Background of Pairings

Tanja Lange

Department of Mathematics and Computer Science

Technische Universiteit Eindhoven

The Netherlands

tanja@hyperelliptic.org

04.09.2007

Pairings

Let $(G_1, \oplus), (G_1', \oplus)$ and $(G, \cdot)$ be groups and let

$$e : G_1 \times G_1' \to G$$

be a map satisfying

- $e(P \oplus Q, R') = e(P, R')e(Q, R')$
- $e(P, R' \oplus S') = e(P, R')e(P, S')$
- The map is non-degenerate in the first argument, i.e. if $e(P, R') = 1$ for all $R' \in G_1'$ for some P then P is the identity in G_1

Then e is called a bilinear map or pairing.

In protocol papers often $G_1 = G_1'$.

Consequences

- Assume that $G_1 = G_1'$ and hence
$$e(P, P) \neq 1.$$
Then for all triples $(P_1, P_2, P_3) \in \langle P \rangle^3$ one can decide whether
$$\log_P(P_3) = \log_P(P_1) \log_P(P_2)$$
by comparing
$$e(P_1, P_2) \stackrel{?}{=} e(P, P_3).$$
Thus the Decision Diffie-Hellman Problem is easy.
- The DL system G_1 is at most as secure as the system G. Even if $G_1 \neq G_1'$ one can transfer the DLP in G_1 to a DLP in G, provided that one can find an element $P' \in G_1'$ such that the map $P \to e(P, P')$ is injective.

Positive Application of Pairings

Joux, ANTS 2000, one round tripartite key exchange

Let P, P' be generators of G_1 and G_1' respectively.
Users A, B and C compute joint secret from their secret contributions a, b, c as follows (A's perspective)

- Compute and send $[a]P, [a]P'$.
- Upon receipt of $[b]P$ and $[c]P'$ put $k = (e([b]P, [c]P'))^a$

The resulting element k is the same for each participant as

$$k = (e([b]P, [c]P'))^a = (e(P, P'))^{abc} = (e([a]P, [c]P'))^b = (e([a]P, [b]P')$$

- Obvious saving in first step if $G_1 = G_1'$.
- Only one user needs to do both computations.

Prerequisites I

We want to define pairings

$$G_1 \times G_2 \longrightarrow G_T$$

preserving the group structure.

- Tate and the Weil pairing both use elliptic curves as first argument. Assume that $\ell \big| |E(\mathbb{F}_q)|$ and $\ell^2 \not| \ |E(\mathbb{F}_q)|$.
- Let ℓ be a prime, let E be an elliptic curve over $\mathbb{F}_q$.
- G_1 is the group of $\mathbb{F}_q$-rational ℓ-torsion points of E, i.e. $G_1 = E[\ell](\mathbb{F}_q)$, $\mathbb{F}_q$-rational points on elliptic curve E of order ℓ.

Prerequisites II

- The pairings we use map to the multiplicative group of a finite extension field $\mathbb{F}_{q^k}$.
- G_T has order ℓ, so by Lagrange ℓ must divide the group order of $\mathbb{F}_{q^k}^*$, this happens if $\ell \mid q^k - 1$.
- The embedding degree k is defined to be the minimal extension degree of $\mathbb{F}_q$ so that the ℓ-th roots of unity are in $\mathbb{F}_{q^k}^*$, i.e.
  $$k \text{ minimal with } \ell \mid q^k - 1.$$
- Attention: if q is not prime then the group of ℓ-th roots of unity can be in a a smaller extension of the prime field! Read Laura Hitt's paper at Pairing 2007.
- For $k > 1$ Tate-Lichtenbaum pairing is degenerate on linear dependent points, i.e. $T_\ell(P, P) = 1$.

Tate-Lichtenbaum pairing I

- Thanks to Isabelle Déchenȅ we can now use the whole machinery of divisors and divisor classes in the “easy” case of elliptic curves.
- Denote by $E(\mathbb{F}_{q^k})[\ell]$ the points on E of order ℓ defined over $\mathbb{F}_{q^k}$.
- Using the embedding of E into Pic^0_E, i.e.

$$P \mapsto P - P_\infty$$

we have:

$$P \in E(\mathbb{F}_{q^k})[\ell] \Rightarrow \exists F_P \text{ such that } \ell(P - P_\infty) \sim \mathrm{div}(F_P),$$

i.e. $\ell(P - P_\infty)$ is a principal divisor.

Tate-Lichtenbaum pairing II

- Given $Q \in E(\mathbb{F}_{q^k})$, find $S \in E(\mathbb{F}_{q^k})$ so that $Q \oplus S, S \notin \{\pm P, P_\infty\}$. (A random choice of S will do.)
- Note that $Q \oplus S - S \sim Q - P_\infty$.
- Tate-Lichtenbaum pairing

$$T_\ell(P, Q) = F_P(Q \oplus S - S) = \frac{F_P(Q \oplus S)}{F_P(S)}.$$

- This map is actually bilinear – easy to see for second argument; slightly harder for first.
- The value is independent of the choices of F_P and S – up to ℓ-th powers.

Tate-Lichtenbaum pairing III

This T_ℓ defines a bilinear and non-degenerate map

$$T_\ell : E(\mathbb{F}_{q^k})[\ell] \times E(\mathbb{F}_{q^k})/\ell E(\mathbb{F}_{q^k}) \to \mathbb{F}_{q^k}^* / \mathbb{F}_{q^k}^{*\ell}$$

as ℓ-folds are in the kernel of T_ℓ.
To achieve unique value in $\mathbb{F}_{q^k}$ rather than class do final exponentiation

$$\tilde{T}_\ell = T_\ell(P, Q)^{(q^k-1)/\ell}.$$

Often

$$T_\ell : E(\mathbb{F}_{q})[\ell] \times E(\mathbb{F}_{q^k})/\ell E(\mathbb{F}_{q^k}) \to \mathbb{F}_{q^k}^* / \mathbb{F}_{q^k}^{*\ell}.$$

The function F_P is built iteratively and evaluated in each round. This is known as Miller's algorithm.

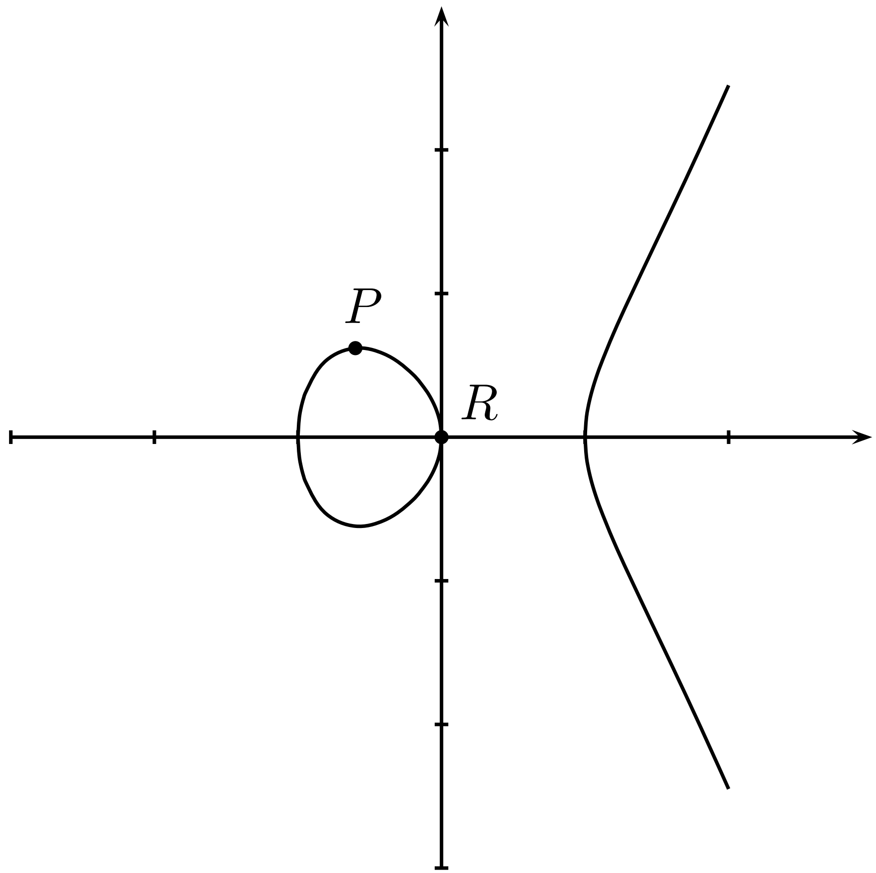
Miller's algorithm

In: $\ell = \sum_{i=0}^{n-1} \ell_i 2^i$, $P, Q \oplus S, S$
Out: $T_\ell(P, Q)$

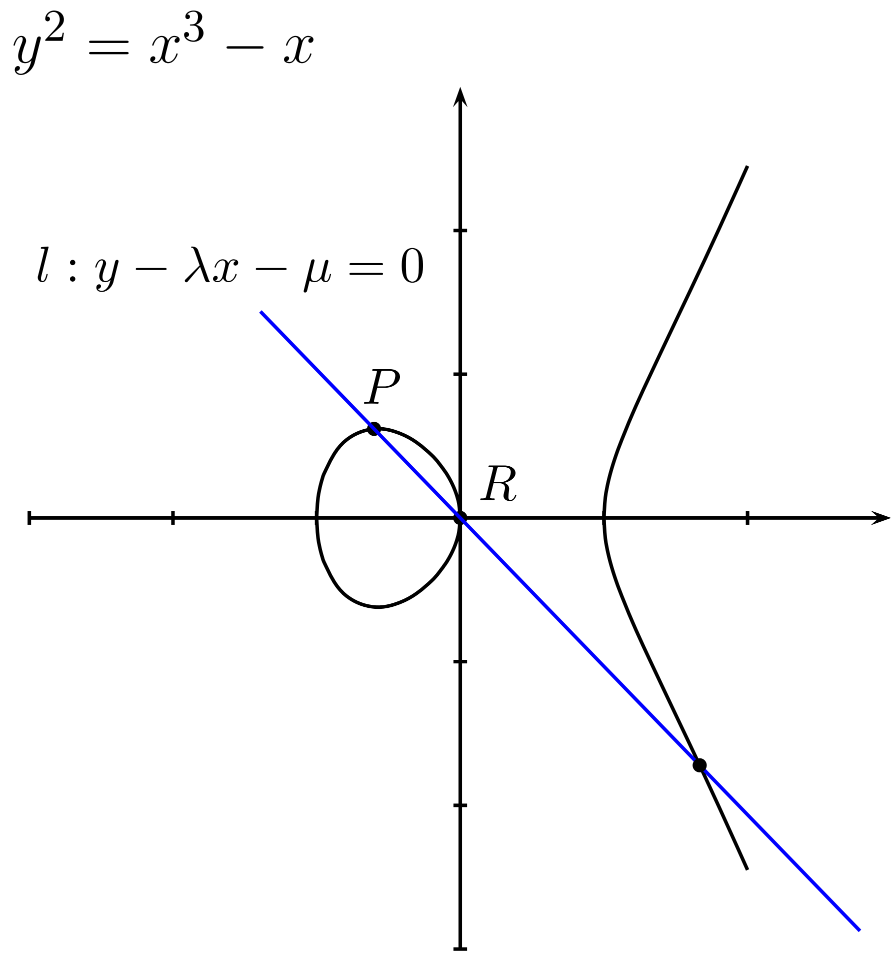
1. $T \leftarrow P$, $F \leftarrow 1$
2. for $i = n-2$ downto 0 do
   (a) Calculate lines l and v in doubling
   $T \leftarrow [2]T$
   $F \leftarrow F^2 \cdot l(Q \oplus S)v(S)/(l(S)v(Q \oplus S))$
   (b) if $\ell_i = 1$ then
   Calculate lines l and v in addition $T \oplus P$
   $T \leftarrow T \oplus P$
   $F \leftarrow F \cdot l(Q \oplus S)v(S)/(l(S)v(Q \oplus S))$
3. return F

Group Law in $E(\mathbb{R}), h = 0$

$y^2 = x^3 - x$

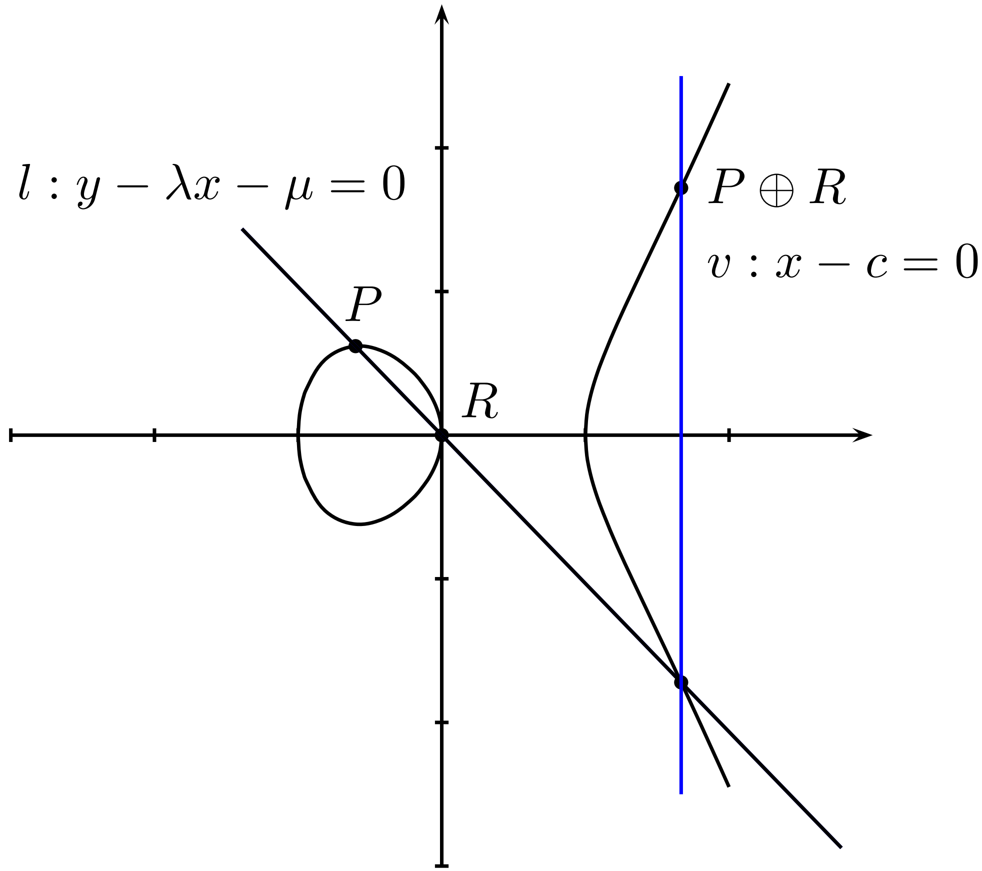


Group Law in $E(\mathbb{R}), h = 0$



Group Law in $E(\mathbb{R}), h = 0$

$y^2 = x^3 - x$



Weil pairing

For an elliptic curve E define

$$\begin{array}{rcl} W_\ell : E(\overline{\mathbb{F}}_q)[\ell] \times E(\overline{\mathbb{F}}_q)[\ell] & \rightarrow & \mu_\ell \\ (P, Q) & \mapsto & \dfrac{F_P(D_Q)}{F_Q(D_P)}, \end{array}$$

where μ_ℓ is the multiplicative groups of the ℓ-th roots of unity in the algebraic closure $\overline{\mathbb{F}}_q$ of $\mathbb{F}_q$ and D_P and D_Q are divisors isomorphic to $P - P_\infty$ or $Q - P_\infty$, respectively. Obviously, $W_\ell(P, P) = 1$.

Weil pairings can be seen as two-fold application of the Tate-Lichtenbaum pairing, note $Q \in E(\mathbb{F}_{q^k})$.

Needs full group of order ℓ in $E(\mathbb{F}_{q^k})$, if $k = 1$ then the Weil pairing is trivial & one needs to use larger field.

Supersingular and ordinary

Definition

Let E be an elliptic curve defined over $\mathbb{F}_q, q = p^r$.
E is supersingular if

- $E[p^s](\overline{\mathbb{F}}_q) = \{P_\infty\}$.
- $|E(\mathbb{F}_q)| = q - t + 1$ with $t \equiv 0 \bmod p$.
- End_E is order in quaternion algebra.

Otherwise it is ordinary and one has $E[p^s](\overline{\mathbb{F}}_q) \cong \mathbb{Z}/p^s\mathbb{Z}$.

These statements hold for all s if they hold for one.
End_E order in quaternion algebra means that there are maps which are linearly independent of the Frobenius endomorphism. They are called distortion maps.

Example

Consider

$$y^2 + y = x^3 + a_4 x + a_6 \text{ over } \mathbb{F}_{2^r},$$

so $q = 2^r$.

Negative of $P = (a, b)$ is $-P = (a, b + 1)$,
$\Rightarrow$ no affine point with $P = -P$ since $b \neq b + 1$,
$\Rightarrow$ even number of affine points, one point P_∞,

$\Rightarrow |E(\mathbb{F}_q)| = q - t + 1 = 2^r - t + 1$ is odd, so t is even.

This curve is supersingular (using the second criterion).

Distortion map I

For supersingular curves it is possible to find maps $\phi : E(\mathbb{F}_q) \to E(\mathbb{F}_{q^k})$ that map to a linearly independent subgroup, i.e.

$$T'_\ell(P,P) \neq 1 \text{ for } T'_\ell(P,P) = T_\ell(P, \phi(P)).$$

(This needs that there are independent endomorphisms, so no chance for ordinary curves).
Examples:

- $y^2 = x^3 + a_4 x$, for $p \equiv 3 \pmod 4$.
  Distortion map $(x, y) \mapsto (-x, iy)$ with $i^2 = -1$
- $y^2 = x^3 + a_6$, for $p \equiv 2 \pmod 3$.
  Distortion map $(x, y) \mapsto (jx, y)$ with $j^3 = 1, j \neq 1$,

In both cases, $\#E(\mathbb{F}_p) = p + 1$, $k = 2$.

Distortion maps II

- Over $\mathbb{F}_{2^d}$ consider
$$y^2 + y = x^3 + x + a_6, \text{ with } a_6 = 0 \text{ or } 1$$
and distortion map
$$(x, y) \mapsto (x+s^2, y+sx+t), \; s, t \in \mathbb{F}_{2^{4d}}, \; s^4+s = 0, \; t^2+t+s^6+s^2 =$$
$\#E(\mathbb{F}_{2^d}) = 2^d + 1 \pm 2^{(d+1)/2}$, $k = 4$.
- Over $\mathbb{F}_{3^d}$ consider
$$y^2 = x^3 + x + a_6, \quad \text{with} \quad a_6 = \pm 1$$
and distortion map
$$(x, y) \mapsto (-x + s, iy) \; \text{ with } \; s^3 + 2s + 2a_6 = 0 \; \text{ and } \; i^2 = -1.$$
$\#E(\mathbb{F}_{3^d}) = 3^d + 1 \pm 3^{(d+1)/2}$, $k = 6$.

Outlook and literature

- Efficient implementation of pairings in Mike Scott's talk
- Much more about pairings during ECC – talks by Laura Hitt, Kate Stange, and Fre Vercauteren.
- Chapters 6. Background on Pairings, 16. Implementation of Pairings, and 24. Pairing-Based Cryptography of the Handbook of Elliptic and Hyperelliptic Curve Cryptography `http://www.hyperelliptic.org/HEHCC`
- Advances in Elliptic Curve Cryptography by I. F. Blake, G. Seroussi, and N. P. Smart (Eds.) has chapter on pairings by Steven D. Galbraith.
- Pairings for Cryptographers by S. D. Galbraith, K. G. Paterson, and N. P. Smart; ePrint Archive: Report 2006/165