

Huff's Model for Elliptic Curves

Marc Joye Mehdi Tibouchi Damien Vergnaud

Technicolor

Ecole Normale Supérieure

ANTS-IX, Nancy, July 19–23, 2010



- Elliptic curves and elliptic curves models
- Huff's model
- Efficient arithmetic on Huff curves
- Generalizations and extensions
- Efficient pairings on Huff curves

Definition (Elliptic curve)

A nonsingular absolutely irreducible projective curve defined over a field \mathbb{F} of genus 1 with one distinguished \mathbb{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

Definition (Elliptic curve)

A nonsingular absolutely irreducible projective curve defined over a field \mathbb{F} of genus 1 with one distinguished \mathbb{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

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

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

where P_∞ is the point at infinity

- The set of \mathbb{F} -rational points on E by means of the chord-and-tangent process turns $E(\mathbb{F})$ into an abelian group with P_∞ as the neutral element

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

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

where P_∞ is the point at infinity

- The set of \mathbb{F} -rational points on E by means of the chord-and-tangent process turns $E(\mathbb{F})$ into an abelian group with P_∞ as the neutral element

- Finite field arithmetic
- Elliptic curve arithmetic
 - The shape of the curve
 - The coordinate systems
 - Addition formulas: What is the cost? Is it unified? Is it complete?
 - Scalar multiplication
- Evaluation of pairings

Some Forms of Elliptic Curves

- There are many 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: $by^2 = x^3 + ax^2 + x$

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: $y^2 = x^4 + 2ax^2 + 1$

Hessian: $x^3 + y^3 + 1 = 3dxy$

Edwards: $x^2 + y^2 = c^2(1 + x^2y^2)$

Twisted Edwards: $ax^2 + y^2 = 1 + dx^2y^2$

- Some of these define curves with singular projective closures but geometric genus 1

Some Forms of Binary Elliptic Curves

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

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

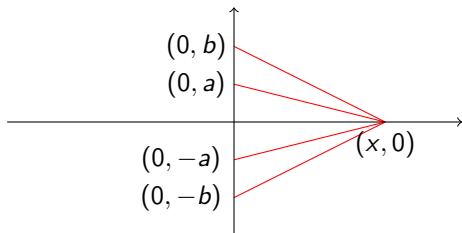
Short Weierstrass: $y^2 + xy = x^3 + ax^2 + b$

Hessian: $x^3 + y^3 + 1 = dxy$

Binary Edwards: $c(x + y) + d(x^2 + y^2) = xy + xy(x + y) + x^2y^2$

A Diophantine problem

$$a, b \in \mathbb{Q}^*, a^2 \neq b^2$$



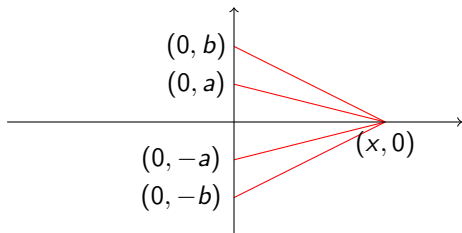
$x \in \mathbb{Q}$ for which $(x, 0)$ is at rational distances from $(0, \pm a)$ and $(0, \pm b)$?

equivalent to

Rational points on $ax(y^2 - 1) = by(x^2 - 1)$?

A Diophantine problem

$$a, b \in \mathbb{Q}^*, a^2 \neq b^2$$



$x \in \mathbb{Q}$ for which $(x, 0)$ is at rational distances from $(0, \pm a)$ and $(0, \pm b)$?

equivalent to

$$\text{Rational points on } ax(y^2 - 1) = by(x^2 - 1) ?$$

Gerald B. Huff. Diophantine problems in geometry and elliptic ternary forms. Duke Math. J., 15:443–453, 1948.

$$aX(Y^2 - Z^2) = bY(X^2 - Z^2)$$

- defines an elliptic curve if $a^2 \neq b^2$ and $a, b \neq 0$ over any field \mathbb{K} of odd characteristic with $(0 : 0 : 1)$ as the neutral element,
- with three points at infinity $(1 : 0 : 0)$, $(0 : 1 : 0)$ and $(a : b : 0)$
- isomorphic to the Weierstrass form:

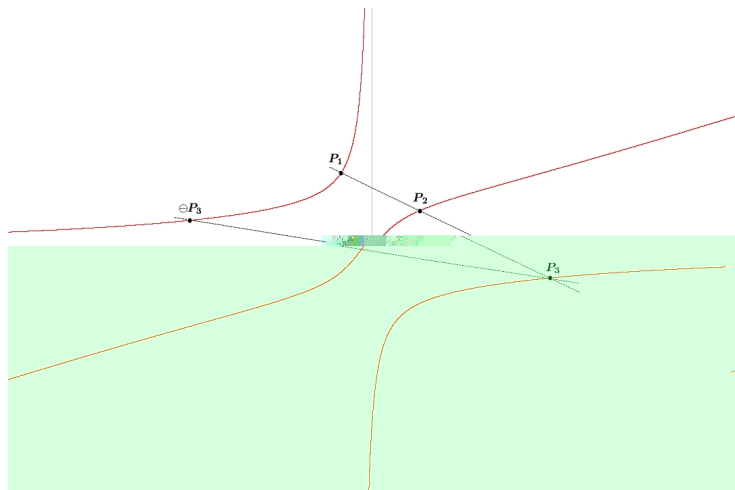
$$V^2W = U(U + a^2W)(U + b^2W)$$

(with $(U : V : W) = (ab(bX - aY) : ab(b^2 - a^2)Z : -aX + bY)$)

$$E : aX(Y^2 - Z^2) = bY(X^2 - Z^2)$$

- $\mathbf{O} = (0 : 0 : 1)$ is an inflection point of $E \rightsquigarrow (E, \mathbf{O})$ is an elliptic curve with \mathbf{O} as neutral element
- chord-and-tangent group law on E
- \rightsquigarrow the inverse of $\mathbf{P}_1 = (X_1 : Y_1 : Z_1)$ is $\ominus \mathbf{P}_1 = (X_1 : Y_1 : -Z_1)$
- $(1 : 0 : 0)$, $(0 : 1 : 0)$ and $(a : b : 0)$ are 2-torsion points of E
 $(\pm 1 : \pm 1 : 1)$ are 4-torsion points; these points form a subgroup isomorphic to $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$
- conversely, in odd characteristic, any elliptic curve with a rational subgroup isomorphic to $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ is isomorphic to a Huff curve (Riemann-Roch exercise)

Huff's Model



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

Unified/Complete Addition Formulas

$$E : ax(y^2 - 1) = by(x^2 - 1), \quad \mathbf{P}_1 \oplus \mathbf{P}_2 \oplus \mathbf{P}_3 = \mathbf{O}$$

- $\mathbf{P}_1 = (x_1, y_1)$, $\mathbf{P}_2 = (x_2, y_2)$, $\mathbf{P}_3 = (-x_3, -y_3)$ with

$$x_3 = \frac{(x_1 + x_2)(1 + y_1 y_2)}{(1 + x_1 x_2)(1 - y_1 y_2)} \text{ and } y_3 = \frac{(y_1 + y_2)(1 + x_1 x_2)}{(1 - x_1 x_2)(1 + y_1 y_2)}$$

whenever $x_1 x_2 \neq \pm 1$ and $y_1 y_2 \neq \pm 1$

- addition law is *unified*: it can be used to double a point
- involves inversions \rightsquigarrow projective coordinates:

$$\begin{cases} X_3 = (X_1 Z_2 + X_2 Z_1)(Y_1 Y_2 + Z_1 Z_2)^2 (Z_1 Z_2 - X_1 X_2) \\ Y_3 = (Y_1 Z_2 + Y_2 Z_1)(X_1 X_2 + Z_1 Z_2)^2 (Z_1 Z_2 - Y_1 Y_2) \\ Z_3 = (Z_1^2 Z_2^2 - X_1^2 X_2^2)(Z_1^2 Z_2^2 - Y_1^2 Y_2^2) \end{cases}$$

can be evaluated with **12m**

Unified/Complete Addition Formulas

$$E : ax(y^2 - 1) = by(x^2 - 1), \quad \mathbf{P}_1 \oplus \mathbf{P}_2 \oplus \mathbf{P}_3 = \mathbf{O}$$

- $\mathbf{P}_1 = (x_1, y_1)$, $\mathbf{P}_2 = (x_2, y_2)$, $\mathbf{P}_3 = (-x_3, -y_3)$ with

$$x_3 = \frac{(x_1 + x_2)(1 + y_1 y_2)}{(1 + x_1 x_2)(1 - y_1 y_2)} \text{ and } y_3 = \frac{(y_1 + y_2)(1 + x_1 x_2)}{(1 - x_1 x_2)(1 + y_1 y_2)}$$

whenever $x_1 x_2 \neq \pm 1$ and $y_1 y_2 \neq \pm 1$

- addition law is *unified*: it can be used to double a point
- involves inversions \rightsquigarrow projective coordinates:

$$\begin{cases} X_3 = (X_1 Z_2 + X_2 Z_1)(Y_1 Y_2 + Z_1 Z_2)^2 (Z_1 Z_2 - X_1 X_2) \\ Y_3 = (Y_1 Z_2 + Y_2 Z_1)(X_1 X_2 + Z_1 Z_2)^2 (Z_1 Z_2 - Y_1 Y_2) \\ Z_3 = (Z_1^2 Z_2^2 - X_1^2 X_2^2)(Z_1^2 Z_2^2 - Y_1^2 Y_2^2) \end{cases}$$

can be evaluated with 12m

Unified/Complete Addition Formulas

$$E : ax(y^2 - 1) = by(x^2 - 1), \quad \mathbf{P}_1 \oplus \mathbf{P}_2 \oplus \mathbf{P}_3 = \mathbf{O}$$

- $\mathbf{P}_1 = (x_1, y_1)$, $\mathbf{P}_2 = (x_2, y_2)$, $\mathbf{P}_3 = (-x_3, -y_3)$ with

$$x_3 = \frac{(x_1 + x_2)(1 + y_1 y_2)}{(1 + x_1 x_2)(1 - y_1 y_2)} \quad \text{and} \quad y_3 = \frac{(y_1 + y_2)(1 + x_1 x_2)}{(1 - x_1 x_2)(1 + y_1 y_2)}$$

whenever $x_1 x_2 \neq \pm 1$ and $y_1 y_2 \neq \pm 1$

- addition law is *unified*: it can be used to double a point
- involves inversions \rightsquigarrow projective coordinates:

$$\begin{cases} X_3 = (X_1 Z_2 + X_2 Z_1)(Y_1 Y_2 + Z_1 Z_2)^2 (Z_1 Z_2 - X_1 X_2) \\ Y_3 = (Y_1 Z_2 + Y_2 Z_1)(X_1 X_2 + Z_1 Z_2)^2 (Z_1 Z_2 - Y_1 Y_2) \\ Z_3 = (Z_1^2 Z_2^2 - X_1^2 X_2^2)(Z_1^2 Z_2^2 - Y_1^2 Y_2^2) \end{cases}$$

can be evaluated with **12m**

- The previous addition formula on a Huff curve is *independent* of the curve parameters
- Moreover, it is almost complete:

Theorem

Let $\mathbf{P}_1 = (X_1 : Y_1 : Z_1)$ and $\mathbf{P}_2 = (X_2 : Y_2 : Z_2)$ be two points on a Huff curve. Then the previous addition formula is valid provided that $X_1X_2 \neq \pm Z_1Z_2$ and $Y_1Y_2 \neq \pm Z_1Z_2$.

- in particular, if \mathbf{P} is of odd order, the addition law in $\langle \mathbf{P} \rangle$ is complete
- useful \rightsquigarrow natural protection against certain *side-channel attacks*

Generalizations and Extensions

- The doubling formula can be sped up by evaluating squarings
The cost of a point doubling then becomes $7m + 5s$ or $10m + 1s$
- Choosing $\mathbf{O}' = (0 : 1 : 0)$ as the neutral element results in translating the group law. We get

$$\begin{cases} X_3 = (X_1 Z_2 + X_2 Z_1)(Y_1 Y_2 + Z_1 Z_2)(Y_1 Z_2 + Y_2 Z_1) \\ Y_3 = (X_1 X_2 - Z_1 Z_2)(Z_1^2 Z_2^2 - Y_1^2 Y_2^2) \\ Z_3 = (Y_1 Z_2 + Y_2 Z_1)(X_1 X_2 + Z_1 Z_2)(Y_1 Y_2 - Z_1 Z_2) \end{cases}$$

This *unified* addition formula can be evaluated with $11m$
The cost of a point doubling then becomes $6m + 5s$

Generalizations and Extensions

- The doubling formula can be sped up by evaluating squarings
The cost of a point doubling then becomes $7m + 5s$ or $10m + 1s$
- Choosing $\mathbf{O}' = (0 : 1 : 0)$ as the neutral element results in translating the group law. We get

$$\begin{cases} X_3 = (X_1 Z_2 + X_2 Z_1)(Y_1 Y_2 + Z_1 Z_2)(Y_1 Z_2 + Y_2 Z_1) \\ Y_3 = (X_1 X_2 - Z_1 Z_2)(Z_1^2 Z_2^2 - Y_1^2 Y_2^2) \\ Z_3 = (Y_1 Z_2 + Y_2 Z_1)(X_1 X_2 + Z_1 Z_2)(Y_1 Y_2 - Z_1 Z_2) \end{cases}$$

This *unified* addition formula can be evaluated with $11m$
The cost of a point doubling then becomes $6m + 5s$

Generalizations and Extensions

- **Twisted curves:** Let $P \in \mathbb{K}[T]$ be a monic polynomial of degree 2, with non-zero discriminant, and such that $P(0) \neq 0$. We can generalize Huff's model and introduce the cubic curve

$$axP(y) = byP(x) \text{ where } a, b \in \mathbb{K}^*$$

With $P(T) = T^2 - d$, the sum of two points can be evaluated with **12m** using projective coordinates

- **Binary fields:** Huff's form can be extended to a binary field as

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

with neutral element $\mathbf{O} = (0, 0)$

- **Twisted curves:** Let $P \in \mathbb{K}[T]$ be a monic polynomial of degree 2, with non-zero discriminant, and such that $P(0) \neq 0$. We can generalize Huff's model and introduce the cubic curve

$$axP(y) = byP(x) \text{ where } a, b \in \mathbb{K}^*$$

With $P(T) = T^2 - d$, the sum of two points can be evaluated with **12m** using projective coordinates

- **Binary fields:** Huff's form can be extended to a binary field as

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

with neutral element $\mathbf{O} = (0, 0)$

Pairings

- E pairing-friendly elliptic curve over \mathbb{F}_q with hn rational points (n a large prime) and even embedding degree k wrt n (i.e. $n|q^k - 1$)
- To compute e.g. the (reduced) Tate pairing:

$$T_n: E(\mathbb{F}_q)[n] \times E(\mathbb{F}_{q^k})/[n]E(\mathbb{F}_{q^k}) \longrightarrow \mu_n$$

one typically uses Miller's algorithm

Algorithm 1 Miller's algorithm for T_n , $n = n_{\ell-1}n_{\ell-1} \cdots n_0^2$

- 1: $f \leftarrow 1$; $\mathbf{R} \leftarrow \mathbf{P}$
- 2: **for** $i = \ell - 2$ down to 0 **do**
- 3: $f \leftarrow f^2 \cdot g_{\mathbf{R},\mathbf{R}}(\mathbf{Q})$; $\mathbf{R} \leftarrow [2]\mathbf{R}$ ▷ Miller doubling
- 4: **if** ($n_i = 1$) **then**
- 5: $f \leftarrow f \cdot g_{\mathbf{R},\mathbf{P}}(\mathbf{Q})$; $\mathbf{R} \leftarrow \mathbf{R} \oplus \mathbf{P}$ ▷ Miller addition
- 6: **end if**
- 7: **end for**
- 8: **return** $f^{(q^k-1)/n}$

Pairings on Huff curves

- The rational function $g_{\mathbf{R},\mathbf{P}}$ in Miller's algorithm is Miller's **line function**, with divisor $\mathbf{R} + \mathbf{P} - \mathbf{O} - (\mathbf{R} \oplus \mathbf{P})$
- The faster we can compute $g_{\mathbf{R},\mathbf{P}}$, the faster the pairing
- For a curve with chord-and-tangent addition, like Weierstrass or Huff but unlike Edwards, $g_{\mathbf{R},\mathbf{P}}$ is simple: equation of the line through \mathbf{R} and \mathbf{P}
- Huff curves have a simple line function and efficient arithmetic \rightsquigarrow convenient for pairings?

Pairings on Huff curves

- The formulas we find don't use the fastest possible addition or doubling \rightsquigarrow not far from the records set for Jacobian coordinates or Edwards, but not as fast
- Actual multiplication counts:
 - mixed Miller addition: $1M + (k + 13)m$
 - full Miller addition: $1M + (k + 15)m$
 - Miller doubling: $1M + 1S + (k + 11)m + 6s$
- Compares to Arène et al.'s records: $1M + (k + 12)m$, $1M + (k + 14)m$, $1M + 1S + (k + 6)m + 5s$ for Edwards
- Room for improvement!

- Alternate representation for elliptic curves
- Efficient arithmetic
- Useful properties
 - unified/complete addition law
 - addition law independent of curve parameters
- Suitable for pairing evaluation

