The Ate pairing – Computational aspects of pairings in cryptography

Fields Institute

October 30, 2006

Florian Hess
Technical University Berlin

Overview

Pairings

Let G_1, G_2, G_T be abelian groups. A pairing is a non-degenerate bilinear map $e : G_1 \times G_2 \to G_T$.

Bilinearity:

- $e(g_1 + g_2, h) = e(g_1, h)e(g_2, h)$,
- $e(g, h_1 + h_2) = e(g, h_1)e(g, h_2)$.

Non-degenerate:

- For every $g \neq 0$ there is h with $e(g, h) \neq 1$.
- For every $h \neq 0$ there is g with $e(g, h) \neq 1$.

Examples:

- Scalar product on euclidean space $\langle \cdot, \cdot \rangle : \mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}$.
- Weil- and Tatepairings on elliptic curves and abelian varieties.

What are pairings good for?

Everything which has do with “linear algebra”:

- Checking for linear independence or dependence,
- Solving for linear combinations $g = \sum_i \lambda_i g_i$,
- ...

Of interest here: Many applications in cryptography!

- Identity based cryptography,
- Pairing based cryptography.

Also leads to some nice applications of computational number theory ...

Suitable pairings

Some basic requirements on pairings in cryptography:

- Group laws of G_1, G_2, G_T and pairing easy to compute.
- Hard DLP in G_1, G_2, G_T.

Weil- and Tatepairings on elliptic curves and Jacobians of curves of genus > 1 over finite fields.

These are the to date only known suitable pairings.

Main issues:

- Existence
- Efficiency
- Security

Overview

1. Introduction

2. Basic definitions and pairing characteristics

3. Existence and constructions

4. Pairing computation: Ate pairing

5. Security issues

6. Further topics

Elliptic Curves

Base field $\mathbb{F}_q$ with $q = p^r$.

E elliptic curve E defined over $\mathbb{F}_q$.

- Point sets $E(\mathbb{F}_{q^k})$ are abelian groups.
- $E(\mathbb{F}_{q^k})[\ell]$ subgroup of points of order ℓ.
- Point at infinity $\infty \in E(\mathbb{F}_q)$ is neutral element.

Assume

- exists subgroup $E(\mathbb{F}_q)[\ell]$ of large prime order $\ell \nmid q$.
- embedding degree is k, that is $\ell \,||\, (q^k - 1)$ and k minimal.

Then $E(\mathbb{F}_{q^k})[\ell] \cong \mathbb{Z}/\ell\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z}$ and $\mu_\ell \subseteq \mathbb{F}_{q^k}^\times$.

Tate pairing

The Tate pairing $\langle \cdot, \cdot \rangle_\ell : E(\mathbb{F}_{q^k})[\ell] \times E(\mathbb{F}_{q^k})/\ell E(\mathbb{F}_{q^k}) \to \mathbb{F}_{q^k}^\times / (\mathbb{F}_{q^k}^\times)^\ell$ is defined as follows.

Let $P \in E(\mathbb{F}_{q^k})[\ell]$ and $f_{n,P} \in \mathbb{F}_{q^k}(E)$ with $(f_{n,P}) = n((P) - (\infty)) - ((nP) - (\infty))$.
Let $Q \in E(\mathbb{F}_{q^k})$. Choose $R \in E(\mathbb{F}_{q^k})$ with $\{Q+R, R\} \cap \{P, \infty\} = \emptyset$.

Then $\langle P, Q \rangle_\ell = f_{\ell,P}(Q+R)/f_{\ell,P}(R) \cdot (\mathbb{F}_{q^k}^\times)^\ell$.

The reduced Tate pairing $t_\ell : E(\mathbb{F}_{q^k})[\ell] \times E(\mathbb{F}_{q^k})[\ell] \to \mu_\ell$ is defined as $t_\ell(P,Q) = \langle P, Q \rangle_\ell^{(q^k-1)/\ell}$.

Endomorphism ring

Endomorphism ring End(E).

- π_q Frobenius endomorphism $(x,y) \mapsto (x^q, y^q)$.
- $[m]$ multiplication-by-m endomorphism.
- $\mathbb{Z}[\pi_q] \subseteq$ 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 $E(\mathbb{F}_{q^k})[\ell] = \langle P \rangle \times \langle Q \rangle$ und $P \in E(\mathbb{F}_q)[\ell]$.

E ordinary if End(E) commutative, else E supersingular.

Pairing characteristics

More properties:

- $\langle P,P \rangle_\ell = \langle Q,Q \rangle_\ell = 1$, $\langle P,Q \rangle_\ell \neq 1$.
- Endomorphism Tr $= c\sum_{i=0}^{k-1} \pi_q^i$ with $kc \equiv 1 \bmod \ell$ yields surjective projection $\langle P \rangle \times \langle Q \rangle \to \langle P \rangle$ with kernel $\langle Q \rangle$ (trace zero subgroup).

A distortion map for $T = \lambda P + \mu Q \neq 0$ is $\psi \in$ End(E) with $\psi(T) \notin \langle T \rangle$.
Tr is a distortion map if $\lambda \neq 0$ and $\mu \neq 0$.
A distortion map exists for $T = P, Q$ if and only if E is supersingular.

Can choose groups G_1 and G_2 for pairing according to needs:

- Hashing possible
- Short representations
- Homomorphisms between groups

Pairing characteristics

Type 1: Supersingular curve with distortion map $Q = \psi(P)$.

- $G_1 = G_2$

Type 2: Ordinary curve with $G_1 = \langle P \rangle$, $G_2 = \langle \lambda P + \mu Q \rangle$, trace map.

- $G_1 \neq G_2$ with one-way homomorphism $G_2 \to G_1$

Type 3: Ordinary curve with $G_1 = \langle P \rangle$, $G_2 = \langle Q \rangle$.

- $G_1 \neq G_2$ no homomorphism

More detailed discussion in Galbraith, Paterson, Smart and Smart, Vercauteren.

Pairing parameters

Most important parameter: Embedding degree k.

DLP security in $E(\mathbb{F}_q)$ grows like $e^{1/2 \log q}$
DLP security in $\mathbb{F}_{q^k}^\times$ grows like $e^{c(k \log q)^{1/3}}$.

Should be balanced, hence $k \approx (\log q)^{2/3}$.

Symm	ECC	RSA	k
80	160	1024	6
128	256	3072	12
256	512	15360	30

Overview

Pairing Constructions

Supersingular curves yield $k \in \{2,3,4,6\}$.

Conditions on q, ℓ, $t = q+1-\#E(\mathbb{F}_q)$ and k:

- $q+1-t = c\ell$, q prime power, ℓ prime, $|t| \leq 2\sqrt{q}$.
- $\phi_k(q) \equiv 0 \bmod \ell$ (implies $q^k - 1 \equiv 0 \bmod \ell$).
- $\rho = \log(q)/\log(\ell)$ should be as small as possible (e.g. ≈ 1).
- $4q - t^2 = Df^2$ with D small for CM method.

Finding solutions for arbitrary k with $\rho \approx 2$ by clever searching algorithms is fairly easy (Cocks-Pinch).

For $\rho \approx 1$ solutions are very scarse! (Luca-Shparlinski, Freeman)

Given k, solutions to q, ℓ with $1 \leq \rho \leq 2$ can often be found as parametric families $q = q(z), \ell = \ell(z)$.

Barreto-Naehrig curves

Let

- $p(z) := 36z^4 + 36z^3 + 24z^2 + 6z + 1$
- $t(z) := 6z^2 + 1$
- $\ell(z) := p(z) + 1 - t(z)$.

Then $\phi_{12}(p(z)) \equiv 0 \bmod \ell(z)$ and $4p(z) - t(z)^2 = 3(6z^2 + 4z + 1)^2$.

Construction of BN-curve:

- Find $z \in \mathbb{Z}$ such that $p(z)$ and $\ell(z)$ are primes.
- Check $\#E(\mathbb{F}_p) = \ell(z)$ for randomly chosen $E : y^2 = x^3 + b$, $b \in \mathbb{F}_p$.
- If ok then E satisfies all conditions and $k = 12$.

No CM construction, suitable E is found after expected 6 tries!

Overview

Classical Tate pairing

Use restricted reduced Tate pairing

$$t_\ell : \langle P \rangle \times \langle Q \rangle \to \mu_\ell, \quad t_\ell(P,Q) = (f_{\ell,P}(Q+R)/f_{\ell,P}(R))^{(q^k-1)/\ell}.$$

First improvement – Lemma: $t_\ell(P,Q) = f_{\ell,P}(Q)^{(q^k-1)/\ell}$.

Miller's algorithm for evaluating Miller functions $f_{\ell,P}(Q)$:

- Based on Miller's formulae: $f_{a+b,P} = f_{a,P} \cdot f_{b,P} \cdot g_{aP,bP}/g_{(a+b)P,-(a+b)P}$ where $g_{U,V}$ is the line through U and V.
- Performs essentially a multiplication ℓP carrying elements in $\mathbb{F}_{q^k}$ along, thus double-and-add loop length $\log_2(\ell)$.

Further improvements possible (Barreto, Kim, Lynn and Scott; Granger, Page and Smart.)

Ate pairing

In the following some new improvements for ordinary elliptic curves.

Joint work with Smart and Vercauteren.

Generalises the Eta pairing of Barreto, Galbraith, O'hEigeartaigh and Scott for supersingular curves.

Yields shortening of the loop length in Miller's algorithm.

- Loop length now between $(1/\phi(k))\log_2(\ell)$ and $(1/2)\log_2(\ell)$.
- Field of definition of "P" between $\mathbb{F}_{q^{k/6}}$ and $\mathbb{F}_{q^{k/2}}$, while "Q" is in $\mathbb{F}_q$.
- Improvement of up to a factor of 6 in our examples.

Ate pairing

Use restricted reduced Tate pairing

$$t_\ell : \langle Q \rangle \times \langle P \rangle \to \mu_\ell, \quad t_\ell(Q,P) = (f_{\ell,Q}(P+R)/f_{\ell,Q}(R))^{(q^k-1)/\ell}.$$

First improvement – Lemma: $t_\ell(Q,P) = f_{\ell,Q}(P)^{(q^k-1)/\ell}$.

Theorem: Let $T = t-1$ with $\#E(\mathbb{F}_q) = q+1-t$ and $T^k \not\equiv 1$. Then

$$\hat{t}_\ell(Q,P) = f_{T,Q}(P)^{(q^k-1)/\ell}$$

is a pairing.

We call $\hat{t}_\ell(Q,P)$ the Ate pairing (why?).

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 $\psi : E' \to E$ defined over $\mathbb{F}_{q^d}$, and d is minimal.

A twisting isomorphism ψ defines

- an isomorphism $E'(\mathbb{F}_{q^d})[\ell] \to E(\mathbb{F}_{q^d})[\ell]$.
- ...

E has a twist of degree d if and only if E has an automorphism of order d (necessarily defined over $\mathbb{F}_q$ if E is ordinary).

Twists and modified Ate pairing

Assume

- E ordinary, $k = ed$ and E has twist E' over $\mathbb{F}_{q^e}$ of degree $d > 1$ with twisting isomorphism $\psi : E' \to E$.
- Let $Q' = \psi^{-1}(Q)$.

Then E' and ψ can be chosen such that $E'(\mathbb{F}_{q^e})[\ell] = \langle Q' \rangle$.

Yields modified Ate pairing

$$\hat{t}'_\ell : \langle Q' \rangle \times \langle P \rangle \to \mu_\ell, \quad \hat{t}'_\ell(Q', P) = \hat{t}_\ell(\psi(Q'), P).$$

Advantages: Runtime and bandwidth savings.

Ate pairing

Lemma:

$$t_\ell(Q,P) = \left(f_{\ell,Q}(P+R)/f_{\ell,Q}(R)\right)^{(q^k-1)/\ell} = f_{\ell,Q}(P)^{(q^k-1)/\ell}.$$

Proof: We have

$$\begin{aligned} e_\ell(P,Q)^{(q^k-1)/\ell} &= \left(f_{\ell,P}(Q)/f_{\ell,Q}(P)\right)^{(q^k-1)/\ell} \\ &= t_\ell(P,Q)/t_\ell(Q,P) \end{aligned}$$

by Miller's formulae for $e_\ell(P,Q)$, and $t_\ell(P,Q) = f_{\ell,P}(Q)^{(q^k-1)/\ell}$. Cancelling out gives $t_\ell(Q,P) = f_{\ell,Q}(P)^{(q^k-1)/\ell}$. $\square$

Ate pairing

Theorem: Let $T = t-1$ with $\#E(\mathbb{F}_q) = q+1-t$ and $T^k \not\equiv 1$.
Then $\hat{t}_\ell(Q,P) = f_{T,Q}(P)^{(q^k-1)/\ell}$ is a pairing.

Proof: Let $N = \gcd(T^k-1, q^k-1)$, $T^k - 1 = LN$. Since $q = T \bmod \ell$, we have $\ell || N$ and $\ell \nmid L$.

$$\begin{aligned} t_\ell(Q,P)^L &= f_{\ell,Q}(P)^{L(q^k-1)/\ell} = f_{N,Q}(P)^{L(q^k-1)/N} = f_{LN,Q}(P)^{(q^k-1)/N} \\ &= f_{T^k-1,Q}(P)^{(q^k-1)/N} = f_{T^k,Q}(P)^{(q^k-1)/N}. \end{aligned}$$

Now $f_{T^k,Q} = f_{T,Q}^{T^{k-1}} f_{T,TQ}^{T^{k-2}} \cdots f_{T,T^{k-1}Q}$ and $TQ = \pi_q(Q)$ and $f_{T,\pi_q(Q)} = f_{T,Q}^{\sigma}$.

We obtain $f_{T^k,Q}(P) = f_{T,Q}(P)^{T^{k-1}+T^{k-2}q+\dots+q^{k-1}}$ and
$t_\ell(Q,P)^L = f_{T,Q}(P)^{c(q^k-1)/N}$ with $c = T^{k-1} + T^{k-2}q + \cdots + q^{k-1} \equiv kq^{k-1} \bmod \ell$.

Since LHS has order ℓ and cofactors are not divisible by ℓ we get

Ate pairing

Proof (ctd).

$t_\ell(Q,P)^d = f_{T,Q}(P)^{(q^k-1)/\ell} = \hat{t}_\ell(Q,P)$ for some $d \not\equiv 0 \bmod \ell$.

Since t_ℓ is a pairing, $\hat{t}_\ell(Q,P)$ is also a pairing. $\square$

Overview

1. Introduction

2. Basic definitions and pairing characteristics

3. Existence and constructions

4. Pairing computation: Ate pairing

5. Security issues

Security issues

Let $e : G_1 \times G_2 \longrightarrow G_T$ be a pairing.

Pairing must be hard to invert (find x, y in $e(x, Q) = z$ and $e(P, y) = z$).
Verheul showed: If the pairing can be inverted, then the CDH on G_1, G_2 and G_T can be solved easily.

Maybe putting Verheul's reasoning upside down: Construct classes of finite fields where the CDH is easy but the DLP is hard?

What are the functions f of smallest degree and values of r such that $P \mapsto f(P)^r$ defines a non-trivial homomorphism?

If $P \mapsto f(P)$ defines a non trivial homomorphism, then $\deg(f) \geq \ell/6$ ...

Thank you for your attention! Questions?