Elliptic Curves, Group Law, Efficient Computation

Ed Dawson and Hüseyin Hışıl
{e.dawson,h.hisil}@isi.qut.edu.au

Information Security Institute
Queensland University of Technology

18 May 2010

Outline

Main concepts

- Finite fields.
  - Large characteristic.
  - Assembly optimizations.
- Point additions.
  - New coordinate systems.
  - New and faster formulae.
- Scalar multiplications.
  - Windowing, NAF
  - Utilization of mixed-coordinates.

This research mainly concentrates on the second item.

Overview

- **Motivation and significance.** Applications of elliptic curves are getting increasing attention in cryptography. Elliptic curve addition law, as the underlying mechanism, is important for high-speed cryptographic software.

- **Aim.** Derivation of the addition law on an arbitrary elliptic curve and efficiently adding points on this elliptic curve using the derived addition law.

- **Outcome.** Practical speedups in higher level operations which depend on point additions. In particular, the contributions immediately find applications in cryptology.

Overview of Contributions

- An investigation of the group law for:
  1. Short Weierstrass form, **S**: $y^2 = x^3 + ax + b$,
  2. Extended Jacobi quartic form, **Q**: $y^2 = dx^4 + 2ax^2 + 1$,
  3. Twisted Hessian form, **H**: $ax^3 + y^3 + 1 = dxy$,
  4. Twisted Edwards form, **E**: $ax^2 + y^2 = 1 + dx^2y^2$,
  5. Twisted Jacobi intersection form, **I**: $bs^2 + c^2 = 1, as^2 + d^2 = 1$.
- Finding a suitable Weierstrass curve which is birationally equivalent to a curve in each form 1-5 by collecting and extending the literature results,

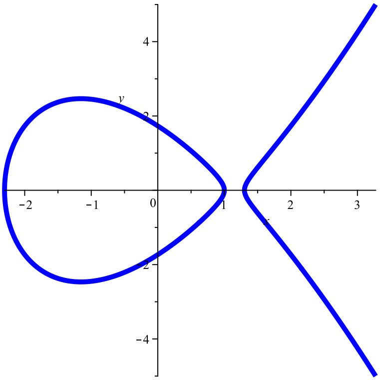
Overview of Contributions

- Bringing together classic and some very recent algebra tools in order to automate the investigation of the group law,
- Group law in affine coordinates for each of the studied forms,
- Simple ways of exception handling/prevention methods,
- Efficient inversion-free algorithms in various coordinate systems,
- Optimized high-speed software implementations to support theoretical results.

Some Notation and Assumptions

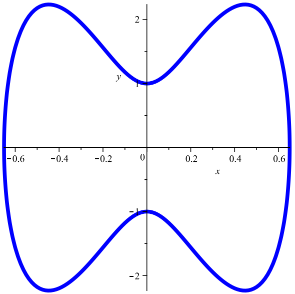
- **M**: Multiplication, **S**: Squaring.
- **I**: Inversion.
- **D**: Multiplication by a curve constant.
- **S** $=$ 0.8**M**,   **D** $=$ 0.25**M**,   **I** $=$ 100**M**.

Short Weierstrass form



- The curve $y^2 = x^3 + Ax + B$ covers all elliptic curves $\mathrm{char} \neq 2, 3$.
- Mixed Jacobian coordinates have been the speed leader for a long time.
- Some standards enforce its use, some not.

Extended Jacobi quartic form



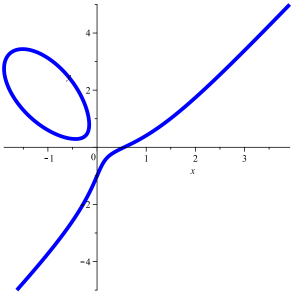
- Covers all elliptic curves with a point of order 2, $\mathrm{char} \neq 2$.
- New mixed coordinates
  - Dbl: $2\mathbf{M} + 5\mathbf{S}$.
  - Add: $6\mathbf{M} + 4\mathbf{S}$.
- Currently best for doubling intensive operations.

The Jacobi quartic curve $\mathbf{Q}: y^2 = dx^4 + 2ax^2 + 1$ is birationally equivalent to $\mathbf{W}: v^2 = u^3 - 4au^2 + (4a^2 - 4d)u$:

$$\psi: E_{\mathbf{Q}} \to E_{\mathbf{W}},\ (x, y) \mapsto \left(\frac{2y+2}{x^2} + 2a, \frac{4y+4}{x^3} + \frac{4a}{x}\right),$$

$$\phi: E_{\mathbf{W}} \to E_{\mathbf{Q}},\ (u, v) \mapsto \left(2\frac{u}{v}, 2(u-2a)\frac{u^2}{v^2} - 1\right).$$

Twisted Hessian form



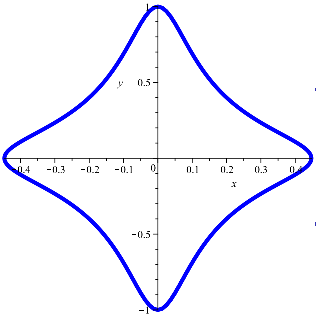
- Covers all elliptic curves with a point of order 3.
- New mixed coordinates
  - Dbl: $3\mathbf{M} + 6\mathbf{S}$.
  - Add: $6\mathbf{M} + 6\mathbf{S}$.
- Interesting for parallel implementations.

The twisted Hessian curve $\mathbf{H}: ax^3 + y^3 + 1 = dxy$ is birationally equivalent to $\mathbf{W}: v^2 = u^3 - \frac{d^4+216da}{48}u + \frac{d^6-540d^3a-5832a^2}{864}$:

$$\psi\colon E_{\mathbf{H}} \to E_{\mathbf{W}},\ (x, y) \mapsto \left(\frac{(d^3-27a)x}{3(3+3y+dx)} - \frac{d^2}{4}, \frac{(d^3-27a)(1-y)}{2(3+3y+dx)}\right),$$

$$\phi\colon E_{\mathbf{W}} \to E_{\mathbf{H}},\ (u, v) \mapsto \left(\frac{18d^2+72u}{d^3-12du-108a+24v}, 1 - \frac{48v}{d^3-12du-108a+24v}\right).$$

Twisted Edwards form



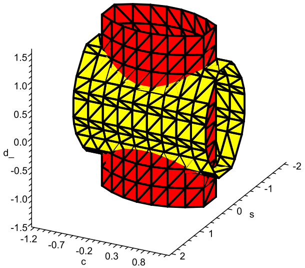
- Covers all elliptic curve covered by Montgomery curves $by^2 = x^3 + ax^2 + x$.
- New mixed coordinates.
  - Dbl: $3\mathbf{M} + 4\mathbf{S}$.
  - Add: $8\mathbf{M}$.
- Currently best for addition intensive operations, very interesting for parallel implementations.

The twisted Edwards curve $\mathbf{E}\colon ax^2 + y^2 = 1 + dx^2y^2$ is birationally equivalent to $\mathbf{W}\colon v^2 = u^3 + 2(a+d)u^2 + (a-d)^2u$:

$$\psi\colon E_{\mathbf{E}} \to E_{\mathbf{W}},\ (x,y) \mapsto \left((1+y)^2\frac{1-dx^2}{x^2}, 2(1+y)^2\frac{1-dx^2}{x^3}\right),$$

$$\phi\colon E_{\mathbf{W}} \to E_{\mathbf{E}},\ (u,v) \mapsto \left(2\frac{u}{v}, \frac{u-a+d}{u+a-d}\right).$$

Twisted Jacobi intersection form



- Covers all elliptic curves with exactly 3 points of order 2.
- New addition for homogeneous projective coordinates.
- New extended coordinates.
  - Dbl: $2\mathbf{M} + 5\mathbf{S}$.
  - Add: $11\mathbf{M}$.

The twisted Jaboci intersection curve $\mathbf{I}\colon bs^2 + c^2 = 1, as^2 + d^2 = 1$ is birationally equivalent to $\mathbf{W}\colon v^2 = u(u-a)(u-b)$:

$$\psi\colon E_{\mathbf{I}} \to E_{\mathbf{W}},\ (s,c,d) \mapsto \left(\frac{(1+c)(1+d)}{s^2}, -\frac{(1+c)(1+d)(c+d)}{s^3}\right), \quad (1)$$

$$\phi\colon E_{\mathbf{W}} \to E_{\mathbf{I}},\ (u,v) \mapsto \left(\frac{2v}{ab-u^2}, 2u\frac{b-u}{ab-u^2} - 1, 2u\frac{a-u}{ab-u^2} - 1\right). \quad (2)$$

The coverage of some forms (two curve constants)

Table: Statistics on the coverage of some forms with two curve constants.

Curve equation	**# of isomorphism classes** ($\approx$)
Short Weierstrass $y^2 = x^3 + ax + b$	$2.00q$
Extended Jacobi quartic $y^2 = dx^4 + 2ax^2 + 1$	$1.33q$
Twisted Hessian $ax^3 + y^3 + 1 = dxy$	$0.88q$
Twisted Edwards $ax^2 + y^2 = 1 + dx^2y^2$	$0.79q$
Twisted Jacobi intersection $bs^2 + c^2 = 1, as^2 + d^2 = 1$	$0.33q$

The coverage of some forms (single curve constant)

Table: Statistics on the coverage of some forms with a single curve constant.

Curve equation	**# of isomorphism classes** ($\approx$)
Extended Jacobi quartic $y^2 = dx^4 \pm x^2 + 1$	$0.80q$
Short Weierstrass $y^2 = x^3 - 3x + b$	$0.75q$
Edwards $\pm x^2 + y^2 = 1 + dx^2y^2$	$0.71q$
Extended Jacobi quartic $y^2 = -x^4 + 2ax^2 + 1$	$0.66q$
Hessian $\pm x^3 + y^3 + 1 = dxy$	$0.58q$
Jacobi quartic $y^2 = x^4 + 2ax^2 + 1$	$0.31q$
Jacobi intersection $\pm s^2 + c^2 = 1, as^2 + d^2 = 1$	$0.31q$

Automated Tool Development

Develop tools to:

1. Automate group law derivation to find the minimal degree point doubling/addition formulae.
   - Magma, Maple.
2. Verify the correctness of derived formulae.
3. Find alternative formulae.

Automated Group Law

Theorem

Let $W/\mathbb{K}$ and $M/\mathbb{K}$ be affine curves. Assume that W and M, each with a fixed $\mathbb{K}$-rational point, are elliptic curves. Assume that W and M are birationally equivalent over $\mathbb{K}$. Let $\phi : W \to M$ and $\psi : M \to W$ be maps such that $\phi \circ \psi$ and $\psi \circ \phi$ are equal to the identity maps id_M and id_W, respectively. Let $+_W : W \times W \to W$ be the affine part of the unique addition law on W. The affine part of the unique addition law on M is given by the compositions

$$+_M = \phi \circ +_W \circ (\psi \times \psi). \tag{3}$$

Automated Group Law

For simplicity assume that W is in Weierstrass form

$$E_{\mathbf{W},a_1,a_3,a_2,a_4,a_6} \; : \; y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

which is a non-singular model for W. Assume also that the rational mapping $+_W$ defined by

$$\begin{aligned} +_W \; : \; & W \times W \to W \\ & (P_1, P_2) \mapsto P_1 + P_2, \end{aligned}$$

gives the group law. Since $+_W$ is a morphism, i.e. the group law is defined for all of $W \times W$ and $+_W$ is already known explicitly for W, determining $+_M$ depends only on the definition of W, ϕ and ψ.

Example: Twisted Edwards curves

- The twisted Edwards curve is the curve

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

  with $ad(a-d) \neq 0$.

- There two points at infinity on the projective closure of $\mathbf{E}_{a,d}$, see [BKL09].
  - These point are $(0:1:0)$ and $(1:0:0)$ and both are singular.
  - A blow-up of $\mathbf{E}_{a,d}$ around $(0:1:0)$ produces two points. These points will be denoted by Ω_1 and Ω_2.
  - A blow-up of $\mathbf{E}_{a,d}$ around $(1:0:0)$ produces two points. These points will be denoted by Ω_3 and Ω_4.

Example: Twisted Edwards curves

Recall the construction:

$$+_M \quad = \quad \phi \circ +_W \circ (\psi \times \psi).$$

Example Maple script:

```
> a2:=2*(a+d): a4:=(a-d)^2:
> M:=(x,y)->(a*x^2+y^2-(1+d*x^2*y^2)):
> W:=(u,v)->(v^2-(u^3+a2*u^2+a4*u)):
> phi:=(u,v)->(2*u/v,(u-a+d)/(u+a-d)):
> psi:=(x,y)->((1+y)^2*(1-d*x^2)/x^2,
             2*(2-(a+d)*x^2+2*(1-d*x^2)*y)/x^3):
> psipsi:=(x1,y1,x2,y2)->(psi(x1,y1),psi(x2,y2)):
> addW:=(u1,v1,u2,v2)->(((v2-v1)/(u2-u1))^2-a2-u1-u2,
                      (v2-v1)/(u2-u1)*(u1-(((v2-v1)/
                      (u2-u1))^2-a2-u1-u2))-v1):
> addM:=phi(addW(psipsi(x1,y1,x2,y2))):
```

Example: Twisted Edwards curves

The derived point addition (if defined):

$$(x_1, y_1) + (x_2, y_2) = (x_3, y_3) \text{ where}$$

$$x_3 = 2((2(2-(a+d)x_2^2+2(1-dx_2^2)y_2)/x_2^3-2(2-(a+d)x_1^2+2(1-dx_1^2)y_1)/x_1^3)^2/((1+y_2)^2(1-dx_2^2)/x_2^2-(1+y_1)^2(1-dx_1^2)/x_1^2)^2-2a-2d-(1+y_1)^2(1-dx_1^2)/x_1^2-(1+y_2)^2(1-dx_2^2)/x_2^2)/((2(2-(a+d)x_2^2+2(1-dx_2^2)y_2)/x_2^3-2(2-(a+d)x_1^2+2(1-dx_1^2)y_1)/x_1^3)/((1+y_2)^2(1-dx_2^2)/x_2^2-(1+y_1)^2(1-dx_1^2)/x_1^2)(2(1+y_1)^2(1-dx_1^2)/x_1^2-(2(2-(a+d)x_2^2+2(1-dx_2^2)y_2)/x_2^3-2(2-(a+d)x_1^2+2(1-dx_1^2)y_1)/x_1^3)^2/((1+y_2)^2(1-dx_2^2)/x_2^2-(1+y_1)^2(1-dx_1^2)/x_1^2)^2+2a+2d+(1+y_2)^2(1-dx_2^2)/x_2^2)-2(2-(a+d)x_1^2+2(1-dx_1^2)y_1)/x_1^3),$$

$$y_3 = ((2(2-(a+d)x_2^2+2(1-dx_2^2)y_2)/x_2^3-2(2-(a+d)x_1^2+2(1-dx_1^2)y_1)/x_1^3)^2/((1+y_2)^2(1-dx_2^2)/x_2^2-(1+y_1)^2(1-dx_1^2)/x_1^2)^2-3a-d-(1+y_1)^2(1-dx_1^2)/x_1^2-(1+y_2)^2(1-dx_2^2)/x_2^2)/((2(2-(a+d)x_2^2+2(1-dx_2^2)y_2)/x_2^3-2(2-(a+d)x_1^2+2(1-dx_1^2)y_1)/x_1^3)^2/((1+y_2)^2(1-dx_2^2)/x_2^2-(1+y_1)^2(1-dx_1^2)/x_1^2)^2-a-3d-(1+y_1)^2(1-dx_1^2)/x_1^2-(1+y_2)^2(1-dx_2^2)/x_2^2),$$

Rational simplification

Problem: Well, we expected to see something "simple", something which can be computed very efficiently.

Solution: Monagan and Pearce's algorithm (2006) finds a fraction with minimal total degree sum of the numerator and denominator.

The algorithm: "...walk up through the degrees of the numerator and denominator and at each step attempt to solve $N\eta - D\delta \equiv 0 \mod I$ ...".

Here,
$I = \langle ax_1^2 + y_1^2 = 1 + dx_1^2y_1^2, ax_2^2 + y_2^2 = 1 + dx_2^2y_2^2 \rangle$,
N is the original numerator,
D is the original denominator,
η is a lower-degree numerator candidate,
δ is a lower-degree denominator candidate.

Rational simplification

Monagan and Pearce's algorithm is implemented in Maple v11+ and an open-source implementation is available in Pearce's thesis.

```
> addM:=simplify(addM,[M(x1,y1),M(x2,y2)],mindeg);
```

The simplified addition formulae are given by

$$(x_1, y_1) + (x_2, y_2) = \left(\frac{x_1y_1 + x_2y_2}{y_1y_2 + ax_1x_2}, \frac{x_1y_1 - x_2y_2}{x_1y_2 - y_1x_2} \right).$$

The point $(0, 1)$ is the identity and the point $(0, -1)$ is of order two.

With some more algebraic investigation, it is possible to derive the following addition law:

input : $P_1, P_2, \Omega_1, \Omega_2, \Omega_3, \Omega_4 \in E_{\mathbf{E}}(\mathbb{K})$ and fixed $\alpha, \delta \in \mathbb{K}$ such that $\alpha^2 = a$ and $\delta^2 = d$.

output : $P_1 + P_2$.

if $P_1 \in \{\Omega_1, \Omega_2, \Omega_3, \Omega_4\}$ **then** $P_t \leftarrow P_1, P_1 \leftarrow P_2, P_2 \leftarrow P_t$.
if $P_2 = \Omega_1$ **then**
  if $P_1 = \Omega_1$ **then return** $(0, 1)$. **else if** $P_1 = \Omega_2$ **then return** $(0, -1)$. **else if** $P_1 = \Omega_3$ **then return** $(-1/\alpha, 0)$. **else if** $P_1 = \Omega_4$ **then return** $(1/\alpha, 0)$. **else if** $P_1 = (0, 1)$ **then return** Ω_1. **else if** $P_1 = (0, -1)$ **then return** Ω_2. **else if** $P_1 = (-1/\alpha, 0)$ **then return** Ω_3. **else if** $P_1 = (1/\alpha, 0)$ **then return** Ω_4. **else return** $(-1/(\alpha\delta x_1), -\alpha/(\delta y_1))$.
else if $P_2 = \Omega_2$ **then**
  if $P_1 = \Omega_1$ **then return** $(0, -1)$. **else if** $P_1 = \Omega_2$ **then return** $(0, 1)$. **else if** $P_1 = \Omega_3$ **then return** $(1/\alpha, 0)$. **else if** $P_1 = \Omega_4$ **then return** $(-1/\alpha, 0)$. **else if** $P_1 = (0, -1)$ **then return** Ω_1. **else if** $P_1 = (0, 1)$ **then return** Ω_2. **else if** $P_1 = (1/\alpha, 0)$ **then return** Ω_3. **else if** $P_1 = (-1/\alpha, 0)$ **then return** Ω_4. **else return** $(1/(\alpha\delta x_1), \alpha/(\delta y_1))$.
else if $P_2 = \Omega_3$ **then**
  if $P_1 = \Omega_1$ **then return** $(-1/\alpha, 0)$. **else if** $P_1 = \Omega_2$ **then return** $(1/\alpha, 0)$. **else if** $P_1 = \Omega_3$ **then return** $(0, -1)$. **else if** $P_1 = \Omega_4$ **then return** $(0, 1)$. **else if** $P_1 = (1/\alpha, 0)$ **then return** Ω_1. **else if** $P_1 = (-1/\alpha, 0)$ **then return** Ω_2. **else if** $P_1 = (0, 1)$ **then return** Ω_3. **else if** $P_1 = (0, -1)$ **then return** Ω_4. **else return** $(1/(\delta y_1), -1/(\delta x_1))$.
else if $P_2 = \Omega_4$ **then**
  if $P_1 = \Omega_1$ **then return** $(1/\alpha, 0)$. **else if** $P_1 = \Omega_2$ **then return** $(-1/\alpha, 0)$. **else if** $P_1 = \Omega_3$ **then return** $(0, 1)$. **else if** $P_1 = \Omega_4$ **then return** $(0, -1)$. **else if** $P_1 = (-1/\alpha, 0)$ **then return** Ω_1. **else if** $P_1 = (1/\alpha, 0)$ **then return** Ω_2. **else if** $P_1 = (0, -1)$ **then return** Ω_3. **else if** $P_1 = (0, 1)$ **then return** Ω_4. **else return** $(-1/(\delta y_1), 1/(\delta x_1))$.
else if $(y_1 y_2 + a x_1 x_2)(x_1 y_2 - y_1 x_2) \neq 0$ **then**
  $x_3 \leftarrow (x_1 y_1 + x_2 y_2)/(y_1 y_2 + a x_1 x_2)$.
  $y_3 \leftarrow (x_1 y_1 - x_2 y_2)/(x_1 y_2 - y_1 x_2)$.
  return (x_3, y_3).
else if $(1 - d x_1 x_2 y_1 y_2)(1 + d x_1 x_2 y_1 y_2) \neq 0$ **then**
  $x_3 \leftarrow (x_1 y_2 + y_1 x_2)/(1 + d x_1 x_2 y_1 y_2)$.
  $y_3 \leftarrow (y_1 y_2 - a x_1 x_2)/(1 - d x_1 x_2 y_1 y_2)$.
  return (x_3, y_3).
else
  if $P_2 = (1/(\alpha\delta x_1), -\alpha/(\delta y_1))$ **then return** Ω_1. **else if** $P_2 = (-1/(\alpha\delta x_1), \alpha/(\delta y_1))$ **then return** Ω_2. **else if** $P_2 = (1/(\delta y_1), 1/(\delta x_1))$ **then return** Ω_3. **else return** Ω_4.
end

Projective Group Laws

1. Efficient group laws.
2. New low-degree inversion-free formulae.
3. New and faster algorithms.
4. New coordinate systems. New mixed coordinates.

Example: Twisted Edwards curves

- Initial results from [BL07b] and [BBJ$^+$08].

This work;

- Additional results for homogeneous projective coordinates, $\mathcal{E}$.
- Additional results for inverted coordinates, $\mathcal{E}^i$.
- A new system: Extended homogeneous projective coordinates, $\mathcal{E}^e$.
- A new system: Mixed homogeneous projective coordinates, $\mathcal{E}^x$.
- Dedicated (i.e. non-unified) addition formulae which is faster than the unified (i.e. valid-for-most-doublings) addition formulae.

Review of twisted Edwards addition formulae

$\mathcal{E}$: Projective coordinates, $(aX^2 + Y^2)Z^2 = Z^4 + dX^2Y^2$, $x = X/Z$, $y = Y/Z$, $10\mathbf{M} + 1\mathbf{S} + 2\mathbf{D}$, [BBJ+08]:

$$\begin{aligned} X_3 &= Z_1Z_2(X_1Y_2 + Y_1X_2)(Z_1^2Z_2^2 - dX_1Y_1X_2Y_2) \\ Y_3 &= Z_1Z_2(Y_1Y_2 - aX_1X_2)(Z_1^2Z_2^2 + dX_1Y_1X_2Y_2) \\ Z_3 &= (Z_1^2Z_2^2 - dX_1Y_1X_2Y_2)(Z_1^2Z_2^2 + dX_1Y_1X_2Y_2) \end{aligned}$$

$\mathcal{E}^i$: Inverted coordinates, $(aX^2 + Y^2)Z^2 = dZ^4 + X^2Y^2$, $x = Z/X$, $y = Z/Y$, $9\mathbf{M} + 1\mathbf{S} + 2\mathbf{D}$, [BBJ+08]:

$$\begin{aligned} X_3 &= (X_1X_2 - aY_1Y_2)(X_1Y_1X_2Y_2 + dZ_1^2Z_2^2) \\ Y_3 &= (X_1Y_2 + Y_1X_2)(X_1Y_1X_2Y_2 - dZ_1^2Z_2^2) \\ Z_3 &= Z_1Z_2(X_1X_2 - aY_1Y_2)(X_1Y_2 + Y_1X_2) \end{aligned}$$

- **Observation:** High degree polynomial expressions
- **Our Strategy:** Further lower the degrees by
  - keeping the track of $\frac{XY}{Z}$ separately.

Extended twisted Edwards coordinates, $\mathcal{E}^e$

- Represent each point (x, y) on $ax^2 + y^2 = 1 + dx^2y^2$ as

  $$(X : Y : T : Z) = (\lambda X : \lambda Y : \lambda T : \lambda Z)$$

  for all nonzero $\lambda \in K$ where T has the property $T = XY/Z$.
- Each $(X : Y : T : Z)$ satisfies $(aX^2 + Y^2)Z^2 = Z^4 + dX^2Y^2$.
- $(X : Y : T : Z) + (0 : 1 : 0 : 1) = (X : Y : T : Z)$.
- $-(X : Y : T : Z) = (-X : Y : -T : Z)$.
- Unified addition in $\mathcal{E}^e$:

$$\begin{aligned}
X_3 &= (X_1Y_2 + Y_1X_2)(Z_1Z_2 - dT_1T_2)\\
Y_3 &= (Y_1Y_2 - aX_1X_2)(Z_1Z_2 + dT_1T_2)\\
T_3 &= (Y_1Y_2 - aX_1X_2)(X_1Y_2 + Y_1X_2)\\
Z_3 &= (Z_1Z_2 - dT_1T_2)(Z_1Z_2 + dT_1T_2)
\end{aligned}$$

Unified addition in $\mathcal{E}^e$

$$
\begin{aligned}
X_3 &= (X_1Y_2 + Y_1X_2)(Z_1Z_2 - dT_1T_2)\\
Y_3 &= (Y_1Y_2 - aX_1X_2)(Z_1Z_2 + dT_1T_2)\\
T_3 &= (Y_1Y_2 - aX_1X_2)(X_1Y_2 + Y_1X_2)\\
Z_3 &= (Z_1Z_2 - dT_1T_2)(Z_1Z_2 + dT_1T_2)
\end{aligned}
$$

- A point addition takes $9\mathbf{M} + 2\mathbf{D}$.

$$
A \leftarrow X_1 \cdot X_2, \quad B \leftarrow Y_1 \cdot Y_2, \quad C \leftarrow dT_1 \cdot T_2, \quad D \leftarrow Z_1 \cdot Z_2,
$$
$$
E \leftarrow (X_1 + Y_1) \cdot (X_2 + Y_2) - A - B, \quad F \leftarrow D - C, \quad G \leftarrow D + C,
$$
$$
H \leftarrow B - aA, \quad X_3 \leftarrow E \cdot F, \quad Y_3 \leftarrow G \cdot H, \quad T_3 \leftarrow E \cdot H, \quad Z_3 \leftarrow F \cdot G.
$$

- Complete addition
  - if a is a square in $\mathbb{K}$ and d is not a square in $\mathbb{K}$.

Operation Counts

System	Double	Add
Edwards (c = 1), [BL07a]	3**M**+4**S**	10**M**+1**S**+1**D**
Inverted Edwards (c = 1), [BL07b]	3**M**+4**S**+1**D**	9**M**+1**S**+1**D**
Twisted Edwards, [BBJLP08]	3**M**+4**S**+1**D**	10**M**+1**S**+2**D**
Inverted twisted Edwards, [BBJLP08]	3**M**+4**S**+2**D**	9**M**+1**S**+2**D**
Twisted Edwards, $\mathcal{E}^e$	4**M**+4**S**+1**D**	9**M** +2**D**

Operation Counts

System	Double	Add
Edwards (c = 1), [BL07a]	3**M**+4**S**	10**M**+1**S**+1**D**
Inverted Edwards (c = 1), [BL07b]	3**M**+4**S**+1**D**	9**M**+1**S**+1**D**
Twisted Edwards, [BBJLP08]	3**M**+4**S**+1**D**	10**M**+1**S**+2**D**
Inverted twisted Edwards, [BBJLP08]	3**M**+4**S**+2**D**	9**M**+1**S**+2**D**
Twisted Edwards, $\mathcal{E}^e$	4**M**+4**S**+1**D**	9**M** +2**D**
Twisted Edwards $(a = -1)$, $\mathcal{E}^e$	4**M**+4**S**	8**M** +1**D**

Operation Counts

System	Double	Add
Edwards (c = 1), [BL07a]	3**M**+4**S**	10**M**+1**S**+1**D**
Inverted Edwards (c = 1), [BL07b]	3**M**+4**S**+1**D**	9**M**+1**S**+1**D**
Twisted Edwards, [BBJLP08]	3**M**+4**S**+1**D**	10**M**+1**S**+2**D**
Inverted twisted Edwards, [BBJLP08]	3**M**+4**S**+2**D**	9**M**+1**S**+2**D**
Twisted Edwards, $\mathcal{E}^e$	4**M**+4**S**+1**D**	9**M** +2**D**
Twisted Edwards $(a = -1)$, $\mathcal{E}^e$	4**M**+4**S**	8**M** +1**D**

$$
\begin{gathered}
A \leftarrow (Y_1 - X_1) \cdot (Y_2 - X_2), \quad B \leftarrow (Y_1 + X_1) \cdot (Y_2 + X_2), \\
C \leftarrow 2d\,T_1 \cdot T_2, \quad D \leftarrow 2Z_1 \cdot Z_2, \quad E \leftarrow B - A, \quad F \leftarrow D - C, \\
G \leftarrow D + C, \quad H \leftarrow B + A, \quad X_3 \leftarrow E \cdot F, \quad Y_3 \leftarrow G \cdot H, \\
T_3 \leftarrow E \cdot H, \quad Z_3 \leftarrow F \cdot G
\end{gathered}
$$

Operation Counts

System	Double	Add
Edwards (c = 1), [BL07a]	3**M**+4**S**	10**M**+1**S**+1**D**
Inverted Edwards (c = 1), [BL07b]	3**M**+4**S**+1**D**	9**M**+1**S**+1**D**
Twisted Edwards, [BBJLP08]	3**M**+4**S**+1**D**	10**M**+1**S**+2**D**
Inverted twisted Edwards, [BBJLP08]	3**M**+4**S**+2**D**	9**M**+1**S**+2**D**
Twisted Edwards, $\mathcal{E}^e$	4**M**+4**S**+1**D**	9**M** +2**D**
Twisted Edwards $(a = -1)$, $\mathcal{E}^e$	4**M**+4**S**	8**M** +1**D**
Twisted Edwards $(a = -1)$, $\mathcal{E}^x$	3**M**+4**S**	8**M** +1**D**

$\mathcal{E}^x$: Mixing $\mathcal{E}^e$ with $\mathcal{E}$.

- For repeated doublings, use $\mathcal{E} \leftarrow 2\mathcal{E}$.
- If a doubling is followed by an addition, use
  1. $\mathcal{E}^e \leftarrow 2\mathcal{E}$ for the doubling step; followed by,
  2. $\mathcal{E} \leftarrow \mathcal{E}^e + \mathcal{E}^e$ for the addition step.

Further Optimizations: Alternative formulae

- The affine point addition formulae dependent upon a and d in [BBJLP08] given by

$$(x_1, y_1), (x_2, y_2) \mapsto \left(\frac{x_1 y_2 + y_1 x_2}{1 + d x_1 x_2 y_1 y_2}, \frac{y_1 y_2 - a x_1 x_2}{1 - d x_1 x_2 y_1 y_2} \right).$$

- However we can use alternative formulae independent of d given by

$$(x_1, y_1), (x_2, y_2) \mapsto \left(\frac{x_1 y_1 + x_2 y_2}{y_1 y_2 + a x_1 x_2}, \frac{x_1 y_1 - x_2 y_2}{x_1 y_2 - y_1 x_2} \right).$$

Example: Twisted Edwards curves

- The explicit dedicated addition formulae are then given by

$$
\begin{aligned}
X_3 &= (X_1Y_2 - Y_1X_2)(T_1Z_2 + Z_1T_2),\\
Y_3 &= (Y_1Y_2 + aX_1X_2)(T_1Z_2 - Z_1T_2),\\
T_3 &= (T_1Z_2 + Z_1T_2)(T_1Z_2 - Z_1T_2),\\
Z_3 &= (Y_1Y_2 + aX_1X_2)(X_1Y_2 - Y_1X_2).
\end{aligned}
$$

- A point addition costs $9\mathbf{M} + 1\mathbf{D}$. Saves an extra $1\mathbf{D}$ over the original formulae.
- A point addition with $a = -1$ costs $8\mathbf{M}$. Saves an extra $1\mathbf{D}$ over the original formulae.
- Use base points of odd order to prevent exception handling.

Operation Counts

System	Double	Add
Edwards, [BL07a]	3**M**+4**S**	10**M**+1**S**+1**D**
Inverted Edwards, [BL07b]	3**M**+4**S**+1**D**	9**M**+1**S**+1**D**
Twisted Edwards, [BBJLP08]	3**M**+4**S**+1**D**	10**M**+1**S**+2**D**
Inverted twisted Edwards, [BBJLP08]	3**M**+4**S**+2**D**	9**M**+1**S**+2**D**
Twisted Edwards, $\mathcal{E}^e$	4**M**+4**S**+1**D**	9**M** +2**D**
Twisted Edwards ($a = -1$), $\mathcal{E}^e$	4**M**+4**S**	8**M** +1**D**
Twisted Edwards ($a = -1$), $\mathcal{E}^x$	3**M**+4**S**	8**M** +1**D**
Twisted Edwards ($a = -1$), $\mathcal{E}^x$	3**M**+4**S**	8**M**

- $(X_1 : Y_1 : T_1 : Z_1) + (X_2 : Y_2 : T_2 : 1)$ costs only 7**M**.

Operation Counts

Table: Operation counts for extended Jacobi quartic form with $a = -1/2$ in different coordinate systems.

System	DBL	ADD
$\mathcal{Q}^w$	-	10**M**+2**S**+2**D**+14**a**, unified, [BJ03]
$\mathcal{Q}$	3**M**+4**S**+ 4**a**	10**M**+7**S**+2**D**+17**a**, unified
	2**M**+5**S**+ 7**a**	10**M**+5**S**+1**D**+10**a**, dedicated
$\mathcal{Q}^e$	3**M**+5**S**+ 4**a**	8**M**+3**S**+2**D**+17**a**, unified
	8**S**+13**a**	7**M**+3**S**+1**D**+19**a**, dedicated
$\mathcal{Q}^x$	3**M**+4**S**+ 4**a**	7**M**+4**S**+3**D**+19**a**, unified
	2**M**+5**S**+ 7**a**	6**M**+4**S**+2**D**+21**a**, dedicated

$\mathcal{Q}^w$: Weighted, $\mathcal{Q}$: Projective, $\mathcal{Q}^e$: Extended, $\mathcal{Q}^x$: Mixed coordinates.

Operation Counts

Table: Operation counts for (twisted) Jacobi intersection form with $b = 1$ in different coordinate systems.

System	DBL	ADD
$\mathcal{I}$	3**M**+4**S** +6**a**, [BL07a] 2**M**+5**S**+1**D**+7**a**	13**M**+2**S**+1**D**+ 7**a**, unified, [LS01] 13**M**+1**S**+2**D**+15**a**, unified 12**M** +11**a**, dedicated
$\mathcal{I}^{m2}$	-	11**M**+1**S**+2**D**+15**a**, unified
$\mathcal{I}^{m1}$	3**M**+4**S** +6**a**, * 2**M**+5**S**+1**D**+7**a**	11**M** + 9**a**, dedicated -

*: Adapted from [BL07a, dbl-2007-bl].

$\mathcal{I}$: Projective, $\mathcal{I}^{m1}$: Modified version 1, $\mathcal{I}^{m2}$: Modified version 2 coordinates.

Operation Counts

Table: Operation counts for (twisted) Hessian form with $a = 1$ in different coordinate systems.

System	DBL	ADD
$\mathcal{H}$	6**M**+3**S**+ 3**a**, [BKL09]	12**M** + 3**a**, unified, [BKL09]
	7**M**+1**S**+ 8**a**	11**M** +17**a**, unified
	3**M**+6**S**+18**a**	12**M** + 3**a**, dedicated
		11**M** +17**a**, dedicated
$\mathcal{H}^e$	9**M**+3**S**+ 3**a**	9**M**+3**S**+ 3**a**, unified
		9**M**+3**S**+ 3**a**, dedicated
	5**M**+6**S**+29**a**	6**M**+6**S**+15**a**, unified
		6**M**+6**S**+15**a**, dedicated

$\mathcal{H}$: Projective, $\mathcal{H}^m$: Modified, $\mathcal{H}^e$: Extended, $\mathcal{H}^x$ Mixed coordinates.

Operation Counts

Table: Operation counts for short Weierstrass form with $a = -3$ in different coordinate systems.

System	DBL	ADD
$\mathcal{P}$, [CC86]	7**M**+3**S**+10**a**, [BL07a]	12**M**+ 5**S**+1**D**+10**a**, unified, [BJ02] 11**M**+ 6**S**+1**D**+15**a**, unified, [BL07a] 11**M**+ 5**S**+1**D**+16**a**, unified 12**M**+ 2**S** + 7**a**, dedicated, [CMO98]
$\mathcal{J}$, [CC86]	4**M**+4**S**+ 9**a**, [HMV03] 3**M**+5**S**+12**a**, [BL07a]	8**M**+10**S**+1**D**+24**a**, unified 12**M**+ 4**S** + 7**a**, dedicated, [CMO98] 11**M**+ 5**S** +11**a**, dedicated, [BL07a]
$\mathcal{J}^c$, [CC86]	4**M**+6**S**+ 4**a**, [CMO98]	7**M**+ 9**S**+1**D**+24**a**, unified 11**M**+ 3**S** + 7**a**, dedicated, [CMO98] 10**M**+ 4**S** +13**a**, dedicated, [BL07a]

$\mathcal{P}$: Projective, $\mathcal{J}$: Jacobian, $\mathcal{J}^c$: Chudnovsky Jacobian.

Table: Sample elliptic curves over $\mathbb{F}_{2^{256}-587}$.

Curve	Equation	h
Short Weierstrass, $E_{\mathbf{S}}$	$y^2 = x^3 - 3x + 2582$	1
Extended Jacobi quartic, $E_{\mathbf{Q}}$	$y^2 = 25629x^4 - x^2 + 1$	2
(Twisted) Hessian, $E_{\mathbf{H}}$	$x^3 + y^3 + 1 = 53010xy$	3
Twisted Edwards, $E_{\mathbf{E}}$	$-x^2 + y^2 = 1 + 3763x^2y^2$	4
(Twisted) Jacobi intersection, $E_{\mathbf{I}}$	$s^2 + c^2 = 1,\ 3764s^2 + d^2 = 1$	4

SMUL

- Scalar MULtiplication: Algorithm 3.38 in [HMV03].
- The integer recoding part of the scalar multiplication: w-LtoR algorithm in [Ava05].
  - Runs on-the-fly as the main loop of the scalar multiplication is performed.
- Look-up table: $3P, 5P, \ldots, 31P$.
  - All points are kept in extended projective coordinates.

SMUL

Table: Cycle-counts (rounded to the nearest one thousand) for 256-bit scalar multiplication with variable base-point (for Core 2).

Curve & coordinate system	**Approximate operation counts**	**Cycles**
Short Weierstrass ($a = -3$), $\mathcal{J}$	$\mathbf{I}$+1598$\mathbf{M}$+1156$\mathbf{S}$+ 0 $\mathbf{D}$+2896$\mathbf{a}$	468,000
(Twisted) Hessian ($a = 1$), $\mathcal{H}$	$\mathbf{I}$+2093$\mathbf{M}$+ 757 $\mathbf{S}$+ 0 $\mathbf{D}$+1177$\mathbf{a}$	447,000
(Twisted) Jacobi intersection ($b = 1$), $\mathcal{I}^{m1}$	$\mathbf{I}$+1295$\mathbf{M}$+1011$\mathbf{S}$+ 0 $\mathbf{D}$+2009$\mathbf{a}$	383,000
Extended Jacobi quartic ($a = -1/2$), $\mathcal{Q}^x$	$\mathbf{I}$+1162$\mathbf{M}$+1110$\mathbf{S}$+102$\mathbf{D}$+1796$\mathbf{a}$	376,000
Twisted Edwards ($a = -1$), $\mathcal{E}^x$	$\mathbf{I}$+1202$\mathbf{M}$+ 969 $\mathbf{S}$+ 0 $\mathbf{D}$+2025$\mathbf{a}$	362,000

Note: Short Weierstrass ($a = -3$) was the fastest before 2006!

Table: Cycle-counts (rounded to the nearest one thousand) for 256-bit scalar multiplication with fixed base-point (for Core 2).

Curve & coordinate system	**Look-up**	**Cycles**
Short Weierstrass ($a = -3$), $\mathcal{J}$	2 KB $\times$ 2	138,000
	8 KB $\times$ 2	121,000
	16 KB $\times$ 2	102,000
	32 KB $\times$ 2	92,000
	64 KB $\times$ 2	86,000
Twisted Edwards ($a = -1$), $\mathcal{E}^e$	2 KB $\times$ 2	124,000
	8 KB $\times$ 2	109,000
	16 KB $\times$ 2	92,000
	32 KB $\times$ 2	82,000
	64 KB $\times$ 2	79,000

Summary

The main aim is revisiting the elliptic curve group law with an emphasis on *more* efficient point additions.

To achieve this aim the research is split into the following successive tasks:

- Collected algebraic tools in order to find maps between curves,
- Developed computer algebra tools to automate the group law derivation using the derived maps and the well-known group law of Weierstrass form elliptic curves,
- Found a systematic way of simplifying rational expressions to make a “simple” statement of the group law,

...

Summary

- Developed an algorithm for each form in order to make a complete description of the group law by appropriately handling all possible cases.
- Developed inversion-free algorithms in various coordinate systems for each form and comparing each coordinate system in terms of efficiency in suitable contexts.
- Developed optimized high-speed software implementations in order to support theoretical results.

Published Material

1 Huseyin Hisil, Gary Carter, and Ed Dawson. New formulae for efficient elliptic curve arithmetic. In *INDOCRYPT 2007*, volume 4859 of *LNCS*, pages 138–151. Springer, 2007.

2 Huseyin Hisil, Kenneth Koon-Ho Wong, Gary Carter, and Ed Dawson. Faster group operations on elliptic curves. In *Australasian Information Security Conference (AISC 2009), Wellington, New Zealand, January 2009*, volume 98, pages 11–19. Conferences in Research and Practice in Information Technology (CRPIT), 2009.

3 Huseyin Hisil, Kenneth Koon-Ho Wong, Gary Carter, and Ed Dawson. Twisted Edwards curves revisited. In *ASIACRYPT 2008*, volume 5350 of *LNCS*, pages 326–343. Springer, 2008.

4 Huseyin Hisil, Kenneth Koon-Ho Wong, Gary Carter, and Ed Dawson. Jacobi quartic curves revisited. In *ACISP 2009*, volume 5594 of *LNCS*, pages 452–468. Springer, 2009.

Thanks.

Roberto M. Avanzi, *A note on the signed sliding window integer recoding and its left-to-right analogue*, SAC 2004, LNCS, vol. 3357, Springer, 2005, pp. 130–143.

Daniel J. Bernstein, Peter Birkner, Marc Joye, Tanja Lange, and Christiane Peters, *Twisted Edwards curves*, AFRICACRYPT 2008, LNCS, vol. 5023, Springer, 2008, pp. 389–405.

Eric Brier and Marc Joye, *Weierstraß elliptic curves and side-channel attacks*, PKC 2002, LNCS, vol. 2274, Springer, 2002, pp. 335–345.

Olivier Billet and Marc Joye, *The Jacobi model of an elliptic curve and side-channel analysis*, AAECC-15, LNCS, vol. 2643, Springer, 2003, pp. 34–42.

Daniel J. Bernstein, David Kohel, and Tanja Lange, *Twisted Hessian curves*, Explicit-Formulas Database, 2009, `http://www.hyperelliptic.org/EFD/g1p/auto-twistedhe`

- Daniel J. Bernstein and Tanja Lange, *Explicit-formulas database*, 2007, `http://www.hyperelliptic.org/EFD`.
- ______, *Faster addition and doubling on elliptic curves*, ASIACRYPT 2007, LNCS, vol. 4833, Springer, 2007, pp. 29–50.
- David V. Chudnovsky and Gregory V. Chudnovsky, *Sequences of numbers generated by addition in formal groups and new primality and factorization tests*, Advances in Applied Mathematics **7** (1986), no. 4, 385–434.
- Henri Cohen, Atsuko Miyaji, and Takatoshi Ono, *Efficient elliptic curve exponentiation using mixed coordinates*, ASIACRYPT'98, LNCS, vol. 1514, Springer, 1998, pp. 51–65.
- Darrel Hankerson, Alfred J. Menezes, and Scott A. Vanstone, *Guide to elliptic curve cryptography*, Springer-Verlag New York, Inc., Secaucus, NJ, USA, 2003.

Pierre Yvan Liardet and Nigel P. Smart, *Preventing SPA/DPA in ECC systems using the Jacobi form.*, CHES 2001, LNCS, vol. 2162, Springer, 2001, pp. 391–401.