Supersingular curves and the Tate pairing

Steven Galbraith

Royal Holloway University of London

http://www.isg.rhul.ac.uk/~sdg/

Includes joint work with David Soldera and Keith Harrison; thanks to Hewlett-Packard Laboratories for support.

A Magic Box

$$E(\mathbb{F}_q) \qquad\qquad\qquad\qquad\qquad\qquad \mathbb{F}^*_{q^k}$$

$$P_1 = (x_1, y_1) \quad \longrightarrow$$

$$\longrightarrow \quad \alpha = e(P_1, P_2)$$

$$P_2 = (x_2, y_2) \quad \longrightarrow$$

Main properties of pairings

Bilinear:

$$e([n]P_1, P_2) = e(P_1, [n]P_2) = e(P_1, P_2)^n$$

Non-degenerate:

$$e(P, P) \neq 1$$

Such maps can be obtained from the Weil and Tate pairings.

History of pairings in cryptography

- Miller (1986)
- Menezes-Okamoto-Vanstone (MOV) (1993)
- Frey-Rück (1994)
- Mitsunari-Sakai-Kasahara (1999)
- Sakai-Oghishi-Kasahara (2000)
- Joux (2000)
- Verheul (2001)
- Boneh-Franklin (2001)
- Joux-Nguyen (2001)
- Many people (2001,2002)

The MOV/Frey-Rück attack on ECDLP

Let $P \in E(\mathbb{F}_q)$ be of order l.

Suppose $Q = [\lambda]P$ for some (unknown) λ.

The MOV/Frey-Rück attack:

- Construct the field $K = \mathbb{F}_{q^k}$.
- Find a point S such that $e(P, S) \neq 1$.
- Compute $\zeta_1 = e(P, S)$ and $\zeta_2 = e(Q, S)$. Note that

$$\zeta_2 = e([\lambda]P, S) = e(P, S)^\lambda = \zeta_1^\lambda.$$

- Solve the discrete logarithm problem in K^* using an index calculus method.

This strategy is effective when $K = \mathbb{F}_{q^k}$ is not too large an extension of $\mathbb{F}_q$.

Supersingular curves are weak for cryptography

Elliptic curves for which k is 'small' are weak for discrete-logarithm-based cryptography.

Theorem: (Menezes, Okamoto and Vanstone) Supersingular elliptic curves have $k \leq 6$.

Hence supersingular curves are considered weak for cryptography.

Even weaker case: Curves E over $\mathbb{F}_q$ with $q - 1$ points.

Three party Diffie-Hellman key exchange

Suppose $g \in \mathbb{F}_q^*$ and three users A, B and C want to agree a random key.

Natural generalisation of Diffie-Hellman key exchange:

1. User A chooses a random secret a and broadcasts g^a.

   Similarly, users B and C broadcast g^b and g^c.
2. User A receives g^b and g^c so computes and broadcasts g^{ab}, g^{ac}. Similarly for users B and C.
3. User A receives g^{bc} and so can compute the shared key g^{abc}. Similarly, users B and C can compute g^{abc}.

This protocol requires two rounds of broadcast messages.

Joux: Three party Diffie-Hellman key exchange

(Verheul version)

- User A chooses a random secret a and broadcasts $[a]P$.

  Similarly, users B and C broadcast $[b]P$ and $[c]P$.
- User A can compute

$$e([b]P, [c]P)^a = e(P, P)^{abc}.$$

  Users B and C can also compute $e(P, P)^{abc}$.

This only requires one round of broadcasts.

Note: Al-Riyami and Paterson show that to achieve authenticated key exchange with key confirmation then the methods of Joux give no improvement over traditional methods.

Security of tripartite key exchange

Eve sees $[a]P, [b]P$ and $[c]P$ and the key is

$$\alpha = e(P, P)^{abc}.$$

If Eve can solve the Diffie-Hellman problem in $E(\mathbb{F}_q)$ then she can compute $[ab]P$ and compute

$$\alpha = e([ab]P, [c]P).$$

If Eve can solve the Diffie-Hellman problem in $\mathbb{F}^*_{q^k}$ then she can also compute α.

For **security** need: $q > 2^{160}$ and $q^k > 2^{1024}$.

For **efficiency** want q^k not too large, so use supersingular curves.

Further applications of pairings in cryptography

- Separation of DDH and CDH (Joux-Nguyen)
- Identity-based encryption (Boneh-Franklin)
- Identity-based signatures (Hess, Cha-Cheon, Paterson)
- Identity-based key exchange (Sakai-Ohgishi-Kasahara, Smart)
- Credentials (Verheul)
- Short signatures (Boneh-Lynn-Shacham)
- Traitor tracing (Mitsunari-Sakai-Kasahara)
- Many more (see Paulo Barreto's pairing-based crypto lounge on the web)

How to make it practical?

For cryptographic applications we need:

1. To find suitable elliptic curves with reasonable parameter sizes.
2. To compute $e(P, Q)$ quickly.
3. To trust the security of the system.

The Tate pairing

Let l be a prime (coprime to q).

Define k such that $l|(q^k-1)$ and write $K = \mathbb{F}_{q^k}$.

Write $E(K)[l]$ for the points defined over K of order l.

The **Tate pairing** is a map

$$E(K)[l] \times (E(K)/lE(K)) \longrightarrow K^*/(K^*)^l.$$

For $S \in E(K)[l]$ and $T \in E(K)$ we write this value as

$$\langle S, T \rangle \in K^*/(K^*)^l.$$

To get a **unique** value we must raise to the power $(q^k - 1)/l$.

Non-rational endomorphisms

If $k > 1$ and $P \in E(\mathbb{F}_q)[l]$. Then

$$\langle P, P \rangle^{(q^k-1)/l} = 1.$$

Suppose there exists an endomorphism φ on E such that $\varphi(P) \notin E(\mathbb{F}_q)$. Then

$$\langle P, \varphi(P) \rangle^{(q^k-1)/l} \neq 1.$$

Such maps φ are called **distortion maps** or **non-rational endomorphisms**.

We define

$$e(P, Q) = \langle P, \varphi(Q) \rangle^{(q^k-1)/l}.$$

Suitable curves

Characteristic greater than three:

Original Boneh-Franklin description used an elliptic curve

$$E : y^2 = x^3 + 1$$

with $\#E(\mathbb{F}_p) = p + 1$ (i.e., $k = 2$).

There are also curves over $\mathbb{F}_{p^2}$ with $k = 3$.

Characteristic two

The elliptic curves

$$E_1 : y^2 + y = x^3 + x$$

and

$$E_2 : y^2 + y = x^3 + x + 1$$

over $\mathbb{F}_2$ have $k = 4$.

So can work over $\mathbb{F}_{2^m}$ with $m \approx 250$ (if there exists a suitable group order).

Characteristic three

The elliptic curves

$$E_1 : y^2 = x^3 - x + 1$$

and

$$E_2 : y^2 = x^3 - x - 1$$

over $\mathbb{F}_3$, have $k = 6$.

A convenient non-$\mathbb{F}_3$-rational endomorphism for E_1 is

$$\psi : (x, y) \longmapsto (\alpha - x, iy)$$

So can take $3^m \approx 2^{170}$ if a suitable group order exists.

Computing the Tate pairing

The Tate pairing is

$$\langle P, Q \rangle = f(D)$$

where f is a function such that

$$(f) = l((P) - (O_E))$$

and where $D \sim (Q) - (O_E)$.

This is computed using Miller's algorithm.

Miller's algorithm

To compute $\langle P, Q \rangle$:

Choose a random point $S \in E(\mathbb{F}_{q^k})$ and compute $Q' = Q + S \in E(\mathbb{F}_{q^k})$.

Set $n = \lfloor \log_2(l) \rfloor - 1$, $T_1 = P$, $f_1 = 1$.

While $n \geq 1$ do

- Calculate the equations of the straight lines l_1 and l_2 arising in a doubling of T_1. Set $T_1 = [2]T_1$ and

$$f_1 = f_1^2 \frac{l_1(Q')l_2(S)}{l_2(Q')l_1(S)}.$$

- If the nth bit of l is one then
  - Calculate the equations of the straight lines l_1 and l_2 arising in an addition of T_1 and P. Set $T_1 = T_1 + P$ and set

$$f_1 = f_1 \frac{l_1(Q')l_2(S)}{l_2(Q')l_1(S)}.$$

- Decrement n.

Return f_1.

Efficient Implementation

See:

- Galbraith, Harrison, Soldera (ANTS-V)
- Barreto, Kim, Lynn, Scott (CRYPTO '02)
- Eisentraeger, Lauter, Montgomery

We compute $\langle P, Q \rangle$ where

$$P \in E(\mathbb{F}_q) \qquad \text{and} \qquad Q \in E(\mathbb{F}_{q^k})$$

so optimise accordingly.

Further tricks:

- Work in a subgroup (if available).
- If the non-rational endomorphism is of the right form then all denominators in Miller's algorithm can be removed.
- Final exponentiation can be improved using Frobenius action.

Comment: Relationship between Tate pairing and Weil pairing.

Tripling in characteristic three

Suppose $P = (x_1, y_1)$ is a point on

$$E : y^2 = x^3 + a_4 x + a_6$$

with $a_4, a_6 \in \mathbb{F}_3$.

Then

$$[3](x_1, y_1) = (x_1^9 + a_6(1 - a_4), -y_1^9)$$

and so tripling requires no divisions!

Further details:
The tangent to E at P has slope $\lambda_2 = 1/y_1$ and the line between (x_1, y_1) and $[2](x_1, y_1)$ has slope $\lambda_3 = y_1^3 - \lambda_2$.

Hence, use a base three Miller algorithm in characteristic three (need one division to compute the straight line equations).

Low Hamming weight

$$\#E_1(\mathbb{F}_{3^{163}}) = N = 3^{163} - 3^{82} + 1 = 7l.$$

The prime l does not have low Hamming weight. So compute Tate pairing with respect to N. Ditto for final exponentiation to the power

$$((3^{163})^6 - 1)/N.$$

If P has order l then the result is an element of order l.

Lemma: Let $P \in E(\mathbb{F}_q)$ have order l, let D be a degree zero divisor on $E(K)$ and let N be a multiple of l which divides $(q^k - 1)/(q - 1)$. Suppose g and g' are functions over $\mathbb{F}_q$ such that $(g) = l(P) - l(O_E)$ and $(g') = N(P) - N(O_E)$. Then

$$g'(D)^{(q^k-1)/N} = g(D)^{(q^k-1)/l}.$$

Proof: Write $N = hl$. Then $g' = cg^h$ for some $c \in \mathbb{F}_q$. QED.

Timings

Milliseconds on a 1GHz Pentium III (code by HP Labs, Bristol)

	$\mathbb{F}_{2^{241}}$	$\mathbb{F}_{2^{271}}$	$\mathbb{F}_{3^{97}}$	$\mathbb{F}_{3^{163}}$
Tate	8.7	13	24	81
BF-Enc	14.3	21	36	127
BF-Dec	11.3	18	29	100

Security issues

Bilinear/Weil/Tate-Diffie-Hellman problem: Given P, Q, $P_1 = [a]P$ and $P_2 = [b]P$ such that $e(P, Q) \neq 1$, compute

$$e([ab]P, Q).$$

This is no harder than either the Diffie-Hellman problem in $E(\mathbb{F}_q)$ or the Diffie-Hellman problem in $\mathbb{F}_{q^k}$.

Theorem: (Verheul) Let $e : G \times G \to H$ be a pairing where

$$H \subset \mathbb{F}_{q^k}^*$$

is the image subgroup. If there is a computable group homomorphism from H to G then the Diffie-Hellman problem in G and H can be solved.

Bit security

For key exchange agree

$$\alpha = e(P, P)^{abc} \in \mathbb{F}^*_{q^k}$$

(1000 bits or more) and want to derive a short key.

Theorem: (Galbraith-Hopkins-Shparlinski) Suppose $\alpha \in \mathbb{F}^*_{p^2}$ and assume BDH is hard. Then the 128 most significant bits of the trace of α can be used to derive a secure key.

Future limitations

Parameters are convenient for current use: $k = 6$ allows 170-bit EC with 1020-bit finite fields.

In future we will require $k > 6$.

This cannot be achieved using supersingular elliptic curves directly.

Silverberg-Rubin

Theorem: Let E be a supersingular elliptic curve over $\mathbb{F}_q$ ($q = p^a$) with embedding degree k. Let r be coprime to $2pk$. Then there exists an abelian variety A over $\mathbb{F}_q$ of dimension $\varphi(r)$ and embedding degree rk. We have

$$A(\mathbb{F}_q) \cong \left\{ P \in E(\mathbb{F}_{q^r}) : \mathrm{Tr}_{\mathbb{F}_{q^r}/\mathbb{F}_{q^m}}(P) = 0_E \right\}$$

for all $m|r$ and $m \neq r$.

Application: Transmit $\varphi(r)$ coordinates of the x-coordinate of such a point $P \in E(\mathbb{F}_{q^r})$ (plus a few extra bits) and this determines the point in $A(\mathbb{F}_q)$.

Using ordinary (non-supersingular) curves

Problems:

- (Verheul) There are no non-rational endomorphisms in this case.

  Cryptosystems can be modified to handle this issue.
- (Balasubramanian-Koblitz) Such curves are very rare.

MNT conditions

Miyaji, Nakabayashi and Takano showed that ordinary elliptic curves E over $\mathbb{F}_q$ with $k = 6$ must have $q + 1 - t$ points where

$$q = 4l^2 + 1 \text{ and } t = 1 \pm 2l.$$

This leads to a CM method construction of such curves.

These methods have been generalised:

- Barreto-Lynn-Scott: Construct nice curves with $k = 12$.
- Dupont-Enge-Morain: Construct not so nice curves with arbitrary k.

Distortion maps

Joux: Suppose $P \in E(\mathbb{F}_q)$ is such that

$$\langle P, P \rangle^{(q^k-1)/l} = 1.$$

Take a non-rational isogeny $\varphi : E \to E'$ and consider

$$\langle \varphi(P), \varphi(P) \rangle.$$

Lemma (Galbraith):

$$\langle \varphi(P), \varphi(Q) \rangle = \langle P, Q \rangle^{\deg(\varphi)}.$$

Hence, Joux's idea does not work.