Edwards Curves and the ECM Factorisation Method

Peter Birkner

Department of Mathematics and Computer Science
Coding Theory and Cryptography, TU/e

EIDMA Cryptography Working Group
15 February 2008

Joint work with Daniel J. Bernstein, Tanja Lange, Christiane Peters
Outline

1. What is ECM and how does it work?
2. What is an Edwards curve?
3. How can Edwards curves make ECM faster?
Pollard’s p-1 Method (1)

**Problem:** Find a prime factor $p$ of the composite integer $N$.

- **Fermat’s little theorem.** $a^{p-1} \equiv 1 \pmod{p}$, if $p$ prime and $a$ coprime to $p$.

- We pick a random element $a \in \{2, \ldots, N-1\}$ and fix a smoothness bound $B$.

- We hope for $p - 1$ (or the order of $a \pmod{p}$) to be $B$-powersmooth, i.e. all prime powers are less than or equal to $B$.

- Set $R := \text{lcm}(1, \ldots, B)$.

- $\text{ord}(a) \pmod{p}$ is $B$-powersmooth $\Rightarrow R$ is a multiple of $\text{ord}(a)$

  Thus $a^R \equiv a^{k \cdot \text{ord}(a)} \equiv 1 \pmod{p} \Rightarrow p | a^R - 1$.

**Result:** $\gcd(a^R - 1, N)$ is a factor of $N$. 

Peter Birkner

Edwards Curves and the ECM Factorisation Method
Pollard’s p-1 Method (2)

This method can fail for two reasons:

1. *N* does not have a prime divisor *p* and an element *a* such that \( \text{ord}(a) \mod p \) is \( B \)-powersmooth, i.e. \( \gcd(a^R - 1, N) = 1 \).
   → Increase smoothness bound *B*.

2. All prime divisors of *N* are found simultaneously, i.e. \( \gcd(a^R - 1, N) = N \).
   → Pick another \( 1 < a < N \) and try again.
   → Ensure that \( \text{ord}(a) \) is **not** \( B \)-powersmooth modulo all prime factors of \( N \) at the same time.
Lenstra’s Elliptic Curve Factorisation Method

**Problem:** Find a factor of the composite integer $N$.

- Let $p$ be a prime factor of $N$.
- Choose an elliptic curve $E$ over $\mathbb{Z}/N$ (Only ring but OK).
- Set $R := \text{lcm}(1, \ldots, B)$ for some smoothness bound $B$.
- Pick a random point $P$ on $E$ (over $\mathbb{Z}/N$) and compute $Q = [R]P$. In projective coordinates: $Q = (X : Y : Z)$.
- If the order $\ell$ of $P$ modulo $p$ is $B$-powersmooth then $\ell | R$ and hence $Q$ modulo $p$ is the neutral element $(0 : 1 : 0)$ of $E$ modulo $p$.

Thus, the $X$ and $Z$-coordinate of $Q$ are multiples of $p$.

$\Rightarrow \gcd(X,N)$ is a divisor of $N$. 

Peter Birkner

Edwards Curves and the ECM Factorisation Method
Remarks

- Big advantage over Pollard p-1: We can vary the curve, which increases the chance of finding at least one curve such that $P$ has smooth order.

- If the computation of an inverse element in $\mathbb{Z}/N$ fails, we have already found a divisor of $N$.

- If the order of $P$ modulo $p$ is $B$-powersmooth for all primefactors $p$ of $N$, then $\gcd(X,N) = N$.

  → To find a non-trivial divisor of $N$, we need one primefactor $p$ such that the order of $P$ modulo $p$ is $B$-powersmooth and one $q$ such that this is not true.

- We start with curves over $\mathbb{Q}$ (rank $> 0$) which have a prescribed torsion subgroup. When reducing those modulo $p$, we already know some divisors of the group order (in case of good reduction).
Suitable Elliptic Curves for ECM (1)

- For ECM we like to have curves over $\mathbb{Q}$ with large torsion subgroup, rank $> 0$ and a point in the non-torsion part, which is of small height. This point is used as the base point $P$ leading to cheap additions.

- **Theorem.** Let $E/\mathbb{Q}$ be an elliptic curve and let $m$ be a positive integer such that $\gcd(m, p) = 1$. If $E$ modulo $p$ is non-singular the reduction modulo $p$

$$E(\mathbb{Q})[m] \to E(\mathbb{F}_p)$$

is injective.

$\Rightarrow$ The order of the $m$-torsion subgroup divides $\#E(\mathbb{F}_p)$.

In particular this increases the smoothness chance of the group order of $E(\mathbb{F}_p)$. 

Peter Birkner
Suitable Elliptic Curves for ECM (2)

The Atkin and Morain Construction

- Atkin and Morain give a construction method for elliptic curves over $\mathbb{Q}$ with rank $> 0$ and torsion subgroup isomorphic to $\mathbb{Z}/2 \times \mathbb{Z}/8$ and a point contained in the non-torsion part.

  → Those curves are generated by a point $(s, t)$ on another curve. The point $(s, t)$ quickly gets a huge height and so do the parameters of the Atkin/Morain curve.

- **Example.** The curve $E : y^2 = x^3 + 212335199041/4662158400x^2 - 202614718501/22106401080x + 187819091161/419284740484$ has torsion part $\mathbb{Z}/2 \times \mathbb{Z}/8$ and rank 1.

- This curve has good reduction at $p = 641$. The Mordell Weil group of $E$ modulo $p$ is isomorphic to $\mathbb{Z}/2 \times \mathbb{Z}/336$ and 16 divides $\#E(\mathbb{F}_{641})$.  


2. What is an Edwards Curve?
What is an Edwards Curve?

- A new way of representing elliptic curves, recently introduced by Edwards. Lange and Bernstein studied the use of Edwards curves in cryptology (Asiacrypt 2007) and provided the efficient arithmetic on those curves.

- See Lange’s last talk at EIDMA seminar for more details.

- Curve equation $x^2 + y^2 = 1 + dx^2y^2$ over $\mathbb{Q}$ for $d \neq 0, 1$ (to avoid singularities).

- Addition law $(x_1, y_1), (x_2, y_2) \mapsto \left( \frac{x_1y_2 + y_1x_2}{1+dx_1x_2y_1y_2}, \frac{y_1y_2 - x_1x_2}{1-dx_1x_2y_1y_2} \right)$.

- If $d$ is not a square the addition law is complete, i.e. it holds for arbitrary inputs.
Example: Edwards Curve with $x^2 + y^2 = 1 + \left(\frac{1699}{22201}\right)^2 \cdot x^2 y^2$ over $\mathbb{R}$
Inverted Edwards Coordinates

- A projective point $(X_1 : Y_1 : Z_1)$ in inverted Edwards coordinates corresponds to the affine point $(Z_1/X_1, Z_1/Y_1)$.

- **Doubling** costs $3M + 4S + 1D$.

- **Addition** of two points costs $9M + 1S + 1D$.

- We use **signed sliding windows** for the scalar multiplication. The cost is $1DBL + \varepsilon ADD$ for each bit of the scalar, where $\varepsilon \to 0$ when the scalar gets large, i.e. asymptotically $3M + 4S + 1D$. 
3. How can Edwards curves make ECM faster?
We can construct Edwards curves over $\mathbb{Q}$ (rank $> 0$) with prescribed torsion-part and small parameters, and find a point in the non-torsion subgroup.

To compute $[R]P$ for ECM we use inverted Edwards coordinates which offers faster scalar multiplication.

The point in the non-torsion part has small height. This means that all additions in the scalar multiplication are additions with a small point.

**Example.** $n = (5^{367} + 1)/(2 \cdot 3 \cdot 73219364069)$

GMP-ECM: 210299 mults. modulo $n$ in 2448 ms.

GMP-EECM: 195111 mults. modulo $n$ in 2276 ms.

$\rightarrow$ Speed-up of 7% (only first experiments).
Theorem of Mazur. Let $E/\mathbb{Q}$ be an elliptic curve. Then the torsion subgroup $E_{\text{tors}}(\mathbb{Q})$ of $E$ is isomorphic to one of the following fifteen groups:

$$\mathbb{Z}/n \text{ for } n = 1, 2, 3, 4, 5, 6, 7, 8, 9, 10 \text{ or } 12$$

$$\mathbb{Z}/2 \times \mathbb{Z}/2n \text{ for } n = 1, 2, 3, 4.$$

All Edwards curves have two points of order 4.

For ECM we are interested in large torsion subgroups. By Mazur’s theorem the largest choices are $\mathbb{Z}/2 \times \mathbb{Z}/6$, $\mathbb{Z}/12$, and $\mathbb{Z}/2 \times \mathbb{Z}/8$.

An Edwards curve over $\mathbb{Q}$ with torsion subgroup $\mathbb{Z}/2 \times \mathbb{Z}/6$ is not possible. (Note, that there is also no twisted Edwards curve with this torsion subgroup. See Paper for details.)
How can we find Edwards curves with prescribed torsion part?

- All Edwards curves have 2 points of order 4, namely $P_4 = (1, 0)$ and $P'_4 = (-1, 0)$.

- We construct a point $P_3$ of order 3 and obtain a curve with torsion part isomorphic to $\mathbb{Z}/12$ generated by the point $P_{12} = P_3 + P_4$ of order 12.

- We can also ensure that the rank is greater than zero and determine a point in the non-torsion part which has small height.
Edwards Curves with a Point of Order 3

- Tripling formulas derived from addition law:

\[
[3](x_1, y_1) = \left( \frac{(x_1^2+y_1^2)^2-(2y_1)^2}{4(x_1^2-1)x_1^2-(x_1^2-y_1^2)^2}x_1, \frac{(x_1^2+y_1^2)^2-(2x_1)^2}{-4(y_1^2-1)y_1^2+(x_1^2-y_1^2)^2}y_1 \right)
\]

- For a point \( P_3 \) of order 3 we have \([3]P = (0, 1)\). (Note, that for a point of order 6 we have \([3]P = (0, -1)\).)

- Thus, the condition is:

\[
\frac{(x_1^2+y_1^2)^2-(2y_1)^2}{4(x_1^2-1)x_1^2-(x_1^2-y_1^2)^2}x_1 = 0
\]

- **Theorem.** If \( u \in \mathbb{Q} \setminus \{0, \pm1\} \) and

\[
x_3 = \frac{u^2 - 1}{u^2 + 1}, \quad y_3 = \frac{(u - 1)^2}{u^2 + 1}, \quad d = \frac{(u^2 + 1)^3(u^2 - 4u + 1)}{(u - 1)^6(u + 1)^2},
\]

then \( (x_3, y_3) \) is a point of order 3 on the Edwards curve given by \( x^2 + y^2 = 1 + dx^2y^2 \).
If $d$ is a rational square, then we have 2 more points of order 2 on the Edwards curve. If we additionally enforce that the curve has a point of order 8, the torsion group is isomorphic to $\mathbb{Z}/2 \times \mathbb{Z}/8$ (due to Mazur).

We always have 2 points of order 4, namely $(\pm 1, 0)$. For a point $P_8$ of order 8 we need $[2]P_8 = (\pm 1, 0)$.

→ Solve this equation using the doubling formulas.

We get a parameterisation for this solution: If $u \neq 0, -1, -2$, then $x_8 = (u^2 + 2u + 2)/(u^2 - 2)$ gives $P_8 = (x_8, x_8)$, which has order 8 on the curve given by $d = (2x_8^2 - 1)/x_8^4$.

To find a suitable curve, put $u = a/b$ and search for solutions $(a, b, e, f)$ with $d$ as above and $(e, f)$ a point on the curve which is not in $\{(0, \pm 1), (\pm 1, 0)\}$ and which has $e \neq f$. This point has infinite order over $\mathbb{Q}$.
Advantages of GMP-EECM over GMP-ECM (1)

- We choose curves with large torsion subgroups (12 or 16 points) and therefore large guaranteed divisors of the order of \(\#E\) modulo \(p\). GMP-ECM uses Suyama curves which have a rational torsion group of order 6.

- We choose curves with parameters and non-torsion points of small height (smaller than Atkin-Morain) and our implementation takes this into account by working with projective base points and projective parameters. The GMP-ECM implementation does not make use of small height elements and instead computes every fraction \(a/b\) modulo \(p\) which means that the numbers get big.
Advantages of GMP-EECM over GMP-ECM (2)

- In inverted Edwards coordinates the cost of a scalar multiplication is $1DBL + \varepsilon ADD$ per bit, where $\varepsilon \to 0$ when the scalar gets large, i.e. asymptotically $3M + 4S + 1D$.

GMP-ECM uses Montgomery curves. The Montgomery ladder needs $5M + 4S + 1D$ per bit; GMP-ECM uses the PRAC algorithm instead of the latter. It needs an average of $9M$ per bit.

- For ECM in constrained environments we recommend using NAF expansions. Then all additions are additions with small points and we use inverted coordinates.
Summary

Until now we already have

- 100 curves with small parameters and torsion subgroup $\mathbb{Z}/12$ or $\mathbb{Z}/2 \times \mathbb{Z}/8$.

- Complete translation of the Atkin-Morain method to Edwards curves.

- Complete translation of the Suyama construction.

- First experiments showed a speed-up of about 7 %.

- (See Cryptology ePrint Archive Report 2008/016 for details.)
Thank you for your attention!