Efficient Computation of Pairings on Elliptic Curves

Michael Naehrig, TU/e

EIDMA/DIAMANT Cryptography Working Group
2 October 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

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

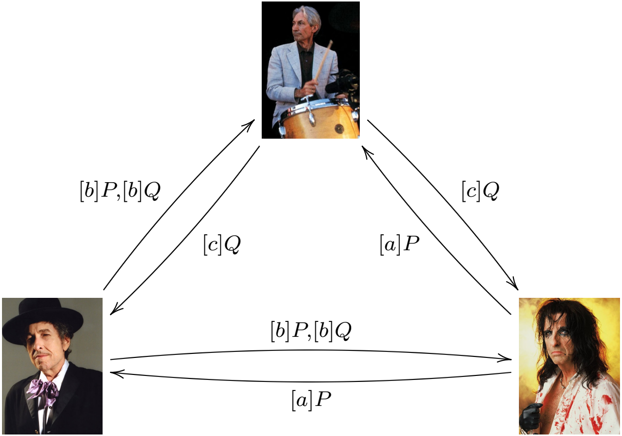
- *efficiently computable*.

Applications of pairings

- Attack DL-based cryptography on elliptic curves (Menezes-Okamoto-Vanstone-1993, Frey-Rück-1994) .
- Construct crypto systems with certain special properties:
  - One-round tripartite key agreement (Joux-2000),
  - Identity-based, non-interactive key agreement (Ohgishi-Kasahara-2000),
  - Identity-based encryption (Boneh-Franklin-2001),
  - Hierarchical IBE (Gentry-Silverberg-2002),
  - Short signatures (Boneh-Lynn-Shacham-2001).
  - Non-interactive proof systems (Groth-Sahai-2008)
  - much more ...

Tripartite key agreement (Joux-2000)

Alice, Bob, and Charlie choose secrets a, b, and c.



$$e([a]P,[b]Q)^c = e([b]P,[c]Q)^a = e([a]P,[c]Q)^b = e(P,Q)^{abc}$$

BLS signatures (Boneh-Lynn-Shacham-2001)

- System parameters:

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

  elements $P \in G_1$, $Q \in G_2$ s.t. $e(P, Q) \neq 1$,
  and a hash function $H : \{0, 1\}^* \to G_1$.
- Alice's private key: $x_A \in \mathbb{Z}$, public key: $Q_A = [x_A]Q$.
- Signature of a message $M \in \{0, 1\}^*$: $\sigma = [x_A]H(M)$.
- Verification $e(\sigma, Q) = e(H(M), Q_A)$.
- Correctness: $e(\sigma, Q) = e([x_A]H(M), Q) = e(H(M), [x_A]Q) = e(H(M), Q_A)$.

Schedule of this talk

Schedule of this talk

(1) Elliptic Curves

Schedule of this talk

(2) Pairings on
(1) Elliptic Curves

Schedule of this talk

(3) Computation of
(2) Pairings on
(1) Elliptic Curves

Schedule of this talk

(4) Efficient
(3) Computation of
(2) Pairings on
(1) Elliptic Curves

Elliptic Curves

Elliptic curves

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

- Weierstrass equation

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

- $E(\mathbb{F}_p) = \{(x, y) \in \mathbb{F}_p^2 : y^2 = x^3 + ax + b\} \cup \{\mathcal{O}\}$,
- $n = \#E(\mathbb{F}_p) = p + 1 - t, \quad |t| \leq 2\sqrt{p}$,
- and $r \mid n$ a large prime divisor of n ($r \neq p$).
- For $\mathbb{F} \supseteq \mathbb{F}_p$:
  $E(\mathbb{F}) = \{(x, y) \in \mathbb{F}^2 : y^2 = x^3 + ax + b\} \cup \{\mathcal{O}\}$,
- $E = E(\overline{\mathbb{F}_p})$, $\overline{\mathbb{F}_p}$ an algebraic closure of $\mathbb{F}_p$.
- E is an abelian group (written additively).

Torsion points and embedding degree

The set of r-torsion points on E is

$$E[r] = \{P \in E \mid [r]P = \mathcal{O}\}.$$

Since $r \mid \#E(\mathbb{F}_p)$, we have $E(\mathbb{F}_p)[r] \neq \emptyset$.
The embedding degree of E w.r.t. r is the smallest integer k with

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

For $k > 1$ we have

$$E[r] \subset E(\mathbb{F}_{p^k}),$$

i. e. $E(\mathbb{F}_p)[r] \subseteq E(\mathbb{F}_{p^k})[r] = E[r]$.

Pairings on Elliptic Curves

The reduced Tate pairing

The reduced Tate pairing

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

defines a non-degenerate, bilinear map, where

- 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 $Q \notin \langle P \rangle$.

Three groups

Assume $r^2 \nmid \#E(\mathbb{F}_p)$, $k > 1$. 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

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

G_1, G_2, and G_3 are cyclic groups of prime order r.

Computation of
Pairings on Elliptic Curves

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

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

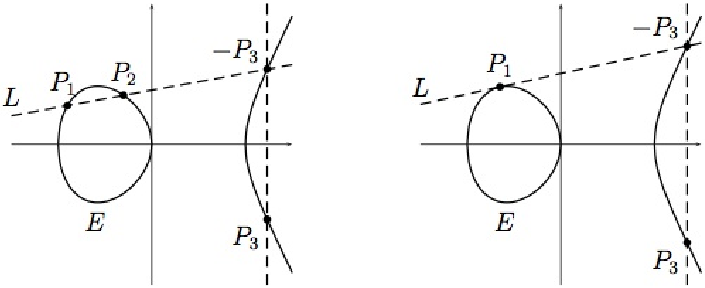
Miller functions and line functions

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_{P_1,P_2}: line through P_1 and P_2, tangent if $P_1 = P_2$,
  v_{P_1}: vertical line through P_1.



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**

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

$R \leftarrow [2]R$

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

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

$R \leftarrow R + P$

end if

end for

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

return f

Specific parameters – pairing-friendly curves

- The embedding degree k needs to be small ($1 < k \leq 50$), to be able to do computations at all.
- 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 (Barreto-N., 2005)

BN curves can be found easily and are ideal for the 128-bit security level.
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 $k = 12$.
- BNtiny: $u = -1, p = 19, n = 13, E : y^2 = x^3 + 3$. $P = (1, 2) \in E(\mathbb{F}_p)$.

Efficient Computation of Pairings on Elliptic Curves

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**

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

$R \leftarrow [2]R$

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

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

$R \leftarrow R + P$

end if

end for

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

return f

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**
$f \leftarrow f^2 \frac{l_{R,R}(Q)}{v_{[2]R}(Q)}$
$R \leftarrow [2]R$
if $(r_i = 1)$ **then**
$f \leftarrow f \frac{l_{R,P}(Q)}{v_{R+P}(Q)}$
$R \leftarrow R + P$
end if
end for
$f \leftarrow f^{\frac{p^k-1}{r}}$
return f

Final exponentiation (easy part)

- Choose k even, then the final exponent is

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

Note that $r \nmid p^{k/2} - 1$, therefore $r \mid p^{k/2} + 1$.

Final exponentiation (easy part)

- Choose k even, then the final exponent is

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

  Note that $r \nmid p^{k/2} - 1$, therefore $r \mid p^{k/2} + 1$.
- Represent the field extension $\mathbb{F}_{p^k} = \mathbb{F}_{p^{k/2}}(\alpha)$, $\alpha^2 = \beta$, where β is a non-square in $\mathbb{F}_{p^{k/2}}$.

Final exponentiation (easy part)

- Choose k even, then the final exponent is

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

  Note that $r \nmid p^{k/2} - 1$, therefore $r \mid p^{k/2} + 1$.
- 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 almost for free,
- and $(f_0 + f_1\alpha)^{p^{k/2}-1} = (f_0 - f_1\alpha)/(f_0 + f_1\alpha)$.

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**

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

$R \leftarrow [2]R$

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

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

$R \leftarrow R + P$

end if

end for

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

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

return f

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**

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

$R \leftarrow [2]R$

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

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

$R \leftarrow R + P$

end if

end for

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

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

return f

Denominator elimination

- Since k is even, all points $Q \in G_2$ have a special form, in particular the x-coordinate $x_Q \in \mathbb{F}_{p^{k/2}}$.
- 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.

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**

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

$R \leftarrow [2]R$

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

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

$R \leftarrow R + P$

end if

end for

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

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

return f

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**

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

$R \leftarrow [2]R$

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

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

$R \leftarrow R + P$

end if

end for

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

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

return f

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**

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

$R \leftarrow [2]R$

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

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

$R \leftarrow R + P$

end if

end for

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

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

return f

Doubling and addition steps

$$\begin{aligned} \mathrm{DBL}: &\quad f \leftarrow f^2 \cdot l_{R,R}(Q), \quad R \leftarrow [2]R \\ \mathrm{ADD}: &\quad f \leftarrow f \cdot l_{R,P}(Q), \quad R \leftarrow R + P \end{aligned}$$

These steps include multiplications/squarings in $\mathbb{F}_{p^k}$, computations in $\mathbb{F}_p$ for the line coefficients, and curve arithmetic in $E(\mathbb{F}_p)$.

- Line functions correspond to the lines in the point doubling/addition,
- reuse intermediate results of point additions for line function coefficients,
- use projective coordinates to avoid inversions.

What about Edwards curves?

Edwards curves provide extremely fast curve arithmetic.
Can we use this advantage for pairings?

$$E_d : x^2 + y^2 = 1 + dx^2y^2$$

- Edwards group law

$$(x_1, y_1) + (x_2, y_2) = (x_3, y_3),$$

$$x_3 = \frac{x_1y_2 + y_1x_2}{1 + dx_1x_2y_1y_2} \text{ and } y_3 = \frac{y_1y_2 - x_1x_2}{1 - dx_1x_2y_1y_2}.$$

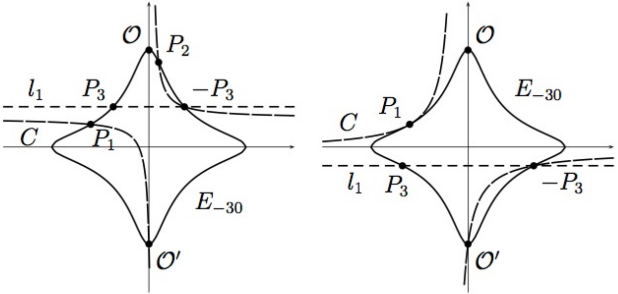
- Neutral element is $\mathcal{O} = (0, 1)$, $-(x_1, y_1) = (-x_1, y_1)$.
  $\mathcal{O}' = (0, -1)$ has order 2; $(1, 0), (-1, 0)$ have order 4.
- Two points at infinity $\Omega_1 = (1 : 0 : 0)$, $\Omega_2 = (0 : 1 : 0)$ with multiplicity 2.

Pairings on Edwards curves

- Line functions do not work: Edwards equation has degree 4, so expect 4 intersection points.
- Quadratic functions: 8 intersection points.
- Replace line by the conic C passing through the 5 points $P_1, P_2, \mathcal{O}', \Omega_1,$ and Ω_2.
  Only *one more* intersection point.

Pairings on Edwards curves

- Line functions do not work: Edwards equation has degree 4, so expect 4 intersection points.
- Quadratic functions: 8 intersection points.
- Replace line by the conic C passing through the 5 points $P_1, P_2, \mathcal{O}', \Omega_1,$ and Ω_2.
  Only *one more* intersection point.



Pairings on Edwards curves

- Can do Miller's algorithm as before,
- only replace line functions by quadratic functions described by the above conic.
- Comparison of costs for computing the coefficients of lines or conics and the double or sum of points:

	DBL	mADD	ADD
Jacobian coord.	$1\mathbf{m} + 11\mathbf{s} + 1\mathbf{m_a}$	$6\mathbf{m} + 6\mathbf{s}$	$15\mathbf{m} + 6\mathbf{s}$
Jacobian ($a = -3$)	$6\mathbf{m} + 5\mathbf{s}$	$6\mathbf{m} + 6\mathbf{s}$	$15\mathbf{m} + 6\mathbf{s}$
Jacobian ($a = 0$, e.g. BN curves)	$3\mathbf{m} + 8\mathbf{s}$	$6\mathbf{m} + 6\mathbf{s}$	$15\mathbf{m} + 6\mathbf{s}$
Edwards	$6\mathbf{m} + 5\mathbf{s}$	$12\mathbf{m}$	$14\mathbf{m}$

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**

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

$R \leftarrow [2]R$

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

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

$R \leftarrow R + P$

end if

end for

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

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

return f

The Miller loop

- If possible, choose r with low hamming weight.
- If not, maybe use Non-Adjacent-Form (NAF):
  $r = (r_{m+1}, \ldots, r_0)_{\mathrm{NAF}},\ r_i \in \{-1, 0, 1\}$

for $(i \leftarrow m;\ i \geq 0;\ i--)$ **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
  if $(r_i = -1)$ **then**
    $f \leftarrow f \cdot l_{R,-P}(Q)$
    $R \leftarrow R - P$
  end if
end for

Loop shortening - eta pairing

Suppose E has a twist of degree δ and $\delta \mid k$. Let $e = k/\delta$ and $T_e = (t-1)^e \mod r$.

- It turns out that the map

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

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

Loop shortening - ate pairing

Let $T = t - 1$.

- The map

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

  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.

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**

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

$R \leftarrow [2]R$

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

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

$R \leftarrow R + P$

end if

end for

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

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

return f

Final exponentiation (hard part)

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

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

Final exponentiation (hard part)

k	$\Phi_k(p)$	$(p^{k/2}+1)/\Phi_k(p)$
6	$p^2 - p + 1$	$p + 1$
10	$p^4 - p^3 + p^2 - p + 1$	$p + 1$
12	$p^4 - p^2 + 1$	$p^2 + 1$
16	$p^8 + 1$	1
18	$p^6 - p^3 + 1$	$p^3 + 1$
24	$p^8 - p^4 + 1$	$p^4 + 1$
30	$p^8 + p^7 - p^5 - p^4$	$p^7 - p^6 + p^5$
	$-p^3 + p + 1$	$+p^2 - p + 1$

Final exponentiation (hard part)

k	$\Phi_k(p)$	$(p^{k/2}+1)/\Phi_k(p)$
6	$p^2 - p + 1$	$p + 1$
10	$p^4 - p^3 + p^2 - p + 1$	$p + 1$
12	$p^4 - p^2 + 1$	$p^2 + 1$
16	$p^8 + 1$	1
18	$p^6 - p^3 + 1$	$p^3 + 1$
24	$p^8 - p^4 + 1$	$p^4 + 1$
30	$p^8 + p^7 - p^5 - p^4$	$p^7 - p^6 + p^5$
	$-p^3 + p + 1$	$+p^2 - p + 1$

- Example $k = 12$:

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

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

p-power Frobenius

Example BN curves with $k = 12$:
note $p \equiv 1 \pmod 6$.

- $\mathbb{F}_{p^2} = \mathbb{F}_p(\alpha)$, $\alpha^2 = \beta$
  Then an element $f \in \mathbb{F}_{p^2}$ can be written as $f = f_0 + f_1\alpha$ with $f_0, f_1 \in \mathbb{F}_p$, thus

$$f^p = (f_0 + f_1\alpha)^p = f_0 - f_1\alpha.$$

p-power Frobenius

Example BN curves with $k = 12$:
note $p \equiv 1 \pmod 6$.

- $\mathbb{F}_{p^2} = \mathbb{F}_p(\alpha)$, $\alpha^2 = \beta$
  Then an element $f \in \mathbb{F}_{p^2}$ can be written as $f = f_0 + f_1\alpha$ with $f_0, f_1 \in \mathbb{F}_p$, thus

$$f^p = (f_0 + f_1\alpha)^p = f_0 - f_1\alpha.$$

- $\mathbb{F}_{p^6} = \mathbb{F}_{p^2}(w)$, $w^3 = \xi$ for $\xi \in \mathbb{F}_{p^2}$ not a cube, not a square
  Write $f = f_0 + f_1 w + f_2 w^2$ with $f_0, f_1, f_2 \in \mathbb{F}_{p^2}$. Then

$$f^p = f_0^p + f_1^p w_p w + f_2^p w_p^2 w^2,$$

  where $w_p = w^{p-1} = \xi^{\frac{p-1}{3}} \in \mathbb{F}_{p^2}$.

p-power Frobenius

- $\mathbb{F}_{p^{12}} = \mathbb{F}_{p^6}(\alpha)$, $\alpha^2 = w$
  Write $f \in \mathbb{F}_{p^{12}}$ as $f = f_0 + f_1\alpha$ with $f_0, f_1 \in \mathbb{F}_{p^6}$, thus

  $$f^p = (f_0 + f_1\alpha)^p = f_0^p + f_1^p \alpha_p \alpha,$$

  where $\alpha_p = \alpha^{p-1} = w^{\frac{p-1}{2}} = \xi^{\frac{p-1}{6}} \in \mathbb{F}_{p^2}$.

p-power Frobenius

- $\mathbb{F}_{p^{12}} = \mathbb{F}_{p^6}(\alpha)$, $\alpha^2 = w$
  Write $f \in \mathbb{F}_{p^{12}}$ as $f = f_0 + f_1\alpha$ with $f_0, f_1 \in \mathbb{F}_{p^6}$, thus

  $$f^p = (f_0 + f_1\alpha)^p = f_0^p + f_1^p \alpha_p \alpha,$$

  where $\alpha_p = \alpha^{p-1} = w^{\frac{p-1}{2}} = \xi^{\frac{p-1}{6}} \in \mathbb{F}_{p^2}$.
- One p-power Frobenius $f \mapsto f^p$ for an element in $\mathbb{F}_{p^{12}}$ can be done with 7 multiplications in $\mathbb{F}_{p^2}$.
- A plain square-and-multiply exponentiation needs at least $\log(p)$ squarings in $\mathbb{F}_{p^{12}}$.

The new hard part

It remains to compute a power to the exponent $\frac{\Phi_k(p)}{r}$.
For BN curves:

$$\frac{\Phi_k(p)}{n} = \frac{p^4 - p^2 + 1}{n} = p^3 + l_2 p^2 + l_1 p + l_0,$$

with

$$\begin{aligned} l_2 &= 6u^2 + 1, \\ l_1 &= -36u^3 - 18u^2 - 12u + 1, \\ l_0 &= -36u^3 - 30u^2 - 18u + 2. \end{aligned}$$

Multi-exponentiation

To compute $f^{(p^4-p^2+1)/n}$,

- first obtain f^p, f^{p^2}, f^{p^3} by three Frobenius applications,
- then compute

$$f^{l_0+l_1p+l_2p^2} = f^{l_0}(f^p)^{l_1}(f^{p^2})^{l_2}$$

  with a multi-exponentiation,
- and finally

$$f^{l_0+l_1p+l_2p^2+p^3} = f^{l_0}(f^p)^{l_1}(f^{p^2})^{l_2}f^{p^3}.$$

The final slide... cheap pairings...

michael@cryptojedi.org