

Pairings on Elliptic Curves I

Fré Vercauteren
ESAT/COSIC - K.U. Leuven - Belgium

ECC Summer School - 2011

Outline

Weil/Tate Pairings

Pairing Computation

Pairings

- ▶ Let $\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T$ be abelian groups. A pairing is a non-degenerate bilinear map $e : \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_T$.
- ▶ 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:
 - ▶ for all $g \neq 1$: $\exists x \in \mathbb{G}_2$ such that $e(g, x) \neq 1$
 - ▶ for all $h \neq 1$: $\exists x \in \mathbb{G}_1$ such that $e(x, h) \neq 1$
- ▶ Examples:
 - ▶ Scalar product on euclidean space $\langle \cdot, \cdot \rangle : \mathbb{R}^n \times \mathbb{R}^n \rightarrow \mathbb{R}$.
 - ▶ Weil, Tate, eta and ate pairings on elliptic curves.

Pairings in cryptography

- ▶ Exploit bilinearity: originally $\mathbb{G}_1 = \mathbb{G}_2$ (supersingular)
- ▶ Menezes-Okamoto-Vanstone: move DLP from \mathbb{G}_1 to \mathbb{G}_T

$$\text{DLP in } \mathbb{G}_1 : (g, x \cdot g) \quad \text{DLP in } \mathbb{G}_T : (e(g, g), e(g, g)^x)$$

- ▶ Decision Diffie-Hellman easy in \mathbb{G}_1

$$\text{DDH} : (g, a \cdot g, b \cdot g, c \cdot g) \text{ test if } e(g, c \cdot g) = e(a \cdot g, b \cdot g)$$

- ▶ Identity based crypto, short signatures, ...

Elliptic curves

- ▶ Base field \mathbb{F}_q with $q = p^r$.
- ▶ E elliptic curve E defined over \mathbb{F}_q (short Weierstrass).
 - ▶ Point sets $E(\mathbb{F}_{q^n})$ are abelian groups.
 - ▶ $E(\mathbb{F}_{q^n})[\ell]$ subgroup of points of order ℓ .
 - ▶ Point at infinity $1 \in E(\mathbb{F}_q)$ is neutral element.
- ▶ Assume
 - ▶ exists subgroup $E(\mathbb{F}_q)[\ell]$ of large prime order $\ell \nmid q$.
 - ▶ embedding degree is k , that is $\ell \nmid (q^k - 1)$ and k minimal.
- ▶ If $k > 1$, then $E(\mathbb{F}_{q^k})[\ell] \cong \mathbb{Z}/\ell\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z}$ and $\mu_\ell \subset \mathbb{F}_{q^k}^\times$.

Pairing friendly curves

- ▶ Embedding degree is smallest $k \in \mathbb{N}$ such that

$$q^k \equiv 1 \pmod{\ell}$$

- ▶ Prime ℓ is large (at least 160 bits) with $\ell \nmid \#E(\mathbb{F}_q)$.
- ▶ By definition q has to be an element of order k in $\mathbb{Z}/\ell\mathbb{Z}$.
- ▶ For random curves E , we thus have $k \ll \ell$, so impossible to compute pairing (result is in \mathbb{F}_{q^k}).
- ▶) Finding good curves is non-trivial!

Pairing friendly curves

- ▶ Security: DLP in $E(\mathbb{F}_q)[\ell]$ should be about as hard as DLP in \mathbb{F}_{q^k} , so need to balance size of ℓ and of q^k .
- ▶ DLP security in $E(\mathbb{F}_q)[\ell]$ grows like $e^{1/2 \log \ell}$
- ▶ 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

- ▶) Finding really good curves is even less trivial!
- ▶ Reference: Taxonomy of pairing friendly elliptic curves.

Evaluating functions

- ▶ Divisor is formal sum of points $D = \sum n_i P_i$
- ▶ Degree of divisor $\deg(D) = \sum n_i$
- ▶ Let f be a function on E and $D = \sum_i n_i P_i$ a divisor then

$$f(D) = \prod_i f(P_i)^{n_i}$$

- ▶ If this is defined and non-zero, i.e. if P_i not appear in (f) .
- ▶ If $\deg(D) = 0$ and $g = cf$ for $c \in \mathbb{F}_q^\times$, then $f(D) = g(D)$.
- ▶ So $f(D)$ only depends on (f) and D .
- ▶ By definition we have: $f(D_1 + D_2) = f(D_1) f(D_2)$, so evaluation is linear.

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

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

- ▶ $f_{n,P}$ is determined up to a constant $c \in \mathbb{F}_q^\times$.
- ▶ $f_{n,P}$ 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 $f_{n,P}(Q) \in \mathbb{F}_q^\times$.

Tate pairing

- ▶ Definition of Tate pairing:

$$h, i_\ell : E(\mathbb{F}_{q^k})[\ell] \rightarrow E(\mathbb{F}_{q^k})/\ell E(\mathbb{F}_{q^k}) \cong \mathbb{F}_{q^k}^*/(\mathbb{F}_{q^k}^*)^\ell$$

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

$$(f_{\ell,P}) = \ell((P) - (1))$$

- ▶ $Q \in E(\mathbb{F}_{q^k})$ and $R \in E(\mathbb{F}_{q^k})$ with $f_{\ell,Q} + R, R \notin f_{\ell,P}, 1 \notin g = ; .$

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

- ▶ Tate pairing is bilinear and non-degenerate.

Weil pairing

- ▶ Weil pairing $e_\ell : E(\mathbb{F}_{q^k})[\ell] \times E(\mathbb{F}_{q^k})[\ell] \rightarrow \mu_\ell$
- ▶ Let $P, Q \in E(\mathbb{F}_{q^k})[\ell]$ and $(f_{\ell,P}/f_{\ell,Q})(1) = 1$.
- ▶ Then $e_\ell(P, Q) = \begin{cases} 1 & \text{for } P = Q \text{ or } P = 1 \text{ or } Q = 1 \\ (1)^\ell f_{\ell,P}(Q)/f_{\ell,Q}(P) & \text{else.} \end{cases}$
- ▶ Weil pairing is bilinear and non-degenerate.
- ▶ The property $e_\ell(P, P) = 1$ is useful for subgroup membership testing.

Outline

Weil/Tate Pairings

Pairing Computation

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

Miller's algorithm: example

- ▶ Let $E : y^2 = x^3 + 11$ over \mathbb{F}_{31} .
- ▶ $E(\mathbb{F}_{31})$ has 25 points and structure $\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$.
- ▶ Generated by $P = [2, 9]$ and $Q = [3, 10]$.
- ▶ Let $\ell = 5$, then $k = 1$ since $5 \nmid (31 - 1)$
- ▶ Step 1: doubling $T = P$ gives $l = 20x + y + 13$ and $v = x + 7$
- ▶ Step 2: doubling T gives $l = 9x + y + 4$ and $v = x + 29$
- ▶ Step 2: adding T and P gives $l = x + 29$

$$f_{5,P} = \frac{(20x + y + 13)^2(9x + y + 4)(x + 29)}{(x + 7)^2(x + 29)}$$

- ▶ Normally do evaluation during loop!

Miller's algorithm: example

- ▶ Tate pairing: $\langle P, Q \rangle_5 = \frac{f_{5,P}(Q+R)}{f_{5,P}(R)}$ for some R
- ▶ Can take $R = Q$ for instance, thus

$$\langle P, Q \rangle_5 = \frac{f_{5,P}([2]Q)}{f_{5,P}(Q)} = \frac{20}{10} = 2$$

- ▶ Can also take $R = [2]Q$, so then obtain

$$\langle P, Q \rangle_5 = \frac{f_{5,P}([3]Q)}{f_{5,P}([2]Q)} = \frac{23}{20} = 12$$

- ▶ Different results since determined up to 5-th powers, i.e.

$$12 = 2 \quad 6 = 2 \quad 11^5 \pmod{31}$$

Tate pairing: simplify evaluation

- ▶ Need two evaluations of Miller function to compute

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

- ▶ Ideally, would simply like to compute $f_{\ell,P}(Q)$
- ▶ Let u_{∞} be a fixed \mathbb{F}_q -rational uniformizer at ∞
- ▶ 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 $\text{lc}_{\infty}(f_{\ell,P})$ is an ℓ -th power, then for $Q \notin P$, ℓ

$$\text{lc}_{\infty}(f_{\ell,P}(Q)) = \text{lc}_{\infty}(f_{\ell,P})^{\ell} \quad (\mathbb{F}_{q^k}^*)^{\ell}$$

- ▶ $\text{lc}_{\infty}(f_{\ell,P})$ being an ℓ -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 $\gcd(\ell, q^d - 1) = 1$ for all positive integers $d \leq k$ and $d < k$.
- ▶ So all elements of the fields \mathbb{F}_{q^d} are ℓ -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 $f_{\ell, P}$ is automatically normalised.

Take $G_1 = E(\mathbb{F}_q)[\ell]$

- ▶ 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 h, i_ℓ only defined up to ℓ -th powers.

$$h, i_\ell : E(\mathbb{F}_{q^k})[\ell] \rightarrow E(\mathbb{F}_{q^k})/\ell E(\mathbb{F}_{q^k}) \times \mathbb{F}_{q^k}^\times / (\mathbb{F}_{q^k}^\times)^\ell$$

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

$$t_\ell(P, Q) = hP, Qi_\ell^{(q^k-1)/\ell}$$

- ▶ Can ignore all factors that are ℓ -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 ℓ

- ▶ Let $N = h\ell$ be a multiple of N with $Njq^k \equiv 1$, then

$$t_\ell(P, Q) = hP, Qi_\ell^{(q^k-1)/\ell} = t_N(P, Q) = hP, Qi_N^{(q^k-1)/N}$$

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

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

else pairing will be 1.

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

Reduced Tate pairing: final exponentiation

- ▶ Final exponentiation is $(q^k - 1)/\ell$
- ▶ 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 $\ell \nmid \Phi_k(q)$
- ▶ Final exponentiation consists of easy and hard part

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

- ▶ 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 embedding degree k
- ▶ $\mathbb{G}_1 = E(\mathbb{F}_q)[\ell]$ and \mathbb{G}_2 has x -coordinates in $\mathbb{F}_{q^{k/2}}$
- ▶ Pairing on $\mathbb{G}_1 \times \mathbb{G}_2$ computed as

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

- ▶ No denominators in computation
- ▶ ℓ or $N = hr$ of low Hamming weight
- ▶ Small characteristic p : work in base p
- ▶ Clever final exponentiation
- ▶ Fast finite field arithmetic: binomial extensions, lazy reduction, ...

Questions?

End of Part I . . . more to come in part II