

# Pairings on Elliptic Curves II

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

ECC Summer School - 2011

# Outline

Choosing  $G_1$  and  $G_2$

Ate Pairing

Optimal Pairing

## Elliptic curves

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

## $r$ -torsion and Frobenius

- ▶ Denote  $\pi_q$  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  $r \mid \#E(\mathbb{F}_q)$ ,  $\pi_q$  has eigenvalues 1 and  $q$  on  $E[r]$ .
- ▶ Embedding degree  $k$  is precisely such that  $q$ -eigenspace of  $\pi_q$  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 $\mathbb{G}_2$ : 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  $\psi$  defines
  - ▶ a vector space isomorphism  $E'(\mathbb{F}_{q^d})[r] \rightarrow E(\mathbb{F}_{q^d})[r]$ .
  - ▶ automorphism of  $E$ :  $\psi^\sigma \circ \psi^{-1}$ , where  $\psi^\sigma$  is  $\psi$  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  $d$  and assume  $d \mid k$
- ▶ Let  $e = k/d$ , then degree  $d$  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  $\phi_d : E' \rightarrow E$  the twisting isomorphism, then

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

- ▶ 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



# Outline

Choosing  $G_1$  and  $G_2$

Ate Pairing

Optimal Pairing

## Ate pairing on $\mathbb{G}_2 \times \mathbb{G}_1$

- ▶ Let  $T \equiv q \pmod r$ ,  $Q \in \mathbb{G}_2$  and  $P \in \mathbb{G}_1$
- ▶ ate pairing:  $f_{T,Q}(P)$  defines a bilinear pairing on  $\mathbb{G}_2 \times \mathbb{G}_1$
- ▶ let  $N = \gcd(T^k - 1, q^k - 1)$  and  $T^k - 1 = LN$ , with  $k$  the embedding degree, then

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

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

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

## Ate pairing: proof sketch

- ▶ Step 1: prove that

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

by considering

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

- ▶ Step 2: prove that (exercise)

$$f_{T^k, Q} = f_{T, Q}^{T^{k-1}} f_{T, [T]Q}^{T^{k-2}} \cdots f_{T, [T^{k-1}]Q}$$

## Ate pairing: proof sketch

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

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

- ▶ So for  $Q \in \mathbb{G}_2$  we have  $[T]Q = \pi_q(Q)$ , since  $q \equiv T \pmod r$
- ▶ Replacing  $[T^i]Q$  by  $\pi_q^i(Q)$  and using that curve and  $P$  are defined over  $\mathbb{F}_q$ , we get

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

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

## Ate pairing on $G_2 \times G_1$

- ▶ Advantage:  $T$  can be smaller than  $r$ , so shorter loop
- ▶ Disadvantage: first input point defined over big field  $\mathbb{F}_{q^k}$ , but can use twists
- ▶ Same proof holds for all  $T \equiv q^j \pmod{r}$
- ▶ Recall that  $r \mid \Phi_k(q)$ , so  $r \mid \Phi_k(T)$
- ▶ So the smallest  $T$  is roughly of size

$$r^{1/\varphi(k)}$$

- ▶ Bound is attained for some families of pairing friendly curves, but not in general.

## Extreme ate

- ▶ Curves with  $t = -1$  give shortest loop in Miller's algorithm.
- ▶ Let  $E : y^2 = x^3 + 4$  over  $\mathbb{F}_p$  with  $p = 41761713112311845269$ , then  $t = -1$ ,  $r = 715827883$ ,  $k = 31$  and  $D = -3$ .
- ▶ Let  $y - \lambda(Q)x - \nu(Q)$  with  $\lambda = 3x_Q/(2y_Q)$  and  $\nu = (-x_Q + 8)/(2y_Q)$  be the tangent at  $Q$ .
- ▶ The function

$$(Q, P) \mapsto (y_P - \lambda(Q)x_P - \nu(Q))^{(q^k - 1)/r}$$

defines a non-degenerate pairing on  $\mathbb{G}_2 \times \mathbb{G}_1$

# Outline

Choosing  $G_1$  and  $G_2$

Ate Pairing

Optimal Pairing

## Creating “new” pairings

- ▶ Given cyclic groups  $\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T$ , a pairing  $e$  is completely determined by  $(P, Q, z)$  with

$$e(P, Q) = z \quad \text{and} \quad \mathbb{G}_1 = \langle P \rangle, \quad \mathbb{G}_2 = \langle Q \rangle$$

- ▶ Any other non-degenerate bilinear pairing is a fixed power of one given pairing
- ▶ Conclusion: on given prime order groups, all pairings can be obtained as powers of Tate
- ▶ However: could be more efficient to compute than Tate



## Creating “new” pairings

- ▶ Let  $E$  be an elliptic curve over  $\mathbb{F}_q$  and let  $r \mid \#E(\mathbb{F}_q)$ , with  $\gcd(r, q) = 1$  and embedding degree  $k$ .
- ▶ Let  $\lambda = Cr$  be a multiple of  $r$ , then the following map

$$a_\lambda : E(\mathbb{F}_{q^k})[r] \times E(\mathbb{F}_{q^k})/rE(\mathbb{F}_{q^k}) \longrightarrow \mu_r \subset \mathbb{F}_{q^k}^* :$$

$$(P, Q) \mapsto a_\lambda(P, Q) = f_{\lambda, P}(Q)^{(q^k-1)/r},$$

with  $f_{\lambda, P}$  normalized, defines a bilinear pairing which is non-degenerate if and only if  $\gcd(r, C) = 1$ .

## Creating “new” pairings

- ▶ Take divisors of both sides, can verify formula

$$f_{ab,P} = f_{a,P}^b \cdot f_{b,[a]Q}$$

- ▶ Can take  $f_{\lambda,P}$  as  $f_{\lambda,P} = f_{Cr,P} = f_{r,P}^C \cdot f_{C,[r]P}$
- ▶ Since  $[r]P = \infty$ , we have  $f_{C,[r]P} = 1$ .
- ▶ Take  $C$ -th power of the reduced Tate pairing

$$t_r(P, Q)^C = f_{r,P}(P)^{C(q^k-1)/r} = a_{\lambda}(P, Q)$$

- ▶ Furthermore, since  $t_r$  has order  $r$  and is non-degenerate, we conclude that  $a_{\lambda}$  is non-degenerate if and only if  $\gcd(r, C) = 1$ .

## Ate pairing on ordinary elliptic curves

- ▶ Optimal pairing: if pairing can be computed using  $\log_2 r/\varphi(k)$  Miller iterations
- ▶ Does not imply that pairing has to be of the form  $f_{S,Q}(P)$
- ▶ For some families of elliptic curves, ate is already optimal
- ▶ Main idea: products and fractions of pairings are also pairings

## Ate pairing on ordinary elliptic curves

- ▶ Consider  $\lambda = Cr = \sum_{i=0}^l c_i q^i$ , then  $f_{\lambda, Q}^{(q^k-1)/r}$  defines a bilinear pairing
- ▶ Expand  $f_{\lambda, Q}$  and divide out ate pairings  $a_{q^i}$

$$a_{[c_0, \dots, c_l]} : \mathbb{G}_2 \times \mathbb{G}_1 \rightarrow \mu_r :$$

$$(Q, P) \mapsto \left( \prod_{i=0}^l f_{c_i, Q}^{q^i}(P) \cdot \prod_{i=0}^{l-1} \frac{f_{[s_{i+1}Q, [c_i q^i]Q]}(P)}{f_{[s_i]Q}(P)} \right)^{(q^k-1)/r}$$

with  $s_i = \sum_{j=i}^l c_j q^j$  defines bilinear pairing

- ▶ If

$$Ckq^{k-1} \not\equiv ((q^k - 1)/r) \cdot \sum_{i=0}^l ic_i q^{i-1} \pmod{r}$$

then the pairing is non-degenerate

## If it looks too good to be true, ...

- ▶  $r | \Phi_k(q)$ , so could try  $\lambda = \Phi_k(q)$ , then  $c_i$  tiny and pairing  $a_{[c_0, \dots, c_i]}$  extremely efficient
- ▶ But: pairing will be degenerate!
- ▶ Could only consider  $\lambda$  of the form

$$\lambda = Cr = \sum_{j=1}^{\varphi(k)-1} c_j q^j$$

## Automagical construction

- ▶ To find best multiples of  $r$ , find short vectors in the lattice (spanned by the rows)

$$L := \begin{pmatrix} r & 0 & 0 & \dots & 0 \\ -q & 1 & 0 & \dots & 0 \\ -q^2 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & & \ddots & \\ -q^{\varphi(k)-1} & 0 & \dots & 0 & 1 \end{pmatrix} .$$

- ▶ Volume of  $L$  is easily seen to be  $r$ , so by Minkowski

$$V \in L \quad \text{with} \quad \|V\|_{\infty} \leq r^{1/\varphi(k)}$$

where  $\|V\|_{\infty} = \max_i |v_i|$

- ▶ The shortest vector  $V$  in  $L$  satisfies

$$\|V\|_{\infty} \geq \frac{r^{1/\varphi(k)}}{\varphi(k)}$$

## An example

- ▶ The family of BN-curves has  $k = 12$  and is given by

$$p(x) = 36x^4 + 36x^3 + 24x^2 + 6x + 1$$

$$r(x) = 36x^4 + 36x^3 + 18x^2 + 6x + 1$$

- ▶ The shortest vectors in the lattice  $L$

$$V_1(x) = [x + 1, x, x, -2x] \quad V_2(x) = [2x, x + 1, -x, x] .$$

- ▶ Short vectors with minimal number of coefficients of size  $x$

$$W(x) = [6x + 2, 1, -1, 1]$$

- ▶ The pairing  $a_{[c_0, \dots, c_l]}$  can be computed as

$$(f_{6x+2, Q}(P) \cdot l_{Q_3, -Q_2}(P) \cdot l_{-Q_2+Q_3, Q_1}(P) \cdot l_{Q_1-Q_2+Q_3, [6x+2]Q})^{(q^k-1)/r}$$

where  $Q_i = Q^{q^i}$  for  $i = 1, 2, 3$ .

# Questions?

End of Part II . . . there is no part III