Supersingular curves in cryptography

Steven Galbraith

Mathematics Department,
Royal Holloway University of London,
UK.

steven.galbraith@rhul.ac.uk

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

Conclusions

You should not use supersingular curves for cryptography.

You should use supersingular curves for cryptography.

Elliptic curves

An **elliptic curve** is non-singular curve E

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

with $a_1, a_2, a_3, a_4, a_6 \in \mathbb{F}_q$.

There is a **point at infinity** O_E.

There is an addition rule on the points $E(\mathbb{F}_q) = \{(x, y) \in E : x, y \in \mathbb{F}_q\} \cup \{O_E\}$.

$$[n]P = \underbrace{P + P + \cdots + P}_{n \text{ times}}.$$

Elliptic curve discrete logarithm problem: Given P and Q find a number λ so that

$$Q = [\lambda]P.$$

The Tate pairing and the Weil pairing

Let l be a prime dividing $\#E(\mathbb{F}_q)$.
Suppose q is not a power of l.

Define K to be the finite field extension $\mathbb{F}_{q^k}$ such that $l|(q^k - 1)$.

Write $E[l]$ for the set of all points of order l.

(Suppose $l^2 \| \#E(\mathbb{F}_q)$.)

The **Weil pairing** and **Tate pairing** are maps

$$\begin{array}{rcl} E[l] \times E[l] & \longrightarrow & K^* \\ P \times Q & \longmapsto & \langle P, Q \rangle \end{array}$$

which have various nice properties, e.g.,

$$\langle [\lambda]P, Q \rangle \equiv \langle P, Q \rangle^{\lambda}.$$

The Tate pairing versus the Weil pairing

Advantages:

- It applies to higher genus curves as well as elliptic curves.
- It requires less computation time to compute.
- It works over smaller fields in some cases.
- It is simpler.

Disadvantages:

- To get a unique value have to exponentiate by $(q^k - 1)/l$.
- Understanding non-degeneracy is more difficult.

The MOV/Frey-Rück attack

Let $P \in E(\mathbb{F}_q)$ be of order l.
Suppose $Q = [\lambda]P$ for some λ.

The Frey-Rück attack is as follows:

- Construct the field $K = \mathbb{F}_{q^k}$ such that $l|(q^k - 1)$.
- Find an auxiliary point $S \in E(K)$ such that $\langle P, S \rangle \not\equiv 1$.
- Compute $\zeta_1 = \langle P, S \rangle$ and $\zeta_2 = \langle Q, S \rangle$.
- Solve the discrete logarithm problem in K^* using an index calculus method (performing linear algebra modulo l).

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

What is k?

Theorem (MOV): If E is a supersingular elliptic curve then $k \leq 6$.

Theorem: There is an integer $k(g)$ such that for all finite fields $\mathbb{F}_q$ and all supersingular abelian varieties of dimension g over $\mathbb{F}_q$ one has $k \leq k(g)$.

Table of values of $k(g)$

g	$k(g)$	$k(g)/g$
1	6	6
2	12	6
3	$30 = \mathrm{lcm}(6,\ 10)$	10
4	$60 = \mathrm{lcm}(10,\ 12)$	15
5	$120 = \mathrm{lcm}(8,\ 10,\ 6)$	24
6	$210 = \mathrm{lcm}(6,10,14)$	35
7	$420 = \mathrm{lcm}(5,7,12)$	60
8	$840 = \mathrm{lcm}(3,5,7,8)$	105

What does this mean for cryptography?

Other applications of the Weil pairing to cryptography

- Sakai, Ohgishi, Kasahara: ID-based key exchange and signature.
- Joux: three-party Diffie-Hellman. (Improved by Verheul)
- Verheul: Escrow El Gamal encryption.
- Joux and Nguyen: DH $\neq$ DDH.
- Boneh-Franklin: Identity-based encryption.
- This conference . . .

Identity-based cryptography (Shamir)

A solution to the problem of management of public keys.

Obtain the public key of a user directly from their identity.

Need:

- Method to transform an identity (e.g., name or email address) into a group element.
- A dealer to provide secret keys corresponding to a user's public key.

Known identity-based encryption schemes:

- Cocks.
- Boneh-Franklin.

Boneh-Franklin encryption (I)

Dealer publishes E, $\mathbb{F}_q$ such that k is ‘small’, and $P \in E(\mathbb{F}_q)$ of order l.

Dealer chooses secret key s and publishes $P' = [s]P$.

The identity of user A gives rise to a point $Q_A \in E(\mathbb{F}_{q^k})$ such that $\langle P, Q_A \rangle \notin (\mathbb{F}^*_{q^k})^l$.

The dealer provides each user with their private key $Q'_A = [s]Q_A$.

Boneh-Franklin encryption (II)

(Tate pairing version)

To send message m to user A:

- Determine the public key Q_A of user A.
- Choose random r and compute $R = [r]P$.
- Compute $S = m \oplus H(\langle P', Q_A \rangle^{(q^k-1)r/l})$.
- Send (R, S).

To decrypt (R, S) user A does:

- $m = S \oplus H(\langle R, Q'_A \rangle^{(q^k-1)/l})$.

Performance depends on cost of computing Tate pairing.

Security

Depends on a new problem:

Weil/Tate-Diffie-Hellman problem: Given P, Q, $P_1 = [a]P$ and $P_2 = [b]P$ such that $\langle P, Q\rangle \notin (\mathbb{F}^*_{q^k})^l$, compute

$$\langle [ab]P, Q\rangle.$$

This is not harder than the Diffie-Hellman problem in $E(\mathbb{F}_q)$ or the Diffie-Hellman problem in $\mathbb{F}_{q^k}$.

For security need $q^k \geq 2^{1024}$.

Comparison of finite fields

- Original Boneh-Franklin description used $\mathbb{F}_p$ where p is a large prime.

  Then $k = 2$ and so $p \geq 2^{512}$.

  Can work in a subgroup.
- Supersingular curves in characteristic two can have $k = 4$, so work over $\mathbb{F}_{2^m}$ with $m \sim 250$.

  Very good efficiency and some bandwidth improvement.
- Supersingular curves in characteristic three can have $k = 6$.

  Example in paper: Using $\mathbb{F}_{3^{163}}$ get same security as Boneh-Franklin with 44% of the bandwidth.

  But, difficult to get a fast implementation in characteristic three.

Can trade bandwidth with computational efficiency.

Open problems

- Determine the largest attained values for k for curves of genus > 1 over finite fields.
- Are there suitable non-supersingular curves over $\mathbb{F}_q$ with small k?

  (see Balasubramanian-Koblitz).
- Are the WDH and TDH problems hard?
- Should you use supersingular curves for cryptography?