Quelques pistes pour accélérer les calculs sur les courbes elliptiques

Laurent Imbert

ARITH – LIRMM, CNRS, Univ. Montpellier 2

Journées C2, Carcans, 17-21 mars 2008

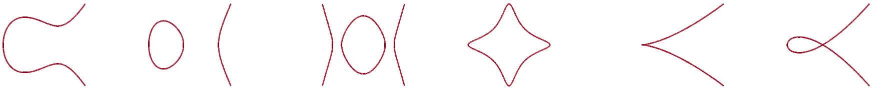
What is an elliptic curve?

Elliptic curves appear in various areas in mathematics: number theory, complex analysis, cryptography, mathematical physics. Their name comes from the studies of elliptic integrals (Euler, Gauss).

An elliptic curve is

- a geometrical object: a nonsingular curve given by an equation

$$y^2 = f(x), \quad \text{with } \deg f = 3, 4$$



- an algebraic object: one can "add" two points on a curve to obtain a third point that is also on the curve.

The equation of an elliptic curve

- An elliptic curve over a field K of characteristic $\neq 2, 3$ is given by an equation of the form

$$E : Y^2 = X^3 + aX + b, \quad \text{with } a, b \in K \tag{1}$$

and $\Delta = -16(4a^3 + 27b^2) \neq 0$
- j-invariant: $1728a^3/4\Delta$
- The set of K-rational points points of an elliptic curve is

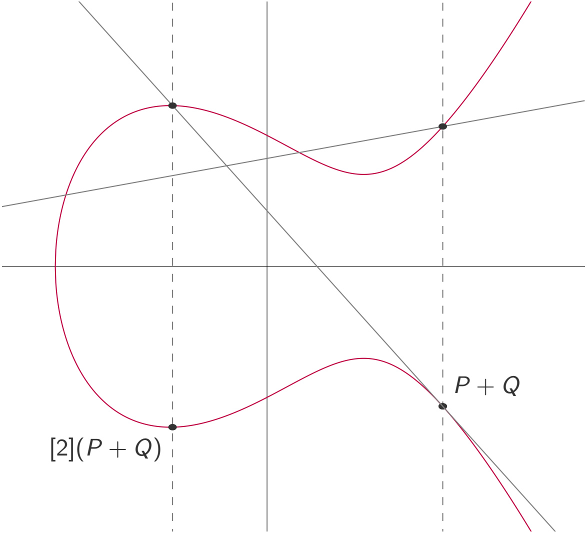
$$E(K) = \{(x, y) \in K \times K \; ; \; Y^2 = X^3 + aX + b\} \cup \{O\}$$

- In the general case, we consider the long Weierstrass form of an elliptic curve

$$Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6,$$

where $a_1, a_2, a_3, a_4, a_6 \in K$.

Adding points on an elliptic curve



Algebraic description of the addition operation

Let $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ be two points on

$$E : Y^2 = X^3 + aX + b.$$

The slope of the line (P_1, P_2) is

$$\lambda = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1} & \text{if } P_1 \neq \pm P2 \\[2ex] \dfrac{3x_1^2 + a}{2y_1} & \text{if } P_1 = P_2 \end{cases}$$

The sum of P and Q is the point

$$P + Q = (\lambda^2 - x_1 - x_2, \quad \lambda(x_1 - x_3) - y_1).$$

Properties of the addition on an elliptic curve

For all $P, Q, R \in E$, the addition law has the following properties:

- $P + O = O + P = P$
- $P + (-P) = O$
- $(P + Q) + R = P + (Q + R)$
- $P + Q = Q + P$

Thus, $(E, +)$ forms an Abelian group.

Abelian groups are widely used in public-key cryptography!

Group based cryptography

Many cryptographic protocols require the use of a finite Abelian group. For practical use one wants a group G such that

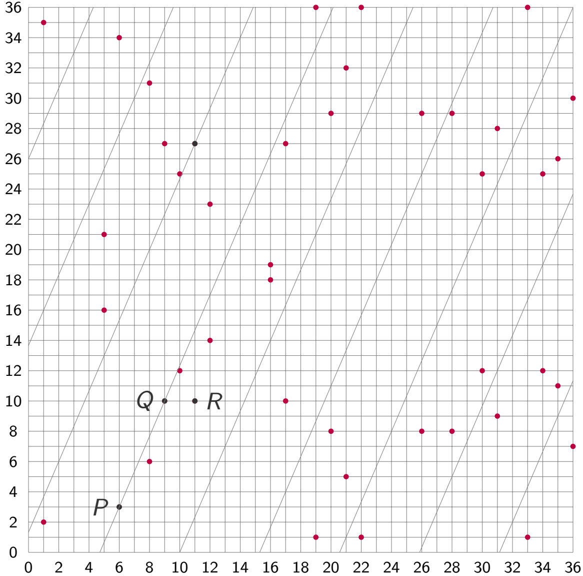
- the group operation is easy to implement (finite algebraic groups are good candidates),
- the computation of discrete logarithms in G is hard.

DLP: Find the least positive integer x (if it exists) such that $h = g^x$ for two elements $g, h \in (G, \times)$. If $\#G$ is prime such a discrete logarithm always exists.

Examples:

- the (multiplicative) subgroup $\mathbb{F}_q^*$ of a finite field
- the group of points of an elliptic curve defined over a finite field

Elliptic curve over a finite field



$E: y^2 = x^3 - 5x + 8$
defined over $\mathbb{F}_{37}$

$P = (6, 3)$

$Q = (9, 10)$

$\lambda = 7/3 = 27$

$x_3 = 27^2 - 6 - 9 = 11$

$y_3 = 27(6 - 11) - 3 = 10$

$R = (11, 10)$

What field can we use?

Software implementations: prime fields $\mathbb{F}_p$, p large prime

- Mersenne primes: $M_n = 2^n - 1$ $(M_{521} = 2^{521} - 1)$
- Pseudo-Mersenne primes: $2^n - c$, c small $(2^{255} - 19)$

Hardware implementations: binary fields $\mathbb{F}_{2^m}$, m large (prime)

- Reduction polynomial: trinomial, pentanomial, all-one polynomial
- Bases: polynomial bases, normal bases

Why not? General extension fields $\mathbb{F}_{p^m}$, p, m prime, p^m large

- Optimal Extension Fields (OEF)

What about sizes?

Security level (in bits)	RSA $\mathbb{Z}/n\mathbb{Z}$, $n = pq$ p, q primes ($\lvert n \rvert$ in bits)	DH, DSA $\mathbb{F}_q^*$ q prime power ($\lvert q \rvert$ in bits)	ECC $\mathbb{F}_p$ p prime ($\lvert p \rvert$ in bits)
80	1024	1024	160
112	2048	2048	224
128	3072	3072	256
192	4096	4096	384
256	15360	15360	512

What curves can we use?

For a given set of parameters (E, K, P, h, n), let $q := \#K = p^m$
A valid curve must satisfy:

- $\#E(K) = h \times n$
- n is prime
- $n > 2^{160}$ to avoid BSGS/Pollard rho attacks
- $n \neq p$ to avoid anomalous attack
- $q^t \not\equiv 1 \pmod{n}$ for all $t \leq 20$ to avoid the MOV attack
- m is prime to avoid Weil descent attacks
- P is on the curve and has order n

These checks are usually done only once by the organisation deploying elliptic curve based solutions.

Cost estimation

- How do we estimate the cost of an algorithm?
- A not-too-bad estimation can be obtained by counting the number of field operations of each type:
  - # field addition/subtraction (A)
  - # field multiplications (M)
  - # field squarings (S)
  - # field inversions (I)
  - # "small" field multiplications, e.g. $\times d$ is denoted by (D)
- Estimates: $I \approx 30M$, $S \approx 0.8M$ over $\mathbb{F}_p$, S "negligible" over $\mathbb{F}_{2^m}$

We don't like inversions!

In projective coordinates, the equation of E becomes

$$E : Y^2Z = X^3 + aXZ^2 + bZ^3$$

$(X : Y : Z)$ denotes an element of $\mathbb{P}^2/K$; i.e. a class of $\overline{K}^3 \setminus \{0, 0, 0\}$ modulo the equivalence relation

$(X : Y : Z) \sim (X' : Y' : Z') \Leftrightarrow \exists \lambda \in \overline{K}^*; X' = \lambda X, Y' = \lambda Y, Z' = \lambda Z$

Only one point of E satisfies $Z = 0$, the point at infinity $O = (0 : 1 : 0)$

- Projective: $(X : Y : Z)$; $(x, y) = (X/Z, Y/Z)$
- Jacobian: $(X : Y : Z)$; $(x, y) = (X/Z^2, Y/Z^3)$
- Chudnovsky Jacobian: $(X : Y : Z : Z^2 : Z^3)$
- Modified Jacobian: $(X : Y : Z : aZ^4)$
- ...

Elliptic curve operations

Curve shape	ADD	reADD	mADD	DBL	mDBL
DIK2	12M + 5S	12M + 5S	8M + 4S	2M + 5S	1M + 5S
DIK3	11M + 6S	10M + 6S	7M + 4S	2M + 7S	1M + 5S
Edwards	10M + 1S	10M + 1S	9M + 1S	3M + 4S	3M + 3S
ExtJQuartic	8M + 3S	8M + 3S	7M + 3S	3M + 4S	1M + 6S
Hessian	12M + 0S	12M + 0S	10M + 0S	7M + 1S	3M + 3S
InvEdwards	9M + 1S	9M + 1S	8M + 1S	3M + 4S	3M + 3S
JacIntersect	13M + 2S	10M + 2S	11M + 2S	3M + 4S	2M + 4S
Jacobian	11M + 5S	10M + 4S	7M + 4S	1M + 8S	1M + 5S
Jacobian-3	11M + 5S	10M + 4S	7M + 4S	3M + 5S	1M + 5S
JQuartic	10M + 3S	9M + 3S	8M + 3S	2M + 6S	1M + 4S
Projective	12M + 2S	12M + 2S	9M + 2S	5M + 6S	3M + 5S
Projective-3	12M + 2S	12M + 2S	9M + 2S	7M + 3S	3M + 5S

Elliptic curve based protocols

Signatures, key agreement and encryption protocols have been adapted to elliptic curves.

ECDSA: Elliptic Curve Digital Signature Algorithm

ECDH: Elliptic Curve Diffie-Hellman (key-agreement)

ECMQV: Authenticated DH key-agreement
(Menezes, Qu, Solinas, Vanstone)

ECIES: Elliptic Curve Integrated Encryption System

Computations and arithmetic needs

Scalar multiplication:

$$k, P \longrightarrow [k]P = P + P + \cdots + P, \quad (k \text{ times })$$

is the main operation.

But various situations can occur...

which have a great influence on the implementation choices.

Computations and arithmetic needs

- generated online at random
- unknown in advance; result of online computations
- known in advance; domain parameter; private key

ECDSA: Elliptic Curve Digital Signature Algorithm

Parameters: (E, K, P, h, n)

Signature:	k	P	$[k]P$	x-coord only
Verification:	k, l	P, Q	$[k]P + [l]Q$	

Computations and arithmetic needs

- generated online at random
- unknown in advance; result of online computations
- known in advance; domain parameter; private key

ECDH: Elliptic Curve Diffie-Hellman key-agreement

Parameters: (E, K, P, h, n)

$$\begin{array}{ccc} \text{Alice} & & \text{Bob} \\ a \quad [a]P & \longrightarrow & P_A \\ P_B & \longleftarrow & b \quad [b]P \\ [a]P_B & = & [b]P_A \end{array}$$

Computations and arithmetic needs

- generated online at random
- unknown in advance; result of online computations
- known in advance; domain parameter; private key

ECIES: Elliptic Curve Integrated Encryption System

Parameters: (E, K, P, h, n)

Encryption: k $[k]P$ only the x-coord is used for decryption
$[k]Q$

Addition chains

When the scalar k is known in advance, one computes $[k]P$ using "short" addition chains.

An addition chain for k is a sequence $1 = u_0 < u_1 < \cdots < u_n = k$ such that, for all $m \geq 1$, $u_m = u_i + u_j$ with $0 \leq i \leq j < m$.

- 289 : $1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, \ldots, 289$
- 289 : $1, 2, 4, 8, 9, 18, 36, 72, 144, 288, 289$

Finding optimal addition chain is very difficult, but good heuristics exists to get raisonably short addition chains.

Scalar multiplication algorithms

Double-and-add: $k = \sum_{i=0}^{n-1} k_i 2^i$, with $k_i \in \{0, 1\}$

$n - 1$ doublings, $n/2$ additions on average

$314159 = 1\ 0\ 0\ 1\ 1\ 0\ 0\ 1\ 0\ 1\ 1\ 0\ 0\ 1\ 0\ 1\ 1\ 1\ 1.$

NAF, CSD: $k_i \in \{\bar{1}, 0, 1\}$

n doublings, $n/3$ additions on average

$\mathrm{NAF}_2(314159) = 1\ 0\ 1\ 0\ \bar{1}\ 0\ 1\ 0\ \bar{1}\ 0\ \bar{1}\ 0\ 1\ 0\ \bar{1}\ 0\ 0\ 0\ \bar{1}$

NAF$_w$, Window methods: $|k_i| < 2^{w-1}$ (proces w bits at a time)

n doublings, $n/(w+1)$ additions on average

$\mathrm{NAF}_3(314159) = 1\ 0\ 0\ 0\ 3\ 0\ 0\ 1\ 0\ 0\ 3\ 0\ 0\ 0\ 3\ 0\ 0\ 0\ \bar{1}$

Double-base chains: $k = \sum_i 2^{a_i} 3^{b_i}$, with $a_i, b_i \geq 0$, $(a_i, b_i) \searrow$

a_0 doublings, b_0 triplings, $O(\log k / \log \log k)$ additions (?)

$314159 = 2^4 3^9 - 2^0 3^6 - 3^3 - 3^2 - 3 - 1$

Montgomery curves

An elliptic curve in the Montgomery form is a curve given by

$$E_M : \; By^2 = x^3 + Ax^2 + x, \quad A, B \in \mathbb{F}_{p^k}, \; p > 3$$

Arithmetic on such curves can be carried out with the x-coordinate only.

$[m+n]P = [m]P + [n]P = [X_{m+n} : - : Z_{m+n}]$

$$X_{m+n} = Z_{m-n} \left((X_m - Z_m)(X_n + Z_n) + (X_m + Z_m)(X_n - Z_n)\right)^2$$
$$Z_{m+n} = X_{m-n} \left((X_m - Z_m)(X_n + Z_n) - (X_m + Z_m)(X_n - Z_n)\right)^2$$

For the doubling operation, we have

$$\begin{aligned} 4X_nZ_n &= (X_n + Z_n)^2 - (X_n - Z_n)^2, \\ X_{2n} &= (X_n + Z_n)^2 (X_n - Z_n)^2, \\ Z_{2n} &= 4X_nZ_n \left((X_n - Z_n)^2 + ((A+2)/4)\,(4X_nZ_n)\right). \end{aligned}$$

The Montgomery ladder

Input: A point P on E_M and a positive integer $k = (k_{n-1} \dots k_0)_2$
Output: The point $[k]P$ on E_M

```
P_1 ← P,   P_2 ← [2]P
for i = k − 1 downto 0 do
    if n_i = 0 then
        P_1 ← [2]P_1,   P_2 ← P_1 + P_2
    else
        P_1 ← P_1 + P_2,   P_2 ← [2]P_2
return P_1
```

Note that $P_2 - P_1 = P$.

Cost: $(6M + 4S)(|k|_2 - 1)$

Conversion to Montgomery curves

$$E_M : \; By^2 = x^3 + Ax^2 + x \quad \longleftrightarrow \quad E_W : y^2 = x^3 + ax + b$$

$E_M \longrightarrow E_W$: always possible

$$a := 1/B^2 - A^2/3B^2$$

$$b := -A^3/27B^3 - aA/3B$$

$E_W \longrightarrow E_M$: conditional

If $\alpha \in \mathbb{F}_p$ is a root of $x^3 + ax + b$

and $3\alpha^2 + a$ is a quadratic residue modulo p

Then set $s := \sqrt{(3\alpha^2 + a)^{-1}}, \quad A := 3\alpha s, \quad B := s$

The change of variables $(x, y) \rightarrow (x/s + \alpha, y/s)$ gives a curve E_M isomorphic to E

DIK curves

In PKC 2006, C. Doche, T. Icart and D. Kohel suggested a family of curves with nice arithmetic properties

DIK2: Elliptic curves such that the multiplication-by-2 map can be split as the product of two isogenies of degree 2

DIK3: Elliptic curves such that the multiplication-by-3 map can be split as the product of two isogenies of degree 3

Isogenies

E_1/K and E_2/K are isogenous over K if there exists a rational map $\varphi : E_1 \to E_2$ with coefficients in K such that $\varphi(O_{E_1}) = O_{E_2}$.

An isogeny is a group homomorphism from $E_1(K)$ to $E_2(K)$:

$$\varphi(P + Q) = \varphi(P) + \varphi(Q)$$

For every (non constant) isogeny $\varphi : E_1 \to E_2$, there exists a unique dual isogeny $\hat{\varphi} : E_2 \to E_1$ such that

$$\hat{\varphi} \circ \varphi = [\ell],$$

where ℓ is the degree of the isogeny φ.

ℓ-division polynomials

There exists explicit formulas to compute $[\ell]P$ relying on ℓ-division polynomials ψ_ℓ.

$$[\ell](x,y) = \left(x - \frac{\psi_{\ell-1}\psi_{\ell+1}}{\psi_\ell^2},\ \frac{\psi_{\ell+2}\psi_{\ell-1}^2 - \psi_{\ell-2}\psi_{\ell+1}^2}{4y\psi_\ell^3} \right)$$

The ψ_n's are defined recursively

The degree of ψ_ℓ is $(\ell^2-1)/2$

Isogenies in practice

Every isogeny of degree ℓ over K can be described as a rational map

$$\varphi(x,y) = \left(\frac{\varphi_1(x,y)}{\psi(x,y)^2}, \frac{\varphi_2(x,y)}{\psi(x,y)^3} \right)$$

where $\varphi_1, \varphi_2, \psi$ are polynomials of degree $\leq \ell$

Scalar multiplication $[\ell]P$ as the composition of two degree-ℓ isogenies should be better than computing $[\ell]P$ using ℓ-division polynomials of degree $(\ell^2 - 1)/2$.

Problem: given ℓ small, find suitable elliptic curves such that $[\ell]$ can be split as the product of two isogenies of degree ℓ.

Finding isogenies

Let E_1 and E_2 be two elliptic curves over K with j-invariants j_1 and j_2 respectively.

There exists a polynomial $\Phi_\ell(X, Y) \in \mathbb{Z}[X, Y]$, called modular polynomial such that

$$\Phi_\ell(j_1, j_2) = 0 \text{ iff } E_1 \text{ and } E_2 \text{ are } \ell\text{-isogenous}$$

Given the j-invariant j of an elliptic curve E, the roots of $\Phi_\ell(X, j)$ are the j-invariant of the elliptic curves that are ℓ-isogenous to E.

For $\ell = 2, 3, 5, 7, 13$, the degree of Φ_ℓ in Y is equal to 1, such that deducing a parameterization of j is straightforward.

Explicit parameterization of curves

Using modular equations, C. Doche, T. Icart and D. Kohel were able to find explicit parameterization of elliptic curves over $\mathbb{F}_p$ with 3-isogenies with coefficients over $\mathbb{F}_p$.

For $j = (u+3)^3(u+27)/u$, we have $\Phi_3(u,j) = 0$ for all u.

For $p > 3$ prime and $u \in \mathbb{F}_p$, the families of elliptic curves given by

$$y^2 = x^3 + 3u(x+1)^2$$

has a multiplication-by-3 map that can be split as the product of two 3-isogenies over $\mathbb{F}_p$,

Elliptic curves with degree 3 isogenies

$$(x_1, y_1) \longrightarrow (x_t, y_t)$$

$$x_t = x_1 + 4u + 12u\left(\frac{x_1+1}{x_1^2}\right)$$

$$y_t = y_1\left(1 - 12u\left(\frac{x_1+2}{x_1^3}\right)\right)$$

$$(x_t, y_t) \longrightarrow (x_3, y_3) = [3]P$$

$$x_3 = \frac{1}{3^2}\left(x_t - 12u + \frac{12u(4u-9)}{x_t} - \frac{4u(4u-9)^2}{x_t^2}\right)$$

$$y_3 = \frac{1}{3^3}y_t\left(1 - \frac{12u(4u-9)}{x_t^2} + \frac{8u(4u-9)^2}{x_t^3}\right)$$

Efficiency aspects

C. Doche, T. Icart and D. Kohel used a variant of Jacobian coordinates where a point P is represented by $(X_1 : Y_1 : Z_1 : Z_1^2)$, where $x = X_1/Z_1^2$ and $y = Y_1/Z_1^3$.

One can verify that $[3]P = (X_3 : Y_3 : Z_3 : Z_3^2)$ is given by

$$
\begin{array}{ccc}
A = (X_1 + 3Z_1^2)^2 & B = uZ_1^2 A & X_t = Y_1^2 + B \\
Y_t = Y_1(Y_1^2 - 3B) & Z_t = X_1 Z_1 & C = Z_t^2 \\
D = ((4u-9)C - X_t)^2 & E = -3uCD & X_3 = Y_t^2 + E \\
Y_3 = Y_t(X_3 - 4E) & Z_3 = 3X_t Z_t & Z_3^2
\end{array}
$$

Cost: $8M + 6S$, can be reduced to $6M + 6S$ when multiplication by u is negligible.

Edwards curves

- H. M. Edwards, A Normal Form for Elliptic Curves, *Bulletin of the AMS*, 44, 393–422, 2007. The elliptic curve given by

$$x^2 + y^2 = a^2(1 + x^2y^2), \quad \text{with } a^5 \neq a \tag{2}$$

  describes an elliptic curve over a field K of odd characteristic
- There is a birational equivalence between (2) and

$$z^2 = (a^2 - x^2)(1 - a^2x^2) \quad \longleftarrow \quad z = y(1 - a^2x^2)$$

- Every elliptic curve can be written in this form, over some extension field
- Edwards gives addition law, shows equivalence with Weierstrass form, proves addition law, gives theta parameterization, . . .

Edwards curves shaped for crypto

- D. Bernstein and T. Lange introduced parameter d to cover more curves over K

$$E : x^2 + y^2 = c^2(1 + dx^2y^2), \text{ avec } cd(1 - dc^4) \neq 0.$$

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

$$x_3 = \frac{x_1y_2 + y_1x_2}{c(1 + dx_1x_2y_1y_2)}, \qquad y_3 = \frac{y_1y_2 - x_1x_2}{c(1 - dx_1x_2y_1y_2)}$$

- Neutral element: affine point of coordonates $(0, c)$
- Negative of a point: $-(x, y) = (-x, y)$
- Doubling: $[2](x, y) = \left(\frac{xy + yx}{c(1 + dxxyy)}, \frac{yy - xx}{c(1 - dxxyy)}\right)$
- Unified group operations

Unified operations

- If d is not a square then Edwards addition law is complete
  - if (x_1, y_1) and (x_2, y_2) on the curve then $dx_1x_2y_1y_2 \neq \pm 1$

- Formula is correct for all affine point including $(0, c)$, $P + (-P)$.

- Doubling formula is exactly identical to addition formula
  - no re-arrangement like in Hessian form where
    $[2](X_1 : Y_1 : Z_1) = (Z_1 : X_1 : Y_1) + (Y_1 : Z_1 : X_1)$.

Edwards addition law in projective coordinates

- The point $(X : Y : Z)$ such that

$$(X^2 + Y^2)Z^2 = c^2(Z^4 + dX^2Y^2)$$

  corresponds to the affine point $(X/Z, Y/Z)$.
- Neutral element: $(0 : c : 1)$
- Negative of a point: $-(X : Y : Z) = (-X : Y : Z)$
- Addition : $(X_1 : Y_1 : Z_1) + (X_2 : Y_2 : Z_2) = (X_3 : Y_3 : Z_3)$

$$\begin{array}{llll} A = Z_1Z_2 & B = A^2 & C = X_1X_2 & D = Y_1Y_2 \\ E = dCD & F = B - E & G = B + E & \end{array}$$

$$\begin{aligned} X_3 &= AF((X_1 + Y_1)(X_2 + Y_2) - C - D) \\ Y_3 &= AG(D - C) \\ Z_3 &= cFG \end{aligned}$$

- Cost: 10M + 1S + 1C + 1D + 7A

Comparisons with other fast unified formulas

Coordinates	Coût add/dbl	Ref
Projective	11M + 6S + 1D	Brier/Joye 03
Projective ($a = -1$)	13M + 3S	Brier/Joye 03
Jacobi intersection	13M + 2S + 1D	Liardet/Smart 01
Jacobi quartic	10M + 3S + 1D	Billet/Joye 01
Hessian	12M	Joye/Quisquater 01
Edwards ($c = 1$)	10M + 1S + 1D	Bernstein/Lange 07

Optimizing Edwards doubling ($c = 1$)

Affine: $[2](x, y)$

$$\left(\frac{xy + yx}{1 + dxxyy}, \frac{yy - xx}{1 - dxxyy}\right)$$
$$= \left(\frac{2xy}{1 + dx^2y^2}, \frac{y^2 - x^2}{1 - dx^2y^2}\right)$$
$$= \left(\frac{2xy}{x^2 + y^2}, \frac{y^2 - x^2}{2 - x^2 - y^2}\right)$$
$$= \left(\frac{(x + y)^2}{x^2 + y^2} - 1, \frac{y^2 - x^2}{2 - x^2 - y^2}\right)$$

Projective: $[2](X_1 : Y_1 : Z_1)$

$$B = (X_1 + Y_1)^2$$
$$C = X_1^2$$
$$D = Y_1^2$$
$$E = C + D$$
$$H = Z_1^2$$
$$J = E - 2H$$
$$X_3 = (B - E)J$$
$$Y_3 = E(C - D)$$
$$Z_3 = EJ$$

Cost: 3M + 4S + 6A

Comparisons

Doubling:

System	Cost
Proj.	5M + 6S
Proj. ($a = -3$)	7M + 3S
Hessian	7M + 1S
DIK 3	2M + 7S
Jac.	1M + 8S
Jac. ($a = -3$)	3M + 5S
Jacobi quartic	2M + 6S
Jacobi intersec.	3M + 4S
Edwards	3M + 4S
DIK 2	2M + 5S

Jac-3 vs. Edwards:

	Jac-3	Edwards
Double	3M + 5S	3M + 4S
Triple	7M + 7S	9M + 4S
Add	11M + 5S	10M + 1S + 1D
Re-Add	10M + 4S	10M + 1S + 1D
Mixed	7M + 4S	9M + 1S + 1D

EFD : Explicit-Formulas Database

`http://www.hyperelliptic.org/EFD/`

That’s all folks!