Computational aspects of pairings in cryptography

Magma 2006

August 2, 2006

Florian Hess

Technical University Berlin

Overview

1. Introduction
2. Basic definitions and pairing characteristics
3. Existence and constructions
4. Pairing computation: Ate pairing
5. Security issues
6. Further topics

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:

- $x \mapsto e(g, x)$ injective, $x \mapsto e(x, h)$ injective for all $g \neq 1$, $h \neq 1$.

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.

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.
- Group orders should be finite.

Suitable pairings

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 $\ell \neq q$.
- 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 $t_\ell(P, Q) = \langle P, Q \rangle_\ell^{(q^k - 1)/\ell}$.

Weil pairing

The Weil pairing $e_\ell : E(\mathbb{F}_{q^k})[\ell] \times E(\mathbb{F}_{q^k})[\ell] \to \mu_\ell$ is defined as follows.

Let $P, Q \in E(\mathbb{F}_{q^k})[\ell]$ and $(f_{\ell,P} / f_{\ell,Q})(\infty) = 1$.

Then $e_\ell(P,Q) = \begin{cases} 1 & \text{for } P = Q \text{ or } P = \infty \text{ or } Q = \infty \\ (-1)^\ell f_{\ell,P}(Q) / f_{\ell,Q}(P) & \text{else.} \end{cases}$

The Weil pairing is non degenerate since $E(\overline{\mathbb{F}}_q)[\ell] \subseteq E(\mathbb{F}_{q^k})$.
The property $e_\ell(P,P) = 1$ is useful for subgroup membership testing.

We have $e_\ell(P,Q)^{(q^k-1)/\ell} = t_\ell(P,Q)/t_\ell(Q,P)$.

Endomorphism ring

Endomorphism ring End(E).

- π_q Frobenius endomorphism $(x,y) \mapsto (x^q, y^q)$.
- $[m]$ multiplication-by-m endomorphism.
- $\mathbb{Z}[\pi_q] \subseteq \mathrm{End}(E)$, $\pi_q^2 - t\pi_q + q = 0$, $|t| \leq 2\sqrt{q}$.

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 $\langle P\rangle \times \langle Q\rangle \longrightarrow \langle P\rangle$ with kernel $\langle Q\rangle$ (trace zero subgroup).

A distortion map for $T = \lambda P + \mu Q \neq 0$ is $\psi \in \mathrm{End}(E)$ 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.

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

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

- $G_1 \ncong G_2$ 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

1. Introduction
2. Basic definitions and pairing characteristics
3. Existence and constructions
4. Pairing computation: Ate pairing
5. Security issues
6. Further topics

Pairing Constructions

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

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

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

Finding solutions for arbitrary k with $\rho \approx 2$ by clever searching algorithms is fairly easy.

Luca-Shparlinski: For $\rho \approx 1$ solutions are very scarse!

Pairing Constructions

Ordinary curves via CM methods:

- MNT curves $\rho = 1$ and $k \in \{3, 4, 6\}$.
- Brezing-Weng $\rho = 5/4$ and $k = 8$, $k = 24$.
  Also $\rho \leq 5/4$ for prime $k \geq 13$.
- Freeman $\rho = 1$ and $k = 10$.
- Barreto-Naehrig curves $\rho = 1$ and $k = 12$.
- Duan-Cui-Chan various other higher values.

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

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

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 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, suitable E is found very fast.

Barreto-Naehrig curves

Why does this work?

Let ζ be primitive 6-th root of unity.

Observations:

- $\mathbb{Z}[\zeta]$ is the maximal order of $\mathbb{Q}(\sqrt{-3})$ of discriminant -3.
- There is $E/\mathbb{F}_{p(z)}$ with trace $t(z)$ and End$(E) = \mathbb{Z}[\zeta]$ by CM.
- Elliptic curve $E/\mathbb{F}_{p(z)}$ in SWF has automorphism of order 6 iff $E : y^2 = x^3 + b$. These curves are ordinary.
- There are 6 isogeny classes of $E/\mathbb{F}_{p(z)}$ with End$(E) = \mathbb{Z}[\zeta]$.

Existence of E and termination of the algorithm after six tries on average follows from the observations.

The particular structure of the BN-curves has further advantages.

Overview

1. Introduction
2. Basic definitions and pairing characteristics
3. Existence and constructions
4. Pairing computation: Ate pairing
5. Security issues
6. Further topics

Classical Tate pairing

Standard reduced Tate pairing $t_\ell : G_1 \times G_2 \to G_T$ with $G_1 = \langle P \rangle$, $G_2 = \langle Q \rangle$ and $G_T = \mu_\ell$.

First improvement:

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

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

- Requires a point multiplication ℓP.
- Requires $\approx 2\log_2(\ell)$ multiplications/squarings in $\mathbb{F}_{q^k}$.
- Requires $\approx \log_2(\ell)$ divisons involving $x(Q)$.

Second improvement:

- Adapt the base in Miller's algorithm.
- If $x(Q)$ is in proper subfield of $\mathbb{F}_{q^k}$, then omit all divisions.

Classical Tate pairing

Third improvement:

- Exploit low hamming weight group orders in Miller's algorithm.
- Exploit special form of exponent in final powering.

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.

Yields shortening of the loop length in Miller's algorithm, while extending the field of definition of P.

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

Ate pairing

Use reduced Tate pairing $t_\ell : G_2 \times G_1 \to G_T$ with
$G_1 = \langle P \rangle$, $G_2 = \langle Q \rangle$ and $G_T = \mu_\ell$.

First improvement:

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

Proof: Have $e_\ell(P,Q)^{(q^k-1)/\ell} = (f_{\ell,P}(Q)/f_{\ell,Q}(P))^{(q^k-1)/\ell} = t_\ell(P,Q)/t_\ell(Q,P)$
and $t_\ell(P,Q) = f_{\ell,P}(Q)^{(q^k-1)/\ell}$. Hence $t_\ell(Q,P) = f_{\ell,Q}(P)^{(q^k-1)/\ell}$. $\square$

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?).

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 $\ell \nmid L$.

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

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

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. $\square$

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

- a vector space isomorphism $E'(\mathbb{F}_{q^d})[\ell] \to E(\mathbb{F}_{q^d})[\ell]$.
- a ring isomorphism $\mathrm{End}(E') \to \mathrm{End}(E)$, $\phi \mapsto \psi\phi\psi^{-1}$.
- 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

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

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

Proof: Choose $\gamma \in \mathrm{Aut}_K(E)$ with $\gamma\pi_q^e(Q) = Q$. There is E' and ψ with $\psi\pi'_{q^e}\psi^{-1} = \gamma\pi_q^e$ for π'_{q^e} Frobenius on E'. Then $\pi'_{q^e}(Q') = Q'$ and $Q' \in E'(\mathbb{F}_{q^e})[\ell]$. Since $\ell \nmid (q^e - 1)$, $E'(\mathbb{F}_{q^e})[\ell] = \langle Q' \rangle$. $\square$

Modified Ate pairing $\hat{t}'_\ell : G'_2 \times G_1 \to G_T$
with $G'_2 = \langle Q' \rangle$, $G_1 = \langle P \rangle$, $G_T = \mu_\ell$ and $\hat{t}'_\ell(Q', P) = \hat{t}_\ell(\psi(Q'), P)$.

Advantages: Runtime and bandwidth savings.

Example

The BN curves.

- $E : y^2 = x^3 + b$ over $\mathbb{F}_p$ with $p \equiv 1 \bmod 6$.
- $\#E(\mathbb{F}_p) = \ell$ and $k = 12$.
- $\phi : (x, y) \mapsto (\zeta^2 x, \zeta^3 y)$ for $\zeta \in \mu_6$, hence E has twist E' of degree 6.
- $E' : \mu y^2 = \lambda x^3 + b$ with $\lambda \in \mathbb{F}_{p^2} \setminus (\mathbb{F}_{p^2})^3$ and $\mu \in \mathbb{F}_{p^2} \setminus (\mathbb{F}_{p^2})^2$.
- $E' \not\cong E$, $\psi : E' \to E$, $\psi(x, y) = (\lambda^{1/3} x, \mu^{1/2} y)$.

Hence compression factor $E/\mathbb{F}_{p^{12}}$ versus $E'/\mathbb{F}_{p^2}$ is 6.
Loop length is $(1/2)\log_2(\ell)$.

Overview

1. Introduction
2. Basic definitions and pairing characteristics
3. Existence and constructions
4. Pairing computation: Ate pairing
5. Security issues
6. Further topics

Security issues

Assume for simplicity $e : G \times G \to G_T$.

Group sizes G and G_T must be large enough to withstand attacks on DLP.

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 and G_T can be solved easily.

Protocols assume various other computation problems associated with pairings and the groups G and G_T. No rigorous analysis or comparison of these so far.

Multivariate attacks give faster algorithms for inverting the pairing?

Further topics

Easy DDH groups and the existence of distortion maps:

- P, aP, bP, abP, cP: $e(aP, bP) = e(P, cP)$ iff $abP = cP$.
- If $e(P, P) = 1$ use $e(P, \psi(P)) \neq 1$.

Compressed pairings: Apply

- techniques from LUC and XTR in finite fields.
- techniques from point reduction/point compression on elliptic curves.

Blinded pairings ...

Use hyperelliptic curves ...

- Offer compression technique not available on elliptic curves.
- More flexibility for embedding degrees?

Thank you for your attention! Questions?