

Realization of Fast Pairings I

Frederik Vercauteren

Pairings in Arithmetic Geometry and Cryptography

Notation

- ▶ Base field \mathbb{F}_q with $q = p^m$.
- ▶ E elliptic curve defined over \mathbb{F}_q .
- ▶ Point sets $E(\mathbb{F}_{q^n})$ are abelian groups.
- ▶ Point at infinity $\mathcal{O} \in E(\mathbb{F}_q)$ is neutral element.
- ▶ $E(\mathbb{F}_{q^n})[r]$ subgroup of points of order r .
- ▶ Assume: exists subgroup $E(\mathbb{F}_q)[r]$ of large prime order r with $\gcd(r, q) = 1$.
- ▶ Embedding degree k with $r \parallel (q^k - 1)$ and k minimal.
- ▶ Note that $\mu_r \subseteq \mathbb{F}_{q^k}^*$, but $\mathbb{F}_p(\mu_r)$ could be contained in smaller extension of \mathbb{F}_p .

Miller functions

- ▶ Let $P \in E$ and $n \in \mathbb{N}$.
- ▶ A Miller function $f_{n,P}$ is any function in $\mathbb{F}_q(E)$ with divisor

$$\operatorname{div}(f_{n,P}) = n(P) - ([n]P) - (n-1)(\infty)$$

- ▶ $f_{n,P}$ is determined up to a constant $c \in \mathbb{F}_q^*$.
- ▶ $f_{n,P}$ has a zero at P of order n .
- ▶ $f_{n,P}$ has a pole at $[n]P$ of order 1.
- ▶ $f_{n,P}$ has a pole at ∞ of order $(n-1)$.
- ▶ For every point $Q \neq P, [n]P, \infty$, we have $f_{n,P}(Q) \in \mathbb{F}_q^*$.

Tate pairing

- ▶ Definition of Tate pairing:

$$\langle \cdot, \cdot \rangle_r : E(\mathbb{F}_{q^k})[r] \times E(\mathbb{F}_{q^k})/rE(\mathbb{F}_{q^k}) \rightarrow \mathbb{F}_{q^k}^*/(\mathbb{F}_{q^k}^*)^r$$

- ▶ Let $P \in E(\mathbb{F}_{q^k})[r]$ and $f_{r,P} \in \mathbb{F}_{q^k}(E)$ with

$$\operatorname{div}(f_{r,P}) = r((P) - (\mathcal{O}))$$

- ▶ $Q \in E(\mathbb{F}_{q^k})$ and $R \in E(\mathbb{F}_{q^k})$ with $\{Q + R, R\} \cap \{P, \mathcal{O}\} = \emptyset$.

$$\begin{aligned}\langle P, Q \rangle_r &= f_{r,P}((Q + R) - (R)) \cdot (\mathbb{F}_{q^k}^*)^r \\ &= f_{r,P}(Q + R)/f_{r,P}(R) \cdot (\mathbb{F}_{q^k}^*)^r\end{aligned}$$

- ▶ Tate pairing is bilinear and non-degenerate

Miller's algorithm

- ▶ Use double-add algorithm to compute $f_{n,P}$ for any $n \in \mathbb{N}$.
- ▶ Exploit relation:

$$f_{m+n,P} = f_{m,P} \cdot f_{n,P} \cdot \frac{l_{[n]P,[m]P}}{v_{[n+m]P}}$$

- ▶ $l_{[n]P,[m]P}$: the line through $[n]P$ and $[m]P$
- ▶ $v_{[n+m]P}$: the vertical line through $[n+m]P$
- ▶ Note that $v_{[n+m]P}(Q) = x(Q) - x([n+m]P)$

Miller's algorithm

Input: $P, Q \in E(\mathbb{F}_{q^k})$ and integer $n \in \mathbb{N}$

Output: $f_{n,P}(Q)$

1. $B \leftarrow \text{Bits}(n)$, $T \leftarrow P$, $f \leftarrow 1$
2. For $i := \#B - 1$ to 1 do
3. $l, v \leftarrow \text{DoubleLines}(T)$
4. $f \leftarrow f^2 \frac{l(Q)}{v(Q)}$
5. $T \leftarrow [2]T$
6. If $B[i] = 1$ Then
7. $l, v \leftarrow \text{AddLines}(T, P)$
8. $f \leftarrow f \frac{l(Q)}{v(Q)}$
9. $T \leftarrow T + P$
10. Return f

Tate pairing: simplify evaluation

- ▶ Need two evaluations of Miller function to compute

$$f_{r,P}(Q + R)/f_{r,P}(R)$$

- ▶ Ideally, would simply like to compute $f_{r,P}(Q)$
- ▶ Let u_∞ be a fixed \mathbb{F}_q -rational uniformizer at \mathcal{O}
- ▶ For $f \in \overline{\mathbb{F}}_q(E)^*$, define $\text{lc}_\infty(f)$ as the leading coefficient of f as a Laurent series in u_∞ .
- ▶ Lemma: if $\text{lc}_\infty(f_{r,P})$ is an r -th power, then for $Q \neq P, \mathcal{O}$

$$\langle P, Q \rangle_r = f_{r,P}(Q) \cdot (\mathbb{F}_{q^k}^*)^r$$

- ▶ $\text{lc}_\infty(f_{r,P})$ being an r -th power is independent of uniformizer chosen

Tate pairing: simplify evaluation

- ▶ Can always make slight adaptation of functions used in Miller's algorithm to normalise.
- ▶ By definition of the embedding degree we have $\gcd(r, q^d - 1) = 1$ for all positive integers $d \mid k$ and $d < k$.
- ▶ So all elements of the fields \mathbb{F}_{q^d} are r -th powers.
- ▶ Conclusion: for $k > 1$ and if P is chosen in a strict subfield $\mathbb{F}_{q^d} \subset \mathbb{F}_{q^k}$, then $f_{r,P}$ is automatically normalised.
- ▶ Note: if $k > 1$, then either P or Q has to be defined over \mathbb{F}_{q^k} , else pairing will evaluate to 1.

Reduced Tate pairing

- ▶ By definition value of $\langle \cdot, \cdot \rangle_r$ only defined up to r -th powers.

$$\langle \cdot, \cdot \rangle_r : E(\mathbb{F}_{q^k})[r] \times E(\mathbb{F}_{q^k})/rE(\mathbb{F}_{q^k}) \rightarrow \mathbb{F}_{q^k}^\times / (\mathbb{F}_{q^k}^\times)^r$$

- ▶ In practice: want unique output of the function
- ▶ Reduced Tate pairing $t_r : E(\mathbb{F}_{q^k})[r] \times E(\mathbb{F}_{q^k})/rE(\mathbb{F}_{q^k}) \rightarrow \mu_r$ is defined as

$$t_r(P, Q) = \langle P, Q \rangle_r^{(q^k-1)/r}$$

- ▶ Can ignore all factors that are r -th powers, so if $k > 1$, can ignore all factors in \mathbb{F}_{q^d} with $d|k$, $d < k$.

Reduced Tate pairing: changing scalar r

- ▶ Let $N = hr$ be a multiple of N with $N|q^k - 1$, then

$$t_r(P, Q) = \langle P, Q \rangle_r^{(q^k-1)/r} = t_N(P, Q) = \langle P, Q \rangle_N^{(q^k-1)/N}$$

- ▶ Can work with low Hamming weight multiple of r
- ▶ Small characteristic p : multiplication by p usually has special form
- ▶ Choose multiple of r with low Hamming weight in base p

Reduced Tate pairing: denominator elimination

- ▶ In Miller's algorithm, all denominators are of the form

$$x(Q) - x([n]P)$$

- ▶ So, if $x(Q)$ and $x(P)$ defined over \mathbb{F}_{q^d} with $d|k$, $d < k$, then can ignore denominators
- ▶ Can choose $P \in E(\mathbb{F}_q)$, but can we choose Q such that $x(Q) \in \mathbb{F}_{q^d}$ with $d|k$, $d < k$?
- ▶ Note: if $P \in E(\mathbb{F}_q)$, then Q has to be in

$$E(\mathbb{F}_{q^k}) \setminus \bigcup_{d|k, d < k} E(\mathbb{F}_{q^d})$$

else pairing will be 1.

- ▶ So only when k is even and $x(Q) \in \mathbb{F}_{q^{k/2}}$.

r -torsion and Frobenius

- ▶ Denote π_q Frobenius endomorphism $(x, y) \mapsto (x^q, y^q)$.
- ▶ $[m]$ multiplication-by- m endomorphism.
- ▶ $\mathbb{Z}[\pi_q] \subseteq \text{End}(E)$, $\pi_q^2 - [t]\pi_q + q = 0$, $|t| \leq 2\sqrt{q}$.
- ▶ Since $r \mid \#E(\mathbb{F}_q)$, π_q has eigenvalues 1 and q on $E[r]$.
- ▶ Embedding degree k is precisely such that q -eigenspace of π_q is \mathbb{F}_{q^k} -rational.

$$\mathbb{G}_1 = E[r] \cap \text{Ker}(\pi_q - [1]) \quad \mathbb{G}_2 = E[r] \cap \text{Ker}(\pi_q - [q])$$

- ▶ If $k > 1$, then $q \not\equiv 1 \pmod{r}$ and thus $E[r] = E(\mathbb{F}_{q^k})[r]$.
- ▶ For $k = 1$, either $E[r]$ is \mathbb{F}_q -rational or \mathbb{F}_{q^r} -rational.

Representing \mathbb{G}_2 : supersingular curves

- ▶ Recall: E is supersingular if and only if $E[p^e] = \{\mathcal{O}\}$, else E is called ordinary.
- ▶ If E is ordinary, then $\text{End}(E)$ is commutative and thus all endomorphisms ψ are defined over field of definition of E .
- ▶ So: if $P \in E(\mathbb{F}_q)$ then $\psi(P) \in \mathbb{F}_q$.
- ▶ If E is supersingular, then $\text{End}(E)$ is non-commutative and non-rational endomorphisms exist, i.e. distortion maps.
- ▶ For $k > 1$, can always find $\psi \in \text{End}(E)$ such that

$$\psi(\mathbb{G}_1) = \mathbb{G}_2$$

- ▶ Conclusion: obtain pairing on $\mathbb{G}_1 \times \mathbb{G}_1$.

Representing \mathbb{G}_2 : supersingular curves

k	Field \mathbb{F}_q	Curve E	Distortion map $(x, y) \mapsto$
2	$p \equiv 2 \pmod{3}$	$y^2 = x^3 + a$	$(\xi_3 x, y)$
2	$p \equiv 3 \pmod{4}$	$y^2 = x^3 + ax$	$(-x, iy)$
4	$q = 2^m, m \text{ odd}$	$y^2 + y = x^3 + x + b$	$(\alpha^2 x + \beta^2, y + \alpha^2 \beta x + \beta)$ $\alpha^2 + \alpha + 1 = 0$ $\beta^2 + (\alpha + 1)\beta + 1 = 0$
6	$q = 3^m, m \text{ odd}$	$y^2 = x^3 - x \pm 1$	$(\alpha - x, iy)$ $\alpha^3 - \alpha - (\pm 1) = 0$

Representing \mathbb{G}_2 : ordinary curves

- ▶ Let E and E' be ordinary elliptic curves 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 $E'(\mathbb{F}_{q^d})[r] \rightarrow E(\mathbb{F}_{q^d})[r]$.
 - ▶ 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 $\psi\pi_q'^d\psi^{-1} = \pi_q^d$.
 - ▶ automorphism of E : $\psi^\sigma \circ \psi^{-1}$, where ψ^σ is ψ with coefficients raised to q -th power.
 - ▶ so for $p \geq 5$, only $d = 2, 3, 4, 6$ are possible.

Representing \mathbb{G}_2 : ordinary curves

- ▶ For $p \geq 5$, set of twists of E is isomorphic with $\mathbb{F}_q^*/(\mathbb{F}_q^*)^d$ with $d = 2$ if $j(E) \neq 0, 1728$, $d = 4$ if $j(E) = 1728$ and $d = 6$ if $j(E) = 0$.
- ▶ Let $D \in \mathbb{F}_q^*$, then the twists corresponding to $D \bmod (\mathbb{F}_q^*)^d$ are given by

$$\begin{array}{lll}
 d = 2 & y^2 = x^3 + a/D^2x + b/D^3 & (x, y) \mapsto (Dx, D^{3/2}y) \\
 d = 4 & y^2 = x^3 + a/Dx & (x, y) \mapsto (D^{1/2}x, D^{3/4}y) \\
 d = 3, 6 & y^2 = x^3 + b/D & (x, y) \mapsto (D^{1/3}x, D^{1/2}y)
 \end{array}$$

Representing \mathbb{G}_2 : ordinary curves

- ▶ Let E have a twist of degree d
- ▶ Denote E_i for $i = 0, \dots, d - 1$ the twists of E
- ▶ Assume that $r > 6$ satisfies $r \parallel \#E(\mathbb{F}_q)$ and $r^2 \parallel \#E(\mathbb{F}_{q^d})$, then there exists a unique twist E_i of degree d such that $r \parallel \#E_i(\mathbb{F}_q)$.
- ▶ Let $z = \gcd(k, d)$ and $e = k/z$, so degree z twist E' over \mathbb{F}_{q^e} exists with $r \mid \#E'(\mathbb{F}_{q^e})$.
- ▶ Let \mathbb{G}'_2 be the unique subgroup of order r of $E'(\mathbb{F}_{q^e})$ and denote $\phi_z : E' \rightarrow E$ the twisting isomorphism, then

$$\mathbb{G}_2 = \phi_z(\mathbb{G}'_2) .$$

- ▶ Conclusion: obtain pairing on $\mathbb{G}_1 \times \mathbb{G}'_2$

Representing \mathbb{G}_2 : use of twists

- ▶ Denominator elimination:
 - ▶ For $k > 1$ even, have quadratic twist of E over $\mathbb{F}_{q^{k/2}}$
 - ▶ Note that for k even, if twisting isomorphism maps x -coordinate into $\mathbb{F}_{q^{k/2}}$ then denominator elimination applies.
- ▶ Faster pairing on $\mathbb{G}_2 \times \mathbb{G}_1$
 - ▶ Miller's algorithm corresponds to computing rQ with $Q \in \mathbb{G}_2$
 - ▶ Can instead compute rQ' with $Q' \in \mathbb{G}'_2$ and then use twisting isomorphism

Reduced Tate pairing: final exponentiation

- ▶ Final exponentiation is $(q^k - 1)/r$
- ▶ Use the algebraic factorisation of $x^k - 1 = \prod_{d|k} \Phi_d(x)$ with Φ_d the d -th cyclotomic polynomial
- ▶ Since k is minimal, we have $r|\Phi_k(q)$
- ▶ Final exponentiation consists of easy and hard part

$$q^k - 1 = \left[\prod_{d|k, d < k} \Phi_d(q) \right] \cdot \frac{\Phi_k(q)}{r}$$

- ▶ Easy part consists of fast q -th powering (plus an inversion)
- ▶ Express hard part in base p and use multi-exponentiation

First milestone for fast pairings

- ▶ Take curve E with even k and a degree d twist over $\mathbb{F}_{q^{k/d}}$ giving group $\mathbb{G}_2 = \phi(\mathbb{G}'_2)$
- ▶ Pairing on $\mathbb{G}_1 \times \mathbb{G}'_2$ computed as

$$t_r(P, Q') = f_{r,P}(\phi(Q'))^{(p^k-1)/r} = t_N(P, Q') = f_{N,P}(\phi(Q'))^{(p^k-1)/N}$$

- ▶ No denominators in computation
- ▶ r or $N = hr$ of low Hamming weight
- ▶ Small characteristic p : work in base p
- ▶ Clever final exponentiation

Eta pairing

- ▶ Pairing on supersingular curves defined on $\mathbb{G}_1 \times \mathbb{G}_1$
- ▶ Distortion map $\psi : \mathbb{G}_1 \rightarrow \mathbb{G}_2$
- ▶ Definition: let $T = t - 1$, with $\#E(\mathbb{F}_q) = q + 1 - t$, then

$$\eta_T : \mathbb{G}_1 \times \mathbb{G}_1 : (P, Q) \mapsto \eta_T(P, Q) = f_{T,P}(\psi(Q))$$

defines a bilinear pairing

- ▶ Let $N = \gcd(T^k - 1, q^k - 1)$ and $T^k - 1 = LN$,

$$t_r(P, Q)^L = \eta_T(P, Q)^{c(q^k - 1)/N}$$

where $c = \sum_{i=0}^{k-1} T^{k-1-i} q^i \equiv kq^{k-1} \pmod r$

- ▶ for $r \nmid L$, the eta pairing is non-degenerate

Eta pairing: proof sketch

- ▶ Step 1: prove that

$$t_r(P, Q)^L = f_{T^k, P}^{(q^k-1)/N}$$

by considering

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

- ▶ Step 2: prove that (exercise)

$$f_{T^k, P} = f_{T, P}^{T^{k-1}} f_{T, TP}^{T^{k-2}} \cdots f_{T, T^{k-1}P}$$

Eta pairing: proof sketch

- ▶ By definition of \mathbb{G}_1 and \mathbb{G}_2 we have

$$\forall P \in \mathbb{G}_1 : \pi_q(P) = P \quad \text{and} \quad \forall Q \in \mathbb{G}_2 : \pi_q(Q) = [q]Q$$

- ▶ Dual of π_q is called Verschiebung and satisfies

$$\pi_q \circ \hat{\pi}_q = [q]$$

- ▶ It follows that on \mathbb{G}_1 and \mathbb{G}_2 we have

$$\forall P \in \mathbb{G}_1 : \hat{\pi}_q(P) = [q]P \quad \text{and} \quad \forall Q \in \mathbb{G}_2 : \hat{\pi}_q(Q) = Q$$

- ▶ So for $P \in \mathbb{G}_1$ we have $[T]P = \hat{\pi}_q(P)$

Eta pairing: proof sketch

- ▶ For purely inseparable endomorphism ψ on E we can take

$$f_{n,\psi}(P) \circ \psi = f_{n,P}^{\deg(\psi)}$$

- ▶ Apply this to $\hat{\pi}_q^i$, then

$$f_{T,\hat{\pi}_q^i}(P) \circ \hat{\pi}_q^i = f_{T,P}^{q^i}$$

- ▶ Since $\hat{\pi}_q(Q) = Q$, we conclude that

$$f_{T,[T^i]P}(Q) = f_{T,P}^{q^i}(Q)$$

- ▶ Substituting in expression for $f_{T^k,P}(Q)$ finishes proof

Second milestone for fast pairings

- ▶ Take supersingular curve E with distortion map

$$\psi : \mathbb{G}_1 \rightarrow \mathbb{G}_2$$

- ▶ Let $T = t - 1$, with $\#E(\mathbb{F}_q) = q + 1 - t$
- ▶ Pairing on $\mathbb{G}_1 \times \mathbb{G}_1$ computed as

$$\eta_T(P, Q) = f_{T,P}(\psi(Q))^{(p^k-1)/r}$$

- ▶ Miller loop has half length of original loop
- ▶ No denominators in computation
- ▶ Clever final exponentiation

Questions?