Faster pairing computation in Edwards coordinates

Sorina Ionica

PRISM, Université de Versailles

(joint work with Antoine Joux)

Journées de Codage et Cryptographie 2008
Edwards coordinates

**Thm:** (Bernstein and Lange, 2007) Let $E$ be an elliptic curve on $F_q$. If $E(F_q)$ has a unique element of order 2 then there is a nonsquare $d \in F_q$ such that $E$ is birationally equivalent over $F_q$ to the *Edwards curve*

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

On the Edwards curve the addition law is

$$(x_1, y_1), (x_2, y_2) \rightarrow \left( \frac{x_1 y_2 + y_1 x_2}{1 + dx_1 x_2 y_1 y_2}, \frac{y_1 y_2 - x_1 x_2}{1 - dx_1 x_2 y_1 y_2} \right)$$
Homogeneous Edwards coordinates

- In cryptographic applications one should use homogeneous Edwards coordinates, i.e. \((X, Y, Z)\) corresponding to \((X/Z, Y/Z)\) on the Edwards curve.

- Addition becomes:

\[
X_3 = Z_1Z_2(X_0Y_1 + Y_0X_1)(Z_1^2Z_2^2 + dX_0X_1Y_0Y_1)
\]

\[
Y_3 = Z_1Z_2(Y_0Y_1 - X_0X_1)(Z_1^2Z_2^2 - dX_0X_1Y_0Y_1)
\]

\[
Z_3 = (Z_1^2Z_2^2 + dX_0X_1Y_0Y_1)(Z_1^2Z_2^2 - dX_0X_1Y_0Y_1)
\]
Edwards versus Jacobian

Let $E$ be an elliptic curve over $F_q$, i.e.

$$E : y^2 = x^3 + ax + b.$$ 

- Jacobian coordinates : $(X, Y, Z)$ such that $(\frac{X}{Z^2}, \frac{Y}{Z^3})$ is a point on the elliptic curve $E$.
- Computations in Edwards coordinates are significantly faster than in Jacobian coordinates!
Table: Performance evaluation: Edwards versus Jacobian

<table>
<thead>
<tr>
<th></th>
<th>Edwards coordinates</th>
<th>Jacobian coordinates</th>
</tr>
</thead>
<tbody>
<tr>
<td>addition</td>
<td>10M+1S</td>
<td>11M+5S (plus S-M tradeoff)</td>
</tr>
<tr>
<td>doubling</td>
<td>3M+4S</td>
<td>1M+8S or 4M+4S for $a = -3$</td>
</tr>
<tr>
<td>mixed addition</td>
<td>9M+1S</td>
<td>8M+3S (plus 2 M-S tradeoffs)</td>
</tr>
<tr>
<td>($Z_2 = 1$)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
What is a pairing?

A pairing is a map

\[ e : G_1 \times G'_1 \rightarrow G_2 \]

where \( G_1, G'_1, G_2 \) are groups of order \( r \) such that the following hold:

- **bilinear:** \( e(aP, Q) = e(P, aQ) = e(P, Q)^a \)
- **non-degenerate:** for every \( P \in G_1 \) different from 0 there is \( Q \in G'_1 \) such that \( e(P, Q) \neq 1 \).

Sorina Ionica
Faster pairing computation in Edwards coordinates
The Tate pairing. Notations.

Let $E$ be an elliptic curve over $F_q$, i.e.

$$E : y^2 = x^3 + ax + b.$$ 

- Let $r | \#E(F_q)$ and $E[r]$ the subgroup of points of order $r$, i.e.
  $$E[r] = \{P \in E(F_q) | rP = O\}$$

- Embedding degree: $k$ minimal with $r | (q^k - 1)$.
- Note $r$-roots of unity $\mu_r \in F_{q^k}^\times$.
- If $k > 1$ then $E(F_{q^k})[r] = E[r]$. 

Sorina Ionica Faster pairing computation in Edwards coordinates
The Tate pairing

- Choose \( P \in E[r] \) and \( Q \in E(F_{q^k}) \).
- Take \( f_{r,P} = r(P) - r(O) \) and \( D = (Q + T) - (T) \), with \( T \) such as the support of \( D \) is different from the support of \( f_{r,P} \).
- The Tate pairing is given by
  \[
  T_r(P, Q) = f_{r,P}(D)^{(q^k-1)/r}
  \]
- Domain and image are
  \[
  T_r(\cdot, \cdot) : E[r] \times E(F_{q^k})/rE(F_{q^k}) \to \mu_r
  \]
Miller’s algorithm

- Introduce for $i \geq 1$ functions $f_{i,P}$ such as 
  \[
  \text{div}\ (f_{i,P}) = i(P) - (iP) - (i - 1)(O)
  \]
- Note $\text{div}\ f_{r,P} = r(P) - r(O)$.
- Establish the Miller equation

\[
f_{i+j,P} = f_{i,P}f_{j,P} \frac{l}{v}
\]

where $l$ and $v$ are such that

\[
\text{div}\ (l) = (iP) + (jP) + (-(i+j)P) - 3(O)
\]

and $\text{div}\ (v) = (-(i+j)P) + ((i+j)P) - 2(O)$. 
Miller’s algorithm

- Use the double and add method to compute $f_{r,P}(D)$.
- Exploit the Miller equation

$$f_{i+j,P} = f_{i,P} f_{j,P} \frac{l}{v}$$

- $l$: the line through $iP$ and $jP$
- $v$: the vertical line through $(i + j)P$.
- Evaluate at $D'$ at every step.
Miller’s algorithm

- Count number of operations in the doubling step in the double and add method to evaluate performance of the algorithm independently from
  - any faster exponentiation techniques
  - the Hamming weight of $r$.
- Up to now best performance in Jacobian coordinates.
Back to Edwards curves

- Note a 4-torsion subgroup defined over $F_q$:

\[ \{ O = (0, 1), T_4 = (1, 0), T_2 = (0, -1), -T_4 = (-1, 0) \} \]

- Take a look at the action of this subgroup on a fixed point $P = (x, y)$:

\[ P \rightarrow \{ P, P + T_4 = (y, -x), P + T_2 = (-x, -y), P - T_4 = (-y, x) \} \]
If $xy \neq 0$ note $p = (xy)^2$ and $s = x/y - y/x$ to characterize the point $P$ up to the action of the 4-torsion subgroup.

Take $E_{s,p} : s^2 p = (1 + dp)^2 - 4p$ and define

$$\phi : E \rightarrow E_{s,p}$$

$$\phi(x, y) = ((xy)^2, \frac{x}{y} - \frac{y}{x}).$$

$\phi$ is separable of degree 4.
And back to an elliptic curve...

- $E_{s,p}$ is elliptic as:

\[
\begin{align*}
s^2p &= (1 + dp)^2 - 4p \\
S^2P &= (Z + dP)^2Z - 4PZ^2 \\
s^2 &= z^3 + (2d - 4)z^2 + dz
\end{align*}
\]

- Consider the standard addition law: $O_{s,p} = (0, 1, 0)$ neutral element and $T_{2,s,p} = (1, 0, 0)$ point of order 2.
Arithmetic of $E_{s,p}$

- Take $P_1$ and $P_2$ two points on $E_{s,p}$
- Take $l_{s,p}$ the line passing through $P_1$ and $P_2$. Take $R$ its third point of intersection with the curve $E_{s,p}$.
- Take $v_{s,p}$ the vertical line through $R$.
- Define $P_1 + P_2$ as the second point of intersection of $v_{s,p}$ with $E_{s,p}$.
- Note that
  \[
  \text{div} (l_{s,p}) = (P_1) + (P_2) + (- (P_1 + P_2)) - 2(T_{2,s,p}) - (O_{s,p})
  \]
  and
  \[
  \text{div} (v_{s,p}) = (P_1 + P_2) + (- (P_1 + P_2)) - 2(T_{2,s,p}).
  \]
Miller’s algorithm on Edwards curves

- Consider slightly modified functions $f_{i,P}^{(4)}$:

$$
\begin{align*}
  f_{i,P}^{(4)} &= i((P) + (P + T_4) + (P + T_2) + (P - T_4)) \\
  &\quad - ((iP) + (iP + T_4) + (iP + T_2) + (iP - T_4)) \\
  &\quad - (i - 1)((O) + (T_4) + (T_2) + (-T_4)).
\end{align*}
$$

- Then $f_{r,P}^{(4)} = r((P) + (P + T_4) + (P + T_2) + (P - T_4)) - r((O) + (T_4) + (T_2) + (-T_4))$.

- Compute the 4-th power of the Tate pairing:

$$
T_r(P, Q)^4 = f_{r,P}^{(4)}(D)^{q^k-1}. 
$$
Miller’s algorithm on the Edwards curve

Establish the Miller equation:

\[ f_{i+j,P}^{(4)} = f_{i,P}^{(4)} f_{j,P}^{(4)} \frac{l}{v}, \]

where \( l/v \) is the function of divisor

\[
\text{div} \left( \frac{l}{v} \right) = ((iP) + (iP + T_4) + (iP + T_2) + (iP - T_4)) \\
+ ((jP) + (jP + T_4) + (jP + T_2) + (jP - T_4)) \\
- (((i + j)P) + ((i + j)P + T_4) + ((i + j)P + T_2) + ((i + j)P - T_4)) \\
- ((0) + (T_4) + (T_2) + (-T_4)).
\]
Miller’s algorithm on the Edwards curve

- Let $P' = \phi(P)$ and $l_{s,p}$ and $v_{s,p}$ such as
  \[
  \text{div} (l_{s,p}) = (iP') + (jP') + ((i + j)P') - 2(T_{2,s,p}) - (O_{s,p})
  \]
  and \[
  \text{div} (v_{s,p}) = ((i + j)P') + (-(i + j)P') - 2(T_{2,s,p}).
  \]
- Get $l/v = \phi^*(l_{s,p}/v_{s,p})$. 

Computations

- **doubling for** $K = (X_1, Y_1, Z_1)$:

\[
X_3 = 2X_1 Y_1 (2Z_1^2 - (X_1^2 + Y_1^2)),
\]
\[
Y_3 = (X_1^2 + Y_1^2)(Y_1^2 - X_1^2),
\]
\[
Z_3 = (X_1^2 + Y_1^2)(2Z_1^2 - (X_1^2 + Y_1^2)).
\]

- **computing** $l$ and $v$:

\[
l(x, y) = l_1(x, y)/l_2 = ((X_1^2 + Y_1^2 - Z_1^2)(X_1^2 - Y_1^2)
\]
\[
\cdot ((2X_1 Y_1(x/y - y/x) - 2(X_1^2 - Y_1^2))
\]
\[
- Z_3(dZ_1^2(xy)^2 - (X_1^2 + Y_1^2 - Z_1^2))))/Z_1^6
\]
\[
v(x, y) = v_1(x, y)/v_2 = (dZ_3^2(xy)^2 - (X_3^2 + Y_3^2 - Z_3^2))/Z_3^2.
\]
Operation count and conclusions

Table: Comparison of costs

<table>
<thead>
<tr>
<th></th>
<th>$k = 1$</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jacobian coordinates</td>
<td>$8s + 12m$</td>
</tr>
<tr>
<td>Edwards coordinates</td>
<td>$6s + 12m$</td>
</tr>
</tbody>
</table>

- similar analysis for $k$ odd (although such curves are less used in practice)
Even embedding degree $k$

- Choose $P$ such that $\langle P \rangle \subset E(F_q)$
- Choose $Q$ such as elements of $\langle Q \rangle$ have one coordinate defined over $F_{q^{k/2}}$
- Compute $T_r(P, Q) = f_{r,P}(Q)(q^k - 1)/r$. 

Sorina Ionica  
Faster pairing computation in Edwards coordinates
Operation count and conclusions

Table: Comparison of costs in the case of $k = 2$

<table>
<thead>
<tr>
<th></th>
<th>$k = 2$</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jacobian coordinates</td>
<td>$6s + 7m + S + M$</td>
</tr>
<tr>
<td>Jacobian coordinates for $a = -3$</td>
<td>$4s + 8m + S + M$</td>
</tr>
<tr>
<td>Edwards coordinates</td>
<td>$3s + 10m + S + M$</td>
</tr>
</tbody>
</table>

- $s, m$ costs of operations in $F_q$ and $S, M$ costs of operations in $F_{q^k}$
Operation count and conclusions

Table: Comparison of costs in the case of $k \geq 4$ even

<table>
<thead>
<tr>
<th>Coordinate System</th>
<th>$k \geq 4$ even</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jacobian coordinates</td>
<td>$6s + (k + 6)m + S + M$</td>
</tr>
<tr>
<td>Jacobian coordinates for $a = -3$</td>
<td>$4s + (k + 7)m + S + M$</td>
</tr>
<tr>
<td>Edwards coordinates</td>
<td>$3s + (k + 9)m + S + M$</td>
</tr>
</tbody>
</table>

- $s, m$ costs of operations in $F_q$ and $S, M$ costs of operations in $F_{q^k}$
Questions...?