
Pairing Lattices

GTEM Workshop on Pairings, IEM Essen
5. Mai 2009

Florian Heß
Technische Universität Berlin

Goal of this talk

Present main results:

Classification

- of all possible pairing functions within certain framework.
- of pairing functions among these with lowest degree.

Discuss some further aspects:

- Security implications.
- Pairing functions of lowest possible degree.
- Proof idea.
- Comparison with endomorphism speed up for point multiplication.
- Generalisations to arbitrary curves.

Standard pairing situation

E ordinary elliptic curve over \mathbb{F}_q with $\#E(\mathbb{F}_q) \equiv 0 \pmod{r}$.

Embedding degree $k \geq 2$ minimal such that $q^k \equiv 1 \pmod{r}$.

π Frobenius endomorphism of E , $(x, y) \mapsto (x^q, y^q)$.

Then

$$E(\mathbb{F}_{q^k})[r] = G_1 \times G_2$$

where

$$\#G_1 = \#G_2 = r, \quad G_1 = \langle P \rangle \text{ and } \pi(P) = P, \quad G_2 = \langle Q \rangle \text{ and } \pi(Q) = qQ.$$

$\mu_r \subseteq \mathbb{F}_{q^k}^\times$ group of r -th roots of unity.

Consider pairings

$$e : G_1 \times G_2 \rightarrow \mu_r.$$

Methodology for pairings

$$e : G_1 \times G_2 \rightarrow \mu_r$$

Tate pairings:

- $e : (P, Q) \mapsto f_P(Q)^{(q^k-1)/r}$ with $f_P \in \mathbb{F}_q(E)$,
- $e : (P, Q) \mapsto f_Q(P)^{(q^k-1)/r}$ with $f_Q \in \mathbb{F}_{q^k}(E)$.

Weil pairings:

- $e : (P, Q) \mapsto wf_P(Q)/f_Q(P)$ with $f_P \in \mathbb{F}_q(E)$, $f_Q \in \mathbb{F}_{q^k}(E)$.

But have $f_P(Q) \notin \mu_r$ or $f_P(Q_1 + Q_2) \neq f_P(Q_1)f_P(Q_2)$, etc.

Pairing lattices

Define $f_{s,h,R} \in \mathbb{F}_{q^k}(E)$ monic for $R \in E(\mathbb{F}_{q^k})[r]$ by

$$\operatorname{div}(f_{s,h,R}) = \sum_{i=0}^d h_i((s^i R) - (O))$$

for $h = \sum_{i=0}^d h_i x^i \in \mathbb{Z}[x]$ with $h(s) \equiv 0 \pmod{r}$.

Let s be a primitive k -th root of unity modulo r^2 .

Then have pairings ($a_{s,h}^{\text{twist}}$ and $e_{s,h}$ require $k \mid \#\operatorname{Aut}(E)$):

$$\begin{aligned} a_{s,h} &: G_2 \times G_1 \rightarrow \mu_r, & (Q, P) &\mapsto f_{s,h,Q}(P)^{(q^k-1)/r}, \\ a_{s,h}^{\text{twist}} &: G_1 \times G_2 \rightarrow \mu_r, & (P, Q) &\mapsto f_{s,h,P}(Q)^{(q^k-1)/r}, \\ e_{s,h} &: G_1 \times G_2 \rightarrow \mu_r, & (P, Q) &\mapsto w f_{s,h,P}(Q) / f_{s,h,Q}(P). \end{aligned}$$

Non-degenerate $\Leftrightarrow h(s) \not\equiv 0 \pmod{r^2}$.

Examples

Use $s \equiv q \pmod{r}$.

Pairing	Function	h with $h(q) \equiv 0 \pmod{r}$
BKLS 2001 / M 2003 (Tate / Weil)	$a_h, a_h^{\text{twist}}, e_h$	r
BGOS 2005 (Eta)	a_h^{twist}	$x - t(E) + 1$
HSV 2006 (Ate)	a_h, a_h^{twist}	$x - t(E) + 1$
MKHO 2007 / ZZH 2007 (optimised ate)	a_h, a_h^{twist}	$x^i - d$
LLP 2008 (R -ate)	a_h, a_h^{twist}	$x^{ij} - d_1 x^i - d_2$
V 2008 (optimal ate)	a_h	arbitrary
ZZ 2008 (Weil)	e_h^c	$x^i - d$
H 2008	$a_h, a_h^{\text{twist}}, e_h$	arbitrary

Silly remark

Observe the naming convention: Tate \rightarrow ate.

- The ate pairing is like the eta pairing but with arguments transposed.
- The ate pairing has shorter loop length than the Tate pairing.

Here is the proposal:

Use the analogous naming convention: Weil \rightarrow eil.

- The eil pairing has shorter loop length than the Weil pairing.
- eil means “hurry” in german!
- any objections from other languages?

\Rightarrow Lattice ate and eil pairings ...

Pairing lattices

Define $f_{s,h,R} \in \mathbb{F}_{q^k}(E)$ monic for $R \in E(\mathbb{F}_{q^k})[r]$ by

$$\operatorname{div}(f_{s,h,R}) = \sum_{i=0}^d h_i((s^i R) - (O))$$

for $h = \sum_{i=0}^d h_i x^i \in \mathbb{Z}[x]$ with $h(s) \equiv 0 \pmod{r}$.

Let s be a primitive k -th root of unity modulo r^2 .

Then have **pairings** ($a_{s,h}^{\text{twist}}$ and $e_{s,h}$ require $k \mid \#\operatorname{Aut}(E)$):

$$\begin{aligned} a_{s,h} &: G_2 \times G_1 \rightarrow \mu_r, & (Q, P) &\mapsto f_{s,h,Q}(P)^{(q^k-1)/r}, \\ a_{s,h}^{\text{twist}} &: G_1 \times G_2 \rightarrow \mu_r, & (P, Q) &\mapsto f_{s,h,P}(Q)^{(q^k-1)/r}, \\ e_{s,h} &: G_1 \times G_2 \rightarrow \mu_r, & (P, Q) &\mapsto w f_{s,h,P}(Q) / f_{s,h,Q}(P). \end{aligned}$$

Non-degenerate $\Leftrightarrow h(s) \not\equiv 0 \pmod{r^2}$.

Properties

Lattice arguments: Let $b_{s,h}$ denote $a_{s,h}$, $a_{s,h}^{\text{twist}}$ or $e_{s,h}$.

- $b_{s,h}$ non-degenerate $\Rightarrow \sum_i |h_i| \geq r^{1/\varphi(k)}$.
- There is h mit $\deg(h) \leq \varphi(k) - 1$ und $\sum_i |h_i| = O(r^{1/\varphi(k)})$ such that $b_{s,h}$ non-degenerate.
- h can be computed using the LLL algorithm.

Observe $\sum_i |h_i|/2 \leq \deg(f_{s,h,R}) \leq \sum_i |h_i|$.

Relation with the classical pairings:

$$a_{s,h}(Q, P) = t(Q, P)^{h(s)/r},$$

$$a_{s,h}^{\text{twist}}(P, Q) = t(P, Q)^{h(s)/r},$$

$$e_{s,h}(P, Q) = e(P, Q)^{h(s)/r}.$$

Properties

Write $Z_Q = \{\pi^i(Q) \mid 0 \leq i \leq k-1\}$.

Completeness:

- Let $f_Q \in \mathbb{F}_{q^k}(E)^\times$ be any function supported on Z_Q .
- Let $s \equiv q \pmod{r}$ and $s^k \equiv 1 \pmod{r^2}$.
- Then there is $h \in \mathbb{Z}[x]$ such that $f_Q(S)^{(q^k-1)/r} = a_{s,h}(Q, S)$ for all $S \in G_1$.

Hence **any** pairing $(P, Q) \mapsto f_Q(P)^{(q^k-1)/r}$ with f_Q supported on Z_Q is equal to $a_{s,h}$ for some h .

Similar result for $a_{s,h}^{\text{twist}}$. What about $e_{s,h}$?

Endomorphism redundancy

Let $n = \text{lcm}(k, \#\text{Aut}(E))$.

Let s be a primitive n -th root of unity modulo r with $s^n \equiv 1 \pmod{r^2}$.

Let $s = uq^d$ for u a primitive e -th root of unity modulo r and $e \mid \#\text{Aut}(E)$.

Let $\alpha \in \text{Aut}(E)$ of order e with $\alpha(Q) = uQ$.

Then have pairings ($a_{s,h}^{\text{twist}}$ and $e_{s,h}$ require $n \mid \#\text{Aut}(E)$):

$$a_{s,h} : G_2 \times G_1 \rightarrow \mu_r, \quad (Q, P) \mapsto \left(\prod_{j=0}^{e-1} f_{s,h,Q}(\alpha^{-j}(P))^{v^j} \right)^{(q^k-1)/r},$$

$$a_{s,h}^{\text{twist}} : G_1 \times G_2 \rightarrow \mu_r, \quad (P, Q) \mapsto \left(\prod_{j=0}^{e-1} f_{s,h,P}(\alpha^j(Q))^{v^j} \right)^{(q^k-1)/r},$$

$$e_{s,h} : G_1 \times G_2 \rightarrow \mu_r, \quad (P, Q) \mapsto w \prod_{j=0}^{e-1} \left(f_{s,h,P}(\alpha^j(Q)) / f_{s,h,Q}(\alpha^{-j}(P)) \right)^{v^j}.$$

Parametric families

Assume

- $n \geq 2$ and $q, s, r \in \mathbb{Z}[t]$ for a parametric family.
- s is primitive n -th root of unity modulo r^2 .

There is $h \in \mathbb{Z}[t][x]$

- with $\deg(h) \leq \varphi(n) - 1$ and $\deg_t(h) = \deg(r)/\varphi(n)$
- such that

$$a_{s(t_0), h(t_0, x)}, \quad a_{s(t_0), h(t_0, x)}^{\text{twist}}, \quad e_{s(t_0), h(t_0, x)}$$

are non-degenerate bilinear **pairings** for all sufficiently large “good” t_0 .

Any such h satisfies $\deg_t(h) \geq \deg(r)/\varphi(n)$.

h can be computed using the function field LLL.

Examples

Use $s(t) \equiv p(t) \pmod{r(t)}$.

Brezing-Weng:

$$k = 10, \varphi(k) = 4,$$

$$p(t) = (t^{12} - t^{10} + t^8 - 5t^6 + 5t^4 - 4t^2 + 4)/4,$$

$$r(t) = \phi_{20}(t) = t^8 - t^6 + t^4 - t^2 + 1,$$

$$h(t, x) = t^2x - 1.$$

Freeman:

$$k = 10, \varphi(k) = 4,$$

$$p(t) = 25t^4 + 25t^3 + 25t^2 + 10t + 3,$$

$$r(t) = 25t^4 + 25t^3 + 15t^2 + 5t + 1,$$

$$h(t, x) = x^4 + 5tx^3 + x^2 - x - 1.$$

Security implications?

Lemma:

Let $f \in \mathbb{F}_{q^k}(E)$. If

$$G_2 \rightarrow \mu_r, Q \mapsto f(Q) \quad \text{or} \quad G_1 \rightarrow \mu_r, P \mapsto f(P)$$

is a homomorphism, then

$$\deg(f) \geq r/6.$$

Example:

$E : y^2 = x^3 + 4$ over \mathbb{F}_q with $q = 41761713112311845269$,
 $r = 715827883$, $k = 31$, $s = -2$, $h = t - s$.

Then

$$a_{s,h} : G_2 \times G_1 \rightarrow \mu_r,$$

$$(Q, P) \mapsto \left(y_P - 3x_Q^2 / (2y_Q) x_P - (-x_Q^3 + 8) / (2y_Q) \right)^{(q^k - 1) / r}$$

is a non-degenerate pairing.

Security implications?

Interpretation:

- Pairing inversion always involves equations of high degree, should generally be hard to solve.
- Pairing lattices do not produce functions of miraculously small degree.
- Easiest form is Hidden Root Problem, maybe want $r^{1/\varphi(k)}$ be sufficiently large ...

Pairing functions of lowest degree?

Tate pairing:

- $\deg(f_{s,h,Q}^{(q^k-1)/r}) \approx (q^k - 1)/r \cdot r^{1/\varphi(k)} \approx r^{k-1+1/\varphi(k)}$.
- Thus log of degree about at least k times larger than necessary.

Eil pairing, $k = 3$ or $k = 6$, $s = t - 1$:

- Extend definition of $f_{s,h,R} \in \mathbb{F}_{q^k}(E)$ monic by

$$\operatorname{div}(f_{s,h,R}) = \sum_{i=0}^d h_i((s^i R) - (O)) - ((h(s)R) - (O)).$$

- Have $\varphi(k) = 2$, $\deg(h) \leq 1$, $\sum_i |h_i| \approx r^{1/2}$.
- Then $\deg(f_{s,h,\cdot}(P)) \approx? r^2$ and $\deg(f_{s,h,P}/f_{s,h,\cdot}(P)) \approx? r^2$.
- Thus log of degree about at least 2 times larger than necessary.

Proof idea - algebraic part

Central equation:

$$f_{s,\psi(T)} \circ \Psi = w_{s,\psi} \cdot f_{s,T}^{\deg(\psi)}.$$

Define

- $W = \{f \mid f : G_2 \times G_1 \rightarrow \mu_r\}$, $W^{\text{bilin}} \subseteq W$.
- $A = \mathbb{Z}[x]/(x^k - 1)$, $I^{(i)} = \{h + (x^k - 1) \mid h(s) \equiv 0 \pmod{r^i}\}$.
- $xf = f^s$, thus W becomes A -module.

Then

- $a_s : I^{(1)} \rightarrow W$, $h + (x^k - 1) \mapsto a_{s,h}$ is A -homomorphism.
- $I^{(2)} \subseteq \ker(a_s)$, $I^{(1)} = Ar + I^{(2)}$, $a_{s,r}$ is Tate pairing.
- Hence $\text{im}(a_s) = W^{\text{bilin}}$ and $\ker(a_s) = I^{(2)}$.

Proof idea - lattice part

Define

- ζ primitive k -th root of unity in $\bar{\mathbb{Q}}$.
- $J = r\mathbb{Z}[\zeta] + (\zeta - s)\mathbb{Z}[\zeta]$.
- $h \in \mathbb{Z}[x]$ mit $h(s) \equiv 0 \pmod{r}$.

Then

- $h(\zeta) \in J$ und $r = N(J) \leq |N(h)| = \prod_{j=1}^{\varphi(k)} |h(\zeta^{(j)})| \leq (\sum_i |h_i|)^{\varphi(k)}$.

Consider $I^{(1)}$ as k -dimensional lattice.

- Then $d(I^{(1)}) = r$.
- Analysis of LLL-reduced basis shows there exists $h \in I^{(1)} \setminus I^{(2)}$ with $\deg(h) \leq \varphi(k) - 1$ and $\sum_i |h_i| = O(r^{\varphi(k)})$.

Discussion

The lattice pairings use the following general principle:

Suppose

- have $a \in \text{Hom}_{\mathbb{Z}}(J, W)$ with $J \subseteq \mathbb{Z}$.
- can extend to $a \in \text{Hom}_{\mathbb{Z}[G]}(I, W)$ with $I \subseteq \mathbb{Z}[G]$, $I \cap \mathbb{Z} = J$.

Different representation $f(r)$ for $r \in J$:

- Let $h = \sum_g h_g g \in I$ with $h \equiv r \pmod{\ker(a)}$, h_g as small as possible.
- Then $f(r) = f(h) = \sum_g h_g f(g)$.

Example:

- $J = \mathbb{Z}$, $W = E(k)$, $a : x \mapsto xP$, $I = \mathbb{Z}[G]$.

Hence

- Pairing lattices and point multiplication with efficient endomorphisms use the same **general principle**.

Generalisation

Generalisation to non-prime r instead of prime r :

- Essentially the same statements possible in case $\gcd(k, r) = 1$.

Generalisation to arbitrary curves:

- central equation still holds
- pairing lattice argument then generic

Efficient computation of pairings

First consider the [Weil pairing](#).

Theorem: Let $\text{div}(f) = rD$ and $\text{div}(h) = rE$. Then

$$e_r([D], [E]) = \prod_P (-1)^{rv_P(D)v_P(E)} (h^{v_P(D)} / f^{v_P(E)})(P),$$

where not necessarily $\text{supp}(D) \cap \text{supp}(E) = \emptyset$.

Suppose A is a place of degree one and $D = \tilde{D} - dA$, $E = \tilde{E} - eA$ with $\tilde{D}, \tilde{E} \geq 0$ and coprime to A . Choose a local uniformiser z at A and scale f, h such that $(f/z^{v_A(f)})(A) = (h/z^{v_A(h)})(A) = 1$.

Then $e_r([D], [E]) = \prod_{P \neq A} (-1)^{rv_P(D)v_P(E)} (h^{v_P(D)} / f^{v_P(E)})(P)$.

This is Miller's efficient evaluation for Weil in general terms.

Efficient computation of pairings

General version of the [ate pairing](#):

Suppose

- C is defined over $k_0 = \mathbb{F}_q$,
- k is the minimal extension of k_0 such that $\mu_r \subseteq k$.

Let $G_1 = \text{Pic}_{k_0}^0(C)/r\text{Pic}_{k_0}^0(C)$. There is a subgroup $G_2 \subseteq \text{Pic}_k^0(C)[r]$ such that $\pi_q([D]) = q[D]$ for $[D] \in G_2$ and

$$a_r : G_2 \times G_1 \rightarrow \mu_r, \quad a_r([D], [E]) = g(\text{Con}_{k/k_0}(E))^{q^{-1}}$$

is bilinear non-degenerate, where $\text{div}(g) = \pi(D) - qD$ and g is scaled correctly with $c \in k^\times$.

Combinations of t_r and $a_r^{(\#k-1)/r}$ lead to smaller degree pairing functions as above.

Interpretation of pairings

It is illustrative to interpret the above pairings in terms of class field theory and Kummer pairings:

Weil pairing:

- The first argument $[D] \in \text{Pic}_k^0(C)[r]$ defines an unramified cyclic regular extension $Fk[f^{1/r}]$ of exponent r of Fk , with $\text{div}(f) = rD$.
- The second argument $[E] \in \text{Pic}_k^0(C)[r]$ defines an automorphism τ_E of $Fk[f^{1/r}]/Fk$ via translation by E , and $e_r([D], [E]) = \tau_E(f^{1/r})/f^{1/r}$.

Tate pairing:

- Same first argument.
- The second argument $[E] \in \text{Pic}_k^0(C)/r\text{Pic}_k^0(C)$ defines an automorphism σ_E of $Fk[f^{1/r}]/Fk$ via the Artin map, and $t_r([D], [E]) = \sigma_E(f^{1/r})/f^{1/r}$.

Interpretation of pairings

Ate pairing:

- The first argument $[D] \in G_2$ defines an unramified cyclic extension $Fk[f^{1/r}]/F$ of exponent $r[k : k_0]$, with $\text{div}(f) = rD$.
- The second argument $[E] \in G_1$ defines an automorphism σ_E of $Fk[f^{1/r}]/F$ via the Artin map, and $a_r([D], [E]) = \sigma_E(f^{1/r}) / (f^{1/r})^{q^{\deg(E)}}$.

Fix a first argument $[D] \in G_2$.

- Tate pairing = Artin map for $Fk[f^{1/r}]/Fk$.
- Ate pairing = Artin map for $Fk[f^{1/r}]/F$.

From this interpretation one can actually derive the definition of the ate pairing; bilinearity and non-degeneracy follow.

Have $t_r([D], \text{Con}_{k/k_0}([E])) = a_r([D], \mathbf{N}_{k_0/k}(\text{Con}_{k/k_0}([E]))) = a_r([D], [E])^{[k:k_0]}$.

Efficient computation of pairings

Saving evaluations due to scaling in the setting of ate pairing:

Assume

- A place of F of degree one (k_0 -rational).
- $[D] \in G_2, [E] \in G_1$.
- $D = \tilde{D} - dA, E = \tilde{E} - eA$ as above.
- $\text{div}(f) = \sum_{i=0}^{[k:k_0]-1} h_i \pi^i(D)$ with $D \in G_2$ and $h(q) \equiv 0 \pmod r$ for $h = \sum_i h_i x^i$.
- $(f/z^{v_A(f)})(A) = 1$ for fixed local uniformiser $z \in F$ of A .

Then $f(E)^{(\#k-1)/r} = f(\tilde{E})^{(\#k-1)/r}$.