Pairings II

Michael Naehrig

Eindhoven Institute for the Protection of Systems and Information
Technische Universiteit Eindhoven
michael@cryptojedi.org

technische universiteit eindhoven

ECC Summer School 2008, Eindhoven
19 September 2008

Reminder

Let $p > 3$ be a prime, $\mathbb{F}_p$ the finite field with p elements and

$$E : Y^2 = X^3 + AX + B$$

an elliptic curve over $\mathbb{F}_p$.

- Let $n = \#E(\mathbb{F}_p)$ be the number of $\mathbb{F}_p$-rational points. We have

  $$n = p + 1 - t, \quad |t| \leq 2\sqrt{p},$$

  where t is the trace of Frobenius.

- Let $r \neq p$ be a large prime dividing $n = \#E(\mathbb{F}_p)$ and k be the embedding degree of E w.r.t. r, i.e.

  $$r \mid p^k - 1,\ r \nmid p^i - 1,\ i < k \iff r \mid \Phi_k(p).$$

Reminder

- The set of r-torsion points $E[r]$ is contained in $E(\mathbb{F}_{p^k})$.
- There are r points of order dividing r in $E(\mathbb{F}_p)$ and the group of r-th roots of unity μ_r is contained in $\mathbb{F}_{p^k}^*$.
- We have the reduced Tate pairing

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

which can be computed using Miller's algorithm, if k is suitably small.

Pairing-friendly curves

An elliptic curve is called pairing-friendly, if

1. the prime r is larger than $\sqrt{p}$,
2. the embedding degree k is small.

- A pairing transfers the DLP from $E[r](\mathbb{F}_p)$ to $\mathbb{F}_{p^k}$,
- for pairing-based protocols, both DLPs should be infeasible to solve.
- Good parameters lead to both DLPs being equally hard.

Security requirements

Recent ECRYPT key length recommendations, 2008 (`www.keylength.com`) tell us that we need the following bitsizes and embedding degrees:

Symmetric	r	$\mathbb{F}_{p^k}$	k
80	160	1248	8
112	224	2432	10
128	256	3248	12

It is important to know which curves have small embedding degrees, to avoid MOV-FR attacks or to implement pairing-based protocols.

Supersingular Curves

- An elliptic curve is called supersingular, iff $t \equiv 0 \pmod{p}$. Otherwise it is called ordinary.
- Supersingular elliptic curves have an embedding degree $k \le 6$.
- For $p > 3$ it even holds:
  From
  $$p \mid t \text{ and } |t| \le 2\sqrt{p}$$
  it follows $t = 0$ and thus $n = p + 1$, so
  $$n \mid p^2 - 1.$$
  Therefore $k \le 2$.
- But $k = 2$ is too small.

Problem

Fix a suitable value for k and find primes r, p and a number n with the following conditions:

- $n = p + 1 - t$, $|t| \leq 2\sqrt{p}$,
- $r \mid n$,
- $r \mid p^k - 1$,
- $t^2 - 4p = DV^2 < 0$, $D, V \in \mathbb{Z}$, D squarefree, $|D|$ small enough to compute the class polynomial.

The last condition is the CM norm equation. Once we found parameters we can construct the curve using CM methods.

- $r \mid p^k - 1$ can be replaced by $r \mid \Phi_k(p)$ or $r \mid \Phi_k(t-1)$ which is better, since Φ_k has degree $\varphi(k) < k$.

The ρ-value

For efficiency reasons we would like to have r as large as possible, $r = n$ is optimal.

- To measure this property we define the ρ-value of E as
$$\rho := \frac{\log(p)}{\log(r)}.$$
- We always have $\rho \geq 1$ where $\rho = 1$ is the best we can achieve.
- A pairing-friendly curve has $\rho < 2$.

MNT curves

Miyaji, Nakabayashi and Takano (MNT, 2001) give parametrisations of p and t as polynomials in $\mathbb{Z}[u]$ s.t.

$$n(u) \mid \Phi_k(p(u)).$$

The method yields ordinary elliptic curves of prime order ($r = n$) with embedding degree $k = 3, 4, 6$.

k	$p(u)$	$t(u)$
3	$12u^2 - 1$	$-1 \pm 6u$
4	$u^2 + u + 1$	$-u$ or $u + 1$
6	$4u^2 + 1$	$1 \pm 2u$

MNT curves

Let's compute an MNT curve. Take $k = 6$, i.e. we parameterise

$$p(u) = 4u^2 + 1,\ t(u) = 2u + 1.$$

- Then we have

$$n(u) = p(u) + 1 - t(u) = 4u^2 - 2u + 1.$$

- We may now plug in integer values for u until we find u_0 s.t. $p(u_0)$ and $n(u_0)$ are both prime.
- Example: $u_0 = 2$ yields $p(u_0) = 17$ and $n(u_0) = 13$.
- But we only have parameters, we do not have the curve.

MNT curves

In order to construct the curve via the CM method we need to find solutions to the norm equation

$$t^2 - 4p = DV^2,$$

and $|D|$ needs to be small.

- We compute

$$t(u)^2 - 4p(u) = (2u+1)^2 - 4(4u^2+1) = -12u^2 + 4u - 3.$$

- Therefore the norm equation becomes

$$-12u^2 + 4u - 3 = DV^2.$$

- For $u_0 = 2$ we obtain $DV^2 = -43$. Assume $|D|$ is too large (and we don't know the class polynomial).

MNT curves

Maybe we first should find solutions to the norm equation. Let's transform the equation:

- Start with
$$-12u^2 + 4u - 3 = DV^2.$$
- Multiply by -3 to get
$$36u^2 - 12u + 9 = -3DV^2.$$
- Complete the square:
$$(6u-1)^2 + 8 = -3DV^2.$$
- We need to solve (replace $6u-1$ by x, V by y)
$$x^2 + 3Dy^2 = -8.$$

MNT curves

How can we solve the equation $x^2 + 3Dy^2 = -8$?

- Theorem: If d is a positive squarefree integer then the equation
$$x^2 - dy^2 = 1$$
has infinitely many solutions. There is a solution (x_1, y_1) such that every solution has the form $\pm(x_m, y_m)$ where
$$x_m + y_m\sqrt{d} = (x_1 + y_1\sqrt{d})^m,\ m \in \mathbb{Z}.$$
- So if $d = -3D$ is positive and squarefree, we can compute infinitely many solutions to our equation if we find a solution (x_1, y_1).
- Use continued fractions to find a single solution.

MNT curves

Consider the field $\mathbb{Q}(\sqrt{d}) \subseteq \mathbb{C}$.

- The norm of $\alpha = x + y\sqrt{d} \in \mathbb{Q}(\sqrt{d})$ is defined to be

$$N(\alpha) = \alpha\overline{\alpha} = (x + y\sqrt{d})(x - y\sqrt{d}) = x^2 - dy^2$$

  so $x^2 - dy^2$ is the norm of the element $x + y\sqrt{d}$.
- We are actually looking for an element of norm -8.
- The norm is multiplicative:

$$N(\alpha\beta) = N(\alpha)N(\beta).$$

- We need to find only one element α of norm -8, then the infinitely many elements $\beta_m = x_m + y_m\sqrt{d}$ of norm 1 will help us to find infinitely many elements of norm -8:

$$N(\alpha\beta_m) = N(\alpha)N(\beta_m) = -8 \cdot 1 = -8.$$

MNT curves

Back to the example: Choose $D = -11$, so $d = 33$.

- The equation becomes

$$x^2 - 33y^2 = -8.$$

- A solution is $(5, 1)$. The corresponding element of $\mathbb{Q}(\sqrt{33})$ is $5 + \sqrt{33}$.
- A solution to

$$x^2 - 33y^2 = 1$$

  is $(23, 4)$ with corresponding element $23 + 4\sqrt{33}$.
- The elements

$$(5 + \sqrt{33})(23 + 4\sqrt{33})^m$$

  all have norm -8, thus yield solutions to the original norm equation.

MNT curves

We now can compute many solutions to the equation $x^2 - 33y^2 = -8$.

$$\begin{aligned}
(5+\sqrt{33})(23+4\sqrt{33})^{-5} &= -76495073 + 13316083\sqrt{33} \\
(5+\sqrt{33})(23+4\sqrt{33})^{-4} &= -1663723 + 289617\sqrt{33} \\
(5+\sqrt{33})(23+4\sqrt{33})^{-3} &= -36185 + 6299\sqrt{33} \\
(5+\sqrt{33})(23+4\sqrt{33})^{-2} &= -787 + 137\sqrt{33} \\
(5+\sqrt{33})(23+4\sqrt{33})^{-1} &= -17 + 3\sqrt{33} \\
(5+\sqrt{33})(23+4\sqrt{33})^{0} &= 5 + \sqrt{33} \\
(5+\sqrt{33})(23+4\sqrt{33})^{1} &= 247 + 43\sqrt{33} \\
(5+\sqrt{33})(23+4\sqrt{33})^{2} &= 11357 + 1977\sqrt{33} \\
(5+\sqrt{33})(23+4\sqrt{33})^{3} &= 522175 + 90899\sqrt{33} \\
(5+\sqrt{33})(23+4\sqrt{33})^{4} &= 24008693 + 4179377\sqrt{33}
\end{aligned}$$

MNT curves

And compute back to find solutions for the original equation $-12u^2 + 4u - 3 = DV^2$. Remember $x = 6u - 1$.

$\alpha\beta^i$	u	V
$-76495073 + 13316083\sqrt{33}$	12749179	13316083
$-1663723 + 289617\sqrt{33}$	-2124863	289617
$-36185 + 6299\sqrt{33}$	6031	6299
$-787 + 137\sqrt{33}$	-131	137
$-17 + 3\sqrt{33}$	3	3
$5 + \sqrt{33}$	1	1
$247 + 43\sqrt{33}$	-41	43
$11357 + 1977\sqrt{33}$	1893	1977
$522175 + 90899\sqrt{33}$	-87029	90899
$24008693 + 4179377\sqrt{33}$	4001449	4179377

MNT curves

We hope that some of the values for u give $p(u)$ and $n(u)$ prime.

- We are lucky. The value $u = 3$ gives

$$p(u) = 37,\ n(u) = 31,\ t(u) = 7.$$

- Construct the curve with the CM method.
- The Hilbert class polynomial for $D = -11$ is

$$H_D(X) = X + 32768.$$

- Its reduction mod p is

$$H(T) = T + 23.$$

- The j-invariant of our curve is thus $j(E) = -23 = 14$.

MNT curves

- From $j(E) = 14$ we find the curve

$$E : y^2 = x^3 + 13x + 11$$

  over the field $\mathbb{F}_{37}$ with 37 elements.
- The curve has 31 points and embedding degree $k = 6$.
- Every point on the curve is a generator, since the group order $n = 31$ is prime.
  The point $(1, 5)$ for example lies on the curve.

The Cocks-Pinch approach

This method works for arbitrary k and uses that $r \mid \Phi_k(t-1)$, i.e. that $t-1$ is a primitive k-th root of unity.

- First choose k, r and a CM discriminant D such that D is a square modulo r and $k \mid r-1$.
- Choose $g \in \mathbb{Z}$ a primitive k-th root of unity modulo r.
- Let $a \in \mathbb{Z}$ s.t. $a \equiv (g+1)/2 \mod r$, then

$$r \mid (2a-1)^k - 1.$$

- Set $b_0 \equiv (a-1)/\sqrt{D} \mod r$, then

$$r \mid (a-1)^2 - Db_0^2.$$

The Cocks-Pinch approach

- Run through integer values for i until

$$p = a^2 - D(b_0 + ir)^2$$

is prime, then $r \mid p + 1 - 2a$, since

$$\begin{aligned} p + 1 - 2a &= a^2 - 2a + 1 - D(b_0 + ir)^2 \\ &\equiv (a-1)^2 - Db_0^2 \mod r \\ &\equiv 0 \mod r. \end{aligned}$$

- Since p is quadratic in a and $b = b_0 + ir$ such curves always have $\rho \approx 2$.

The Brezing-Weng method

Brezing and Weng apply the Cocks-Pinch approach, but they parametrize r, t, p as polynomials.

- Choose k and D and choose an irreducible polynomial $r(x)$ which generates a number field K containing $\sqrt{D}$ and a primitive k-th root of unity.
- In this setting do the Cocks-Pinch construction.
- The ρ-value of curves constructed with this method depends on the degrees of r, t, p.
- One can often choose the degrees such that the ρ-value is less than 2.

Generalisation of the MNT approach

We need to find parametrisations for p and n such that

$$n(u) \mid \Phi_k(p(u)).$$

A result by Galbraith, McKee and Valença (2004) helps when p is parametrised as a quadratic polynomial.

- Lemma: Let $p(u) \in \mathbb{Q}[u]$ be a quadratic polynomial, ζ_k a primitive k-th root of unity in $\mathbb{C}$. Then

  $$\Phi_k(p(u)) = n_1(u)n_2(u)$$

  for irreducible polynomials $n_1(u), n_2(u) \in \mathbb{Q}[u]$ of degree $\varphi(k)$, if and only if the equation

  $$p(z) = \zeta_k$$

  has a solution in $\mathbb{Q}(\zeta_k)$.

Larger embedding degree

The MNT results can be obtained by applying this lemma. But we get more:

- For $k = 12$ we get the following

$$\Phi_{12}(6u^2) = n(u)n(-u),$$

  where $n(u) = 36u^4 + 36u^3 + 18u^2 + 6u + 1$.
- This does not help, since $6u^2$ can never be a prime.
- But since $n = p + 1 - t$ we use $p \equiv t - 1 \pmod{n}$, i.e.

$$n \mid \Phi_k(p) \iff n \mid \Phi_k(t-1).$$

  We might as well parametrise $t(u) - 1 = 6u^2$.

BN curves

BN curves (Barreto, N.) have embedding degree $k = 12$.
Choose

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

We then have $t(u) = 6u^2 + 1$,

$$n(u) \mid \Phi_{12}(p(u))$$

and

$$t(u)^2 - 4p(u) = -3(6u^2 + 4u + 1)^2,$$

i. e. the conditions are satisfied in $\mathbb{Z}[u]$ (as polynomials).

BN curves

- Since the norm equation is of the required form with $D = -3$ already as polynomials, there is no need to solve an equation as in the MNT case.
- Only try different values for u until $p(u)$ and $n(u)$ are prime.
- Since $D = -3$ always, there is no need to use the CM method, since such curves always have j-invariant $j = 0$ and are of the form

$$y^2 = x^3 + b.$$

- We only need to try different values for b until the curve has the right order.
- It is very easy to find BN curves of a certain bitsize.
- And they have many advantages for efficient implementation of pairings.

A BN curve with 256 bits

The curve

$$E : y^2 = x^3 + 3$$

over $\mathbb{F}_p$ with

$$\begin{aligned} p = \; & 115792089236777279154921612155485810787 \\ & 751121520685114240643525203619331750863 \end{aligned}$$

has

$$\begin{aligned} n = \; & 115792089236777279154921612155485810787 \\ & 410839153764967643444263417404280302329 \end{aligned}$$

points and embedding degree $k = 12$. The group $E(\mathbb{F}_p)$ is generated by $(1, 2)$.
($u = -7530851732707558283$,
$t = 340282366920146597199261786215051448535$)

Freeman curves

Freeman curves have embedding degree $k = 10$. Choose

$$\begin{aligned} n(u) &= 25u^4 + 25u^3 + 15u^2 + 5u + 1, \\ p(u) &= 25u^4 + 25u^3 + 25u^2 + 10u + 3. \end{aligned}$$

We then have $t(u) = 10u^2 + 5u + 3$,

$$n(u) \mid \Phi_{10}(p(u))$$

and

$$t(u)^2 - 4p(u) = -(15u^2 + 10u + 3).$$

To solve the norm equation we also need to solve a Pell equation as in the classical MNT case.

Pairing-friendly elliptic curves

There are methods for constructing pairing-friendly elliptic curves with a prime order group of rational points in the following cases:

$k \in \{3, 4, 6\}$:	Miyaji, Nakabayashi, Takano (2001),
$k = 10$:	Freeman (2006),
$k = 12$:	Barreto, N. (2005).

For all other embedding degrees there are methods to construct pairing-friendly elliptic curves, but the groups of rational points are no longer of prime order.

For an overview see the ”Taxonomy of pairing-friendly elliptic curves” (Freeman, Scott, Teske, 2006).
`http://eprint.iacr.org/2006/372`