Ate Pairing on Hyperelliptic Curves

R. Granger, F. Hess, R. Oyono, N. Thériault
F. Vercauteren

EUROCRYPT 2007 - Barcelona

Pairings

- Let G_1, G_2, G_T be groups of prime order ℓ. A pairing is a non-degenerate bilinear map $e : G_1 \times G_2 \to G_T$.
- 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 $g \neq 1$: $\exists x \in G_2$ such that $e(g, x) \neq 1$
  - for all $h \neq 1$: $\exists x \in G_1$ such that $e(x, h) \neq 1$
- Examples:
  - Scalar product on euclidean space $\langle \cdot, \cdot \rangle : \mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}$.
  - Weil- and Tate pairings on elliptic curves and abelian varieties.

Pairings in cryptography

- Exploit bilinearity: original schemes $G_1 = G_2$
  - MOV: DLP reduction from G_1 to G_T

$$\text{DLP in} G_1 : (g, xg) \Rightarrow \text{DLP in } G_T : (e(g,g), e(g,g)^x)$$

  - Decision DH easy in G_1

$$\text{DDH} \; : (g, ag, bg, cg) \text{ test if } e(g, cg) = e(ag, bg)$$

- Identity based crypto, short signatures, . . .
- (Too?) many new hardness assumptions and applications

This paper

- New pairing on hyperelliptic curves called ate pairing
- Generalises and unifies previous work by:
  - BGOS05: eta pairing on supersingular curves
  - HSV06: ate pairing on elliptic curves
- What's in a name?
  - ate = Tate - T
  - ate = reverse(eta)
- Spelling: ate and not Ate (please manually correct)

Elliptic curves

- Let E be an elliptic curve over a finite field $\mathbb{F}_q$, i.e.

$$E : y^2 = x^3 + ax + b \quad \text{for } p > 5$$

- Point sets $E(\mathbb{F}_{q^k})$ define an abelian group by
  - Chord-tangent method
  - Point at infinity $\infty \in E(\mathbb{F}_q)$ is neutral element.
- Hasse-Weil: number of points in $E(\mathbb{F}_q)$ is $q + 1 - t$ with

$$|t| \leq 2\sqrt{q}$$

Torsion subgroups

- $E[\ell]$ subgroup of points of order dividing ℓ, i.e.

$$E[\ell] = \{P \in E(\overline{\mathbb{F}}_q) \mid \ell P = \infty\}$$

- Structure of $E[\ell]$ for $\gcd(\ell, q) = 1$ is $\mathbb{Z}/\ell\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z}$.
- Let $\ell | \# E(\mathbb{F}_q)$, then $E(\mathbb{F}_q)[\ell]$ gives at least one component.
- Embedding degree: k minimal with $\ell \mid (q^k - 1)$.
- Note ℓ-roots of unity $\mu_\ell \subseteq \mathbb{F}_{q^k}^\times$.
- If $k > 1$ then $E(\mathbb{F}_{q^k})[\ell] = E[\ell]$.

Frobenius endomorphism

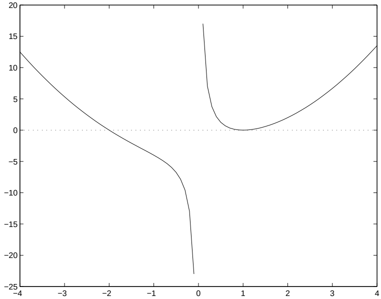
- Frobenius: $\varphi : E \to E : (x, y) \mapsto (x^q, y^q)$
- Characteristic polynomial: $\varphi^2 - [t] \circ \varphi + [q] = 0$
- Eigenvalues on $E[\ell]$: 1 and q since $\ell \mid \#E(\mathbb{F}_q)$
- For $k > 1$ have $q \neq 1 \bmod \ell$, thus decomposition of $E[\ell]$ into Frobenius eigenspaces:

  $$E[\ell] = E(\mathbb{F}_{q^k})[\ell] = \langle P \rangle \times \langle Q \rangle$$

  with $\varphi(P) = P$ and $\varphi(Q) = qQ$
- Notation used before: $G_1 = \langle P \rangle$ and $G_2 = \langle Q \rangle$

Functions and divisors

- Consider the function $f = \frac{(x-1)^2(x+2)}{x}$ on $\mathbb{P}^1$



- Divisor of f: $(f) = 2(P_1) + (P_{-2}) - (P_0) - 2(P_\infty)$
- Support of (f): $\mathrm{Supp}((f)) = \{P_1, P_{-2}, P_0, P_\infty\}$
- Given divisor (f), function is determined up to constant.

Miller functions

- Let $P \in E(\mathbb{F}_q)$ 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

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

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

- Note: $f_{\ell,P}$ has zero of order ℓ at P and pole of order ℓ at ∞.
- Tate pairing is defined as (assuming normalisation)

$$\boxed{\langle P, Q\rangle_\ell = f_{\ell,P}(Q)}$$

- Technical stuff: need to adjust domain and image

$$\langle \cdot, \cdot \rangle_\ell : E(\mathbb{F}_{q^k})[\ell] \times E(\mathbb{F}_{q^k})/\ell E(\mathbb{F}_{q^k}) \longrightarrow \mathbb{F}_{q^k}^\times/(\mathbb{F}_{q^k}^\times)^\ell$$

- Reduced Tate pairing: $e(P, Q) = \langle P, Q\rangle_\ell^{(q^k-1)/\ell}$

Computing Tate pairing

- Miller's algorithm: double-add algorithm using bits of ℓ
- Loop length for Tate is $\log_2(\ell)$
- Many optimisations when restricting domain to $G_1 \times G_2$
- BUT: Tate pairing still defined on the whole of $E[\ell] \times E/\ell E$
- GOAL: construct efficient pairing only defined on $G_1 \times G_2$?

Ate pairing

- Like Tate, but evaluating 'smaller' Miller function $f_{s,P}$
- Recall $E/\mathbb{F}_q$ with $\#E(\mathbb{F}_q) = q + 1 - t$ and $\ell | \#E(\mathbb{F}_q)$
- Define $T = t - 1$, then $T \equiv q \bmod \ell$

Pairing Zoo

Pairing	Domain	Where	Who	s	Red
Tate	$E[\ell] \times E/\ell E$	All HECs	Miller	ℓ	No
eta	$G_1 \times G_2$	SuSi	BGOS	T	No
ate EC	$G_2 \times G_1$	All ECs	HSV	T	No
ate HEC	$G_2 \times G_1$	All HECs	GHOTV	q	Yes

Elliptic ate pairing

- Theorem: Let $T = t - 1$ and $T^k \neq 1$. Then

$$a(\cdot,\cdot) : G_2 \times G_1 \to \mathbb{F}_{q^k}/(\mathbb{F}_{q^k})^{\ell} : (Q,P) \mapsto f_{T,Q}(P)$$

  is a pairing, called the elliptic ate pairing
- Loop length is now $\log_2(T)$, but first argument over $\mathbb{F}_{q^k}$
- Need final powering by $(q^k - 1)/\ell$ to map into μ_ℓ, i.e. reduced ate pairing
- In general $T \simeq \sqrt{q}$, but could be as small as $\ell^{1/\varphi(k)}$
- Need to use twists to make ate faster than Tate

Extreme elliptic ate

- Smallest non-degenerate ate pairing for $T = 2$, i.e. $t = 3$.
- Pairing now becomes extremely simple:

$$(Q,P) \mapsto \left(\frac{y(P) - \lambda(Q)x(P) - \mu(Q)}{x(P) - x(2Q)}\right)^{(q^k-1)/\ell}$$

  with $y = \lambda(Q)x + \mu(Q)$ tangent line at Q
- Recall t can only be as small as $\ell^{1/\varphi(k)}$ so k has to be large
- Example: $k = 197$, p 374-bit, ℓ 185-bit, $D = -59$

  r = 26828803997912886929710867041891989490486893845712448833
  p = 359634406619359131700235434104695240017984343417407631809006508191326374003984448896211933602599397210289053724447

Hyperelliptic ate pairing

- Take $C/\mathbb{F}_q$ hyperelliptic curve and $\ell|\#J_C(\mathbb{F}_q)$
- Let $G_1 = J_C[\ell] \cap \mathrm{Ker}(\varphi - [1])$ and $G_2 = J_C[\ell] \cap \mathrm{Ker}(\varphi - [q])$ then

  $$a(\cdot,\cdot) : G_2 \times G_1 \to \mu_\ell : (\overline{D}_2, \overline{D}_1) \mapsto f_{q,D_2}(D_1)$$

  defines a non-degenerate, bilinear pairing called the hyperelliptic ate pairing
- No need for final powering, maps directly into μ_ℓ

Pairing inversion in polynomial time

R.I.P.

$>$ 1000 papers

Pairing inversion in polynomial time

?

Pairing inversion (see GHV)

- Most pairings can be written as

$$(P, Q) \mapsto f_{s,P}(Q)^d$$

  with d is the final exponentiation (FE)
- E.g. Tate : $s = \ell$ and $d = (q^k - 1)/\ell$
- Miller inversion (MI): invert $f_{s,P}(\cdot)$
- Tate: security in MI, FE does not add security!
- Ate: families where MI is polynomial time only
  $\Rightarrow$ security totally in FE!
- BUT: does not imply weakness if used correctly . . .

Conclusion

- New pairing with domain two eigenspaces of Frobenius
- Pairing reduced by itself, so no final exponentiation
- Efficiency not so good, except if twists are available
- Elliptic ate with $D = -3$ remains best pairing to use
- Applications to pairing inversion (see GHV)