Aspects of Pairing Inversion

Steven Galbraith, Florian Hess & Fré Vercauteren

ECC 2007 - Dublin

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:
  - $e(P_1 + P_2, Q) = e(P_1, Q)e(P_2, Q)$,
  - $e(P, Q_1 + Q_2) = e(P, Q)e(P, Q_2)$.
- Non-degenerate:
  - for all $P \neq 0$: $\exists x \in G_2$ such that $e(P, x) \neq 1$
  - for all $Q \neq 0$: $\exists x \in G_1$ such that $e(x, Q) \neq 1$
- 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.

Isomorphisms via pairings

- Since G_1, G_2, G_T have prime order r, they're isomorphic.
- Pairing with first argument fixed, gives isomorphism between G_2 and G_T:

$$\phi_2 : G_2 \to G_T : Q \mapsto \phi_2(Q) = e(P, Q)$$

- Pairing with second argument fixed, gives isomorphism between G_1 and G_T:

$$\phi_1 : G_1 \to G_T : P \mapsto \phi_1(P) = e(P, Q)$$

- Generates all isomorphisms between G_i and G_T, without need to compute DLOGs.

DLP, CDH & DDH

Let $G, +$ be a group of prime order r.

- DLP: Given a tuple (P, aP) compute a.
- CDH: Given a triple (P, aP, bP) compute abP.
- DDH: Given a quadruple (P, aP, bP, cP) decide if $abP = cP$.

Pairings in cryptography

- Exploit bilinearity!
- MOV: DLP reduction from G_1 to G_T: DLP in$G_1 : (P, xP)$

$$\Rightarrow \text{DLP in } G_T : (\phi_1(P), \phi_1(xP)) = (e(P,Q), e(xP,Q))$$

- Decision DH in G_1: DDH $: (P, aP, bP, cP)$

$$\text{test if } e(cP,Q) = e(aP,bQ)$$

  but how get bQ? Possible if computable isomorphism $\psi_1 : G_1 \to G_2$ with $\psi_1(P) = Q$.
- Identity based crypto, short signatures, ...

Pairing inversion problems

- **Fixed Argument Pairing Inversion 1 (FAPI-1)** problem: Given $P \in G_1$ and $z \in G_T$, compute $Q \in G_2$ such that $e(P, Q) = z$.
- **Fixed Argument Pairing Inversion 2 (FAPI-2)** problem: Given $Q \in G_2$ and $z \in G_T$, compute $P \in G_1$ such that $e(P, Q) = z$.
- **Generalised Pairing Inversion (GPI)**: Given $z \in G_T$, find $P \in G_1$ and $Q \in G_2$ with $e(P, Q) = z$.

FAPI's and CDH

Generalisation of Verheul's result:

- $e : G_1 \times G_2 \rightarrow G_T$ is non-degenerate bilinear pairing on cyclic groups of prime order r.
- Suppose one can solve FAPI-1 **and** FAPI-2 in polynomial time.
- Then one can solve CDH in G_1, G_2 and G_T in polynomial time.

FAPI's and CDH

Proof for G_1: O_i is FAPI-i oracle.

- Let (P, aP, bP) be a CDH input in G_1.
- Choose random $Q \in G_2$ and compute $z = e(aP, Q)$.
- Call $O_1(P, z)$ to get aQ.
- Now compute $z' = e(bP, aQ)$ and call $O_2(Q, z')$ to get abP.

FAPI's and isomorphisms

- If one can solve FAPI-1 in polynomial time
- then one can compute all group isomorphisms $\psi_1 : G_1 \to G_2$ in polynomial time.
- Let $P \in G_1$ and $Q \in G_2$ be generators, then can compute ψ_1 such that $\psi_1(P) = Q$.
- Similar result holds for FAPI-2.

FAPI's and DDH

- If one can solve FAPI-1 in polynomial time
- then one can solve DDH in G_1 in polynomial time.
- Proof: Let (P, aP, bP, cP) be DDH quadruple. Want to test if $e(cP, Q) = e(bP, aQ)$? How to get aQ?
- Choose $Q \in G_2$ and let $\psi_1 : G_1 \to G_2$ be such that $\psi_1(P) = Q$. Compute $aQ = \psi_1(aP)$.

Pairing inversion and BDH

- **Bilinear-Diffie-Hellman problem (BDH-1)** is: given $P, aP, bP \in G_1$ and $Q \in G_2$ to compute $e(P, Q)^{ab}$.
- If one can solve FAPI-1 in polynomial time
- then one can solve BDH-1 in polynomial time.
- Proof: Let (P, aP, bP, Q) be BDH-1 quadruple.
- Let $\psi_1 : G_1 \to G_2$ be such that $\psi_1(P) = Q$. Compute $aQ = \psi_1(aP)$ and obtain $z = e(bP, aQ) = e(P, Q)^{ab}$.
- No implications for finite field crypto?

Notation

- 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 for all $k \geq 1$.
- Hasse-Weil: number of points in $E(\mathbb{F}_q)$ is $q + 1 - t$ with

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

- t is called trace of Frobenius.

Torsion subgroups

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

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

- 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 $E(\mathbb{F}_{q^k})[r] = E[r]$.

Trace and embedding degree

- Recall $r \mid \#E(\mathbb{F}_q)$ and $\#E(\mathbb{F}_q) = q + 1 - t$
- So $q \equiv t - 1 \bmod r$.
- Since $x^k - 1 = \prod_{d|k} \Phi_d(x)$, have $r | \Phi_k(q)$.
- Conclusion: $r | \Phi_k(t-1)$, so $|\Phi_k(t-1)| \geq r$.
- $|t|$ can be as small as $r^{1/\varphi(k)}$, but not smaller.

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 $G_2 = \langle Q \rangle$

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 $f_{n,P}(Q) \in \mathbb{F}_q^\times$.

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

Tate pairing

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

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

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

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

- Domain and image are:

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

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

Ate pairing

- Non-degenerate pairing defined on $G_2 \times G_1$ only.
- Let S be integer with $S \equiv q \mod r$ and $N = \gcd(S^k - 1, q^k - 1)$
- Let $c_S = \sum_{i=0}^{k-1} S^{k-1-i} q^i \bmod N$. Then

$$a_S : G_2 \times G_1 \to \mu_r, \quad (Q, P) \mapsto f_{S,Q}^{\mathrm{norm}}(P)^{c_S(q^k-1)/N}$$

  defines a bilinear pairing,
- Typical choices for S are:
  - $S = t - 1$ with t trace of Frobenius.
  - $S = q$, then no final exponentiation necessary.
- In general $t - 1 \simeq \sqrt{q}$, but could be as small as $r^{1/\varphi(k)}$.

Pairing Zoo

Pairing	Domain	Where	Who	s	Red
Tate	$E[r] \times E/rE$	All HECs	Miller	r	No
eta	$G_1 \times G_2$	SuSi	BGOS	$t-1$	No
ate EC	$G_2 \times G_1$	All ECs	HSV	$t-1$	No
ate EC	$G_1 \times G_2$	SuSi	HSV	$t-1$	No
ate HEC	$G_2 \times G_1$	All HECs	GHOTV	q	Yes
ate HEC	$G_1 \times G_2$	SuSp	GHOTV	q	Yes

Extreme elliptic ate

- Curves with $t = -1$ give shortest loop in Miller's algorithm.
- Let $E : y^2 = x^3 + 4$ over $\mathbb{F}_p$ with $p = 4176171311231184 5269$, then $t = -1$, $r = 715827883$, $k = 31$ and $D = -3$.
- Let $y - \lambda(Q)x - \nu(Q)$ with $\lambda = 3x_Q^2/(2y_Q)$ and $\nu = (-x_Q^3 + 8)/(2y_Q)$ be the tangent at Q.
- The function

$$(Q, P) \mapsto \left(y_P - \lambda(Q)x_P - \nu(Q)\right)^{(q^k-1)/(3r)}$$

defines a non-degenerate pairing on $G_2 \times G_1$.

Extreme elliptic ate: corollary

- Since

$$(Q, P) \mapsto (y_P - \lambda(Q)x_P - \nu(Q))^{(q^k-1)/(3r)}$$

  defines a non-degenerate pairing on $G_2 \times G_1$
- we have corollary that for all $P \in G_1$ and $Q \in G_2$ the expressions

$$\frac{(y_P - \lambda(Q)x_P - \nu(Q))^2}{(y_{[2]P} - \lambda(Q)x_{[2]P} - \nu(Q))} \quad \text{and} \quad \frac{(y_P - \lambda(Q)x_P - \nu(Q))^2}{(y_P - \lambda([2]Q)x_P - \nu([2]Q))}$$

  are $3r$-th powers.

Miller inversion

- Most pairings can be expressed as

$$e(P, Q) := f_{s,P}(Q)^d$$

  for integers s and d and $f_{s,P}$ a Miller function.
- Possible approach: find correct d-th root first and then solve for Q in $f_{s,P}(Q)$
- **Miller inversion**: Let P be fixed, let S be a set of points and take $z \in \mathbb{F}_{q^k}^*$. Compute a point $Q \in S$ such that $z = f_{s,P}(Q)$ or if no such point exists then output 'no solution'.

Miller inversion in polytime

- Setting: Ate pairing on $G_2 \times G_1$.
- Let $S \geq 2$ and Q have order > 2. Then $f_{s,Q}(x, y)$ can be written as

$$f_{s,Q}(x, y) = \frac{f_1(x) + yf_2(x)}{(x - x_{[s]Q})}$$

with $\deg f_1(x) \leq (S + 1)/2$ and $\deg f_2(x) \leq S/2 - 1$.

- Miller inversion is equivalent with finding root of

$$P(x) := (f_1(x) - z(x - x_{[s]Q}))^2 - f_2(x)^2(x^3 + ax + b)$$

of degree at most $S + 1$.

- Note: polynomial defined over $\mathbb{F}_{q^k}$, but root over $\mathbb{F}_q$.

Miller inversion in polytime

- Finding root of $P(x) \in \mathbb{F}_{q^k}[x]$ in $\mathbb{F}_q$ is computing $\gcd(x^q - x, P(x))$.
- Takes $O(|t|^2 \log q)$ operations in $\mathbb{F}_{q^k}$ or $O(|t|^2 k^2 (\log q)^3)$ bit-operations.
- If $|t|$ and k grow as a polynomial function of $\log r$, one can solve MI in polynomial time.
- Lemma: There exist families of parameters of pairing friendly curves for which the Miller inversion problem can be solved in polynomial time.

FAPI-1 for ate pairing on small trace curves

- Recall extreme elliptic ate pairing

$$a_2(Q,P) \mapsto \left(y_P - \lambda(Q)x_P - \nu(Q)\right)^{(q^k-1)/(3r)}$$

- Problem: given $Q = (x_Q, y_Q)$ and a target $z \in \mu_r \subseteq \mathbb{F}_{q^k}^*$, need to solve

$$(y - \lambda(Q)x - \nu(Q))^{(q^k-1)/(3r)} = z$$

for some $(x, y) \in E(\mathbb{F}_q)$.

FAPI-1 for ate pairing on small trace curves

- But: there are $d = (q^k - 1)/(3r)$ possible roots of z.
- Only one of them of form $y - \lambda x - \nu$ for some $(x, y) \in E(\mathbb{F}_q)$.
- Easy to compute random d-th roots of z, but hard to select the correct root.
- Can generate many more equations by $a_2(uQ, P) = z^u$.
- Simpler problem: given many pairs $(a, z) \in \mathbb{F}_{q^k}^2$, with $z = (a + x)^d$ for some $x \in \mathbb{F}_q$, find x.
- Easy when $d \nmid (q^k - 1)$, but how hard for $d \mid (q^k - 1)$?

FAPI-1 $\leq_P$ MI

- Is solving MI sufficient to solve FAPI-1?
- Most people: no, since given $z_0 = f_{s,P}(Q)^d$, still need to try out all d possible roots.
- Idea: what if you take a random d-th root?
- Tate-Lichtenbaum pairing:

$$t(\cdot,\cdot) : E(\mathbb{F}_q)[r] \times E(\mathbb{F}_{q^k})/rE(\mathbb{F}_{q^k}) \longrightarrow \mathbb{F}_{q^k}^*/(\mathbb{F}_{q^k}^*)^r$$

- Reduced TL pairing into μ_r: $e(\cdot,\cdot) = t(\cdot,\cdot)^{(q^k-1)/r}$

FAPI-1 $\leq_P$ MI

- For $P \in E(\mathbb{F}_q)[r]$ let $S_2(P)$ denote set $\{Q \in E(\mathbb{F}_{q^k})\}$ with

$$e(P, Q) = 1$$

- Suppose $e(P, Q_1) = e(P, Q_2)$, then clearly

$$Q_3 := Q_1 - Q_2 \in S_2(P)$$

- If $\#S_2(P)$ is big enough, then likely that there exists $Q' \in E(\mathbb{F}_{q^k})$ with $Q' := Q + R$ with $R \in S_2(P)$ and

$$f_{s,P}(Q') = z$$

for a random root z of z_0.

FAPI-1 $\leq_P$ MI

- TL pairing: already have $rE(\mathbb{F}_{q^k}) \subset S_2(P)$, but this only gives q^k/r^2 points.
- For $k > 1$, also have $E(\mathbb{F}_{q^e}) \subset S_2(P)$ for all $e|k$.
- At least have that $E(\mathbb{F}_q)[r] \subset S_2(P)$.
- Since $r \| E(\mathbb{F}_q)$, $E(\mathbb{F}_q)[r] \cap rE(\mathbb{F}_{q^k}) = \{O\}$ and thus

$$|S_2(P)| \geq |E(\mathbb{F}_q)[r]||rE(\mathbb{F}_{q^k})| \approx rq^k/r^2 \approx d.$$

- Suggests that for the TL pairing with $k > 1$, FAPI-1 $\leq_P$ MI.
- Above fails for ate pairing since only defined on $G_2 \times G_1$.

A degree bound

- Ate pairing gave isomorphism of G_1 with μ_r of the form
$$f_{s,Q}(\cdot)^d$$
with $f_{s,Q}$ function of low degree.
- However: total degree of $f_{s,Q}(\cdot)^d$ still very high.
- Lemma: Let E be an elliptic curve and $f \in \mathbb{F}_{q^k}(E)$. Assume that $Q \mapsto f(Q)^d$ defines a non-constant homomorphism $G_2 \to \mu_r$ for some positive exponent d. Then $d \deg(f) \geq (1/6)\#G_2$.

Conclusions

- FAPI's and implications for crypto.
- MI can be easy.
- Extreme elliptic ate leads to new supposedly hard problem?
- For TL pairing have FAPI-1 $\leq_P$ MI.
- No homomorphisms of low degree into μ_r.
- Inverting pairings still hard . . .