Another Approach to Pairing Computation in Edwards Coordinates

Sorina Ionica

PRISM, Université de Versailles

joint work with Antoine Joux

What is a pairing?

A pairing is a map

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

where $G_1, G_1^{'}$ are groups of order r noted additively and G_2 is a group of order r noted multiplicatively such that the following hold:

- bilinear: $e(aP, Q) = e(P, aQ) = e(P, Q)^a$
- nondegenerate: for every $P \in G_1$ different from 0 there is $Q \in G_1^{'}$ such that $e(P, Q) \neq 1$.

Pairings in Elliptic Curve Cryptograhy

- Pairings on elliptic curves: the Weil pairing, the Tate, Ate and Eta pairings.

- Applications:
  - one round protocol for tripartite Diffie-Hellman
  - identity-based encryption
  - short signatures
  - etc.

The Tate pairing. Notations.

Let E be an elliptic curve over finite field F_q with $q \geq 5$, i.e.

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

- Let $r | \sharp E(F_q)$ and $E[r]$ the r-torsion subgroup, i.e. the subgroup of points of order r in $E(\overline{F_q})$.
- If $r | \sharp E(F_q)$ then $E(F_q)[r]$ gives at least one component.
- Embedding degree: k minimal with $r | (q^k - 1)$.
- Note r-roots of unity $\mu_r \in F_{q^k}^{\times}$.

The Tate pairing

- If $k > 1$ then $E(F_{q^k})[r] = E[r]$.
- Choose $P, Q \in E[r]$ and $G_1 =< P >$, $G_1^{'} =< Q >$.
- Take $f_{r,P}$ such that $\mathrm{div}(f_{r,P}) = r(P) - r(O)$ and $D = (Q + T) - (T)$, with T such as the support of D is different from the support of $f_{r,P}$.
- For crypto use:

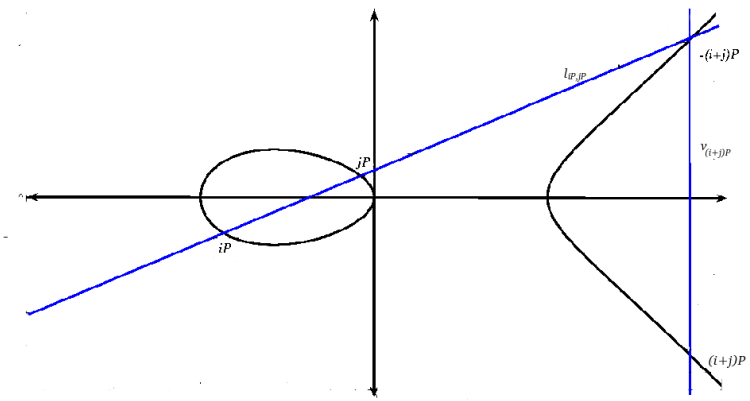
$$T_r(\cdot, \cdot) : G_1 \times G_1^{'} \rightarrow \mu_r$$

$$T_r(P, Q) = f_{r,P}(D)^{(q^k-1)/r}$$

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



$$f_{i+j,P} = f_{i,P} f_{j,P} \frac{l_{iP,jP}}{v_{(i+j)P}}$$

where $l_{iP,jP}$ and $v_{(i+j)P}$ are such that

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

$$\mathrm{div}\,(v_{(i+j)P}) = (-(i+j)P) + ((i+j)P) - 2(O)$$

Miller's algorithm

$$
\begin{aligned}
f_{1,P}(D) &= 1 \\
f_{2,P}(D) &= f_{1,P}^2(D)\frac{l_{P,P}(D)}{v_{2P}(D)} \\
f_{3,P}(D) &= f_{1,P}(D)f_{2,P}(D)\frac{l_{P,2P}(D)}{v_{3P}(D)} \\
&.. \\
&.. \\
f_{r,P}(D) &= f_{r-1,P}(D)f_{1,P}(D)l_{(r-1)P,P}(D)
\end{aligned}
$$

Use the double-and-add method to compute $f_{r,P}(D)$ (the Tate pairing!) in $O(log_2 r)$!

Miller's algorithm or double-and-add

- Choose a random point $T \in E(F_{q^k})$ and compute $Q' = Q + T \in E(F_{q^k})$.
- Let $n \leftarrow [\log_2(r)]$, $K \leftarrow P$, $f \leftarrow 1$.
- while $n \geq 1$
  - Compute equations of l and v arising in the doubling of K.
  - $K \leftarrow 2K$ and $f \leftarrow f^2(l(Q')v(T))/(v(Q')l(T))$.
  - the n-th bit of r is 1
    - Compute equations of l and v arising in the addition of K and P.
    - $K \leftarrow P + K$ and $f \leftarrow f(l(Q')v(T))/((l(T)v(Q'))$.
  - Let $n \leftarrow n - 1$.
- end while

Implementing Miller's algorithm

- The doubling part of the double-and-add method is most important
  - Use faster exponentiation techniques (sliding window method, NAF)
  - Choose r with low Hamming weight
- Choose $P \in E(F_q)[r]$ and $Q \in E(F_{q^k})[r]$.
- Take k even and get major speed-ups by using twists and working in subfields
- Up to now best performance in Jacobian coordinates: (X, Y, Z) such that $(\frac{X}{Z^2}, \frac{Y}{Z^3})$ is a point on the elliptic curve E.

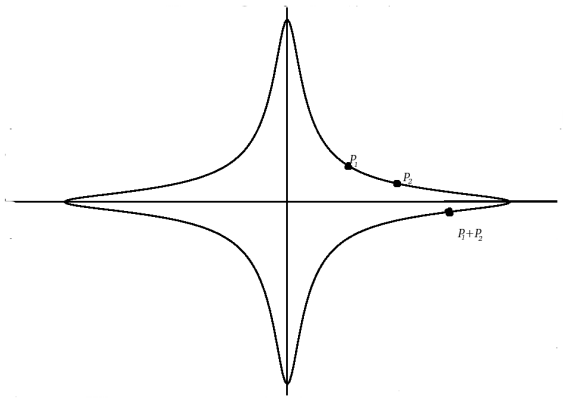
Edwards curves

- Let E be an elliptic curve on F_q such that $E(F_q)$ has an element of order 4.
- There is a nonsquare $d \in F_q$ such that E is birationally equivalent over F_q to the *Edwards curve*

$$x^2 + y^2 = 1 + d(xy)^2.$$

On the Edwards curve the addition law is

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



Edwards versus Jacobian

Actually use homogenous Edwards coordinates to avoid inversions: (X, Y, Z) corresponding to $(X/Z, Y/Z)$ on the Edwards curve.

	Edwards coordinates	Jacobian coordinates
addition	$10\mathbf{m}+1\mathbf{m}$	$11\mathbf{m}+5\mathbf{s}$
doubling	$3\mathbf{m}+4\mathbf{s}$	$1\mathbf{m}+8\mathbf{s}$ or $3\mathbf{m}+5\mathbf{s}$ for $a=-3$
mixed addition ($Z_2=1$)	$9\mathbf{m}+1\mathbf{s}$	$7\mathbf{m}+4\mathbf{s}$

- $\mathbf{s}, \mathbf{m}$ are the costs of operations in F_q ($\mathbf{s} = 0.8\mathbf{m}$).

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 $P = (x, y)$:

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

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 :

$$s^2 p = (1 + dp)^2 - 4p$$

$$\downarrow (P,S,Z)$$

$$S^2 P = (Z + dP)^2 Z - 4PZ^2$$

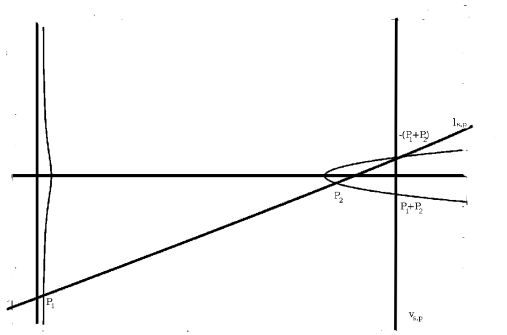
$$\downarrow (P=1)$$

$$s^2 = z^3 + (2d - 4)z^2 + dz$$

- 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 $l_{s,p}$ 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.
- $P_1 + P_2$ is the second point of intersection of $v_{s,p}$ with $E_{s,p}$.



$\text{div}\,(l_{s,p}) = (P_1) + (P_2) + (-(P_1 + P_2)) - 2(T_{2,s,p}) - (O_{s,p})$ 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 $f_{i,P}^{(4)}$:

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

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

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

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

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

Miller's algorithm on the Edwards curve

- Let $P' = \phi(P)$ and $l_{s,p}$ and $v_{s,p}$ such as
  $\text{div}\,(l_{s,p}) = (iP') + (jP') + ((i+j)P') - 2(T_{2,s,p}) - (O_{s,p})$
  and $\text{div}\,(v_{s,p}) = ((i+j)P') + (-(i+j)P') - 2(T_{2,s,p})$.

$$f_{i+j,P'} = f_{i,P'} f_{j,P'} \frac{l_{s,p}}{v_{s,p}}$$

$$\downarrow \phi^*$$

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

- Compute $l/v = \phi^*(l_{s,p}/v_{s,p})$.

Computing l and v

For the doubling step:

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

For the mixed addition step:

$$\begin{aligned} l(x,y) &= ((X_1^2+Y_1^2-Z_1^2-dZ_1^2(X_0Y_0)^2)(X_1Y_1(\frac{x}{y}-\frac{y}{x})- \\ &\quad (X_1^2-Y_1^2))-(X_1^2-Y_1^2-X_1Y_1(\frac{X_0}{Y_0}-\frac{Y_0}{X_0})) \\ &\quad \cdot(dZ_1^2(xy)^2-(X_1^2+Y_1^2-Z_1^2))) \\ &\quad /(X_1Y_1(X_1^2+Y_1^2-Z_1^2-dZ_1^2(X_0Y_0)^2)); \\ v(x,y) &= (dZ_3^2(xy)^2-(X_3^2+Y_3^2-Z_3^2))/(X_3^2+Y_3^2-Z_3^2). \end{aligned}$$

Comparison of costs for the doubling step of Miller's algorithm

	$k = 2$	$k \geq 4$
Jacobian coordinates	$10\mathbf{s} + 3\mathbf{m} + \mathbf{S} + \mathbf{M}$	$11\mathbf{s} + (k+1)\mathbf{m} + \mathbf{S} + \mathbf{M}$
Jacobian coordinates for $a = -3$	$4\mathbf{s} + 8\mathbf{m} + \mathbf{S} + \mathbf{M}$	$4\mathbf{s} + (k+7)\mathbf{m} + \mathbf{S} + \mathbf{M}$
Das/Sarkar Edwards coordinates (supersingular curves)	$6\mathbf{s} + 9\mathbf{m} + \mathbf{S} + \mathbf{M}$	-
Edwards coordinates	$4\mathbf{s} + 9\mathbf{m} + \mathbf{S} + \mathbf{M}$	$4\mathbf{s} + (k+8)\mathbf{m} + \mathbf{S} + \mathbf{M}$

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

Comparison of costs for the mixed addition step of the Miller operation in the case of k even

	$k = 2$	$k \geq 4$
Jacobian coordinates	$3\mathbf{s} + 11\mathbf{m} + \mathbf{M}$	$3\mathbf{s} + (k+9)\mathbf{m} + 1\mathbf{M}$
Das/Sarkar Edwards coordinates (supersingular curves)	$1\mathbf{s} + 17\mathbf{m} + \mathbf{M}$	-
Edwards coordinates	$4\mathbf{s} + 15\mathbf{m} + \mathbf{M}$	$4\mathbf{s} + (k+14)\mathbf{m} + 1\mathbf{M}$

A useful scenario

- Take $E : y^2 = x^3 + x$
- Take $q = 2^{520} + 2^{363} - 2^{360} - 1$ ($q \equiv 3 \mod 4$)
- Then $r = 2^{160} + 2^3 - 1$ and the embedding degree $k = 2$
- The Edwards form is $x^2 + y^2 = 1 - (xy)^2$, so $d = -1$.

A useful scenario

- Suppose you want to implement a protocol in Edwards coordinates.
  - protection from side channel attacks
- You need to compute the pairing of two points $e(P, Q)$, where Q is a fixed point.
- You have $P = (X_0, Y_0, 1)$ in Edwards coordinates
- Switch to Jacobian coordinates (via $\psi(X_0, Y_0) = ((1 + Y_0)/(1 - Y_0), (1 + Y_0)/(X_0(1 - Y_0)))$) and compute the pairing on the Weierstrass form.
  - faster, but you need one inversion with Montgomery's trick!

An inversion free algorithm

- Stick to Edwards coordinates and use our method to implement the pairing
- We need $\phi(X_0, Y_0) = ((X_0 Y_0)^2, \frac{X_0}{Y_0} - \frac{Y_0}{X_0})$ to compute the l-functions of the mixed addition step.
- Replace $l \leftarrow (X_0 Y_0) l$ in the mixed addition step.
- The mixed addition will be more expensive ($+1\mathbf{m}$) but NO INVERSIONS!

Questions. . . ?