Realization of Fast Pairings II

Frederik Vercauteren

Pairings in Arithmetic Geometry and Cryptography
Notation

- Base field $\mathbb{F}_q$ with $q = p^m$.
- $E$ elliptic curve defined over $\mathbb{F}_q$.
- Assume: exists subgroup $E(\mathbb{F}_q)[r]$ of large prime order $r$ with $\gcd(r, q) = 1$.
- Embedding degree: $k$, that is $r|(q^k - 1)$ and $k$ minimal.
- Let $\pi_q$ Frobenius endomorphism $(x, y) \mapsto (x^q, y^q)$ and

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

- Trace of Frobenius $t$: $\#E(\mathbb{F}_q) = q + 1 - t$
Ate pairing on $G_2 \times G_1$

- Let $T \equiv q \mod r$, $Q \in G_2$ and $P \in G_1$
- Ate pairing: $f_{T,Q}(P)$ defines a bilinear pairing on $G_2 \times G_1$
- 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 $c = \sum_{i=0}^{k-1} T^{k-1-i}q^i \equiv kq^{k-1} \mod r$
- 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

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

▶ Step 2: prove that (exercise)

\[ f_{T^k, Q} = f_{T, Q}^{T^k-1} f_{T, TQ}^{T^k-2} \cdots f_{T, T^{k-1}Q} \]
Ate pairing: proof sketch

- By definition of $G_1$ and $G_2$ we have

\[ \forall P \in G_1 : \pi_q(P) = P \quad \text{and} \quad \forall Q \in G_2 : \pi_q(Q) = [q]Q \]

- So for $Q \in G_2$ we have $[T]Q = \pi_q(Q)$, since $q \equiv T \mod r$

- Let $\psi \in \text{End}(E)$ and assume that $\text{Ker}(\psi) = \{O\}$, then

\[ f_{n,\psi}(P) \circ \psi = f_{n,\deg(\psi)} \]

- Note that $\psi$ can be either automorphism or purely inseperable.
Ate pairing: proof sketch

▶ By definition: \( \text{div}(f_n, \psi(P)) = n(\psi(P)) - ([n]\psi(P)) - (n-1)(O) \)

▶ Explicit computation gives

\[
\psi^*(\text{div}(f_n, \psi(P))) = \deg(\psi)[n(P) - ([n]P) - (n-1)(O)] = \text{div}(f_{n,P}^{\deg(\psi)})
\]

▶ Finally, \( \psi^*(\text{div}(f_n, \psi(P))) = \text{div}(f_n, \psi(P) \circ \psi) \)

▶ Apply this to \( \pi_q^i \), then

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

▶ Since \( \pi_q(P) = P \), we conclude that

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

▶ Substituting in expression for \( f_{T^k,Q}(P) \) finishes proof
Ate pairing on $\mathbb{G}_2 \times \mathbb{G}_1$

- **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** $T \equiv q^i \mod r$
- **Recall that** $r | \Phi_k(q)$, so $r | \Phi_k(T)$
- **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 \( G_2 \times G_1 \).
Ate pairing on $G_1 \times G_2$

- Main disadvantage of ate: first input point defined over $\mathbb{F}_{q^k}$
- Why not obtain pairing on $G_1 \times G_2$?
- Main ingredient needed: endomorphism $\psi$ with trivial kernel such that

$$\forall P \in G_1 : \psi(P) = [q]P \quad \forall Q \in G_2 : \psi(Q) = Q$$
Eta pairing

- Pairing on supersingular curves defined on $G_1 \times G_1$
- Distortion map $\phi : G_1 \rightarrow G_2$
- Definition: let $T \equiv q \mod r$,

$$\eta_T : G_1 \times G_1 \rightarrow \mu_r : (P, Q) \mapsto \eta_T(P, Q) = f_{T, P}(\phi(Q))^{(q^k-1)/r}$$

defines a bilinear pairing
- Proof is the same as for ate but using dual $\hat{\pi}_q$ of Frobenius
- If $E$ supersingular then $\hat{\pi}_q$ is purely inseperable
Twisted ate pairing

- Assume that $E$ admits a twist $E'$ of degree $d$ and set $m = \gcd(k, d)$ and $e = k/m$
- Alternative representation of $\mathbb{G}_2$ as

$$\mathbb{G}_2 = E[r] \cap \text{Ker}([\xi_m]^e_q - 1)$$

for a unique primitive $m$-th root of unity $\xi_m$

- $[\xi_m]^e_q$ has trivial kernel and satisfies

$$\forall P \in \mathbb{G}_1 : [\xi_m]^e_q(P) = [T^e]P \quad \forall Q \in \mathbb{G}_2 : [\xi_m]^e_q(Q) = Q$$

- Obtain twisted ate pairing on $\mathbb{G}_1 \times \mathbb{G}_2$

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

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

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

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

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

- Can take \( f_{\lambda, P} \) as \( f_{\lambda, P} = f_{Cr, P} = f_{r, P}^C \cdot f_{C, [r]P} \)

- Since \([r]P = \mathcal{O}\), 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 \( \gcd(r, C) = 1 \).
Creating “new” pairings

- Alternative to obtain possibly simpler final exponentiation
- Let $N = \gcd(q^k - 1, \lambda)$ and $C = \lambda/N$, then

$$f_{\lambda,Q}^{(q^k - 1)/N}$$

defines a bilinear pairing which is non-degenerate if and only if $\gcd(r, C) = 1$.

- For some $N$, the final exponentiation $(q^k - 1)/N$ has low Hamming weight in base $q$
Ate pairing on ordinary elliptic curves

- Optimal pairing: if pairing can be computed using $\log_2 \frac{r}{\varphi(k)}$ 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 $a_{q^i}$.

$$a_{[c_0, \ldots, c_l]} : G_2 \times G_1 \to \mu_r :$$

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

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

- If

$$Ckq^{k-1} \neq ((q^k - 1)/r) \cdot \sum_{i=0}^{l} ic_i q^{i-1} \mod r$$

then the pairing is non-degenerate.
If it looks too good to be true, . . .

- \( r \mid \Phi_k(q) \), so could try \( \lambda = \Phi_k(q) \), then \( c_i \) tiny and pairing \( a_{[c_0, \ldots, c_i]} \) 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)

\[
L := \begin{pmatrix}
  r & 0 & 0 & \cdots & 0 \\
-\varrho & 1 & 0 & \cdots & 0 \\
-\varrho^2 & 0 & 1 & \cdots & 0 \\
\vdots & \vdots & \ddots & \ddots & \vdots \\
-\varrho^{\varphi(k)-1} & 0 & \cdots & 0 & 1
\end{pmatrix}.
\]

- 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 \( \| V \|_\infty = \max_i |v_i| \)
Automagical construction

- The shortest vector $V$ in $L$ satisfies
  $$\| V \|_\infty \geq \frac{r^{1/\varphi(k)}}{\varphi(k)}$$

- Idea of proof: consider number field $\mathbb{Q}[\xi_k] \cong \mathbb{Q}[x]/\Phi_k(x)$
- Prime ideal: $p = (r, \xi_k - q)$
- Short vectors in $L$ give elements in $p$ of small norm
- But norm of the ideal is $r$ so
  $$r \leq |\text{No}(\sum_{i=0}^{\varphi(k)-1} v_i \xi_k^i)| = |\text{Res}(V(x), \Phi_k(x))|$$
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 $a_{[c_0, \ldots, c_l]}$ can be computed as
  \[
  (f_{6x+2}, Q(P) \cdot I_{Q_3} - Q_2(P) \cdot I_{-Q_2+Q_3}, Q_1(P) \cdot I_{Q_1-Q_2+Q_3}, [6x+2]Q)^{(q^k-1)/r}
  \]
  where $Q_i = Q^{q^i}$ for $i = 1, 2, 3$. 

Frederik Vercauteren  
Realization of Fast Pairings II
Questions?