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

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

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:

$$
\begin{aligned}
X_3 &= Z_1Z_2(X_0Y_1 + Y_0X_1)(Z_1^2Z_2^2 + dX_0X_1Y_0Y_1)\\
Y_3 &= Z_1Z_2(Y_0Y_1 - X_0X_1)(Z_1^2Z_2^2 - dX_0X_1Y_0Y_1)\\
Z_3 &= (Z_1^2Z_2^2 + dX_0X_1Y_0Y_1)(Z_1^2Z_2^2 - dX_0X_1Y_0Y_1)
\end{aligned}
$$

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!

Edwards versus Jacobian

Table: Performance evaluation: Edwards versus Jacobian

	Edwards coordinates	Jacobian coordinates
addition	10**M**+1**S**	11**M**+5**S** (plus **S**-**M** tradeoff)
doubling	3**M**+4**S**	1**M**+8**S** or 4**M**+4**S** for $a = -3$
mixed addition ($Z_2 = 1$)	9**M**+1**S**	8**M**+3**S** (plus 2 **M**-**S** tradeoffs)

What is a pairing?

A pairing is a map

$$e : G_1 \times G_1^{'} \to G_2$$

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 $e(P, Q) \neq 1$.

The Tate pairing. Notations.

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

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

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

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 $\mathrm{div}\,(f_{i,P}) = i(P) - (iP) - (i-1)(O)$
- Note $\mathrm{div}\, f_{r,P} = r(P) - r(O)$.
- Establish the Miller equation

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

where l and v are such that

$$\mathrm{div}\,(l) = (iP) + (jP) + (-(i+j)P) - 3(O)$$

$$\text{and } \mathrm{div}\,(v) = (-(i+j)P) + ((i+j)P) - 2(O).$$

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

$$P \to \{P, P+T_4 = (y,-x), P+T_2 = (-x,-y), P-T_4 = (-y,x)\}$$

Back to Edwards curves

- 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

$$\begin{aligned} \phi : E &\rightarrow E_{s,p} \\ \phi(x, y) &= ((xy)^2, \frac{x}{y} - \frac{y}{x}). \end{aligned}$$

- ϕ is separable of degree 4.

And back to an elliptic curve...

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

$$\begin{array}{rcl} s^2p & = & (1+dp)^2 - 4p \\ & \downarrow & (P,S,Z) \\ S^2P & = & (Z+dP)^2Z - 4PZ^2 \\ & \downarrow & (P=1) \\ s^2 & = & z^3 + (2d-4)z^2 + dz \end{array}$$

- 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
  $\mathrm{div}\ (l_{s,p}) = (P_1) + (P_2) + (-(P_1 + P_2)) - 2(T_{2,s,p}) - (O_{s,p})$
  and $\mathrm{div}\ (v_{s,p}) = (P_1 + P_2) + (-(P_1 + P_2)) - 2(T_{2,s,p})$.

Miller's algorithm on Edwards curves

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

$$\begin{aligned} f^{(4)}_{i,P} &= i((P) + (P+T_4) + (P+T_2) + (P-T_4)) \\ &- ((iP) + (iP+T_4) + (iP+T_2) + (iP-T_4)) \\ &- (i-1)((O) + (T_4) + (T_2) + (-T_4)). \end{aligned}$$

- Then $f^{(4)}_{r,P} = r((P) + (P+T_4) + (P+T_2) + (P-T_4)) - r((O) + (T_4) + (T_2) + (-T_4))$.
- Compute the 4-th power of the Tate pairing:

$$T_r(P,Q)^4 = f^{(4)}_{r,P}(D)^{\frac{q^k-1}{r}}.$$

Miller's algorithm on the Edwards curve

Establish the Miller equation:

$$f^{(4)}_{i+j,P} = f^{(4)}_{i,P} f^{(4)}_{j,P} \frac{l}{v},$$

where l/v is the function of divisor

$$\begin{aligned}
\mathrm{div}(\frac{l}{v}) &= ((iP) + (iP + T_4) + (iP + T_2) + (iP - T_4)) \\
&+ ((jP) + (jP + T_4) + (jP + T_2) + (jP - T_4)) \\
&- (((i+j)P) + ((i+j)P + T_4) + ((i+j)P + T_2) + ((i+j)P \\
&- ((0) + (T_4) + (T_2) + (-T_4)).
\end{aligned}$$

Miller's algorithm on the Edwards curve

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

Computations

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

$$\begin{aligned} X_3 &= 2X_1Y_1(2Z_1^2 - (X_1^2 + Y_1^2)), \\ Y_3 &= (X_1^2 + Y_1^2)(Y_1^2 - X_1^2), \\ Z_3 &= (X_1^2 + Y_1^2)(2Z_1^2 - (X_1^2 + Y_1^2)). \end{aligned}$$

- computing l and v:

$$\begin{aligned} l(x,y) &= l_1(x,y)/l_2 = ((X_1^2 + Y_1^2 - Z_1^2)(X_1^2 - Y_1^2) \\ &\cdot ((2X_1Y_1(x/y - y/x) - 2(X_1^2 - Y_1^2)) \\ &- Z_3(dZ_1^2(xy)^2 - (X_1^2 + Y_1^2 - Z_1^2)))/Z_1^6 \\ v(x,y) &= v_1(x,y)/v_2 = (dZ_3^2(xy)^2 - (X_3^2 + Y_3^2 - Z_3^2))/Z_3^2. \end{aligned}$$

Operation count and conclusions

Table: Comparison of costs

	$k = 1$
Jacobian coordinates	$8\mathbf{s} + 12\mathbf{m}$
Edwards coordinates	$6\mathbf{s} + 12\mathbf{m}$

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

Even embedding degree k

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

Operation count and conclusions

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

	$k = 2$
Jacobian coordinates	$6\mathbf{s} + 7\mathbf{m} + \mathbf{S} + \mathbf{M}$
Jacobian coordinates for $a = -3$	$4\mathbf{s} + 8\mathbf{m} + \mathbf{S} + \mathbf{M}$
Edwards coordinates	$3\mathbf{s} + 10\mathbf{m} + \mathbf{S} + \mathbf{M}$

- $\mathbf{s}, \mathbf{m}$ costs of operations in F_q and $\mathbf{S}, \mathbf{M}$ costs of operations in F_{q^k}

Operation count and conclusions

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

	$k \geq 4$ even
Jacobian coordinates	$6\mathbf{s} + (k+6)\mathbf{m} + \mathbf{S} + \mathbf{M}$
Jacobian coordinates for $a = -3$	$4\mathbf{s} + (k+7)\mathbf{m} + \mathbf{S} + \mathbf{M}$
Edwards coordinates	$3\mathbf{s} + (k+9)\mathbf{m} + \mathbf{S} + \mathbf{M}$

- $\mathbf{s}, \mathbf{m}$ costs of operations in F_q and $\mathbf{S}, \mathbf{M}$ costs of operations in F_{q^k}

Questions...?