Computing Pairings on Elliptic Curves

Michael Naehrig

17 July 2009

Pairings

A pairing is a map

$$e : G_1 \times G_2 \to G_3$$

$((G_1, +), (G_2, +), (G_3, \cdot)$ finite abelian groups), which is

- *bilinear*,

$$\begin{aligned} e(P_1 + P_2, Q_1) &= e(P_1, Q_1) e(P_2, Q_1), \\ e(P_1, Q_1 + Q_2) &= e(P_1, Q_1) e(P_1, Q_2), \end{aligned}$$

- *non-degenerate*, given $0 \neq P \in G_1$ there is a $Q \in G_2$ with

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

- *efficiently computable*.

Pairing-friendly elliptic curves

Take an elliptic curve over $\mathbb{F}_p$ ($p > 3$) with

- Weierstrass equation $E : y^2 = x^3 + ax + b$,
- $E(\mathbb{F}_p) = \{(x, y) \in \mathbb{F}_p^2 : y^2 = x^3 + ax + b\} \cup \{\mathcal{O}\}$,
- $n = \#E(\mathbb{F}_p) = p + 1 - t, \quad |t| \leq 2\sqrt{p}$,
- $r \mid n$ a large prime divisor of n ($r \neq p$, $r \geq \sqrt{p}$),
- and embedding degree $1 < k \leq 50$.

The embedding degree of E w.r.t. r is the smallest integer k with

$$r \mid p^k - 1.$$

The reduced Tate pairing

Assume $r^2 \nmid \#E(\mathbb{F}_p)$. The reduced Tate pairing

$$\begin{aligned} t_r : E(\mathbb{F}_p)[r] \times E(\mathbb{F}_{p^k})[r] &\rightarrow \mu_r \subset \mathbb{F}_{p^k}^*, \\ (P, Q) &\mapsto f_{r,P}(Q)^{\frac{p^k-1}{r}}. \end{aligned}$$

defines a non-degenerate, bilinear map, where

- $E(\mathbb{F}_p)[r] \subset E(\mathbb{F}_{p^k})[r] = \{P \in E(\mathbb{F}_{p^k}) \mid [r]P = \mathcal{O}\}$,
- μ_r is the group of r-th roots of unity in $\mathbb{F}_{p^k}^*$,
- $f_{r,P}$ is a function with divisor $(f_{r,P}) = r(P) - r(\mathcal{O})$,
- for $P \in E(\mathbb{F}_p)[r]$, we have $t_r(P, P) = 1$,
- take $Q \notin \langle P \rangle$, i.e. from $E(\mathbb{F}_{p^k})[r] \setminus E(\mathbb{F}_p)[r]$.

Three groups

Define the following groups:

- $G_1 = E(\mathbb{F}_{p^k})[r] \cap \ker(\phi_p - [1]) = E(\mathbb{F}_p)[r]$,
- $G_2 = E(\mathbb{F}_{p^k})[r] \cap \ker(\phi_p - [p])$,
- $G_3 = \mu_r \subset \mathbb{F}_{p^k}^*$.

ϕ_p is the p-power Frobenius on E, i. e. $\phi_p(x, y) = (x^p, y^p)$.
Let

$$G_1 = \langle P \rangle, \quad G_2 = \langle Q \rangle.$$

We have $E(\mathbb{F}_{p^k})[r] = G_1 \oplus G_2$, and we compute the Tate pairing as

$$\begin{aligned} t_r : G_1 \times G_2 &\rightarrow G_3, \\ (P, Q) &\mapsto f_{r,P}(Q)^{\frac{p^k - 1}{r}}. \end{aligned}$$

Specific parameters

- DLPs must be hard in all three groups.
- For efficiency reasons balance the security as much as possible.
- Define $\rho = \log(p)/\log(r)$.

Security level (bits)	Extension field size of p^k (bits)	EC base point order r (bits)	ratio $\rho \cdot k$
80	1024	160	6.40
112	2048	224	9.14
128	3072	256	12.00
192	7680	384	20.00
256	15360	512	30.00

NIST recommendations

My favorite examples... BN curves

If $u \in \mathbb{Z}$ such that

$$\begin{aligned} p = p(u) &= 36u^4 + 36u^3 + 24u^2 + 6u + 1, \\ n = n(u) &= 36u^4 + 36u^3 + 18u^2 + 6u + 1 \end{aligned}$$

are both prime, then there exists an elliptic curve

- with equation $E : y^2 = x^3 + b,\ b \in \mathbb{F}_p$,
- $r = n = \#E(\mathbb{F}_p)$ is prime, i. e. $\rho \approx 1$,
- the embedding degree is $k = 12$.

BN curves can be found easily.

- BNtiny: $u = -1, p = 19, n = 13, E : y^2 = x^3 + 3$.
  $P = (1, 2) \in E(\mathbb{F}_p)$.

Computing the pairing

There are two parts:

1. compute $f_{r,P}(Q)$,
2. the final exponentiation to the power $(p^k - 1)/r$.

For the first part, consider Miller functions $f_{i,P}$, $i \in \mathbb{Z}$.
These are functions with divisor

- $(f_{i,P}) = i(P) - ([i]P) - (i-1)(\mathcal{O})$.

Then

- $(f_{r,P}) = r(P) - ([r]P) - (r-1)(\mathcal{O}) = r(P) - r(\mathcal{O})$.

Miller functions and line functions

Miller functions can be computed recursively with

- $f_{1,P} = 1$,
- $f_{2i,P} = f_{i,P}^2 \cdot l_{[i]P,[i]P}/v_{[2i]P}$,
- $f_{i+1,P} = f_{i,P} \cdot l_{[i]P,P}/v_{[i+1]P}$,

where

- $l_{R,S}$: line through R and S, tangent if $R = S$,
  v_R: vertical line through R.

Evaluate at $Q = (x_Q, y_Q)$:

- $l_{R,S}(Q) = y_Q - y_R - \lambda(x_Q - x_1)$,
- $v_R(Q) = x_Q - x_R$,

with $R = (x_R, y_R)$ and the line has slope λ.

Miller's algorithm

Input: $P \in G_1, Q \in G_2, r = (r_m, \ldots, r_0)_2$

Output: $t_r(P,Q) = f_{r,P}(Q)^{\frac{p^k-1}{r}}$

$R \leftarrow P$, $f \leftarrow 1$

for $(i \leftarrow m-1;\ i \geq 0;\ i--)$ **do**

$\quad f \leftarrow f^2 \frac{l_{R,R}(Q)}{v_{[2]R}(Q)}$

$\quad R \leftarrow [2]R$

$\quad$ **if** $(r_i = 1)$ **then**

$\quad\quad f \leftarrow f \frac{l_{R,P}(Q)}{v_{R+P}(Q)}$

$\quad\quad R \leftarrow R + P$

$\quad$ **end if**

end for

$f \leftarrow f^{\frac{p^k-1}{r}}$

return f

Some improvements

- If possible, choose r with low Hamming-weight.
- Choose k even, then the final exponentiation is

$$\frac{p^k - 1}{r} = (p^{k/2} - 1)\frac{p^{k/2} + 1}{r}.$$

  Note that $r \nmid p^{k/2} - 1$.
- Represent the field extension $\mathbb{F}_{p^k} = \mathbb{F}_{p^{k/2}}(\alpha)$, $\alpha^2 = \beta$, where β is a non-square in $\mathbb{F}_{p^{k/2}}$.
- Then $f = f_0 + f_1\alpha$ with $f_0, f_1 \in \mathbb{F}_{p^{k/2}}$, computing $(f_0 + f_1\alpha)^{p^{k/2}} = f_0 - f_1\alpha$ is for free,
- and $(f_0 + f_1\alpha)^{p^{k/2}-1} = (f_0 - f_1\alpha)/(f_0 + f_1\alpha)$.
- And ask Peter Montgomery for good exponentiation methods and field arithmetic!

Representation of G_2

- Let $\delta = 6$ if $a = 0$, $\delta = 4$ if $b = 0$, and $\delta = 2$ else.
- If $\delta \mid k$, there exists a unique twist E' of E of degree δ with $r \mid \#E'(\mathbb{F}_{p^{k/\delta}})$.
- Define $G_2' = E'(\mathbb{F}_{p^{k/\delta}})[r]$.
- There exists an element $\xi \in \mathbb{F}_{p^{k/\delta}}$, not a δ-th power, s.t. the map $\psi : G_2' \to G_2$,

$$
\begin{aligned}
Q' = (x_{Q'}, y_{Q'}) &\mapsto (\xi x_{Q'}, \xi^{3/2} y_{Q'}) && \text{if } \delta = 2, \\
Q' = (x_{Q'}, y_{Q'}) &\mapsto (\xi^{1/2} x_{Q'}, \xi^{3/4} y_{Q'}) && \text{if } \delta = 4, \\
Q' = (x_{Q'}, y_{Q'}) &\mapsto (\xi^{1/3} x_{Q'}, \xi^{1/2} y_{Q'}) && \text{if } \delta = 6,
\end{aligned}
$$

  is a group isomorphism.

Denominator elimination

- All points $Q \in G_2$ have a special form, in particular the x-coordinate $x_Q = \xi^{2/\delta} x_{Q'} \in \mathbb{F}_{p^{k/2}}$.
- The value of the vertical line function $v_R(Q) = x_Q - x_R \in \mathbb{F}_{p^{k/2}}$.
- The first part of the final exponentiation thus gives

$$v_R(Q)^{p^{k/2}-1} = 1.$$

- Remove all denominators in Miller's algorithm.
- Similarly, all values in proper subfields of $\mathbb{F}_{p^k}$ are mapped to 1 by the final exponentiation.

Improved Miller

Input: $P \in G_1, Q \in G_2, r = (r_m, \ldots, r_0)_2$

Output: $t_r(P, Q) = f_{r,P}(Q)^{\frac{p^k-1}{r}}$

$R \leftarrow P$, $f \leftarrow 1$

for $(i \leftarrow m-1;\ i \geq 0;\ i--)$ **do**

$f \leftarrow f^2 \cdot l_{R,R}(Q)$

$R \leftarrow [2]R$

if $(r_i = 1)$ **then**

$f \leftarrow f \cdot l_{R,P}(Q)$

$R \leftarrow R + P$

end if

end for

$f \leftarrow f^{p^{k/2}-1}$

$f \leftarrow f^{\frac{p^{k/2}+1}{r}}$

return f

Loop shortening - eta pairing

Let $e = k/\delta$ and $T_e = (t-1)^e \mod r$.

- It turns out that the map

$$\begin{aligned} \eta_{T_e} : G_1 \times G_2 &\rightarrow G_3, \\ (P, Q) &\mapsto f_{T_e,P}(Q)^{(p^k-1)/r}. \end{aligned}$$

  is a pairing, called the eta pairing.
- One can take $T_e^j \mod r$ for $1 \leq j \leq \delta - 1$ instead of T_e. Choose the shortest non-trivial power.

Loop shortening - ate pairing

Let $T = t - 1$.

- The map

$$\begin{array}{rcl} a_T : G_2 \times G_1 & \longrightarrow & G_3, \\ (Q, P) & \longmapsto & f_{T,Q}(P)^{(p^k-1)/r}. \end{array}$$

  is a pairing, called the ate pairing.
- As for the eta pairing, we can replace T by $T^j \mod r$ for $1 \leq j \leq k-1$ to possibly get a shorter loop.
- Note that groups are swapped. Curve arithmetic in Miller's algorithm must now be done over a field extension. Use G_2'.

The final exponentiation

Let Φ_k be the kth cyclotomic polynomial.

- The embedding degree condition

$$r \mid p^k - 1,\ r \nmid p^m - 1 \text{ for } m < k$$

  is equivalent to $r \mid \Phi_k(p)$.
- $\Phi_k(p) \mid p^{k/2} + 1$.
- The second part of the final exponent can be written as

$$\frac{p^{k/2}+1}{r} = \frac{p^{k/2}+1}{\Phi_k(p)} \cdot \frac{\Phi_k(p)}{r}.$$

The final exponentiation

- $\frac{p^{k/2}+1}{\Phi_k(p)}$ is a polynomial in p with very small coefficients, and can be computed with some applications of the p-power Frobenius automorphism and some multiplications.
- Example $k = 12$:

$$\frac{p^6+1}{r} = (p^2+1) \cdot \frac{p^4-p^2+1}{r}.$$

- Compute $f^{(p^6+1)/r} = ((f^p)^p \cdot f)^{(p^4-p^2+1)/r}$.

The final slide... cheap pairings...