

---

# Pairing Lattices

Pairing 2008, Royal Holloway  
2. September 2008

Florian Heß  
Technische Universität Berlin

---

## Goal of this talk

Present main results of the paper:

Classification

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

Discuss some aspects not mentioned in the paper:

- Security implications.
- Pairing functions of lowest possible degree.
- Different proof idea.
- Discussion of generalisation.

---

# 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  $q^k \equiv 1 \pmod r$ .

$\pi$  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

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

---

## Functions on elliptic curves

$\mathbb{F}_q(E)$  field of rational functions (in the coordinates) of  $E$   
with coefficients in  $\mathbb{F}_q$ .

$f \in \mathbb{F}_q(E)^\times$  defines

- a map  $E(\overline{\mathbb{F}}_q) \rightarrow \overline{\mathbb{F}}_q \cup \{\infty\}$ .
- has zeros and poles  $P \in E(\overline{\mathbb{F}}_q)$  with well defined orders  $v_P(f)$ .
- a divisor  $\text{div}(f) = \sum_{P \in E(\overline{\mathbb{F}}_q)} v_P(f)P$ .

$\text{div}(f)$  determines  $f \in \mathbb{F}_q(E)^\times$  up to scalar multiple from  $\mathbb{F}_q^\times$ .

**Very useful:** Implicit definition of „monic“  $f$  via  $\text{div}(f)$ !

$$P = (x = a), \quad O = (x = \infty), \quad \text{div}(f) = 1000P - 1000O \Rightarrow f = (x - a)^{1000}.$$

# 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.

# Miller's algorithm and the degree

Miller's algorithm (generalised) computes  $f(P)$  efficiently when

- $f$  is defined via  $\text{div}(f)$ ,
- $\text{div}(f)$  has small support and possibly large coefficients.

$$f = \prod_{i=1}^n (x - a_i)^{e_i} \Rightarrow f(b) = \prod_{i=1}^n (b - a_i)^{e_i}.$$

**Degree** of  $f \in \mathbb{F}_q(E)^\times$

- is number of zeros  $P$  of  $f$  counted with  $v_P(f)$ ,
- equals number of poles  $P$  of  $f$  counted with  $-v_P(f)$ .
- relates approximately to degree of numerator (or denominator) of  $f$  as rational function in coordinates of  $E$ .

Efficient computation of  $f(P) \not\Leftarrow \text{deg}(f)$  small!

# Pairing lattices

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

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

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

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

Then have pairings

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

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

# Examples

Tate pairings	function	$s$	$h$
Original Tate	$a_{s,h}, a_{s,h}^{\text{twist}}$	-	$r$
Ate	$a_{s,h}, a_{s,h}^{\text{twist}}$	$\text{trace}(E) - 1$	$t - s$
Optimised ate	$a_{s,h}, a_{s,h}^{\text{twist}}$	$q^i \pmod r$	$t - s$
R-ate	$a_{s,h}, a_{s,h}^{\text{twist}}$	$q^i \pmod r$	$t^j + c_1 t + c_2$
Vercouteren	$a_{s,h}$	$q$	arbitrary
H	$a_s, a_s^{\text{twist}}$	$q^i \pmod{r^2}$	arbitrary

Weil pairings	function	$s$	$h$
Original Weil	$e_{s,h}$	-	$r$
Zhao-Zhang	$e_{s,h}^c$	$q^i \pmod r$	$t - s$
H	$e_{s,h}$	$q^i \pmod{r^2}$	arbitrary

## Fun 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

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

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

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

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

Then have **pairings**

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

**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:

$$\begin{aligned} a_{s,h}(Q, P) &= t(Q, P)^{h(s)/r}, \\ a_{s,h}^{\text{twist}}(P, Q) &= t(P, Q)^{h(s)/r}, \\ e_{s,h}(P, Q) &= e(P, Q)^{h(s)/r}. \end{aligned}$$

## 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

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

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

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

## 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

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

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

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

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

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  $\deg(f_{s,h,(P)}) \approx r^2$  and  $\deg(f_{s,h,P}/f_{s,h,(P)}) \approx r^2$ .
- Thus log of degree about at least 2 times larger than necessary.

## Proof idea - algebraic part

Central equation:

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

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  $\operatorname{im}(a_s) = W^{\text{bilin}}$  and  $\ker(a_s) = I^{(2)}$ .

## Proof idea - lattice part

Define

- $\zeta$  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  $f(r) = f(h) = \sum_g h_g f(g)$ .

Hence

- Pairing lattices and point multiplication with efficient endomorphisms use the same **general principle**.
- Can we use **larger**, possibly **non-abelian** groups  $G$  than  $G = C_n$  in the pairing lattice construction?