Optimal Ate Pairings

Fré Vercauteren

25 April 2008 - Rennes

Pairings

- Let G_1, G_2, G_T be groups of prime order r. 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, ...

Creating “new” pairings

- Given G_1, G_2, G_T a pairing e is completely determined by (P, Q, z) with

$$e(P, Q) = z \quad \text{and } G_1 = \langle P \rangle, G_2 = \langle Q \rangle$$

- 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

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 $\mathcal{O} \in E(\mathbb{F}_q)$ 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

- $E[r]$ subgroup of points of order dividing r, i.e.

$$E[r] = \{P \in E(\overline{\mathbb{F}}_q) \mid rP = \mathcal{O}\}$$

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

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 $E[r]$: 1 and q since $r \mid \#E(\mathbb{F}_q)$
- For $k > 1$ have $q \neq 1 \bmod r$, thus decomposition of $E[r]$ into Frobenius eigenspaces:

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

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

Recap of setup

- Elliptic curve $E/\mathbb{F}_q$ with $r | \#E(\mathbb{F}_q)$
- Security parameter k with $(q^k - 1) \equiv 0 \bmod r$

$$\Rightarrow r \mid \Phi_k(q)$$

- Nice basis of $E(\mathbb{F}_{q^k})[r]$ consisting of φ-eigenspaces

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

with $\varphi(P) = P$ and $\varphi(Q) = qQ$

Functions and divisors

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

$$(f) = \sum_{P \in E(\overline{\mathbb{F}}_q)} \mathrm{ord}_P(f)(P)$$

  where $\mathrm{ord}_P(f)$ denotes the order of vanishing of f at P
- 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 $\deg(D) = 0$ and $g = cf$ for $c \in \mathbb{F}_q^\times$, then $f(D) = g(D)$.

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

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

- $f_{n,P}$ 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 $\mathcal{O}$ of order $(n-1)$.
- For every point $Q \neq P, [n]P, \mathcal{O}$, we have $f_{n,P}(Q) \in \mathbb{F}_q^\times$.

Tate pairing

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

$$(f_{r,P}) = r(P) - r(\mathcal{O})$$

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

$$\boxed{\langle P, Q\rangle_r = f_{r,P}(Q)}$$

- Domain and image:

$$\langle \cdot, \cdot \rangle_r : E(\mathbb{F}_{q^k})[r] \times E(\mathbb{F}_{q^k})/rE(\mathbb{F}_{q^k}) \rightarrow \mathbb{F}_{q^k}^{\times}/(\mathbb{F}_{q^k}^{\times})^r$$

- Reduced Tate pairing: $t(P, Q) = \langle P, Q\rangle_r^{(q^k-1)/r}$

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 $[n+m]P$
- Evaluate at Q in every step

Computing Tate pairing

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

Ate pairing

- Power of Tate pairing defined on $G_2 \times G_1$, but evaluates smaller Miller function
- Idea: consider power of Tate

$$t(Q,P)^m = f_{r,Q}(P)^{m(q^k-1)/r} = f_{mr,Q}(P)^{(q^k-1)/r}$$

- Follows from

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

- If $r \nmid m$, then $f_{mr,Q}(P)$ also defines non-degenerate pairing
- Ate: specific multiple of r and simplification of function

Ate pairing

- Fix any $\lambda \equiv q \bmod r$, then $r \mid (\lambda^k - 1)$, since $r \mid (q^k - 1)$.
- Define $m = (\lambda^k - 1)/r$, then $f_{\lambda^k - 1, Q} = f_{\lambda^k, Q}$
- Using $[\lambda^i]Q = [q^i]Q$ gives

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

- Since $\varphi(P) = P$ and $\varphi(Q) = [q]Q$ we get

$$f_{\lambda^k, Q}(P) = f_{\lambda, Q}(P)^{\sum_{i=0}^{k-1} \lambda^{k-1-i} q^i}$$

- Thus: $f_{\lambda, Q}(P)$ defines a non-degenerate pairing if $r \nmid m$

Ate pairing

- Minimal size of λ: have $\Phi_k(q) \equiv 0 \bmod r$ and $\lambda \equiv q \bmod r$
- Thus: $\Phi_k(\lambda) \equiv 0 \bmod r$, so λ at least $r^{1/\varphi(k)}$
- Recall: $r | q + 1 - t$, so can always take $\lambda = t - 1$
- Similar reasoning works for $\lambda_i \equiv q^i \bmod r$
- Ate pairings: $f_{\lambda_i, Q}(P)$ with $\lambda_i \equiv q^i \bmod r$ for some i
- In several cases, one root of $\Phi_k(x) \bmod r$ has size $r^{1/\varphi(k)}$
- Question: can this bound always be achieved?

Optimal pairing

- 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 $f_{\lambda,Q}(P)$
- For some families of elliptic curves, Ate is already optimal
- Main idea: products and fractions of pairings are also pairings

Generating more pairings

- Let $\lambda = mr = \sum_{i=0}^{l} c_i q^i$ with small coefficients c_i
- Expand f_λ and divide out powers of Ate pairings

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

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

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

- If

$$mkq^{k-1} \not\equiv ((q^k - 1)/r) \cdot \sum_{i=0}^{l} i c_i q^{i-1} \bmod r\,,$$

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 $a_{[c_0,\ldots,c_l]}$ extremely efficient
- But: pairing will be degenerate!
- Should only consider λ of the form

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

Automagical construction

- The best multiple λ can be obtained as short vectors in

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

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

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

where $\parallel V \parallel_\infty = \max_i |v_i|$.

Lower bound on shortest vector

- The shortest vector V in L satisfies

$$\|V\|_2 \geq \frac{r^{1/\varphi(k)}}{\|\Phi_k\|_2} \quad \text{and} \quad \|V\|_\infty \geq \frac{r^{1/\varphi(k)}}{\varphi(k)}$$

- Idea of proof: consider number field $\mathbb{Q}[\xi_k] \simeq \mathbb{Q}[x]/\Phi_k(x)$
- Prime ideal: $\mathfrak{p} = (r, \xi_k - q)$
- Short vectors in L give elements in $\mathfrak{p}$ of small norm
- But norm of the ideal is r so

$$r \leq |\mathrm{No}(\sum_{i=0}^{\varphi(k)-1} v_i \xi_k^i)| = |\mathrm{Res}(V(x), \Phi_k(x))| \,.$$

An example

- BN-curves have $k = 12$ 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 are

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

- Short vectors with minimal number of coefficients of size x

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

Conclusion

- New construction for Ate pairings
- Automagically finds best set of parameters
- Lower bound on what is possible
- For all parametrised families of curves obtain optimal pairing