Binary Edwards Curves in Elliptic Curve Cryptography

Graham Enos

UNC Charlotte Department of Mathematics and Statistics

Dissertation Defense, March 29, 2013

Outline

Motivation

Edwards curves are extremely useful for cryptography; they offer better safety from the ground up.
Less work has been done on binary Edwards curves.

Contributions

In this dissertation, we

Contributions

In this dissertation, we

1. show that binary Edwards curves are safer than some other recently proposed normal forms

Contributions

In this dissertation, we

1. show that binary Edwards curves are safer than some other recently proposed normal forms
2. calculate pairings on binary Edwards curves

Contributions

In this dissertation, we

1. show that binary Edwards curves are safer than some other recently proposed normal forms
2. calculate pairings on binary Edwards curves
3. give two new cryptographic applications of binary Edwards curves

Contributions

In this dissertation, we

1. show that binary Edwards curves are safer than some other recently proposed normal forms
2. calculate pairings on binary Edwards curves
3. give two new cryptographic applications of binary Edwards curves
4. construct e2c2, a modern C++11 library for Edwards elliptic curve cryptography

Contributions

In this dissertation, we

1. show that binary Edwards curves are safer than some other recently proposed normal forms
2. calculate pairings on binary Edwards curves
3. give two new cryptographic applications of binary Edwards curves
4. construct e2c2, a modern C++11 library for Edwards elliptic curve cryptography

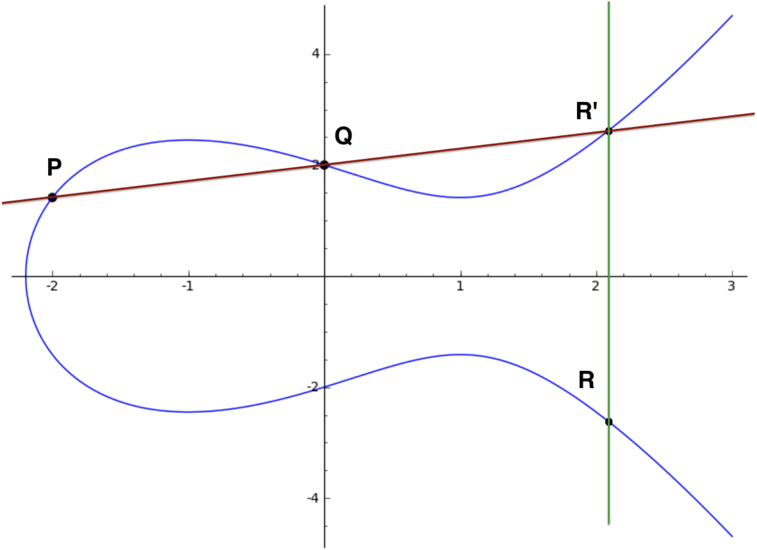
First: some background on elliptic curves, cryptography, and Edwards curves

Elliptic Curves and Cryptography

In the 80s, Koblitz and Miller proposed using the group of points on an elliptic curve as the basis for public key cryptography.

- They offer strong security for much smaller key sizes.
- They have a nice geometric description of the group law.

Weierstrass Group Law



Side-Channel Worries

However, there are some issues. . .

Side-Channel Worries

However, there are some issues...

- What if $P = \infty$? What if $Q = \infty$?

Side-Channel Worries

However, there are some issues...

- What if $P = \infty$? What if $Q = \infty$?
- What if $P = Q$?

Side-Channel Worries

However, there are some issues...

- What if $P = \infty$? What if $Q = \infty$?
- What if $P = Q$?
- What if $P.x = Q.x = 0$?

Side-Channel Worries

However, there are some issues...

- What if $P = \infty$? What if $Q = \infty$?
- What if $P = Q$?
- What if $P.x = Q.x = 0$?
- What if $P = -Q$?

Side-Channel Worries

However, there are some issues...

- What if $P = \infty$? What if $Q = \infty$?
- What if $P = Q$?
- What if $P.x = Q.x = 0$?
- What if $P = -Q$?

The group law has to check for all of these.

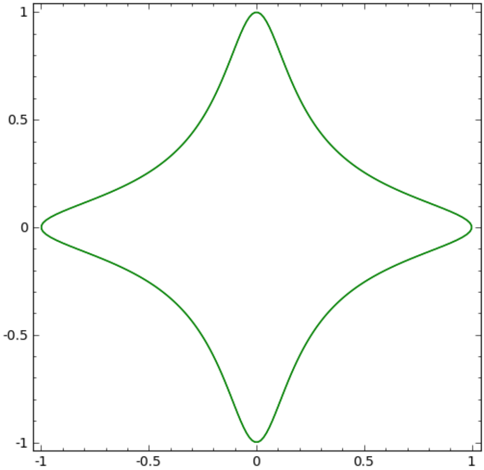
Edwards Curves

Edwards gave a new normal form in 2007, which was then extended by Bernstein and Lange:

$$E_{O,c,d}: \quad x^2 + y^2 = c^2(1 + dx^2y^2)$$

such that $cd(1 - dc^4) \neq 0$.

Edwards Curves



Edwards ECC

Complete and unified group law

Edwards ECC

Complete and unified group law

$\Longrightarrow$ No special cases (doubling, identity element, etc.)

Edwards ECC

Complete and unified group law

$\Longrightarrow$ No special cases (doubling, identity element, etc.)

$\Longrightarrow$ Less prone to side-channel attacks

Edwards ECC

Complete and unified group law

$\Longrightarrow$ No special cases (doubling, identity element, etc.)

$\Longrightarrow$ Less prone to side-channel attacks

$\therefore$ Safer from the ground up

Twisted Edward Curves

These are quadratic twists of Edwards curves, cover more cases; more work is done with them nowadays.
Their group law is also unified and complete.

Characteristic Two

Those were only defined over fields of characteristic $\neq 2$.
Characteristic 2 is nice from an implementation standpoint.
Bernstein et.al. to the rescue!

Binary Edwards Curves

$$E_{B,d_1,d_2}: \quad d_1(x+y)+d_2(x^2+y^2)=xy(x+1)(y+1)$$

If the field's defining polynomial has degree ≥ 3, all binary elliptic curves are birationally equivalent over the base field to a complete binary Edwards curve.

Binary Edwards Group Law

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

$$
\begin{aligned}
x_3 &= \frac{N_x}{D_x} \\
y_3 &= \frac{N_y}{D_y} \\
N_x &= d_1(x_1 + x_2) + d_2(x_1 + y_1)(x_2 + y_2) + \\
&\quad (x_1 + x_1^2)(x_2(y_1 + y_2 + 1) + y_1 y_2) \\
D_x &= d_1 + (x_1 + x_1^2)(x_2 + y_2) \\
N_y &= d_1(y_1 + y_2) + d_2(x_1 + y_1)(x_2 + y_2) + \\
&\quad (y_1 + y_1^2)(y_2(x_1 + x_2 + 1) + x_1 x_2) \\
D_y &= d_1 + (y_1 + y_1^2)(x_2 + y_2)
\end{aligned}
$$

Binary Edwards Group Law

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

$$
\begin{aligned}
x_3 &= \frac{N_x}{D_x} \\
y_3 &= \frac{N_y}{D_y} \\
N_x &= d_1(x_1 + x_2) + d_2(x_1 + y_1)(x_2 + y_2) + \\
&\quad (x_1 + x_1^2)(x_2(y_1 + y_2 + 1) + y_1 y_2) \\
D_x &= d_1 + (x_1 + x_1^2)(x_2 + y_2) \\
N_y &= d_1(y_1 + y_2) + d_2(x_1 + y_1)(x_2 + y_2) + \\
&\quad (y_1 + y_1^2)(y_2(x_1 + x_2 + 1) + x_1 x_2) \\
D_y &= d_1 + (y_1 + y_1^2)(x_2 + y_2)
\end{aligned}
$$

complete and unified

New Normal Forms

More normal forms have been recently proposed claiming unified and complete group laws.

New Normal Forms

More normal forms have been recently proposed claiming unified and complete group laws.
Most of them are, but only modulo the ideal generated by the curve equation.

New Normal Forms

More normal forms have been recently proposed claiming unified and complete group laws.

Most of them are, but only modulo the ideal generated by the curve equation.

All three types of Edwards have a simple neutral element and a symmetric group law; no need to reduce modulo an ideal.

Farashahi & Joye

$$\mathbf{H}_{c,d}: \quad X^3 + Y^3 + cZ^3 = dXYZ$$

Suppose we let $P = (X_1 : Y_1 : Z_1)$ and $Q = (X_2 : Y_2 : Z_2)$

Farashahi & Joye

$P + Q = (X_3 : Y_3 : Z_3)$, where

$$X_3 = cY_2Z_1^2Z_2 - X_1X_2^2Y_1$$
$$Y_3 = X_2Y_1^2Y_2 - cX_1Z_1Z_2^2$$
$$Z_3 = X_1^2X_2Z_2 - Y_1Y_2^2Z_1$$

Farashahi & Joye

$P + Q = (X_3 : Y_3 : Z_3)$, where

$$X_3 = cY_2Z_1^2Z_2 - X_1X_2^2Y_1$$
$$Y_3 = X_2Y_1^2Y_2 - cX_1Z_1Z_2^2$$
$$Z_3 = X_1^2X_2Z_2 - Y_1Y_2^2Z_1$$

but $Q + P = (X_4 : Y_4 : Z_4)$, such that

$$X_4 = cY_1Z_1Z_2^2 - X_1^2X_2Y_2$$
$$Y_4 = X_1Y_1Y_2^2 - cX_2Z_1^2Z_2$$
$$Z_4 = X_1X_2^2Z_1 - Y_1^2Y_2Z_2$$

Farashahi & Joye

$P + Q = (X_3 : Y_3 : Z_3)$, where

$$X_3 = cY_2Z_1^2Z_2 - X_1X_2^2Y_1$$
$$Y_3 = X_2Y_1^2Y_2 - cX_1Z_1Z_2^2$$
$$Z_3 = X_1^2X_2Z_2 - Y_1Y_2^2Z_1$$

but $Q + P = (X_4 : Y_4 : Z_4)$, such that

$$X_4 = cY_1Z_1Z_2^2 - X_1^2X_2Y_2$$
$$Y_4 = X_1Y_1Y_2^2 - cX_2Z_1^2Z_2$$
$$Z_4 = X_1X_2^2Z_1 - Y_1^2Y_2Z_2$$

Asymmetry of group law $\implies$ need to reduce modulo the equation for $\mathbf{H}_{c,d}$

Wang, Tang, & Yang

$$\widetilde{M_d}: \quad X^2Y + XY^2 + dXYZ + Z^3 = 0$$

Wang, Tang, & Yang

$$\widetilde{M_d}: \quad X^2Y + XY^2 + dXYZ + Z^3 = 0$$

Arithmetic is quite flawed...

Wu, Tang, & Feng

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

Neutral element: $\mathcal{O} = (1 : 1 : 0)$

Wu, Tang, & Feng

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

Neutral element: $\mathcal{O} = (1 : 1 : 0)$

Unusual choice of neutral element $\implies$ need to reduce modulo curve equation to see that $P + \mathcal{O} = P$

Diao & Fouotsa

$$\mathcal{E}_\lambda : 1 + x^2 + y^2 + x^2y^2 = \lambda xy$$

Diao & Fouotsa

$$\mathcal{E}_\lambda : 1 + x^2 + y^2 + x^2y^2 = \lambda xy$$

Addition:

$$(x_1, y_1) + (x_2, y_2) = \left(\frac{x_1 + y_1x_2y_2}{y_2 + x_1y_1x_2}, \frac{x_1x_2 + y_1y_2}{1 + x_1x_2y_1y_2} \right)$$

while

$$(x_2, y_2) + (x_1, y_1) = \left(\frac{x_2 + x_1y_1y_2}{y_1 + x_1x_2y_2}, \frac{x_1x_2 + y_1y_2}{1 + x_1x_2y_1y_2} \right)$$

Diao & Fouotsa

$$\mathcal{E}_\lambda : 1 + x^2 + y^2 + x^2y^2 = \lambda xy$$

Addition:

$$(x_1, y_1) + (x_2, y_2) = \left(\frac{x_1 + y_1x_2y_2}{y_2 + x_1y_1x_2}, \frac{x_1x_2 + y_1y_2}{1 + x_1x_2y_1y_2} \right)$$

while

$$(x_2, y_2) + (x_1, y_1) = \left(\frac{x_2 + x_1y_1y_2}{y_1 + x_1x_2y_2}, \frac{x_1x_2 + y_1y_2}{1 + x_1x_2y_1y_2} \right)$$

asymmetric group law

Diao & Fouotsa

$$\mathcal{E}_\lambda : 1 + x^2 + y^2 + x^2y^2 = \lambda xy$$

Addition:

$$(x_1, y_1) + (x_2, y_2) = \left(\frac{x_1 + y_1x_2y_2}{y_2 + x_1y_1x_2}, \frac{x_1x_2 + y_1y_2}{1 + x_1x_2y_1y_2} \right)$$

while

$$(x_2, y_2) + (x_1, y_1) = \left(\frac{x_2 + x_1y_1y_2}{y_1 + x_1x_2y_2}, \frac{x_1x_2 + y_1y_2}{1 + x_1x_2y_1y_2} \right)$$

asymmetric group law

Binary Edwards curves are still king!

Pairings and Cryptography

Pairings are bilinear forms over elliptic curves.

They've proven useful in cryptography, e.g. "MOV attack" and "Boneh-Franklin ID-based encryption."

Some work's been done on pairings for twisted Edwards curves, but not binary.

Pairings and Cryptography

Pairings are bilinear forms over elliptic curves.

They've proven useful in cryptography, e.g. "MOV attack" and "Boneh-Franklin ID-based encryption."

Some work's been done on pairings for twisted Edwards curves, but not binary.

Their calculation hinges on finding a *Miller function* f with appropriate divisor $div_P(f) = n(P) - n(\mathcal{O})$.

Following Das & Sarkar

Idea: map from E_{B,d_1,d_2} to a Weierstrass curve, compute the pairing there, then map back

Following Das & Sarkar

Idea: map from E_{B,d_1,d_2} to a Weierstrass curve, compute the pairing there, then map back

Theorem

Let $P_1, P_2 \in E_{B,d_1,d_2}$ such that $P_1 + P_2 = P_3$; then the Miller function $h(x, y)$ such that

$$div(h) = (P_1) + (P_2) - (P_3) - \mathcal{O}$$

is given by $\frac{N}{D}$, where

$$D = (u1 + u2)(u_3 d_1(d_1 XZ + d_1 YZ + XY) + \sqrt{a_6} Z(X + Y))$$

Das & Sarkar, continued

$P_1 \neq P_2 \implies$

$$\begin{aligned} N = {} & Z(X+Y)d_1^2(v_1u_2 + u_1v_2 + u_1\sqrt{a_6} + u_2\sqrt{a_6}) \\ & + \sqrt{a_6}(u_1+u_2)d_1(XY+XZ+YZ) \\ & + YXd_1(v_1u_2+u_1v_2) \\ & + \sqrt{a_6}(XZu_1b + YZu_1b + XZu_2b + YZu_2b \\ & + XYu_1 + XZu_1 + XZv_1 + YZv_1 + XYu_2 + XZu_2 \\ & + XZv_2 + YZv_2) \end{aligned}$$

$P_1 = P_2 \implies$

$$\begin{aligned} N = {} & u_1Z(X+Y)d_1^2(u_1^2 + \sqrt{a_6}) \\ & + u_1d_1(XYu_1^2 + XY\sqrt{a_6} + XZ\sqrt{a_6} + YZ\sqrt{a_6}) \\ & + \sqrt{a_6}(XZu_1^2 + YZu_1^2 + XZu_1b + YZu_1b \\ & + XYu_1 + XZu_1 + XZv_1 + YZv_1) \end{aligned}$$

Directions for Future Work

Arène et.al. gave a new geometric interpretation of the twisted group law $\implies$ calculation of pairings on $E_{T,a,d}$ directly.
We'd like to do the same for E_{B,d_1,d_2}, but the geometry is different...
We give a theorem that's (hopefully) a step in the right direction.

Following Arène et.al.

Theorem

Let $P_1, P_2 \in E_{B,d_1,d_2}(K)$ be two affine, not necessarily distinct, points. Let C be the conic passing through $\Omega_1, \Omega_2, \mathcal{O}', P_1$, and P_2 which must have the form

$$c_{XY}(XY + Z^2) + c_{XZ}(XZ + Z^2) + c_{YZ}(YZ + Z^2)$$

(If some of the above points are equal, we consider C and E_{B,d_1,d_2} to intersect with at least that multiplicity at the corresponding point.) Then the coefficients of the conic C are uniquely determined (up to scalars) as follows:

Arène et.al., continued

1. $P_1 \neq P_2, P_1 \neq \mathcal{O}', P_2 \neq \mathcal{O}' \implies$

$$
\begin{aligned}
c_{XY} &= Z_1 Z_2 \left[X_1(Y_2 + Z_2) + Y_1(X_2 + Z_2) + Z_1(X_2 + Y_2)\right] \\
c_{XZ} &= Y_1 Z_2(X_1 Y_2 + X_1 Z_2 + Z_1 Z_2) \\
&\quad + Y_2 Z_1(Y_1 X_1 + Z_1 X_1 + Z_1 Z_2) \\
c_{YZ} &= X_1 Z_2(Y_1 X_2 + Y_1 Z_2 + Z_1 Z_1) \\
&\quad + X_2 Z_1(X_1 Y_2 + Z_1 Y_2 + Z_1 Z_2)
\end{aligned}
$$

2. $P_1 \neq P_2 = \mathcal{O}' \implies c_{XY} = Z_1, c_{XZ} = Z_1, c_{YZ} = X_1$
3. $P_1 = P_2 \implies$

$$
\begin{aligned}
c_{XY} &= X_1^2 Y_1 + X_1 Y_1^2 + d_1 X_1 Z_1^2 + X_1^2 Z_1 + d_1 Y_1 Z_1^2 \\
&\quad + Y_1^2 Z_1 + X_1 Z_1^2 + Y_1 Z_1^2 \\
c_{XZ} &= X_1^2 Y_1 + d_1 Y_1^2 Z_1 + X_1 Y_1^2 + d_1 X_1 Z_1^2 + X_1^2 Z_1 \\
&\quad + d_1 Y_1 Z_1^2 + X_1 Y_1 Z_1 + d_1 Z_1^3 + Y_1 Z_1^2 \\
c_{YZ} &= d_1 X_1^2 Z_1 + d_2 X_1^2 Z_1 + d_2 Y_1^2 Z_1 + X_1^2 Z_1 + d_1 Z_1^3 + X_1 Z_1^2
\end{aligned}
$$

E_{B,d_1,d_2} in Cryptography

We offer two applications of binary Edwards curves:

1. `ECOH's Echo`, a PBKDF
2. A compartmented id-based secret sharing scheme with un/signcryption

`ECOH`'s Echo

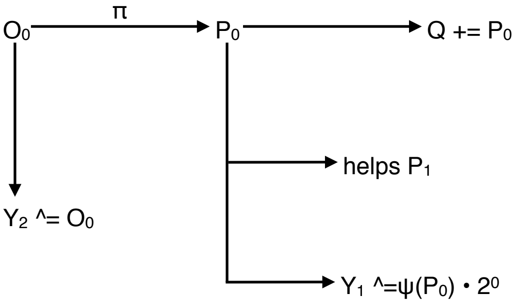
This is a scalable PBKDF, for which we can increase computation time as computers get faster.

We modify `ECOH`, entrant to the SHA-3 competition.

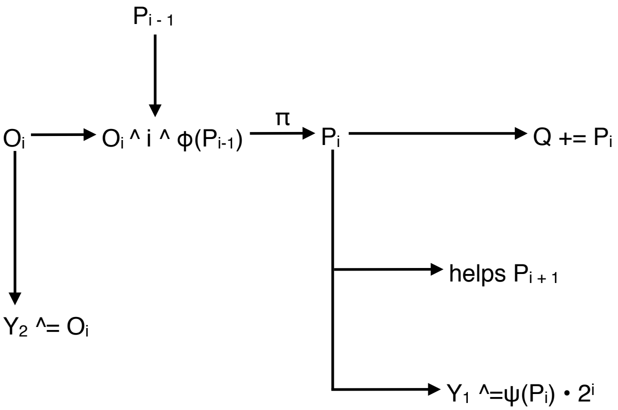
Fixing its main issue, a second preimage attack, in turn leads to resistance to parallelization.

We build up Q from input, taking into account output of each previous step.

ECOH's Echo, First Round



ECOH's Echo, Subsequent Rounds



ECOH's Echo, Finish

Finally,

$$
\begin{aligned}
X_1 &\leftarrow \pi(Y_1) \\
X_2 &\leftarrow \pi\left(Y_1 \oplus Y_2\right) \\
Q &\leftarrow Q + X_1 + X_2
\end{aligned}
$$

Return $\varphi(Q)$

Compartmented ID-Based Secret Sharing and Signcryption

My scheme extends a *secret sharing* (send a message to n entities in such a way that t of them must cooperate to put it back together) to a *compartmented scheme* (send a message to an organization broken into t compartments, one representative of each must cooperate).

Compartmented ID-Based Secret Sharing and Signcryption

My scheme extends a *secret sharing* (send a message to n entities in such a way that t of them must cooperate to put it back together) to a *compartmented scheme* (send a message to an organization broken into t compartments, one representative of each must cooperate).

It involves *signcryption* so each compartment can verify the cooperation of the others and the signature of the original sender.

Compartmented ID-Based Secret Sharing and Signcryption

My scheme extends a *secret sharing* (send a message to n entities in such a way that t of them must cooperate to put it back together) to a *compartmented scheme* (send a message to an organization broken into t compartments, one representative of each must cooperate).

It involves *signcryption* so each compartment can verify the cooperation of the others and the signature of the original sender.

Its cryptography is based on pairings.

e2c2

In order to explore the theory and implementation of Edwards curves for elliptic curve cryptography, I've created a modern C++11 software library called `e2c2`.

It tries to bridge the gap between "proof-of-concept" and "production-ready."

It's certainly not ready for cryptographic primetime, but it gets quite decent speed, even on my puny laptop, and the security afforded by the simplicity of implementing Edwards curves is very advantageous.

Interlude

e2c2 demonstration

Contributions

To sum up, we saw

1. that binary Edwards curves are safer than some other recently proposed normal forms
2. how to calculate pairings on binary Edwards curves
3. (a glimpse of) two new cryptographic applications of binary Edwards curves
4. a demonstration of `e2c2`, a modern C++11 library for Edwards elliptic curve cryptography

Publication Hopes

I'm pursuing publication of some of this work

1. Chapter 4 is online `http://eprint.iacr.org/2013/015`, and has been submitted to *IACR's CRYPTO2013* conference
2. I'm in the process of revising a paper on the compartmented sharing scheme per reviewers' comments from the *Information Processing Letters*; see `http://eprint.iacr.org/2012/528` for a previous version
3. Recently a password hashing contest has been announced, see `https://password-hashing.net/`, and Dr. Zheng and I are hoping to submit `ECOH's Echo`

Thanks

Many thanks to Dr. Zheng, Dr. Hetyei, rest of my defense committee, UNCC Math Department.

Questions

Any questions?