

The Mathematics of Pairings II

Frederik Vercauteren
MAGMA - University of Sydney
ESAT/COSIC - K.U. Leuven - Belgium

Pairing based Cryptography Workshop - 2006

Outline

Curve Construction

Ate Pairing

Properties of Pairing-Friendly Curves

- ▶ Need elliptic curve E over \mathbb{F}_q with:
- ▶ Large prime $\ell \mid \#E(\mathbb{F}_q)$
- ▶ Embedding degree k “small enough”, i.e.

$$q^k - 1 = 0 \pmod{\ell} \quad \text{or} \quad \Phi_k(q) = 0 \pmod{\ell}$$

- ▶ For random q and E , always have $k \simeq \ell$, so useless for pairing computation.

Supersingular Curves

- ▶ Let $\#E(\mathbb{F}_q) = q + 1 - t$, then E is called supersingular if and only if

$$\gcd(t, q) > 1$$

- ▶ For q large prime p implies $t = 0$, since $|t| \leq 2\sqrt{q}$.
- ▶ Theorem: if E is supersingular, then $k \in \{1, 2, 3, 4, 6\}$.
 - ▶ $k = 6$ only possible if $q = 3^n$.
 - ▶ $k = 4$ only possible if $q = 2^n$.
 - ▶ For large prime $q = p$, have $k \leq 2$, since $\#E(\mathbb{F}_p) = p + 1$.

Supersingular Curves: Examples

- ▶ Let $q = p$ be a large prime, then the following curves are supersingular

$$p = 3 \pmod{4} \quad y^2 = x^3 + ax, \quad \text{for any } a \in \mathbb{F}_q^\times$$

$$p = 5 \pmod{6} \quad y^2 = x^3 + b, \quad \text{for any } b \in \mathbb{F}_q^\times$$

- ▶ Very easy to construct.
- ▶ Main disadvantage: $k = 2$ is fixed.
- ▶ Exercise: prove that above curves have $p + 1$ points.
- ▶ Hint: in the first case, note -1 is a non-square; in the second case, note $z \mapsto z^3$ is bijection.

Supersingular Curves: Distortion Map

- ▶ Let $P \in E(\mathbb{F}_q)$, then a distortion map for P is $\psi \in \text{End}(E)$ with $\psi(P) \notin \langle P \rangle$.
- ▶ Distortion maps only exist for supersingular curves.
- ▶ Example: $p = 3 \pmod{4}$ and $E : y^2 = x^3 + ax$.
- ▶ Let $\mathbb{F}_{p^2} = \mathbb{F}_p(i)$ with $i^2 = -1$,
- ▶ Then $\psi : (x, y) \mapsto (-x, iy)$ is a distortion map.
- ▶ Given any pairing $e(\cdot, \cdot) : E(\mathbb{F}_q)[\ell] \times E(\mathbb{F}_{q^k})[l]$, can obtain modified pairing

$$\hat{e}(\cdot, \cdot) : E(\mathbb{F}_q)[\ell] \times E(\mathbb{F}_q)[\ell] : (P, Q) \mapsto (P, \psi(Q))$$

- ▶ Note in this case: $\hat{e}(P, P) \neq 1$.

Ordinary Curves

- ▶ If E is not supersingular, then E is called ordinary.
- ▶ Problem: how to find ordinary E with small k ?
- ▶ Conditions:

$$\#E(\mathbb{F}_q) = h\ell \quad \text{and} \quad \Phi_k(q) = 0 \pmod{\ell},$$

for some $q = p^n$, prime ℓ , small k and $h \in \mathbb{N}$.

- ▶ Write $\#E(\mathbb{F}_q) = q + 1 - t$, then $q = t - 1 \pmod{\ell}$ so

$$\Phi_k(t - 1) = 0 \pmod{\ell}$$

- ▶ Can find tuples (q, t, ℓ, k) , but how to find elliptic curve?

Complex Multiplication

- ▶ Given q, t such that there exists E with $\#E = q + 1 - t$.
- ▶ Can find E using Complex Multiplication method,
- ▶ BUT: only when the discriminant D is small, i.e. $D < 2^{30}$.
- ▶ Discriminant D is square-free part of $4q - t^2$, i.e.

$$4q - t^2 = c^2 D$$

- ▶ Since q is at least 2^{160} , very unlikely for random q and t .

Constructing Ordinary Curves

Need to find tuples (q, t, ℓ, k) , with

- ▶ q and ℓ prime.
- ▶ $\ell | q + 1 - t$, trace $|t| \leq 2\sqrt{q}$.
- ▶ $\ell | q^k - 1$ and $\ell \nmid q^i - 1$ for $i < k$ or $\Phi_k(t - 1) = 0 \pmod{\ell}$.
- ▶ $4q - t^2 = Dc^2$ for small positive integer D
- ▶ If $q + 1 - t = h\ell$ then

$$Dc^2 = 4h\ell - (t - 2)^2$$

- ▶ $\rho = \log(q) / \log(\ell)$ should be as small as possible (e.g. ≈ 1).

Cocks-Pinch Algorithm

- ▶ Fix k and D first, then choose ℓ and try to compute the rest.
- ▶ t follows from $\Phi_k(t-1) = 0 \pmod{\ell}$ ($k \mid \ell - 1$).
- ▶ Compute $c = (t-2)/\sqrt{-D} \pmod{\ell}$ ($-D$ square mod ℓ).
- ▶ Let $q = (t^2 + Dc^2)/4$, then if q is integer and prime, done.
- ▶ Effective since probability that q is prime high enough.
- ▶ Advantages:
 - ▶ Easy to implement.
 - ▶ Efficient algorithm.
 - ▶ Can choose ℓ fairly freely.
- ▶ Main problem: t about the same size as ℓ , so q is twice the size of ℓ , i.e. $\rho \approx 2$.
- ▶ Luca-Shparlinski: For $\rho \approx 1$ solutions are very scarce!

MNT Curves

- ▶ Miyaji, Nakabayashi and Takano categorized all prime order curves with $k = 3, 4, 6$
- ▶ If E is an ordinary elliptic curve with prime order $q + 1 - t$ and embedding degree k if and only if $\exists x$ with

| k | q | t |
|-----|---------------|-----------------|
| 3 | $12x^2 - 1$ | $-1 \pm 6x$ |
| 4 | $x^2 + x + 1$ | $-x$ or $x + 1$ |
| 6 | $4x^2 + 1$ | $1 \pm 2x$ |

- ▶ Choose D and try to solve CM equation using the above.
- ▶ Some curves can be found (testing various D), but not many.

Families of Curves

- ▶ Choose D fixed, but use polynomials for other parameters.
- ▶ Recall original CM equation:

$$Dc^2 = 4q - t^2 = 4h\ell - (t - 2)^2$$

- ▶ Look for polynomials $q(x)$, $t(x)$, $c(x)$, $\ell(x)$ such that

$$Dc(x)^2 = 4q(x) - t(x)^2 \quad \text{and} \quad \Phi_k(t(x) - 1) = 0 \pmod{\ell(x)}$$

- ▶ Try to find x such that $\ell(x)$ and $q(x)$ is prime; again probability is quite high.

Barreto-Naehrig Curves

- ▶ $p(x) = 36x^4 + 36x^3 + 24x^2 + 6x + 1$.
- ▶ $t(x) = 6x^2 + 1$.
- ▶ $\ell(x) = p(x) + 1 - t(x)$.
- ▶ Then $\Phi_{12}(p(x)) \equiv 0 \pmod{\ell(x)}$ and

$$4p(x) - t(x)^2 = 3(6x^2 + 4x + 1)^2.$$

- ▶ Construction of BN-curve:
 - ▶ Find x such that $p(\pm x)$ and $\ell(\pm x)$ are primes.
 - ▶ Check $\#E(\mathbb{F}_p) = \ell(\pm x)$ for randomly chosen

$$E : y^2 = x^3 + b, b \in \mathbb{F}_p.$$

- ▶ Then E satisfies all conditions and $k = 12$.
- ▶ No CM construction necessary!

Outline

Curve Construction

Ate Pairing

Recap on Tate Pairing

- ▶ Let $P \in E(\mathbb{F}_q)[\ell]$ and $f_{\ell,P} \in \mathbb{F}_q(E)$ with

$$(f_{\ell,P}) = \ell(P) - \ell(\infty)$$

- ▶ The Tate pairing (assuming $f_{\ell,P}$ normalised) was defined as

$$\langle P, Q \rangle_{\ell} = f_{\ell,P}(Q)$$

for $Q \in E(\mathbb{F}_{q^k})$ with $Q \neq P, \infty$.

- ▶ Can loop in Miller's algorithm be shorter than $\log_2(\ell)$?
- ▶ Supersingular curves: Barreto, Galbraith, O'hEigeartaigh and Scott.
- ▶ All curves: Hess, Smart and Vercauteren, but need to swap arguments.

Endomorphism ring

- ▶ Endomorphism ring $\text{End}(E)$.
 - ▶ π_q Frobenius endomorphism $(x, y) \mapsto (x^q, y^q)$.
 - ▶ $[m]$ multiplication-by- m endomorphism.
 - ▶ $\mathbb{Z}[\pi_q] \subseteq \text{End}(E)$, $\pi_q^2 - t\pi_q + q = 0$, $|t| \leq 2\sqrt{q}$.
- ▶ The Frobenius π_q has two eigenspaces in $E(\mathbb{F}_{q^k})[\ell]$ for the eigenvalues $1, q$.
- ▶ Let $P, Q \in E(\mathbb{F}_{q^k})[\ell]$ with $\pi_q(P) = P$ and $\pi_q(Q) = qQ$.
- ▶ Then $E(\mathbb{F}_{q^k})[\ell] = \langle P \rangle \times \langle Q \rangle$ and $P \in E(\mathbb{F}_q)[\ell]$ for $k > 1$.

Ate pairing I

- ▶ Take $P \in E(\mathbb{F}_q)[r]$ and $Q \in E[r]$ with $\pi_q(Q) = qQ$.
- ▶ Theorem: Let $T = t - 1$ with $\#E(\mathbb{F}_q) = q + 1 - t$ and $T^k \neq 1$. Then

$$\hat{t}_\ell(Q, P) = f_{T, Q}(P)$$

is a pairing, called the Ate pairing.

- ▶ P and Q are swapped compared with Tate pairing.
- ▶ Arguments are restricted to eigenspaces of Frobenius.
- ▶ Loop length is now $\log_2(T)$, but first argument over \mathbb{F}_{q^k} .

Ate pairing: Efficiency?

- ▶ Loop length: $\log_2(T)$ vs. $\log_2(\ell)$ for Tate, but to compute $f_{T,Q}$ need point operations over \mathbb{F}_{q^k} .
- ▶ In general $T \simeq \sqrt{q}$, but could be as small as $\ell^{1/\varphi(k)}$.
- ▶ With above definition, Ate will almost always be slower than Tate!
- ▶ Need an extra trick to work over smaller field in first argument.

Twists

- ▶ Let E' be another elliptic curve defined over \mathbb{F}_q .
- ▶ We call E' a twist of E of degree d if there is an isomorphism $\psi : E' \rightarrow E$ defined over \mathbb{F}_{q^d} , and d is minimal.
- ▶ A twisting isomorphism ψ defines
 - ▶ a vector space isomorphism $E'(\mathbb{F}_{q^d})[\ell] \rightarrow E(\mathbb{F}_{q^d})[\ell]$.
 - ▶ a ring isomorphism $\text{End}(E') \rightarrow \text{End}(E)$, $\phi \mapsto \psi\phi\psi^{-1}$.
 - ▶ carries the q^d -power Frobenius of E' to that of E , hence $\psi\pi_q'^d\psi^{-1} = \pi_q^d$.

Twists and modified Ate pairing

- ▶ Assume
 - ▶ $k = ed$ and E has twist E' over \mathbb{F}_{q^e} of degree $d > 1$,
 - ▶ twisting isomorphism $\psi : E' \rightarrow E$, $Q' = \psi^{-1}(Q)$.
- ▶ Then E' and ψ can be chosen such that $E'(\mathbb{F}_{q^e})[\ell] = \langle Q' \rangle$.
- ▶ Modified Ate pairing $\hat{t}'_\ell : G'_2 \times G_1 \rightarrow G_T$ with $G'_2 = \langle Q' \rangle$,
 $G_1 = \langle P \rangle$, $G_T = \mu_\ell$

$$\hat{t}'_\ell(Q', P) = \hat{t}_\ell(\psi(Q'), P)$$

- ▶ Advantages: runtime and bandwidth savings.
- ▶ Field of definition of Q between $\mathbb{F}_{q^{k/6}}$ and $\mathbb{F}_{q^{k/2}}$.
- ▶ For sextic twists, up to 6 times faster than Tate pairing.

Questions?

End of Part II . . . there is no part III