{b}, ay/\sqrt{b})$ with $t = a/\sqrt{b}$.

New curve: $S_t : x^2y + xy^2 + txy + x + y = 0$

- two variant form:

  $$x^2y + xy^2 + axy + b(x + y) = 0$$

  is isomorphic to

  $$x^2y + xy^2 + txy + (x + y) = 0$$

  via $(x, y) \to (ax/\sqrt{b}, ay/\sqrt{b})$ with $t = a/\sqrt{b}$.

- $$S_{a,b} : x^2y + xy^2 + axy + (x + y) + b(x^2 + y^2) = 0$$

  is isomorphic to

  $$v^2 + uv = u^3 + (b/a)u^2 + a^{-8}(1 + ab).$$

Addition law on $S_t : x^2y + xy^2 + txy + x + y = 0$

- $O = (1 : 1 : 0)$ is an inflection point of S_t. (S_t, O) is an elliptic curve with O as neutral element

Addition law on $S_t : x^2y + xy^2 + txy + x + y = 0$

- $O = (1 : 1 : 0)$ is an inflection point of S_t. (S_t, O) is an elliptic curve with O as neutral element
- Chord-and-tangent group law on S_t.

Addition law on $S_t : x^2y + xy^2 + txy + x + y = 0$

- $O = (1 : 1 : 0)$ is an inflection point of S_t. (S_t, O) is an elliptic curve with O as neutral element
- Chord-and-tangent group law on S_t.
- The inverse of $P_1 = (X_1 : Y_1 : Z_1)$ is $(Y_1 : X_1 : Z_1)$.

Addition law on $S_t : x^2y + xy^2 + txy + x + y = 0$

- $O = (1 : 1 : 0)$ is an inflection point of S_t. (S_t, O) is an elliptic curve with O as neutral element
- Chord-and-tangent group law on S_t.
- The inverse of $P_1 = (X_1 : Y_1 : Z_1)$ is $(Y_1 : X_1 : Z_1)$.
- The unified formula:
  $(X_1 : Y_1 : Z_1) + (X_2 : Y_2 : Z_2) =$
  $((X_1X_2+Z_1Z_2)\cdot((X_1X_2+Y_1Y_2)(Y_1Z_2+Y_2Z_1)+tY_1Y_2(Z_1Z_2+X_1X_2)) :$
  $(Y_1Y_2+Z_1Z_2)\cdot((X_1X_2+Y_1Y_2)(X_1Z_2+X_2Z_1)+tX_1X_2(Z_1Z_2+Y_1Y_2)) :$
  $(X_1X_2 + Y_1Y_2)(X_1X_2 + Z_1Z_2)(Y_1Y_2 + Z_1Z_2))$.

Addition law on $S_t : x^2y + xy^2 + txy + x + y = 0$

- $O = (1 : 1 : 0)$ is an inflection point of S_t. (S_t, O) is an elliptic curve with O as neutral element
- Chord-and-tangent group law on S_t.
- The inverse of $P_1 = (X_1 : Y_1 : Z_1)$ is $(Y_1 : X_1 : Z_1)$.
- The unified formula:
  $(X_1 : Y_1 : Z_1) + (X_2 : Y_2 : Z_2) =$
  $((X_1X_2+Z_1Z_2)\cdot((X_1X_2+Y_1Y_2)(Y_1Z_2+Y_2Z_1)+tY_1Y_2(Z_1Z_2+X_1X_2)) :$
  $(Y_1Y_2+Z_1Z_2)\cdot((X_1X_2+Y_1Y_2)(X_1Z_2+X_2Z_1)+tX_1X_2(Z_1Z_2+Y_1Y_2)) :$
  $(X_1X_2 + Y_1Y_2)(X_1X_2 + Z_1Z_2)(Y_1Y_2 + Z_1Z_2))$.
- Affine unified addition

$$(x_1, y_1) + (x_2, y_2) = \left(\frac{(x_1x_2 + y_1y_2)(y_1 + y_2) + ty_1y_2(1 + x_1x_2)}{(x_1x_2 + y_1y_2)(1 + y_1y_2)}, \right.$$
$$\left. \frac{(x_1x_2 + y_1y_2)(x_1 + x_2) + tx_1x_2(1 + y_1y_2)}{(x_1x_2 + y_1y_2)(1 + x_1x_2)} \right).$$

New curve: $S_t : x^2y + xy^2 + txy + x + y = 0$

New curve: $S_t : x^2y + xy^2 + txy + x + y = 0$

-

Lemma

An elliptic curve E defined over $\mathbb{F}_{2^m}$ satisfies $4 \mid \sharp E(\mathbb{F}_{2^m})$ if and only if E is isomorphic to an elliptic curve of the form $x^2y + xy^2 + txy + x + y = 0$.

New curve: $S_t : x^2y + xy^2 + txy + x + y = 0$

-

Lemma

An elliptic curve E defined over $\mathbb{F}_{2^m}$ satisfies $4 \mid \sharp E(\mathbb{F}_{2^m})$ if and only if E is isomorphic to an elliptic curve of the form $x^2y + xy^2 + txy + x + y = 0$.

-

New curve: $S_t : x^2y + xy^2 + txy + x + y = 0$

-

Lemma

An elliptic curve E defined over $\mathbb{F}_{2^m}$ satisfies $4 \mid \sharp E(\mathbb{F}_{2^m})$ if and only if E is isomorphic to an elliptic curve of the form $x^2y + xy^2 + txy + x + y = 0$.

-

Theorem

Let the curve $S_t : x^2y + xy^2 + txy + x + y = 0$ be defined over $\mathbb{F}_{2^m}$ and let $G \subset S_t(\mathbb{F}_{2^m})$ be a subgroup that does not contain points $(0 : 1 : 0)$, $(1 : 0 : 0)$ or $(0 : 0 : 1)$. Then the unified addition formula is complete.

Cost of unified formula

- $$\begin{aligned} A &= X_1 \cdot X_2,\ B = Y_1 \cdot Y_2,\ C = Z_1 \cdot Z_2, \\ D &= (X_1 + Z_1) \cdot (X_2 + Z_2) + A + C, \\ E &= (Y_1 + Z_1) \cdot (Y_2 + Z_2) + B + C,\ F = (A + C)^2, \\ G &= (B + C)^2,\ H = A \cdot (B + C),\ I = B \cdot C,\ J = A^2, \\ K &= B^2,\ X_3 = (J + H + I) \cdot E + tB \cdot F, \\ Y_3 &= (H + K + I) \cdot D + tA \cdot G,\quad Z_3 = (J + H + I) \cdot (B + C). \end{aligned}$$

Cost of unified formula

- $$\begin{aligned} A &= X_1 \cdot X_2,\ B = Y_1 \cdot Y_2,\ C = Z_1 \cdot Z_2, \\ D &= (X_1 + Z_1) \cdot (X_2 + Z_2) + A + C, \\ E &= (Y_1 + Z_1) \cdot (Y_2 + Z_2) + B + C,\ F = (A + C)^2, \\ G &= (B + C)^2,\ H = A \cdot (B + C),\ I = B \cdot C,\ J = A^2, \\ K &= B^2,\ X_3 = (J + H + I) \cdot E + tB \cdot F, \\ Y_3 &= (H + K + I) \cdot D + tA \cdot G,\quad Z_3 = (J + H + I) \cdot (B + C). \end{aligned}$$

- This algorithm costs $12M + 4S + 2D$, where the $2D$ is multiplication by the curve parameter t.

Cost of doubling formula

- $$\begin{aligned} 2(X_1 : Y_1 : Z_1) &= (Y_1^2(X_1^2 + Z_1^2)^2 : X_1^2(Y_1^2 + Z_1^2)^2 \\ &\quad : (1/t)(X_1^2 + Y_1^2)(X_1^2 + Z_1^2)(Y_1^2 + Z_1^2)). \end{aligned}$$

Cost of doubling formula

- $$\begin{aligned} 2(X_1 : Y_1 : Z_1) &= (Y_1^2(X_1^2 + Z_1^2)^2 : X_1^2(Y_1^2 + Z_1^2)^2 \\ &\quad : (1/t)(X_1^2 + Y_1^2)(X_1^2 + Z_1^2)(Y_1^2 + Z_1^2)). \end{aligned}$$

- $$\begin{aligned} A &= X_1^2,\ B = Y_1^2,\ C = Z_1^2,\ D = Y_1 \cdot (A + C), \\ E &= X_1 \cdot (B + C) \\ X_3 &= D^2,\ Y_3 = E^2, \\ Z_3 &= (1/t)(D + E + Z_1 \cdot (A + B))^2. \end{aligned}$$

Cost of doubling formula

- $$\begin{aligned} 2(X_1 : Y_1 : Z_1) &= (Y_1^2(X_1^2 + Z_1^2)^2 : X_1^2(Y_1^2 + Z_1^2)^2 \\ &\quad : (1/t)(X_1^2 + Y_1^2)(X_1^2 + Z_1^2)(Y_1^2 + Z_1^2)). \end{aligned}$$

- $$\begin{aligned} A &= X_1^2,\ B = Y_1^2,\ C = Z_1^2,\ D = Y_1 \cdot (A + C), \\ E &= X_1 \cdot (B + C) \\ X_3 &= D^2,\ Y_3 = E^2, \\ Z_3 &= (1/t)(D + E + Z_1 \cdot (A + B))^2. \end{aligned}$$

- Costs $3M + 6S + 1D$, where the $1D$ is the multiplication by $1/t$.

Comparing

We denote Edwards coordinates by $\mathcal{E}$, projective coordinates by $\mathcal{P}$, and extended López-Dahab coordinates [11] by $\mathcal{L}$.

Table: Comparisons of points operations in binary fields

Models	Addition	Doubling
$\mathcal{L}$, Weierstrass [1]	13M+4S	2M+4S+2D
$\mathcal{E}$, Binary Edwards [2]	18M+2S+7D	2M+6S+3D
$\mathcal{E}$, Binary Edwards, $d_1 = d_2$ [2]	16M+1S+4D	2M+5S+2D
$\mathcal{E}$, Binary Huff [10]	13M+3S+2D	6M+5S+2D
$\mathcal{P}$, Hessian curve [4]	12M	6M+3S+2D
$\mathcal{P}$, new model in this paper	12M+4S+2D	3M+6S+1D

Differential Addition

- Differential addition means computing $Q + P$ by giving P, Q, and $Q - P$ or computing $2P$ by giving P.

Differential Addition

- Differential addition means computing $Q + P$ by giving P, Q, and $Q - P$ or computing $2P$ by giving P.
- w-differential addition in calculating $w(P + Q)$ from $w(P), w(Q)$ and $w(P - Q)$ for a certain coordinate function w.

Differential Addition

- Differential addition means computing $Q + P$ by giving P, Q, and $Q - P$ or computing $2P$ by giving P.
- w-differential addition in calculating $w(P + Q)$ from $w(P), w(Q)$ and $w(P - Q)$ for a certain coordinate function w.
- For $P = (X : Y : Z)$, $w(P) = (XY : Z^2)$ with projective homogeneous coordinates.

Differential Addition

- Differential addition means computing $Q + P$ by giving P, Q, and $Q - P$ or computing $2P$ by giving P.
- w-differential addition in calculating $w(P + Q)$ from $w(P), w(Q)$ and $w(P - Q)$ for a certain coordinate function w.
- For $P = (X : Y : Z)$, $w(P) = (XY : Z^2)$ with projective homogeneous coordinates.
- For $P = (x, y)$, $w(P) = xy$ with affine coordinates.

Differential Addition

- Differential addition means computing $Q+P$ by giving P, Q, and $Q-P$ or computing $2P$ by giving P.
- w-differential addition in calculating $w(P+Q)$ from $w(P), w(Q)$ and $w(P-Q)$ for a certain coordinate function w.
- For $P=(X:Y:Z)$, $w(P)=(XY:Z^2)$ with projective homogeneous coordinates.
- For $P=(x,y)$, $w(P)=xy$ with affine coordinates.
- write $Q-P=(x_1,y_1)$, $P=(x_2,y_2)$, $Q=(x_3,y_3)$, $2P=(x_4,y_4)$ and $Q+P=(x_5,y_5)$, $w_i=x_iy_i$ for $i=1,2,3,4,5$.

Differential Addition

- Differential addition means computing $Q+P$ by giving P, Q, and $Q-P$ or computing $2P$ by giving P.
- w-differential addition in calculating $w(P+Q)$ from $w(P), w(Q)$ and $w(P-Q)$ for a certain coordinate function w.
- For $P=(X:Y:Z)$, $w(P)=(XY:Z^2)$ with projective homogeneous coordinates.
- For $P=(x,y)$, $w(P)=xy$ with affine coordinates.
- write $Q-P=(x_1,y_1)$, $P=(x_2,y_2)$, $Q=(x_3,y_3)$, $2P=(x_4,y_4)$ and $Q+P=(x_5,y_5)$, $w_i=x_iy_i$ for $i=1,2,3,4,5$.
- Then

$$w_4=\frac{1+w_2^4}{t^2w_2^2}, w_1+w_5=\frac{t^2w_2w_3}{w_2^2+w_3^2} \quad \text{and} \quad w_1w_5=\frac{1+w_2^2w_3^2}{w_2^2+w_3^2}.$$

Cost of projective w-coordinate differential addition

- Assume that w_i are given as fractions W_i/Z_i.

Cost of projective w-coordinate differential addition

- Assume that w_i are given as fractions W_i/Z_i.
- $$A = Z_2 \cdot Z_3,\ B = W_2 \cdot w_3,\ C = (A+B)^2,$$
  $$D = (W_2 + Z_2) \cdot (W_3 + Z_3) + A + B,$$
  $$W_5 = Z_1 \cdot C,\ Z_5 = W_1 \cdot D^2$$

  which cost $5M + 2S$ for differential addition.

Cost of projective w-coordinate differential addition

- Assume that w_i are given as fractions W_i/Z_i.
- $$A = Z_2 \cdot Z_3,\ B = W_2 \cdot w_3,\ C = (A+B)^2,$$
  $$D = (W_2 + Z_2) \cdot (W_3 + Z_3) + A + B,$$
  $$W_5 = Z_1 \cdot C,\ Z_5 = W_1 \cdot D^2$$

  which cost $5M + 2S$ for differential addition.
- The doubling formulas

$$A = W_2^2,\ C = Z_2^2,$$
$$W_4 = (A+C)^2,\ Z_4 = t^2 A \cdot C$$

cost $1M + 3S + 1D$,

Comparing of differential addition

Table: Comparisons of differential addition over binary fields

Models	doubling	addition	Total
Weierstrass [1]	1M+3S+1D	4M+1S	5M+4S+1D
Binary Edwards [2]	1M+3S+1D	4M+1S+1D	5M+4S+2D
Binary Huff [10]	1M+3S+1D	4M+2S	5M+5S+1D
Hessian curve [4]	1M+3S+1D	4M+1S+1D	5M+4S+2D
Gaudry, Lubicz [5]	1M+3S+1D	4M+2S	5M+5S+1D
this paper	1M+3S+1D	4M+2S or 4M+1S+1D	5M+5S+1D or 5M+4S+2D

Summary

- New representation for binary elliptic curves.

Summary

- New representation for binary elliptic curves.
- Efficient arithmetic.

Summary

- New representation for binary elliptic curves.
- Efficient arithmetic.
- Useful properties: unified/complete addition law.

Summary

- New representation for binary elliptic curves.
- Efficient arithmetic.
- Useful properties: unified/complete addition law.
- Fast differential addition.

Thanks for listening!

- D.J. Bernstein and T. Lange, Explicit-formulas database. URL: http://www.hyperelliptic.org/EFD.
- D.J. Bernstein, T. Lange, and R.R. Farashahi, Binary Edwards curves, CHES 2008, vol. 5154 of LNCS , pp. 244-265, Springer, 2008.
- É. Brier, and M. Joye, Weierstrass elliptic curves and side-channel attacks, PKC 2002, Vol. 2274 of LNCS, pp. 335-345, Springer, 2002.
- R. Farashahi and M. Joye, Efficient arithmetic on hessian curves. PKC 2010, Vol. 6056 of LNCS, pp. 243–260, Springer, 2010.
- P. Gaudry and D. Lubicz, The arithmetic of characteristic 2 Kummer surfaces and of elliptic Kummer lines, Finite Fields and Their Applications(2009), 15(2), pp. 246-260.
- K.U. Järvinen and J. Skytta. Fast Point Multiplication on Koblitz Curves: Parallelization Method and Implementations. Microproc. Microsyst. 2009:33(2), pp. 106-116.

- K.H. Kim and S.I. Kim, A new method for speeding up arithmetic on elliptic curves over binary fields (2007). URL: http://eprint.iacr.org/2007/181.
- N. Koblitz. Elliptic curve cryptosystems, Mathematics of Computation, 1987:48(177), 203–209.
- T. Lange, A note on Lápez-Dahab coordinates, Tatra Mountains Mathematical Publications 33(2006), pp. 75-81. URL: http://eprint.iacr.org/2004/323.
- J. Devigne and M. Joye, Binary Huff Curves, RSA 2011, vol. 6558 of LNCS, pp. 340-355, Springer, 2011.
- J. López and R. Dahab, Fast multiplication on elliptic curves over GF(2^m) without precomputation, CHES 1999, vol. 1717 of LNCS, pp. 316-327, Springer, 1999.
- A.J. Menezes, Elliptic Curve Public Key Cryptosystems, Kluwer Academic Publishers, 1993.

- V. Miller. Use of elliptic curves in cryptography, CRYPTo 1985, vol. 218 of LNCS, pp. 417C426, Springer, 1986.
- S.S. Roy, C. Rebeiro, D. Mukhopadhyay, J. Takahashi and T. Fukunaga. Scalar Multiplication on Koblitz Curves using τ^2-NAF. Cryptology ePrint Archive, Report 2011/318, URL: http://eprint.iacr.org/2011/318.
- P.L. Montgomery, Speeding the Pollard and elliptic curve methods of factor- ization, Mathematics of Computation 48(1987), pp. 243-264.
- M. Stam, On Montgomery-like representations for elliptic curves over GF(2^k), PKC 2003, vol. 2567 of LNCS, pp. 240-253, Springer, 2003.
- W.A. Stein (ed.), Sage Mathematics Software (Version 4.6), The Sage Group, 2010, http://www.sagemath.org.
- J.H. Silverman, The Arithmetic of Elliptic Curves, volume 106 of Graduate Texts in Mathematics, Springer-Verlag, 1986.