
Musings about the Eta Pairing

Dublin, 15.06.2005

Florian Hess
Technical University Berlin

1

Dublin 15.06.2005

Overview

1. General reasons why the Eta pairing approach works.
2. A possible construction?

2

Dublin 15.06.2005

Elliptic Curves

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

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

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

Endomorphism ring $\text{End}(E)$.

- π_q Frobenius endomorphism $(x, y) \mapsto (x^q, y^q)$.
- $[m]$ multiplication-by- m endomorphism.
- $\mathbb{Z}[\pi_q] \subseteq \text{End}(E)$, $\pi_q^2 - t\pi_q + q = 0$, $|t| \leq 2\sqrt{q}$.
- $\text{End}(E)$ is a ring without zero divisors, non-commutative $\Leftrightarrow E$ supersingular.

3

Dublin 15.06.2005

Basic setting

We consider the following setting.

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

Elliptic curve E over \mathbb{F}_q

- with subgroup $E(\mathbb{F}_q)[\ell]$ of large prime order $\ell \neq q$.
- with embedding degree k , hence $\ell \mid (q^k - 1)$ and k minimal.

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

The modified Tate pairing $\langle \cdot, \cdot \rangle_\ell : E(\mathbb{F}_{q^k})[\ell] \times E(\mathbb{F}_{q^k})[\ell] \rightarrow \mu_\ell$ is non-degenerate.

4

Dublin 15.06.2005

Basic setting

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

- $E(\mathbb{F}_{q^k})[\ell] = \langle P \rangle \times \langle Q \rangle$.
- $\langle P, P \rangle_\ell = \langle Q, Q \rangle_\ell = 1$, $\langle P, Q \rangle_\ell \neq 1$.
- $P \in E(\mathbb{F}_q)[\ell]$.
- $\text{Tr} = c \sum_{i=0}^{k-1} \pi_q^i$ with $kc \equiv 1 \pmod{\ell}$ yields projection from $\langle P \rangle \times \langle Q \rangle$ onto $\langle P \rangle$ with kernel $\langle Q \rangle$.

P is nicely represented, find better representation for Q !

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 $\psi\pi_q^d\psi^{-1} = \pi_q^d$.

It follows $\psi\pi_q'\psi^{-1} = \gamma\pi_q$ for some automorphism γ of E of order d (corresponding to $\zeta \in \mu_d$ of order d).

Thus $\gamma^{-1}\psi\pi_q' = \pi_q\psi$, and $\gamma^{-1}\psi = \pi_q\psi\pi_q'^{-1} = \psi^q$ on $E'(\mathbb{F}_{q^d})[\ell]$.

Twists

Consider previous situation for $\mathbb{F}_{q^{k/d}}$ as bottom and \mathbb{F}_{q^k} as top field, with $d | k$. Then $\psi\pi_q'\psi^{-1} = \gamma\pi_q^{k/d}$ and $\gamma^{-1}\psi = \psi^{q^{k/d}}$. If $Q' \in E'(\mathbb{F}_{q^{k/d}})[\ell]$, then $\gamma\pi_q^{k/d}(\psi(Q')) = \psi(Q')$.

Vice versa, assume that $\mu_d \subseteq \mathbb{Q}[\pi_q] \cap \text{End}(E)$ holds and let $\zeta \in \mu_d$ of order d . Let γ be the corresponding automorphism of E . There exists a twist E' of E over $\mathbb{F}_{q^{k/d}}$ of degree d with $\psi\pi_q'\psi^{-1} = \gamma\pi_q^{k/d}$ and $\gamma^{-1}\psi = \psi^{q^{k/d}}$.

Since $\pi_q^k = 1$ on $\langle Q \rangle$, we can choose γ such that $\gamma\pi_q^{k/d} = 1$ on $\langle Q \rangle$.

Let $Q' = \psi^{-1}(Q)$. Then $\pi_q^{k/d}(Q') = Q'$ and hence $Q' \in E'(\mathbb{F}_{q^{k/d}})[\ell] \cong \mathbb{F}_\ell$.

This yields a better representation for Q .

Eta pairing

The automorphism γ operates

- on $\langle Q \rangle$ like multiplication by $q^{-k/d} \pmod{\ell}$,
- on $\langle P \rangle$ like multiplication by $q^{k/d} \pmod{\ell}$ (since $\gamma\hat{\gamma} = 1$).

Let $\lambda = (t-1)^{k/d} \equiv q^{k/d} \pmod{\ell}$. Then $\lambda^d \equiv 1 \pmod{\ell}$ with d minimal.

Let $f_{n,P} \in \mathbb{F}_q(E)$ with $(f_{n,P}) = n((P) - (\infty)) - ((nP) - (\infty))$.

Can take $\langle P, Q' \rangle_{\lambda^{d-1}} = f_{\lambda^{d-1}, P}(\psi(Q'))^{(q^k-1)/\ell} = f_{\lambda^d, P}(\psi(Q'))^{(q^k-1)/\ell}$.

Then $f_{\lambda^d, P}(\psi(Q')) = \prod_{i=0}^{d-1} f_{\lambda, \lambda^i P}(\psi(Q'))^{\lambda^{d-1-i}}$ and $f_{\lambda, \gamma P} \circ \gamma = f_{\lambda, P}$, since $\gamma(\infty) = \infty$.

Eta pairing

Thus

$$\begin{aligned} f_{\lambda, \lambda^i P}(\psi(Q')) &= f_{\lambda, \gamma^i P}(\psi(Q')) = f_{\lambda, P}(\gamma^{-i}(\psi(Q'))) = f_{\lambda, P}(\psi^{q^{ik/d}}(Q')) \\ &= f_{\lambda, P}(\psi(Q'))^{q^{ik/d}}. \end{aligned}$$

Being the power of a non-degenerate pairing we see that

$$\eta : E(\mathbb{F}_q)[\ell] \times E'(\mathbb{F}_{q^{k/d}})[\ell] \rightarrow \mu_\ell, \quad \eta(P, Q') = f_{\lambda, P}(\psi(Q'))^{(q^k - 1)/\ell}$$

defines a non-degenerate pairing.

Size of λ is $(k/(2d)) \log_2(q)$.

9

Dublin 15.06.2005

Applications

Supersingular elliptic curves in BGOS.

- $E : y^2 = x^3 - x + b$ over \mathbb{F}_{3^m} , $\gcd(m, 6) = 1$.
- $E' = E$, $\psi : E' \rightarrow E$, $\psi(x, y) = (\rho - x, iy)$ for $i^2 = -1$ and $\rho^3 = \rho + b$.
- $\phi : E \rightarrow E$, $\phi(x, y) = (x - b, -y)$, $\text{ord}(\phi) = 6$, $\phi \in \mathbb{Q}(\pi_q) \cap \text{End}(E) = \mathbb{Z}[\zeta_3]$.
- $k = 6$, $d = 6$.
- $E : y^2 + y = x^3 + x + b$ over \mathbb{F}_{2^m} , m odd.
- $E' = E$, $\psi : E' \rightarrow E$, $\psi(x, y) = (x + s^2, y + sx + t)$ with $s^2 = s + 1$ and $t^2 = t + s$.
- $\phi : E \rightarrow E$, $\phi(x, y) = (x + 1, y + x)$, $\text{ord}(\phi) = 4$, $\phi \in \mathbb{Q}(\pi_q) \cap \text{End}(E) = \mathbb{Z}[i]$.
- $k = 4$, $d = 4$.

10

Dublin 15.06.2005

Applications

The BN curves.

- $E : y^2 = x^3 + b$ over \mathbb{F}_p with $p \equiv 1 \pmod{6}$.
- $E' \neq E$, $\psi : E' \rightarrow E$, $\psi(x, y) = (\lambda^{1/3}x, \mu^{1/2}y)$ for $\lambda \in \mathbb{F}_p \setminus (\mathbb{F}_p)^3$ and $\mu \in \mathbb{F}_p \setminus (\mathbb{F}_p)^2$.
- $\phi : E \rightarrow E$, $\phi(x, y) = (\zeta_3x, \zeta_2y)$, $\text{ord}(\phi) = 6$, $\phi \in \mathbb{Q}(\pi_q) \cap \text{End}(E) = \mathbb{Z}[\zeta_3]$.
- $k = 12$, $d = 6$.

Hence get Eta pairing of length $\log_2(p)$.

Good twists can only be done when enough roots of unity.

Also seems to help with embedding degree.

Hence $\mathbb{Q}(\pi_q) \cap \text{End}(E) \in \{\mathbb{Z}[i], \mathbb{Z}[\zeta_3]\}$.

11

Dublin 15.06.2005

Generalisation

Using isogenies rather than isomorphisms.

- Let $\psi : E' \rightarrow E$ be an isogeny of small degree.
- Then $\phi \mapsto \psi\phi\hat{\psi} \otimes \deg(\psi)^{-1}$ yields an isomorphism $\text{End}(E') \otimes \mathbb{Q} \rightarrow \text{End}(E) \otimes \mathbb{Q}$.
- The Frobenius endomorphisms are mapped to each other, like before.
- We obtain the existence of $\zeta \in \text{End}(E) \otimes \mathbb{Q}$ with $\zeta^{-1}\psi = \psi^q$.
- For ζ to correspond to an automorphism of E it seems one would need the requirement $\mathbb{Q}(\pi_q) \cap \text{End}(E)$ be maximal.

Better 'twisting' achievable? (\Rightarrow No.)

How create such ψ ?

12

Dublin 15.06.2005

General Eta pairing

Consider curve C of genus g with point ∞ .

Replace point group by Jacobian $\text{Jac}(C)$.

$\text{Jac}(C)(\mathbb{F}_{q^s}) =$ abelian group of rational divisor classes of degree zero.

Embedding degree and Tate pairing arise analogously.

Have again Frobenius endomorphism π_q with $\pi_q^{2g} + \dots + q^g = 0$.

Roots are pairwise conjugate complex numbers of absolute value $q^{1/2}$.

$\mathbb{Z}[\pi_q] \subseteq \text{End}(\text{Jac}(C))$.

We assume that the characteristic polynomial $t^{2g} + \dots + q^g$ is irreducible.

13

Dublin 15.06.2005

General Eta pairing

We can choose $P \in \text{Jac}(C)(\mathbb{F}_q)[L]$ and $Q \in \text{Jac}(C)(\mathbb{F}_{q^k})[L]$ with $\pi_q(P) = P$, $\pi_q(Q) = qQ$ and $\langle P, Q \rangle_\ell \neq 1$. (?)

Let γ be a \mathbb{F}_q -rational automorphism of order $d \mid k$ of C with $\gamma(\infty) = \infty$.

Twisting using γ gives a twist C' of degree d defined over $\mathbb{F}_{q^{k/d}}$ and an isomorphism $\psi : C' \rightarrow C$ such that $\psi \pi_{q^{k/d}}' \psi^{-1} = \gamma \pi_q^{k/d}$.

Similar to above we obtain $\gamma^{-1} \psi = \psi^{q^{k/d}}$.

We can choose γ such that $\gamma \pi_q^{k/d} = 1$ on $\langle Q \rangle$. With $Q' = \psi^{-1}(Q)$ we have $\pi_{q^{k/d}}'(Q') = Q'$, hence $Q' \in \text{Jac}(C')(\mathbb{F}_{q^{k/d}})[L] \cong \mathbb{F}_\ell$.

14

Dublin 15.06.2005

General Eta pairing

The automorphism γ operates

- on $\langle Q \rangle$ like multiplication by $q^{-k/d} \pmod{\ell}$,
- on $\langle P \rangle$ like multiplication by $q^{k/d}$ (since $\gamma \hat{\gamma} = 1$).

Let $\lambda \equiv q^{k/d} \pmod{\ell}$. Then $\lambda^d \equiv 1 \pmod{\ell}$ with d minimal.

It is possible to work with points P, Q, Q' and the divisors $(P) - (\infty), (Q) - (\infty), (Q') - (\infty)$ instead of general divisors P, Q, Q' in the following, using tricks like denominator elimination.

Let $f_{n,P} \in \mathbb{F}_q(C)$ with $(f_{n,P}) = n((P) - (\infty)) - ((nP) - d_{n,P}(\infty))$, where (nP) and $d_{n,P}(\infty)$ denote effective divisors of minimal possible degree.

Have $(f_{\lambda^i, P}) = \lambda^i((P) - (\infty)) - ((\gamma^i(P)) - (\infty))$, $(f_{\lambda^d, P}) = (f_{\lambda^{d-1}, P})$, and $f_{\lambda^{i+1}, P} = f_{\lambda^i, P}^{\lambda} f_{\lambda, \lambda^i P}$.

15

Dublin 15.06.2005

General Eta pairing

Can take $\langle P, Q' \rangle_{\lambda^{d-1}} = f_{\lambda^{d-1}, P}(\psi(Q'))^{(q^k-1)/\ell} = f_{\lambda^d, P}(\psi(Q'))^{(q^k-1)/\ell}$.

Then $f_{\lambda^d, P}(\psi(Q')) = \prod_{i=0}^{d-1} f_{\lambda, \lambda^i P}(\psi(Q'))^{\lambda^{d-1-i}}$ and $f_{\lambda, \gamma P} \circ \gamma = f_{\lambda, P}$.

Thus

$$\begin{aligned} f_{\lambda, \lambda^i P}(\psi(Q')) &= f_{\lambda, \gamma^i P}(\psi(Q')) = f_{\lambda, P}(\gamma^{-i}(\psi(Q'))) = f_{\lambda, P}(\psi^{q^{ik/d}}(Q')) \\ &= f_{\lambda, P}(\psi(Q'))^{q^{ik/d}}. \end{aligned}$$

Being the power of a non-degenerate pairing we see that

$\eta : \text{Jac}(C)(\mathbb{F}_q)[\ell] \times \text{Jac}(C')(\mathbb{F}_{q^{k/d}})[\ell] \rightarrow \mu_\ell$, $\eta(P, Q') = f_{\lambda, P}(\psi(Q'))^{(q^k-1)/\ell}$ defines a non-degenerate pairing.

Size of λ is $(k/d) \log_2(q)$, should be half that value.

16

Dublin 15.06.2005

Constructions

Quick remark.

Take elliptic curve E over \mathbb{F}_q with $E(\mathbb{F}_q)[\ell] \cong \mathbb{F}_\ell$.

Take elliptic curve E' over \mathbb{F}_q with $E'(\mathbb{F}_q)[\ell] = 0$ and $E'(\mathbb{F}_{q^k})[\ell] \neq 0$.

Can one find a covering curve C where the torsion from E and E' can be non trivially paired via C ?

Conditions on E and E' weaker than MNT conditions.

(\Rightarrow Does not work!)

Thank you for your attention!