Implementing the Tate pairing

Steven Galbraith

Mathematics Department

Royal Holloway University of London, UK.

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

Joint with Keith Harrison and David Soldera

Hewlett-Packard Laboratories,

Bristol, UK.

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 Tate pairing (special case)

Let E be an elliptic curve over $\mathbb{F}_q$.

Let $l | \#E(\mathbb{F}_q)$ be a prime not equal to the characteristic of the field $\mathbb{F}_q$.

Define $K = \mathbb{F}_{q^k}$ to be the finite field extension of $\mathbb{F}_q$ obtained by adjoining the lth roots of unity to $\mathbb{F}_q$ (i.e., $k = \mathrm{ord}_l(q)$).

The **Tate pairing** is a function

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

For $P \in E(K)[l]$ and $Q \in E(K)$ we write this equivalence class representative as

$$\langle P, Q \rangle \in K^*/(K^*)^l.$$

Note that:

- $[K^* : (K^*)^l] = l$.
- $E(K)/lE(K)$ is a group of exponent l.

Some properties of the Tate pairing

1. (Bilinear) $\langle P_1 + P_2, Q\rangle \equiv \langle P_1, Q\rangle\langle P_2, Q\rangle$ and $\langle P, Q_1 + Q_2\rangle \equiv \langle P, Q_1\rangle\langle P, Q_2\rangle$.
   Hence $\langle [n]P, Q\rangle \equiv \langle P, [n]Q\rangle \equiv \langle P, Q\rangle^n$.
2. (Non-degenerate) If $\langle P, Q\rangle \in (K^*)^l$ for all $Q \in E(K)$ then $P = \mathcal{O}_E$.
3. The Tate pairing is defined up to lth powers.
   A unique value can be obtained by raising to the power
   $$(q^k - 1)/l.$$
4. If $P \in E(\mathbb{F}_q)$ and $l \nmid (q-1)$ then
   $$\langle P, P\rangle \equiv 1.$$

Modified Tate pairing

Suppose $l | \# E(\mathbb{F}_q)$ and $l \not| (q-1)$.

Let $P \in E(\mathbb{F}_q)$ have order l and let $Q \in \langle P \rangle$.

Suppose there is a non-rational endomorphism φ of E such that $\varphi(Q) \notin E(\mathbb{F}_q)$. Then

$$\langle P, \varphi(Q) \rangle \not\equiv 1.$$

Therefore, for applications, we use the bilinear function

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

This function gives rise to a Decision-Diffie-Hellman oracle and can be used to build various cryptosystems.

Security

For cryptographic applications:

- the Diffie-Hellman problem in $\langle P \rangle$ must be hard, so $l > 2^{160}$.
- the Diffie-Hellman problem in the subgroup of $\mathbb{F}_{q^k}^*$ must be hard, so $q^k > 2^{1024}$.

Can achieve this using supersingular curves.

Most interesting cases

The elliptic curves

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

over $\mathbb{F}_2$ (where $a = 0, 1$) have $k = 4$.
Non-rational endomorphism

$$\varphi(x, y) = (u^2 x + s^2, y + u^2 s x + s)$$

where $u^2 + u + 1 = 0$ and $s^2 + (u + 1)s + 1 = 0$.

Work over $\mathbb{F}_{2^m}$ with $m \approx 250$ (if there is a suitable group order).

$\star\star\star$

The elliptic curves

$$E : y^2 = x^3 - x \pm 1$$

over $\mathbb{F}_3$, have $k = 6$.
Non-$\mathbb{F}_3$-rational endomorphism

$$\varphi(x, y) = (\alpha - x, iy)$$

where $i^2 = -1$ and $\alpha^3 - \alpha + 1 = 0$.

Work over $\mathbb{F}_{3^m}$ where $m \approx 107$ (if there is a suitable group order).

Computing the Tate pairing

Let $P \in E(K)[l]$ and $Q \in E(K)$.

Since $[l]P = \mathcal{O}_E$ there is a function g such that $(g) = l(P) - l(\mathcal{O}_E)$.

Let $S \in E(K)$ be a random point.

Then

$$\langle P, Q \rangle = g(Q + S)/g(S)$$

modulo $(K^*)^l$.

Miller's algorithm (1986)

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.

Implementation techniques

1. Can work in a subgroup of $E(\mathbb{F}_q)$.
2. Since $P \in E(\mathbb{F}_q)$ can perform many operations in the small field $\mathbb{F}_q$ instead of the large field $\mathbb{F}_{q^k}$.

   Thus represent $\mathbb{F}_{q^k}$ as an extension of $\mathbb{F}_q$.
3. Postpone divisions in Miller's algorithm to the end.
4. Use window methods.
5. Can choose the auxiliary point $S \in E(\mathbb{F}_q)$.
6. (Barreto et al) Ignore calculations in Miller's algorithm which give values in $\mathbb{F}_q$.
7. (Barreto et al) Use structure of φ to optimise calculations.
8. (Barreto et al) Optimise final exponentiation using Frobenius action.
9. Use projective coordinates.

Note: Relationship between Tate pairing and Weil pairing.

Finite field implementation

Efficient characteristic 2 arithmetic is well-known.

Characteristic 3 arithmetic can also be efficiently done using bit operations.

Hardwire basis for $\mathbb{F}_{q^k}/\mathbb{F}_q$ and optimise multiplication operations for that basis.

Tripling in characteristic three

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

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

over $\mathbb{F}_{3^m}$.

Then (if $a_4 = -1$ and $a_6 \in \mathbb{F}_{3^m}$)

$$[3](x_1, y_1) = (x_1 + y_1^2 + y_1^6, -y_1^9)$$

so tripling is division free (but need one division to compute the straight line equations).

Barreto et al have (for $a_4, a_6 \in \mathbb{F}_3$)

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

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 $\lambda_3 = y_1^3 - \lambda_2$.

Conclusion: Use a base three Miller algorithm in characteristic three (signed trinary expansions).

Low Hamming Weight

Instead of using window methods, choose l to optimise performance.

In some cases we do not have flexibility to choose l.

Example:

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

The prime l does not have low Hamming weight. So compute Tate pairing with respect to N instead.

Final exponentiation is to the power

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

which also has low Hamming weight.

If P has order l then the Tate pairing gives an element of order l.

Compatibility result

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 $(g) = l(P) - l(\mathcal{O}_E)$ and $(g') = N(P) - N(\mathcal{O}_E)$. 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

Cost of evaluation of function $e(P,Q)$ includes Tate pairing and finite field exponentiation.

Milliseconds on a 1GHz Pentium III.

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

Note: Above timings include methods of Barreto et al.