Pairings and DLP-III

Tanja Lange
Technische Universiteit Eindhoven

Pairings

Let $(G_1, +), (G_1', +)$ and $(G_T, \cdot)$ be groups of prime order ℓ and let

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

be a map satisfying

$e(P + Q, R') = e(P, R')e(Q, R'),$
$e(P, R' + S') = e(P, R')e(P, S').$

Request further that e is non-degenerate in the first argument, i.e., if for some P $e(P, R') = 1$ for all $R' \in G_1'$, then P is the identity in G_1

Such an e is called a *bilinear map* or *pairing*.

Consequences of pairings

Assume that $G_1 = G_1'$,
in particular $e(P, P) \neq 1$.

Then for all triples
$(aP, bP, cP) \in \langle P \rangle^3$
one can decide in time
polynomial in $\log \ell$ whether
$c = \log_P(cP) = \log_P(aP) \log_P(bP) = ab$
by comparing
$e(aP, bP) \; = \; e(P,)^{ab}$ and
$e(P, cP) = e(P,)^c$.

This means that the decisional
Diffie-Hellman problem is easy.

The DL system G_1 is at most as secure as the system G_T.

Even if $G_1 \neq G_1'$ one can
transfer the DLP in G_1
to a DLP in G_T,
provided one can find an element
$P' \in G_1'$ such that the map
$P \rightarrow e(P, P')$ is injective.
This is easy
if G_1' can be sampled.

Pairings are interesting attack tool if DLP in G_T is easier to solve; e.g. if G_T has index calculus attacks.

We want to define pairings
$G_1 \times G_1' \to G_T$
preserving the group structure.

The pairings map from
an elliptic curve $G_1 \subset E/\mathbf{F}_q$
to the multiplicative group of a
finite extension field $\mathbf{F}_{q^k}$.

To embed the points of order ℓ
into $\mathbf{F}_{q^k}$ there need to be ℓ-th
roots of unity are in $\mathbf{F}_{q^k}^*$.

The *embedding degree* k satisfies
k is minimal with $\ell \mid q^k - 1$.

E is supersingular if
$E[p^s](\overline{\mathbf{F}}_q) = \{P_\infty\}$.
$t \equiv 0 \bmod p$.
Endomorphism ring of E
is order in quaternion algebra.

Otherwise it is ordinary and one
has $E[p^s](\overline{\mathbf{F}}_q) = \mathbf{Z}/p^s\mathbf{Z}$.
These statements hold for all s if
they hold for one.

Example:
$y^2 + y = x^3 + a_4 x + a_6$ over $\mathbf{F}_{2^r}$
is supersingular, as a point of
order 2 would satisfy $y_P = y_P + 1$
which is impossible.

Embedding degrees

Let $E/\mathbf{F}_p$ be supersingular and $p \geq 5$, i.e $p > 2\sqrt{p}$.

Hasse's Theorem states
$|t| \leq 2\sqrt{p}$.
E supersingular implies
$t \equiv 0 \bmod p$, so $t = 0$ and
$|E(\mathbf{F}_p)| = p + 1$.

Obviously
$(p+1) \mid p^2 - 1 = (p+1)(p-1)$
so $k \leq 2$ for supersingular curves over prime fields.

Distortion maps

For supersingular curves there exist homomorphisms
$\phi : E(\mathbf{F}_q) \to E(\mathbf{F}_{q^k})$
so that $e(P, \phi(P)) = \tilde{e}(P, P) \neq 1$
for $P \neq \infty$.
Such a map is called a *distortion map*.

These maps are convenient for protocol design because they give a pairing
$\tilde{e} : G_1 \times G_1 \to G_T$
for $\tilde{e}(P, P) = e(P, \phi(P))$.

Examples:

1. $y^2 = x^3 + x$,

for $p \equiv 3 \pmod 4$.

Distortion map

$(x, y) \mapsto (-x, \sqrt{-1}y)$.

2. $y^2 = x^3 + a_6$,

for $p \equiv 2 \pmod 3$.

Distortion map $(x, y) \mapsto (jx, y)$

with $j^3 = 1, j \neq 1$.

In both cases,

$\#E(\mathbf{F}_p) = p + 1$.

$p = 1000003 \equiv 3 \bmod 4$ and
$y^2 = x^3 - x$ over $\mathbf{F}_p$.
Has $1000004 = p + 1$ points.
$P = (101384, 614510)$ is a point of order 500002.
$nP = (670366, 740819)$.
Construct $\mathbf{F}_{p^2}$ as $\mathbf{F}_p(i)$.
$\phi(P) = (898619, 614510i)$.

Invoke computer algebra and compute
$e(P, \phi(P)) = 387265 + 276048i$;
$e(Q, \phi(P)) = 609466 + 807033i$.
Solve DLP in $\mathbf{F}_p(i)$
to get $n = 78654$.
(Btw. this is the clock).

Summary of pairings

Menezes, Okamoto, and Vanstone for E supersingular:
For $p = 2$ have $k \leq 4$.
For $p = 3$ we $k \leq 6$
Over $\mathbf{F}_p$, $p \geq 5$ have $k \leq 2$.
These bounds are attained.

Not only supersingular curves:
MNT curves are non-supersingular curves with small k.
Other examples constructed for pairing-based cryptography –
but small k unlikely to occur for random curve.

Index calculus in prime fields

Index calculus is a method to compute discrete logarithms. Works in many situations but depends on group (not generic attack)

p prime, elements of $\mathbf{F}_p$ represented by numbers in $\{0, 1, \ldots, p-1\}$;
g generator of multiplicative group.

If $h \in \mathbf{F}_p$ factors as
$h = h_1 \cdot h_2 \cdots h_n$ then

$$h = g^{a_1} \cdot g^{a_2} \cdots g^{a_n}$$
$$= g^{a_1 + a_2 + \ldots + a_n},$$

with $h_i = g^{a_i}$.

Knowledge of the a_i,
i.e., of the discrete logarithms of
h_i to base g,
gives knowledge of the discrete
logarithm of h to base g.

If h factors appropriately . . .

If h factors appropriately?!

Ensure by finding h' with known DL s.t. $h \cdot h'$ factors over the h_i. So far: instead of finding *one* DL we have to find *many* DLs *and* they have to fit to h *and* we have to find a suitable h' *and* factor numbers.

Two different settings –
the integers modulo p and
the integers themselves.
Factorization takes place over **Z**, while the left hand side is reduced modulo p.

Select $F = \{g_1, g_2, \ldots, g_m\}$
so that $\bar{h} < p$ is likely to factor
into powers of g_i.
F called *factor base*.

An equation of form
$\bar{h} = g_1^{n_1} \cdot g_2^{n_2} \cdots g_m^{n_m}$,
with $n_i \in \mathbf{Z}$ is called a *relation*.
Choose F as small primes , e.g.
$g_1 = 2, g_2 = 3, g_3 = 5, \ldots$

Generate many relations with
known DL of $\tilde{h}_j = g^{k_j}$
$\tilde{h}_j = g^{k_j} = g_1^{n_{j1}} \cdot g_2^{n_{j2}} \cdots g_m^{n_{jm}}$.
(This means discarding
g^{k_j} if it does not factor .)

Matrix of relations

For each relation
$\tilde{h}_j = g^{k_j} = g_1^{n_{j1}} \cdot g_2^{n_{j2}} \cdots g_m^{n_{jm}}$

enter the row

$$(n_{j1} n_{j2} \ldots n_{jm} | k_j)$$

into a matrix $M =$

$$\begin{pmatrix} n_{11} & \ldots & n_{1i} & \ldots & n_{m1} & k_1 \\ n_{21} & \ldots & n_{2i} & \ldots & n_{m2} & k_2 \\ \vdots & & \vdots & & \vdots & \vdots \\ n_{l1} & \ldots & n_{li} & \ldots & n_{lm} & k_l \end{pmatrix}$$

The i-th column

corresponds to the unknown a_i

so that $g_i = g^{a_i}$.

Computing DLPs

Use linear algebra to solve for a_is.
This step does not depend on the target DLP $h = g^a$.
A single relation $h \cdot g^k$ factoring over F gives the DLP.

Running time (with much more clever way of finding relations) $O(\exp(c \log p^{1/3} \log(\log p)^{2/3}))$ for some c.
This is subexponential in $\log p$!
Notation: write this complexity as $L(1/3, c)$.

Similar for $\mathbf{F}_{2^n}$

Elements of $\mathbf{F}_{2^n}$ are represented as $\mathbf{F}_{2^n} = \{\sum_{i=0}^{n-1} c_i x^i | c_i \in \mathbf{F}_2, 0 \le i < n\}$, i.e. polynomials of degree less than n modulo an irreducible polynomial $f(x) \in \mathbf{F}_2[x]$.

Factoring into powers of small primes is replaced by factoring into irreducible polynomials of small degree.

Same approach works for all finite fields $\mathbf{F}_{p^n}$ in $O(\exp(c' \log p^{1/3} \log(\log p)^{2/3}))$. Smaller p have smaller constant c.

Same approach works for all finite fields $\mathbf{F}_{p^n}$ in $O(\exp(c' \log p^{1/3} \log(\log p)^{2/3}))$.
Smaller p have smaller constant c.

If DLP in $\mathbf{F}_{q^k}^*$ is weak can break pairing system in target group $G_T \subset \mathbf{F}_{q^k}^*$.
Big computation in 2011: Hayashi, Shinohara, Shimoyama, and Takagi solved DLP in $\mathbf{F}_{3^{6 \cdot 97}}^*$
This field was considered as target field for pairings over supersingular curves $E/\mathbf{F}_{3^{97}}$ with embedding degree 6.

More recent development

Flurry of papers with breathtaking improvements and new records by Joux and by Göloglu, Granger, McGuire, and Zumbrägel (GGMZ)

Joux 2012-12-24, 1175-bit and 1425-bit

Joux 2013-02-11 $\mathbf{F}^*_{2^{1778}}$

GGMZ 2013-02-19 $\mathbf{F}^*_{2^{1971}}$

Joux 2013-03-22 $\mathbf{F}^*_{2^{4080}}$

GGMZ 2013-04-11 $\mathbf{F}^*_{2^{6120}}$

Joux 2013-05-21 $\mathbf{F}^*_{2^{6168}}$

Do not use supersingular curves for pairings!

Most recent

Barbulescu, Gaudry, Joux, Thomé
2013-06-18
Quasi-polynomial time algorithm
to compute DLs in $\mathbf{F}_{p^n}^*$.
Strongly depends on p, so only
efficient for small p.
Best speeds for composite n.

Also interesting
Joux 2013-02-20 $L(1/4 + o(1), c)$

Summary of other attacks

Definition of embedding degree does not cover all attacks.
For $\mathbf{F}_{p^n}$ watch out that pairing can map to $\mathbf{F}_{p^{km}}$ with $m < n$.
Watch out for this when selecting curves over $\mathbf{F}_{p^n}$!

Anomalous curves:
If $E/\mathbf{F}_p$ has $\#E(\mathbf{F}_p) = p$ then transfer $E(\mathbf{F}_p)$ to $(\mathbf{F}_p, +)$.
Very easy DLP.
Not a problem for Koblitz curves, attack applies to order-p subgroup.

Weil descent:

Maps DLP in E over $\mathbf{F}_{p^{mn}}$
to DLP on variety J over $\mathbf{F}_{p^n}$.
J has larger dimension; elements represented as polynomials of low degree. $\Rightarrow$ index calculus.

This is efficient if dimension of J is not too big.

Particularly nice to compute with J if it is the Jacobian of a hyperelliptic curve C.
For genus g get complexity $\tilde{O}(p^{2-\frac{2}{g+1}})$ with the factor base described before, since polynomials have degree $\leq g$.