Pairings on Edwards Curves

Michael Naehrig

Eindhoven Institute for the Protection of Systems and Information
Technische Universiteit Eindhoven
`michael@cryptojedi.org`

Pairings in Arithmetic Geometry and Cryptography
Essen, 05.05.2009

joint work with Christophe Arène (IML), Tanja Lange (TU/e), and Christophe Ritzenthaler (IML)

Edwards curves

Let K be a field of characteristic $\neq 2$, $d \in K$, $d \notin \{0, 1\}$.

$$E_d : x^2 + y^2 = 1 + dx^2y^2$$

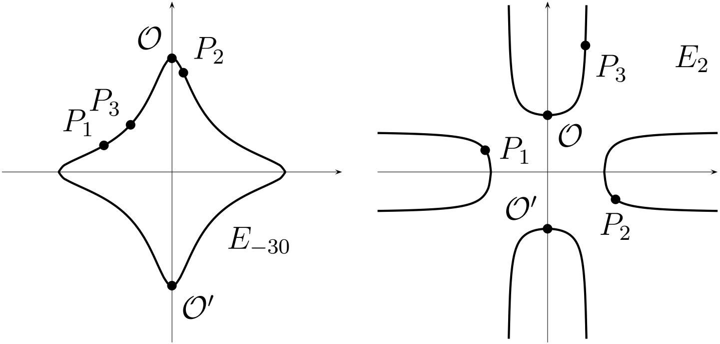
- Associative operation on most points defined by Edwards addition law

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

$$x_3 = \frac{x_1y_2 + y_1x_2}{1 + dx_1x_2y_1y_2} \text{ and } y_3 = \frac{y_1y_2 - x_1x_2}{1 - dx_1x_2y_1y_2}.$$

- Neutral element is $\mathcal{O} = (0, 1)$, $-(x_1, y_1) = (-x_1, y_1)$. $\mathcal{O}' = (0, -1)$ has order 2; $(1, 0), (-1, 0)$ have order 4.

Edwards curves



(a) $P_3 = P_1 + P_2$,
$x_{P_1} = -0.6$, $x_{P_2} = 0.1$

(b) $P_3 = P_1 + P_2$,
$x_{P_1} = -1.1$, $x_{P_2} = 1.2$

Relationship to elliptic curves

- Every elliptic curve with point of order 4 is birationally equivalent to an Edwards curve.
- Let $P_4 = (u_4, v_4)$ have order 4, shift u s.t. $[2]P_4 = (0,0)$. Then Weierstraß form:

$$v^2 = u^3 + (v_4^2/u_4^2 - 2u_4)u^2 + u_4^2 u.$$

- Define $d = 1 - (4u_4^3/v_4^2)$. Then the coordinates

$$x = v_4 u/(u_4 v),\ y = (u - u_4)/(u + u_4)$$

satisfy
$$x^2 + y^2 = 1 + dx^2y^2.$$

- Inverse map $u = u_4(1+y)/(1-y),\ v = v_4 u/(u_4 x)$.
- Finitely many exceptional points ($v(u + u_4) = 0$).
- Addition on Edwards and Weierstraß corresponds.

Nice features of the addition law

- Neutral element is affine point, this avoids special routines (for $\mathcal{O}$ one of the inputs or the result).

$$\begin{aligned} P+Q &= \left(\frac{x_1y_2+y_1x_2}{1+dx_1x_2y_1y_2}, \frac{y_1y_2-x_1x_2}{1-dx_1x_2y_1y_2}\right), \\ [2]\,P &= \left(\frac{x_1y_1+y_1x_1}{1+dx_1^2y_1^2}, \frac{y_1^2-x_1^2}{1-dx_1^2y_1^2}\right). \end{aligned}$$

- If d is not a square in K, the denominators $1+dx_1x_2y_1y_2$ and $1-dx_1x_2y_1y_2$ are never 0; addition law is *complete*.
- Having addition law work for doubling removes some checks from the code; addition law also works for adding $P+(-P)$ or the neutral element.

Fast addition law

- Very fast point addition (10M + 1S + 1D). Even faster with Inverted Edwards coordinates (9M+1S+1D) and Extended Edwards coordinates (8M+1S+1D).
- Dedicated doubling formulas need only 3M + 4S.
- Fastest scalar multiplication in the literature.
- For comparison: IEEE standard P1363 provides “the fastest arithmetic on elliptic curves” by using Jacobian coordinates on Weierstraß curves.
  - Point addition 12M + 4S.
  - Doubling 4M + 4S.
- For more curve shapes, better algorithms (even for Weierstraß curves) and many more operations (mixed addition, re-addition, tripling, scaling,. . .) see `www.hyperelliptic.org/EFD`.

Twisted Edwards curves

Let $a, d \in K^*,\ a \neq d$.

$$\mathrm{E}_{a,d}:\ ax^2 + y^2 = 1 + dx^2y^2$$

- Isomorphic to plain Edwards curve $\mathrm{E}_{1,d/a}$ for $a = \square$.
- Set of twisted Edwards curves invariant under quadratic twists.
- Addition formulas very similar to Edwards curves

$$x_3 = \frac{x_1y_2 + y_1x_2}{1 + dx_1x_2y_1y_2} \text{ and } y_3 = \frac{y_1y_2 - ax_1x_2}{1 - dx_1x_2y_1y_2}.$$

- Arithmetic complete only for $a = \square, d \neq \square$.
- Operation count same as Edwards (except for 1A)

Pairings on Edwards curves

Das, Sarkar [Pairing 2008]:

- Map points to a curve in Weierstraß form using birational map and compute pairing there.
- Express functions $g_{R,R}$ and $g_{R,P}$ in the Miller loop by transformation to Montgomery form.
- Explicit formulas for supersingular curves with $k = 2$.

Ionica, Joux [Indocrypt 2008]:

- Compute Miller functions on a curve

$$v^2u = (1 + du)^2 - 4u.$$

- Actually compute 4th power of the Tate pairing.
- Explicit formulas for even k.

A geometric interpretation of the addition law

- Find a function $g_{P_1,P_2} = h_1/h_2$ s.t.

$$\mathrm{div}(g_{P_1,P_2}) = (P_1) + (P_2) - (P_3) - (\mathcal{O}),$$

  for some point P_3 and $\mathcal{O} = (0, 1)$.
- Then

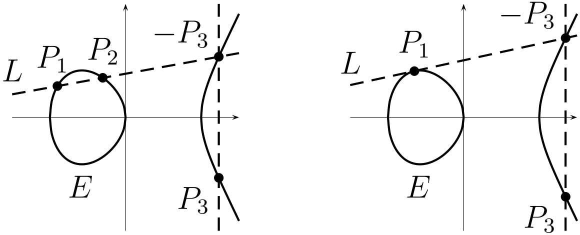
$$(P_1) - (\mathcal{O}) + (P_2) - (\mathcal{O}) \sim (P_3) - (\mathcal{O}),$$

  i. e. $P_1 + P_2 = P_3$.
- Can use line functions for elliptic curves in Weierstraß form.

Weierstraß

- Line through P_1 and P_2 divided by vertical line through third intersection point:

$$\big((P_1)+(P_2)+(-P_3)-3(\mathcal{O})\big)-\big((P_3)+(-P_3)-2(\mathcal{O})\big)$$
$$=(P_1)+(P_2)-(P_3)-(\mathcal{O}).$$



(c) Addition (d) Doubling

Addition and doubling on $E : y^2 = x^3 - x$ over $\mathbb{R}$.

Edwards

- Edwards equation has degree 4, so expect $4 \cdot \deg(h)$ intersection points by intersection with a function h.
- Functions h_1, h_2 cannot be linear (would have 4 intersection points; need to eliminate 2 out of each).
- Quadratic functions h_1, h_2 could offer enough freedom of cancellation (8 intersection points).
- General quadratic polynomial:

$$c_{X^2}X^2 + c_{Y^2}Y^2 + c_{Z^2}Z^2 + c_{XY}XY + c_{XZ}XZ + c_{YZ}YZ$$

- Problem: a conic is determined by 5 points; not enough control over intersection points.

Conic sections

- Solution: observe that points at infinity

$$\Omega_1 = (1:0:0) \text{ and } \Omega_2 = (0:1:0)$$

  are singular and have multiplicity 2.
- Conic C determined by passing through the 5 points

$$P_1, P_2, \mathcal{O}', \Omega_1, \text{ and } \Omega_2$$

  has only *one more* intersection point, say $-P_3$.
- Let h_1 be the function corresponding to C:

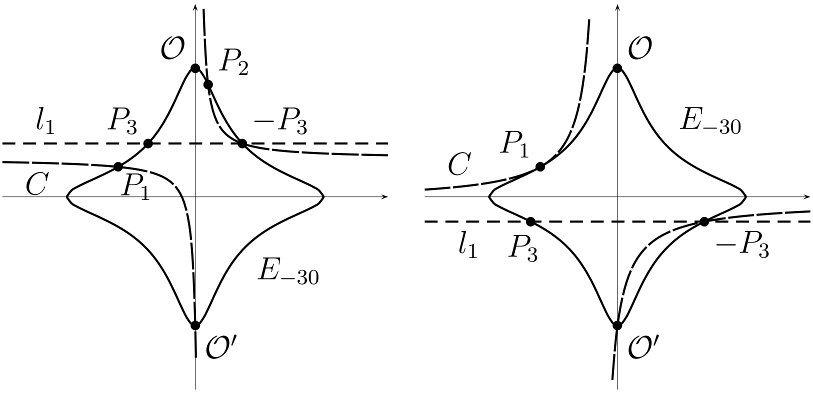
$$\operatorname{div}(h_1) = (P_1) + (P_2) + (\mathcal{O}') + (-P_3) - 2(\Omega_1) - 2(\Omega_2)$$

Conic sections

- Use h_2 to "replace" $\mathcal{O}'$ by $\mathcal{O}$ and $-P_3$ by P_3.
- Can be done with product $h_2 = l_1 l_2$ of two lines, a horizontal line l_1 through P_3 and a vertical line l_2 through $\mathcal{O}$.
- $\mathrm{div}(l_1) = (P_3) + (-P_3) - 2(\Omega_2)$,
  $\mathrm{div}(l_2) = (\mathcal{O}) + (\mathcal{O}') - 2(\Omega_1)$

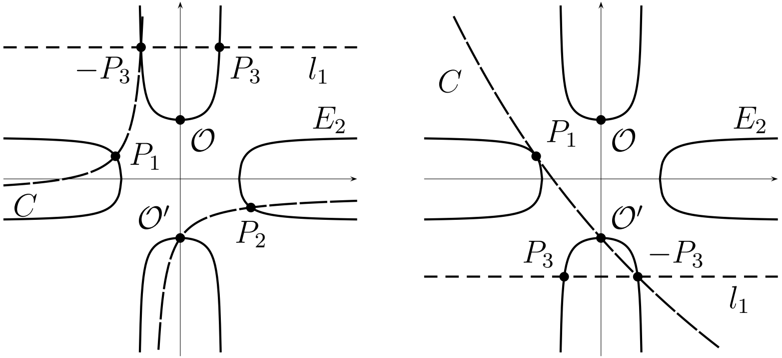
$$\begin{aligned}
\mathrm{div}(h_1/(l_1 l_2)) &= (P_1) + (P_2) + (\mathcal{O}') + (-P_3) \\
&\quad -2(\Omega_1) - 2(\Omega_2) \\
&\quad -(P_3) - (-P_3) + 2(\Omega_2) \\
&\quad -(\mathcal{O}) - (\mathcal{O}') + 2(\Omega_1) \\
&= (P_1) + (P_2) - (P_3) - (\mathcal{O})
\end{aligned}$$

Pictures I



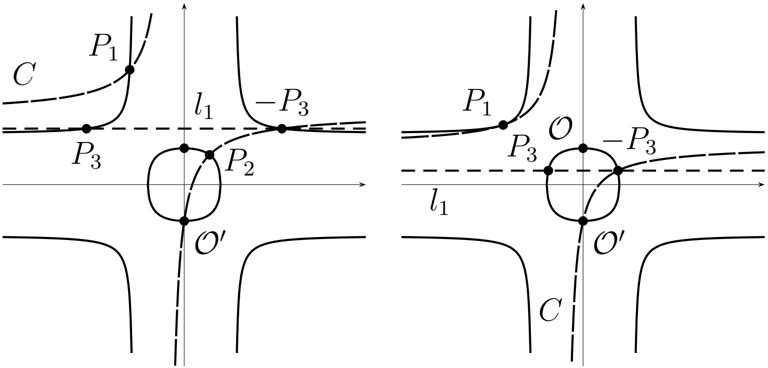
Addition and doubling over $\mathbb{R}$ for $d < 0$.

Pictures II



Addition and doubling over $\mathbb{R}$ for $d > 1$.

Pictures III



Addition and doubling over $\mathbb{R}$ for $0 < d < 1$.

Explicit functions

- Need to compute $g_{P_1,P_2} = h_1/(l_1 l_2)$ from coefficients of the points P_1, P_2.
- Let $P_3 = (X_3 : Y_3 : Z_3)$. Then the horizontal line through P_3 is given by

$$l_1 = Z_3 Y - Y_3 Z.$$

- The vertical line through $\mathcal{O}$ is given by

$$l_2 = X.$$

- Conic through $\mathcal{O}', \Omega_1$, and Ω_2 has shape

$$C : c_{Z^2}(Z^2 + YZ) + c_{XY} XY + c_{XZ} XZ = 0,$$

where $(c_{Z^2} : c_{XY} : c_{XZ}) \in \mathbb{P}^2(K)$.

Theorem

$P_1 = (X_1 : Y_1 : Z_1), P_2 = (X_2 : Y_2 : Z_2) \in E_{a,d}, Z_1, Z_2 \neq 0$

(a) If $P_1 \neq P_2$, $P_1, P_2 \neq \mathcal{O}'$, then

$$\begin{aligned} c_{Z^2} &= X_1X_2(Y_1Z_2 - Y_2Z_1), \\ c_{XY} &= Z_1Z_2(X_1Z_2 - X_2Z_1 + X_1Y_2 - X_2Y_1), \\ c_{XZ} &= X_2Y_2Z_1^2 - X_1Y_1Z_2^2 + Y_1Y_2(X_2Z_1 - X_1Z_2). \end{aligned}$$

(b) If $P_1 \neq P_2 = \mathcal{O}'$, then $c_{Z^2} = -X_1,\ c_{XY} = Z_1,\ c_{XZ} = Z_1$.

(c) If $P_1 = P_2$, then

$$\begin{aligned} c_{Z^2} &= X_1Z_1(Z_1 - Y_1), \\ c_{XY} &= dX_1^2Y_1 - Z_1^3, \\ c_{XZ} &= Z_1(Z_1Y_1 - aX_1^2). \end{aligned}$$

Proof

(a) $P_1 \neq P_2$ and $P_1, P_2 \neq \mathcal{O}'$

- From $P_1, P_2 \in C$, we get

$$\begin{aligned} c_{Z^2} Z_1(Z_1 + Y_1) + c_{XY} X_1 Y_1 + c_{XZ} X_1 Z_1 &= 0, \\ c_{Z^2} Z_2(Z_2 + Y_2) + c_{XY} X_2 Y_2 + c_{XZ} X_2 Z_2 &= 0. \end{aligned}$$

- The formulas follow from the (projective) solutions

$$c_{Z^2} = \begin{vmatrix} X_1 Y_1 & X_1 Z_1 \\ X_2 Y_2 & X_2 Z_2 \end{vmatrix}, \ c_{XY} = \begin{vmatrix} X_1 Z_1 & Z_1^2 + Y_1 Z_1 \\ X_2 Z_2 & Z_2^2 + Y_2 Z_2 \end{vmatrix},$$

$$c_{XZ} = \begin{vmatrix} Z_1^2 + Y_1 Z_1 & X_1 Y_1 \\ Z_2^2 + Y_2 Z_2 & X_2 Y_2 \end{vmatrix}.$$

Proof

(c) First $P_1 = P_2 \notin \{\mathcal{O}, \mathcal{O}'\}$:
Consider $P_1 = (x_1, y_1) = (X_1/Z_1, Y_1/Z_1)$.

- Since $P_1 \in C$: $c_{XZ} = -c_{XY}y_1 - c_{Z^2}(y_1 + 1)/x_1$.
- Intersection multiplicity of $E_{a,d}$ and C in P_1 needs to be larger than 1: tangents in P_1 equal.
- The tangents are

$$\begin{aligned}
(c_{XY}y_1 + c_{XZ})(x - x_1) + (c_{XY}x_1 + c_{Z^2})(y - y_1) &= 0, \\
2x_1(a - dy_1^2)(x - x_1) + 2y_1(1 - dx_1^2)(y - y_1) &= 0
\end{aligned}$$

- They are equal if $(c_{XY}x_1 + c_{Z^2})2x_1(a - dy_1^2) = (c_{XY}y_1 + c_{XZ})2y_1(1 - dx_1^2)$.

Proof

- Combine the two equations, multiply by x_1, apply curve equation:

$$(1+y_1)(1-dx_1^2y_1)c_{Z^2} = -x_1(1-y_1^2)c_{XY}.$$

- $P_1 \neq \mathcal{O}'$ ($y_1 \neq -1$):

$$(1-dx_1^2y_1)c_{Z^2} = -x_1(1-y_1)c_{XY}$$

- Choose $c_{Z^2} = -x_1(1-y_1)$ and $c_{XY} = 1-dx_1^2y_1$.
- Then

$$c_{XZ} = ax_1^2 - y_1.$$

  The formulas follow from homogenization.
- Verify that special cases are obtained by same formulas.

Miller's algorithm

Let $k > 1$ be the embedding degree of $E_{a,d}$ w.r.t. r,
$P \in E_{a,d}(\mathbb{F}_p)[r]$, $Q \in E_{a,d}(\mathbb{F}_{p^k})$,
$r = (r_{l-1}, \ldots, r_1, r_0)_2$.
Compute the Tate pairing as:

1. $R \leftarrow P$, $f \leftarrow 1$
2. for $i = l - 2$ to 0 do
   - 2.1 $f \leftarrow f^2 \cdot g_{R,R}(Q),\ R \leftarrow 2R$ //doubling step
   - 2.2 if $r_i = 1$ then
     $f \leftarrow f \cdot g_{R,P}(Q),\ R \leftarrow R + P$ //addition step
3. $f \leftarrow f^{(p^k-1)/n}$

Miller functions on twisted Edwards curves

Assume an even embedding degree k.

- Represent $\mathbb{F}_{p^k} = \mathbb{F}_{p^{k/2}}(\alpha)$ where $\alpha^2 = \delta \in \mathbb{F}_{p^{k/2}}$.
- Use quadratic twist $E_{\delta a, \delta d}(\mathbb{F}_{p^{k/2}})$ to represent second pairing argument $Q = \psi(Q')$:

$$\begin{array}{rcl} \psi : E_{\delta a,\delta d}(\mathbb{F}_{p^{k/2}}) & \longrightarrow & E_{a,d}(\mathbb{F}_{p^k}), \\ Q' = (x_0, y_0) & \longmapsto & (x_0\alpha, y_0). \end{array}$$

- Here $y_0 \in \mathbb{F}_{p^{k/2}}$ lies in a proper subfield of $\mathbb{F}_{p^k}$.
- In Miller's algorithm compute
  $f^2 \cdot g_{R,R}(\psi(Q'))$ (doubling step) and
  $f \cdot g_{R,P}(\psi(Q'))$ (addition step).

Miller functions on twisted Edwards curves

- Compute

$$\frac{h_1}{l_1 l_2}(x_0\alpha, y_0) = \frac{c_{Z^2}(1+y_0) + c_{XY}x_0\alpha y_0 + c_{XZ}x_0\alpha}{(Z_3 y_0 - Y_3)x_0\alpha}$$
$$= \frac{c_{Z^2}\frac{1+y_0}{x_0\delta}\alpha + c_{XY}y_0 + c_{XZ}}{Z_3 y_0 - Y_3},$$

  where $(X_3 : Y_3 : Z_3)$ are the coord. of $[2]R$ or $R+P$,
- in $2(k/2)\mathbf{m}$ over $\mathbb{F}_p$ given the coefficients c_{Z^2}, c_{XY}, c_{XZ} and precomputed $\eta = \frac{1+y_0}{x_0\delta}$.
- Note that $Z_3 y_Q - Y_3 \in \mathbb{F}_{p^{k/2}}$. Discard it since final exponentiation maps it to 1 anyway.

Pairing-friendly Edwards curves

How to get Edwards curves with small embedding degree?

- Construct pairing-friendly curves in Weierstraß form and then transform to Edwards or twisted Edwards form.
- Only requirement is that the group order is a multiple of 4.
- If have a point of order 4, get plain Edwards curve.
- If not, get twisted Edwards curve. Can be transformed to plain Edwards form by using 2-isogenies.

Pairing-friendly Edwards curves

- Need curves with $4 \mid \#E(\mathbb{F}_p)$.
- Use generalized MNT construction for curves with cofactor 4 as done by Galbraith, McKee, Valença.
- Parametrizations for embedding degree $k = 6$ and cofactor 4.

Case	$q(\ell)$	$t(\ell)$	$n(\ell)$
1	$16\ell^2 + 10\ell + 5$	$2\ell + 2$	$4\ell^2 + 2\ell + 1$
2	$112\ell^2 + 54\ell + 7$	$14\ell + 4$	$28\ell^2 + 10\ell + 1$
3	$112\ell^2 + 86\ell + 17$	$14\ell + 6$	$28\ell^2 + 18\ell + 3$
4	$208\ell^2 + 30\ell + 1$	$-26\ell - 2$	$52\ell^2 + 14\ell + 1$
5	$208\ell^2 + 126\ell + 19$	$-26\ell - 8$	$52\ell^2 + 38\ell + 7$

Pairing-friendly Edwards curves

- First solve the norm equation

$$t(\ell)^2 - 4q(\ell) = -Dv^2.$$

- Case 1 in the table:

$$t(\ell) = 2\ell + 2,\ q(\ell) = 16\ell^2 + 10\ell + 5$$

Transform equation into corresponding Pell equation by completing the square:

$$t(\ell)^2 - 4\,q(\ell) = -D\,y^2 \quad \Longleftrightarrow \quad x^2 - 15\,D\,y^2 = -44,$$

where $x = 15\ell + 4$.

Pairing-friendly Edwards curves

- Constructed curves over $\mathbb{F}_p$ have order

$$\#E(\mathbb{F}_p) = 4hr$$

  for a prime r and cofactor h.
- Since embedding degree is fixed to 6, balance the DLPs; eCrypt report on key sizes suggests the following bitsizes:

r	p	p^6	h
160	208	1248	46
192	296	1776	102
224	405	2432	179
256	541	3248	283
512	2570	15424	2056

Examples

$D = 1$, $\lceil \log(n) \rceil = 363$, $\lceil \log(h) \rceil = 7$, $\lceil \log(p) \rceil = 371$

$$\begin{aligned} p &= 324289037284274348719606384560284091622819395824325759 45\\ & 3063215355940262801001994668162495897393723963742016914 1,\\ n &= 1110578894809158728491802686850287985009655465151800546 0\\ & 623832064312035897815509951488907964532000965993787241,\\ h &= 73,\\ d &= 1621445186421371743598031922801420458114096979121628797 2\\ & 6531607677970131400500997334081247948696861981871008457 1. \end{aligned}$$

$D = 7230$, $\lceil \log(n) \rceil = 165$, $\lceil \log(h) \rceil = 34$, $\lceil \log(p) \rceil = 201$

$$\begin{aligned} p &= 2051613663768129606093583432875887398415301962227490187508801,\\ n &= 44812545413308579913957438201331385434743442366277,\\ h &= 7 \cdot 733 \cdot 2230663,\\ d &= 8895565706623541572106396621533758622612053798228797163324 49. \end{aligned}$$

Explicit formulas

- Use explicit formulas with extended Edwards coordinates by Hisil, et. al. [Asiacrypt 2008] for point doubling and addition in Miller's algorithm.
- Can reuse large parts of the computation for coefficients of the conic.
- Use even embedding degree and quadratic twist to represent second pairing argument Q, i.e. multiplications with coordinates x_Q and y_Q cost $k/2$ multiplications in $\mathbb{F}_p$.
- Compute conic coefficients in doubling step with $6\mathbf{m} + 5\mathbf{s} + 1\mathbf{m_a}$, in addition step with $14\mathbf{m} + 1\mathbf{m_a}$ (mixed addition $12\mathbf{m} + 1\mathbf{m_a}$).

Comparison of operation counts

	DBL	mADD	ADD
$\mathcal{J}$	$1\mathbf{m} + 11\mathbf{s} + 1\mathbf{m_{a_4}}$	$9\mathbf{m} + 3\mathbf{s}$	—
$\mathcal{J}, a_4 = -3$	$7\mathbf{m} + 4\mathbf{s}$	$9\mathbf{m} + 3\mathbf{s}$	—
$\mathcal{J}, a_4 = 0$	$6\mathbf{m} + 5\mathbf{s}$	$9\mathbf{m} + 3\mathbf{s}$	—
$\mathcal{E}$	$8\mathbf{m} + 4\mathbf{s} + 1\mathbf{m_d}$	$14\mathbf{m} + 4\mathbf{s} + 1\mathbf{m_d}$	—
$\mathcal{E}$, this paper	$6\mathbf{m} + 5\mathbf{s} + 1\mathbf{m_a}$	$12\mathbf{m} + 1\mathbf{m_a}$	$14\mathbf{m} + 1\mathbf{m_a}$

All formulas need additional km + 1M for (mixed) addition steps and km + 1M + 1S for doubling steps.

Comparison of operation counts

	DBL	mADD	ADD
$\mathcal{J}$	$1\mathbf{m}+11\mathbf{s}+1\mathbf{m_{a_4}}$	$9\mathbf{m}+3\mathbf{s}$	—
this paper	$1\mathbf{m}+11\mathbf{s}+1\mathbf{m_{a_4}}$	$6\mathbf{m}+6\mathbf{s}$	$15\mathbf{m}+6\mathbf{s}$
$\mathcal{J}, a_4=-3$	$7\mathbf{m}+4\mathbf{s}$	$9\mathbf{m}+3\mathbf{s}$	—
this paper	$6\mathbf{m}+5\mathbf{s}$	$6\mathbf{m}+6\mathbf{s}$	$15\mathbf{m}+6\mathbf{s}$
$\mathcal{J}, a_4=0$	$6\mathbf{m}+5\mathbf{s}$	$9\mathbf{m}+3\mathbf{s}$	—
this paper	$3\mathbf{m}+8\mathbf{s}$	$6\mathbf{m}+6\mathbf{s}$	$15\mathbf{m}+6\mathbf{s}$
$\mathcal{E}$	$8\mathbf{m}+4\mathbf{s}+1\mathbf{m_d}$	$14\mathbf{m}+4\mathbf{s}+1\mathbf{m_d}$	—
$\mathcal{E}$, this paper	$6\mathbf{m}+5\mathbf{s}+1\mathbf{m_a}$	$12\mathbf{m}+1\mathbf{m_a}$	$14\mathbf{m}+1\mathbf{m_a}$

Explicit formulas and more curve examples in preprint

`http://eprint.iacr.org/2009/155`