Applications of Number Theory and Algebraic Geometry to Cryptography

Karl Rubin

Department of Mathematics
UC Irvine

October 28, 2006 / Global KMS Day

Public key cryptography

Cryptography is used when one party (Alice) wants to send secret information to another party (Bob) over an insecure channel (like the Internet).

A traditional way to do this is for Alice and Bob to meet in advance and agree on a secret key or codebook, that can be used to encrypt and decrypt messages. This is not always practical.

In public key cryptography, Alice can encrypt a message for Bob using public (non-secret) information. Only Bob knows the private (secret) key required for decryption.

Public key cryptography

Let $\mathbb{F}_p$ be the finite field with p elements, and $\mathbb{F}_p^\times$ its multiplicative group.

Diffie-Hellman key agreement

1. *Public information: a prime p and a generator g of* $\mathbb{F}_p^\times$
2. *Alice's secret information: an integer a, $1 \le a \le p-1$.*
   Bob's secret information: an integer b, $1 \le b \le p-1$.
3. *Alice sends g^a to Bob, Bob sends g^b to Alice.*
4. *Alice and Bob each compute $g^{ab} = (g^b)^a = (g^a)^b$.*

The eavesdropper (Eve) knows g, g^a, and g^b. Can Eve compute g^{ab}?

Diffie-Hellman key agreement

Diffie-Hellman Problem

Given g, g^a, and g^b, compute g^{ab}.

Cleary, we can solve the Diffie-Hellman Problem if we can solve the Discrete Log Problem:

Discrete Log Problem

Given g and g^λ, compute λ.

What about the converse? Is the Diffie-Hellman Problem easier than the Discrete Log Problem?

Discrete logs in a general cyclic group

Suppose G is a finite cyclic group, and g is a generator. Given g^λ, one can compute λ, the discrete log:

Naïve method: in at most $|G|$ steps

Pollard rho: in $O(\sqrt{|G|})$ steps

(If we can factor $|G|$, and ℓ is the largest prime factor, then Pollard rho works in $O(\sqrt{\ell})$ steps.)

To be "secure" from an eavesdropper, the number of steps required should be at least 2^{80}, so $|G|$ should be divisible by a prime $\ell > 2^{160}$.

Discrete logs in $\mathbb{F}_q^\times$

Suppose q is a prime power. The best algorithms for computing discrete logs in $\mathbb{F}_q^\times$ (index calculus: function field sieve, number field sieve) take

$$L_q(1/3, c) := e^{c \log(q)^{1/3} \log\log(q)^{2/3}}$$

steps. This is

- smaller than any power of q,
- larger than any power of $\log(q)$.

To be "secure", one should take $q > 2^{1024}$.
Thus in secure Diffe-Hellman key agreement,

- the transmissions will be at least 1024 bits,
- the computations take place in a group of size $> 2^{1024}$.

Discrete logs in $\mathbb{F}_q^\times$

Compare this to the Discrete Log Problem in a general cyclic group, which requires only $|G| > 2^{160}$.

Are there better groups to use for cryptography?

We will look at

- algebraic tori,
- elliptic curves and abelian varieties.

The $\mathbf{T}_2$ cryptosystem

Suppose p is a prime. Define a subgroup $G \subset \mathbb{F}_{p^2}^\times$ by

$$G := \{x \in \mathbb{F}_{p^2}^\times : x^{p+1} = 1\}.$$

Equivalently, if $\mathbb{F}_{p^2} = \mathbb{F}_p(\sqrt{D})$ then

$$G := \{a + b\sqrt{D} \in \mathbb{F}_{p^2}^\times : a^2 - Db^2 = 1\}.$$

The best known attack on the discrete log problem in G is the attack on all of $\mathbb{F}_{p^2}^\times$, namely $L_{p^2}(1/3, c)$. So G will be “secure” if $p > 2^{512}$.

The $\mathbf{T}_2$ cryptosystem

The map

$$a + b\sqrt{D} \mapsto \frac{1+a}{b}$$

is a bijection from $G - \{\pm 1\}$ to $\mathbb{F}_p - \{0\}$, with inverse

$$\alpha \mapsto \frac{\alpha + \sqrt{D}}{\alpha - \sqrt{D}}.$$

This allows us to *compress* elements of G, so that they can be transmitted using only $\log_2(p)$ bits, instead of $\log_2(p^2)$.

In other words, the group G is as secure as $\mathbb{F}_{p^2}^\times$, but uses only half the bandwidth for transmissions.

The $\mathbf{T}_2$ cryptosystem

This is the "$\mathbf{T}_2$" cryptosystem of Rubin & Silverberg (2003).

Using a different map $G \to \mathbb{F}_p$, defined by

$$a + b\sqrt{D} \;\mapsto\; 2a$$

gives the "LUC" cryptosystem of Smith et al. (1993).

- advantage of LUC: some computations are easier
- advantage of $\mathbf{T}_2$: the map $G \to \mathbb{F}_p$ is (almost) a bijection
- advantage of $\mathbf{T}_2$: it can be generalized, to achieve even greater efficiency

Algebraic tori

Definition

$\mathbf{G}_m$ is the algebraic group with the property that $\mathbf{G}_m(F) = F^\times$ for every field F.

Definition

If L/F is a finite extension, the *Weil restriction of scalars* $\mathrm{Res}_F^L \mathbf{G}_m$ is an algebraic group of dimension $[L : F]$ with the property that

$$(\mathrm{Res}_F^L \mathbf{G}_m)(K) = (L \otimes_F K)^\times$$

for every field K containing F.

In particular $(\mathrm{Res}_F^L \mathbf{G}_m)(F) = L^\times$.

Algebraic tori

Definition

An algebraic group V over a field F is an *algebraic torus* if $V \cong \mathbf{G}_m^d$ over some finite extension K of F, for some $d \geq 0$.

Example

$$\mathrm{Res}_F^L \mathbf{G}_m \cong \mathbf{G}_m^{[L:F]} \quad \text{over } L,$$

so $\mathrm{Res}_F^L \mathbf{G}_m$ is an algebraic torus of dimension $[L : F]$.

Algebraic tori

Fix a prime p. Then

$$(\mathrm{Res}_{\mathbb{F}_p}^{\mathbb{F}_{p^n}} \mathbf{G}_m)(\mathbb{F}_p) \cong \mathbb{F}_{p^n}^\times$$

If $d \mid n$ there is a norm map $N_{n/d} : \mathrm{Res}_{\mathbb{F}_p}^{\mathbb{F}_{p^n}} \mathbf{G}_m \to \mathrm{Res}_{\mathbb{F}_p}^{\mathbb{F}_{p^d}} \mathbf{G}_m$ such that

$$\begin{tikzcd}
(\mathrm{Res}_{\mathbb{F}_p}^{\mathbb{F}_{p^n}} \mathbf{G}_m)(\mathbb{F}_p) \arrow[r, "\sim"] \arrow[d, "N_{n/d}"'] & \mathbb{F}_{p^n}^\times \arrow[d, "N_{n/d}"] \\
(\mathrm{Res}_{\mathbb{F}_p}^{\mathbb{F}_{p^d}} \mathbf{G}_m)(\mathbb{F}_p) \arrow[r, "\sim"] & \mathbb{F}_{p^d}^\times
\end{tikzcd}$$

commutes.

Algebraic tori

Definition

$$\mathbf{T}_n := \ker\left(\mathrm{Res}^{\mathbb{F}_{p^n}}_{\mathbb{F}_p}\mathbf{G}_m \xrightarrow{\oplus N_{n/d}} \bigoplus_{d|n, d\neq n} \mathrm{Res}^{\mathbb{F}_{p^d}}_{\mathbb{F}_p}\mathbf{G}_m\right).$$

- $\mathbf{T}_1 = \mathbf{G}_m$
- $\mathbf{T}_n(\mathbb{F}_p) \cong \{x \in \mathbb{F}_{p^n}^\times : N_{n/d}(x) = 1 \text{ for every } d \mid n,\, d \neq n\}$
  $= \{x \in \mathbb{F}_{p^n}^\times : x^{\Phi_n(p)} = 1\}$
  where Φ_n is the n-th cyclotomic polynomial (the monic polynomial of degree $\varphi(n)$) whose roots are the primitive n-th roots of unity; φ is the Euler φ function). Thus $|\mathbf{T}_n(\mathbb{F}_p)| = \Phi_n(p) \approx p^{\varphi(n)}$.
- $\mathbf{T}_2(\mathbb{F}_p) \cong \{x \in \mathbb{F}_{p^2}^\times : x^{p+1} = 1\}$
  the group we saw earlier in the $\mathbf{T}_2$ cryptosystem.

Algebraic tori

Theorem

1. $Res^{\mathbb{F}_{p^n}}_{\mathbb{F}_p}\mathbf{G}_m$ *is isogenous over* $\mathbb{F}_p$ *to* $\oplus_{d|n}\mathbf{T}_d$
2. $\mathbf{T}_n$ *is an algebraic torus of dimension* $\varphi(n)$.

Conjecture (Voskresenskiĭ)

The algebraic torus $\mathbf{T}_n$ *is birationally isomorphic to* $\mathbf{A}^{\varphi(n)}$ *over* $\mathbb{F}_p$.

Here $\mathbf{A}^{\varphi(n)}$ is $\varphi(n)$-dimensional affine space, and birationally isomorphic means there are rational maps (quotients of polynomials) that give a bijection between "almost all" of $\mathbf{T}_n$ and "almost all" of $\mathbf{A}^{\varphi(n)}$.

Algebraic tori

If Voskresenskiĭ's Conjecture is true, then elements of $\mathbf{T}_n(\mathbb{F}_p)$ can be *compressed*, using the birational isomorphism $\mathbf{T}_n \xrightarrow{\sim} \mathbf{A}^{\varphi(n)}$ to represent elements of $\mathbf{T}_n(\mathbb{F}_p) \subset \mathbb{F}_{p^n}^\times$ with only $\varphi(n)$ elements of $\mathbb{F}_p$, rather than n elements of $\mathbb{F}_p$.

Thus for security we need

- $|\mathbf{T}_n(\mathbb{F}_p)| \approx p^{\varphi(n)} > 2^{160}$
- $p^n > 2^{1024}$

i.e.

$$log_2(p^{\varphi(n)}) > \max\{160, 1024\frac{\varphi(n)}{n}\}.$$

Note: $\log_2(p^{\varphi(n)})$ is the number of bits that must be transmitted for each element of $\mathbf{T}_n(\mathbb{F}_p)$.

Algebraic tori

Minimum sizes of p to ensure security:

n	1	2	3	4	5	6	$\cdots$	30
$\log_2(p) >$	1024	512	342	256	205	171	$\cdots$	35
$\frac{\varphi(n)}{n}$	1	.50	.67	.50	.80	.33	$\cdots$	.27
$\log_2(p^{\varphi(n)}) >$	1024	512	684	512	820	342	$\cdots$	280

Voskresenskiĭ's Conjecture

Conjecture (Voskresenskiĭ)

The algebraic torus $\mathbf{T}_n$ *is birationally isomorphic to* $\mathbf{A}^{\varphi(n)}$ *over* $\mathbb{F}_p$*.*

- Voskresenskiĭ's Conjecture is trivially true when $n = 1$.

$$\mathbf{T}_1 = \mathbf{G}_m \hookrightarrow \mathbf{A}^1 \quad \text{by the natural injection}$$

- Voskresenskiĭ's Conjecture is true when $n = 2$.

$$\mathbf{T}_2 = \{(x, y) : x^2 - Dy^2 = 1\} \to \mathbf{A}^1 \quad \text{by} \quad (x, y) \mapsto (1 + x)/y$$

This gives the $\mathbf{T}_2$-cryptosystem.

Voskresenskiĭ's Conjecture

Theorem (Klyachko)

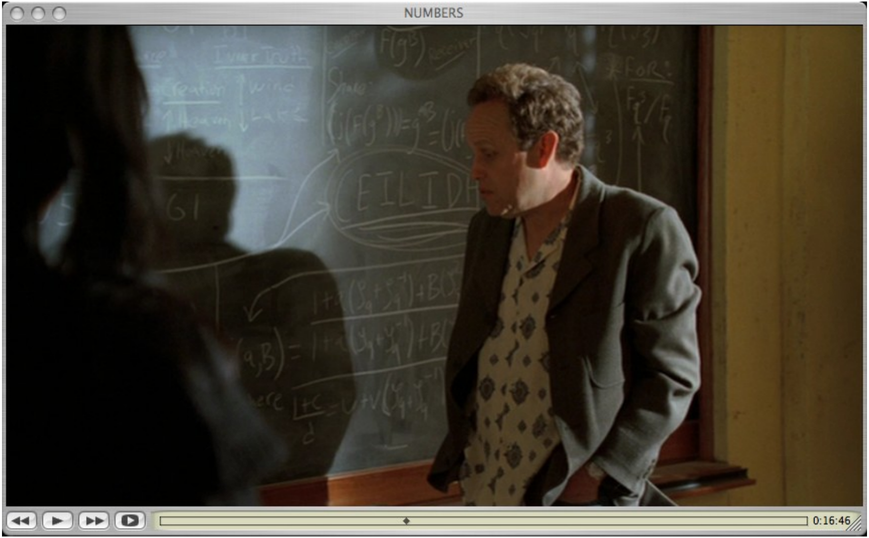
Voskresenskiĭ's Conjecture is true if n is divisible by at most 2 distinct primes.

Recall:

n	1	2	3	4	5	6	$\cdots$	30
$\log_2(p) >$	1024	512	342	256	205	171	$\cdots$	35
$\frac{\varphi(n)}{n}$	1	.50	.67	.50	.80	.33	$\cdots$	.27
$\log_2(p^{\varphi(n)}) >$	1024	512	684	512	820	342	$\cdots$	280

In particular, $\mathbf{T}_6$ is birationally isomorphic to $\mathbf{A}^2$. This gives rise to the CEILIDH cryptosystem (Rubin & Silverberg 2003).

NUMB3RS, May 12, 2006



Voskresenskiĭ's Conjecture

Using the trace map

$$\mathrm{Tr}_{\mathbb{F}_{p^6}/\mathbb{F}_{p^2}} : \mathbf{T}_6(\mathbb{F}_p) \to \mathbb{F}_{p^2} \cong \mathbf{A}^2(\mathbb{F}_p)$$

instead of a birational isomorphism from $\mathbf{T}_6$ to $\mathbf{A}^2$ gives the XTR cryptosystem of Lenstra and Verheul (2000).

Voskresenskiĭ's Conjecture

Open Question

Is $\mathbf{T}_{30}$ birationally isomorphic to $\mathbf{A}^8$?

If so, this would give a new cryptosystem with more efficient transmission sizes.

Open Question

How secure is the Discrete Log Problem in $\mathbb{F}_{p^{30}}^\times$?

There are indications that the Discrete Log Problem in $\mathbb{F}_{p^{30}}^\times$ might be easier than the general Discrete Log Problem in $\mathbb{F}_\ell^\times$ with a prime $\ell \approx p^{30}$.

Summary of torus-based cryptography

- If there is a birational isomorphism $f : \mathbf{T}_n \to \mathbf{A}^{\varphi(n)}$, then f can be used to *compress* elements of $\mathbf{T}_n(\mathbb{F}_p) \subset \mathbb{F}_{p^n}^\times$.
- This compression reduces transmission size by a factor of $\varphi(n)/n$, while still relying on the security of the Discrete Log Problem in $\mathbb{F}_{p^n}^\times$.
- This can be done (explicitly) when
  - $n = 1$ (the "classical" case, no compression),
  - $n = 2$ (compression factor $1/2$)
  - $n = 6$ (compression factor $1/3$)
- The next useful case is $n = 30$ (compression factor $4/15 \approx .27$). It is not known if $\mathbf{T}_{30}$ is birationally isomorphic to $\mathbf{A}^8$.
- The next useful case after that would be $n = 210$ (compression factor $8/35 \approx .23$). But this may be impractical for other reasons.

Elliptic curves

An *elliptic curve* over $\mathbb{F}_q$ is a curve defined by an equation

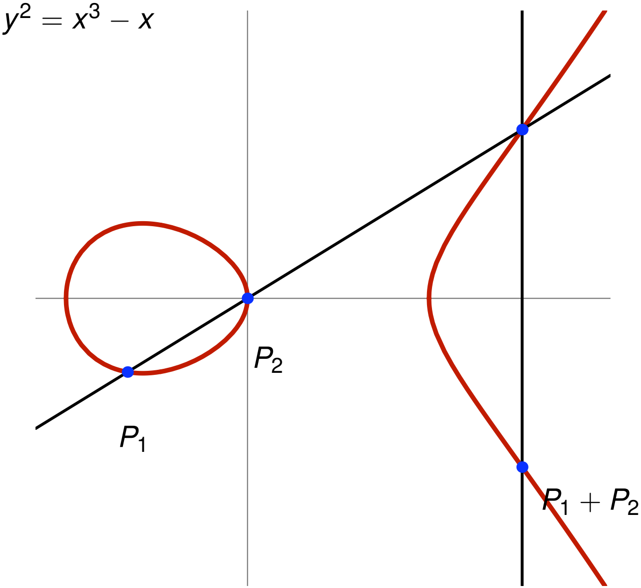
$$y^2 = x^3 + ax + b$$

with $a, b \in \mathbb{F}_q$ and $4a^3 + 27b^2 \neq 0$

(or a slightly more complicated equation if the characteristic of $\mathbb{F}_q$ is 2 or 3).

The set of points $E(\mathbb{F}_q)$ (including the point at infinity) has a natural commutative group law.

Elliptic curve group law



Elliptic curve group law

The group law can also be written algebraically:

If $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$, then $P_1 + P_2 = (x_3, y_3)$ where x_3, y_3 are given as follows:

1. set $\lambda := \begin{cases} (y_2 - y_1)/(x_2 - x_1) & \text{if } P_1 \neq P_2, \\ (3x_1^2 + a)/2y_1 & \text{if } P_1 = P_2, \end{cases}$
2. set $x_3 := \lambda^2 - x_1 - x_2$,
3. set $y_3 := \lambda(x_1 - x_3) - y_1$.

Elliptic curve group law

Theorem (Hasse 1934)

$$q+1-2\sqrt{q} \leq |E(\mathbb{F}_q)| \leq q+1+2\sqrt{q}.$$

Therefore

$$|E(\mathbb{F}_q)| \approx q.$$

Theorem (Schoof 1985)

There is a polynomial-time algorithm for computing $|E(\mathbb{F}_q)|$.

Discrete logs in $E(\mathbb{F}_q)$

One can use the groups $E(\mathbb{F}_q)$ for cryptography (Miller, Koblitz, 1985). A necessary condition for security is that the Discrete Log Problem in $E(\mathbb{F}_q)$ is hard.

The best algorithm for computing discrete logs in $E(\mathbb{F}_q)$ for a *general* elliptic curve E over $\mathbb{F}_q$ takes $O(\sqrt{|E(\mathbb{F}_q)|}) = O(\sqrt{q})$ steps.

Many (but not all!) elliptic curves E over $\mathbb{F}_q$ are believed to be secure.

It is important to know which E are not secure.

Example

If $|E(\mathbb{F}_q)| = q$, then computing discrete logs in $E(\mathbb{F}_q)$ is easy.

The Weil pairing

Suppose E is an elliptic curve over $\mathbb{F}_q$, and ℓ is a prime not dividing q. Let k be the order of q in $\mathbb{F}_\ell^\times$, so $\mathbb{F}_{q^k}$ is the smallest extension of $\mathbb{F}_q$ containing $\boldsymbol{\mu}_\ell$, the group of ℓ-th roots of unity in $\bar{\mathbb{F}}_q$.

Definition

$E[\ell] := \{P \in E(\bar{\mathbb{F}}_q) : \ell P = 0\}$.

Fact

- $E[\ell] \cong \mathbb{F}_\ell^2$
- *If* $|E(\mathbb{F}_q)|$ *is divisible by* ℓ *but not by* ℓ^2*, then* $\mathbb{F}_q(E[\ell]) = \mathbb{F}_{q^k}$.

The Weil pairing

Theorem (Weil, Miller)

There is a nondegenerate skew-symmetric bilinear pairing

$$\langle\ ,\ \rangle_\ell : E[\ell] \times E[\ell] \longrightarrow \boldsymbol{\mu}_\ell$$

that is computable in polynomial time.

Suppose $C \subset E(\mathbb{F}_q)$ is a subgroup of order ℓ.

The Weil pairing can be used to reduce the Discrete Log Problem in C to the Discrete Log Problem in $\mathbb{F}_{q^k}^\times$, where k is the order of $q \pmod{\ell}$ (Menezes, Okamoto & Vanstone 1993).

The Weil pairing

MOV reduction

1. *Suppose $C \subset E(\mathbb{F}_q)$ is a subgroup of order ℓ, P is a generator of C, and $Q \in E[\ell] - C$.*

2. *Define an injective homomorphism*

$$f : C \to \mathbb{F}_{q^k}^\times \quad \text{by} \quad f(R) = \langle R, Q \rangle_\ell \in \boldsymbol{\mu}_\ell \subset \mathbb{F}_{q^k}^\times.$$

3. *Given $\{P, \lambda P\}$, compute*

$$\{f(P), f(\lambda P)\} = \{g, g^\lambda\}$$

   where $g = f(P)$ is a generator of $\boldsymbol{\mu}_\ell \subset \mathbb{F}_{q^k}^\times$.

4. *Compute λ from $\{g, g^\lambda\}$, as a discrete log computation in $\mathbb{F}_{q^k}^\times$.*

Example: $y^2 = x^3 - x$

Example

Let E be the elliptic curve $y^2 = x^3 - x$ and $q \equiv 3 \pmod 4$. Then

- $|E(\mathbb{F}_q)| \;=\; q + 1$
- If ℓ is a prime dividing $q + 1$, then $q \equiv -1 \pmod \ell$ so the order of $q \pmod \ell$ is 2.
- The Weil pairing reduces computation of discrete logs in $E(\mathbb{F}_q)$ to computation of discrete logs in $\mathbb{F}_{q^2}^\times$.

Thus to be secure in this case, we must have $q > 2^{512}$.

Example: $y^2 = x^3 - x$

Example

Let E be the elliptic curve $y^2 = x^3 - x$ and $p = 2^{163} + 16893$. Then

- $|E(\mathbb{F}_p)| \;=\; p + 6473158660473377637781611$
- $\ell = |E(\mathbb{F}_p)|/8$ is prime and $\ell > 2^{160}$
- The order of $p \pmod{\ell}$ is $\ell - 1$.
- The Weil pairing reduces computation of discrete logs in $E(\mathbb{F}_p)$ to computation of discrete logs in $\mathbb{F}^\times_{p^{\ell-1}}$.

But $\ell > 2^{160}$, so we can't even write down an element of $\mathbb{F}^\times_{p^{\ell-1}}$, and this "reduction" is useless. Cryptography in $E(\mathbb{F}_p)$ is secure against known attacks.

Pairing-based signatures

There are other applications of the Weil pairing.

Boneh-Lynn-Shacham signature scheme 2001

1. *Fix an elliptic curve E over $\mathbb{F}_q$, a subgroup $C \subset E(\mathbb{F}_q)$ of order ℓ, and a point $Q \in E[\ell] - C$.*
2. *Alice chooses a secret integer a, $1 \leq a \leq \ell$.*
3. *Public information: q, E, ℓ, Q, aQ.*
4. *Alice encodes the message as a point $M \in C$.*
5. *Alice sends the signed message (M, aM) to Bob.*
6. *Bob receives the pair (M, N). To verify the signature, Bob checks that*
$$\langle M, aQ\rangle_\ell = \langle N, Q\rangle_\ell.$$

Since a is secret, only Alice can compute aM.

Embedding degrees

In order to use the Weil pairing, the integer k (the order of $q \pmod{\ell}$) cannot be too large.

Definition

The order k of q in $\mathbb{F}_\ell^\times$ is called the *embedding degree*.

($\mathbb{F}_{q^k}$ is the smallest extension of $\mathbb{F}_q$ such that the subgroup $C \subset E(\mathbb{F}_q)$ of order ℓ embeds into $\mathbb{F}_{q^k}^\times$.)

For a random elliptic curve, $k \approx \ell$ which is very large.

We say that E is *pairing-friendly* if k is not too large (so that the Weil pairing is computable) and not too small (so that the Discrete Log Problem is not too easy).

Pairing-friendly elliptic curves

It is easy to find elliptic curves with embedding degree $k = 2$. For example:

$$E : y^2 = x^3 - x, \quad q \equiv 3 \pmod 4$$
$$E : y^2 = x^3 + 1, \quad q \equiv 2 \pmod 3$$

These are *supersingular* elliptic curves:

Definition

An elliptic curve E over $\mathbb{F}_q$ is $\begin{cases} \textit{supersingular} & \text{if } E[q] = 0, \\ \textit{ordinary} & \text{if } E[q] \neq 0. \end{cases}$

Pairing-friendly elliptic curves

Possible embedding degrees for supersingular elliptic curves:

characteristic	embedding degrees
2	1, 2, 3, 4
3	1, 2, 3, 6
≥ 5	1, 2

- supersingular curves are easy to construct
- embedding degrees are not too large
- maybe the embedding degrees are too small?

Pairing-friendly elliptic curves

- It is harder to find examples of ordinary (i.e., non-supersingular) elliptic curves with embedding degrees that are not too large.
- Elliptic curves with embedding degree greater than 6 but not too large would allow for shorter signatures with the same level of security.
- Methods for constructing such curves have been developed by Miyaji, Nakabayashi, Takano, Barreto, Lynn, Scott, Cocks, Pinch, Brezing, Weng, Naehrig, Freeman, ...

Abelian varieties

Definition

An *abelian variety* is a connected projective algebraic group.

- Elliptic curves are exactly the one-dimensional abelian varieties.
- The Jacobian of a curve of genus g is an abelian variety of dimension g.
- If A is an abelian variety over $\mathbb{F}_q$, the group $A(\mathbb{F}_q)$ can be used for cryptography in the same way as $\mathbb{F}_q^\times$ or $E(\mathbb{F}_q)$ with an elliptic curve E.
- If A is an abelian variety, then (except for possibly finitely many primes ℓ) there is a Weil pairing

$$A[\ell] \times A[\ell] \to \boldsymbol{\mu}_\ell.$$

Pairing-friendly abelian varieties

Definition

If A is an abelian variety over $\mathbb{F}_q$, and ℓ is a prime dividing $|A(\mathbb{F}_q)|$, then

- the *embedding degree* is again the order of q in $\mathbb{F}_\ell^\times$,
- A is *pairing friendly* if the embedding degree is not too small and not too large,
- the *security parameter* is the embedding degree divided by the dimension of A.

Definition

An abelian variety over $\mathbb{F}_q$ is *supersingular* if it is isogenous over $\bar{\mathbb{F}}_q$ to a product of supersingular elliptic curves.

Supersingular abelian varieties

Theorem (Galbraith; Choie, Jeong & Lee; Rubin & Silverberg)

The largest security parameters of simple supersingular abelian varieties are:

dimension	1	2	3	4	5	6
characteristic 2	4	6		5		6
characteristic 3	6	2	6	$7\frac{1}{2}$		7
characteristic 5	2	3		$3\frac{3}{4}$		3
characteristic 7	2	3	$4\frac{2}{3}$	3		7
characteristic 11	2	3		3	2	3
characteristic ≥ 13	2	3		3		3

(a blank entry means there are no simple supersingular abelian varietes of that dimension in that characteristic).

Supersingular abelian varieties

We construct supersingular abelian varieties with "optimal" security parameters in a way analogous to what we did with algebraic tori.

Recall the decomposition

$$\mathrm{Res}_{\mathbb{F}_p}^{\mathbb{F}_{p^n}} \mathbf{G}_m \sim \oplus_{d|n} \mathbf{T}_d$$

Abelian varieties

If E is an elliptic curve over $\mathbb{F}_q$, then the Weil restriction of scalars $\mathrm{Res}_{\mathbb{F}_q}^{\mathbb{F}_{q^n}} E$ is an abelian variety over $\mathbb{F}_q$ of dimension n, and

$$(\mathrm{Res}_{\mathbb{F}_q}^{\mathbb{F}_{q^n}} E)(\mathbb{F}_q) \cong E(\mathbb{F}_{q^n}).$$

Theorem

Suppose E is an elliptic curve over $\mathbb{F}_q$. For every $d \geq 1$ there is an abelian variety $\mathbf{E}_d$ over $\mathbb{F}_q$ of dimension $\varphi(d)$ such that for every n,

- $Res_{\mathbb{F}_q}^{\mathbb{F}_{q^n}} E \sim \bigoplus_{d \mid n} \mathbf{E}_d$.
- $\mathbf{E}_n(\mathbb{F}_q) \cong \{P \in E(\mathbb{F}_{q^n}) : Tr_{\mathbb{F}_{q^n}/\mathbb{F}_{q^d}} P = 0 \text{ for every } d \mid n, d \neq n\}$,
- $\mathbf{E}_n$ *is isogenous over* $\mathbb{F}_{q^n}$ *to* $E^{\varphi(n)}$.

Supersingular abelian varieties

Theorem (Rubin & Silverberg 2002)

Suppose

- E *is a supersingular elliptic curve over* $\mathbb{F}_q$,
- *the embedding degree of* E *is* k,
- n *is relatively prime to* $2qk$.

Then $\mathbf{E}_n$ *is a supersingular abelian variety over* $\mathbb{F}_q$ *of dimension* $\varphi(n)$, *with security parameter* $k\frac{n}{\varphi(n)}$.

Supersingular abelian varieties

Example

- take $q = 3^d$ with d odd
- take $E : y^2 = x^3 - x \pm 1$
- $|E(\mathbb{F}_q)| = q \pm \sqrt{3q} + 1$, and the embedding degree is 6
- take $n = 5$

The theorem shows that

- $\mathbf{E}_5$ is a supersingular abelian variety of dimension 4
- the security parameter of $\mathbf{E}_n$ is $6 \cdot (5/\varphi(5)) = 7\frac{1}{2}$.

Supersingular abelian varieties

Best supersingular security parameters

dimension	1	2	3	4	5	6
characteristic 2	4	6		5		6
characteristic 3	6	2	6	$7\frac{1}{2}$		7
characteristic 5	2	3		$3\frac{3}{4}$		3
characteristic 7	2	3	$4\frac{2}{3}$	3		7
characteristic 11	2	3		3	2	3
characteristic ≥ 13	2	3		3		3

- $q = 3^d$, d odd; $E : y^2 = x^3 - x \pm 1$; $n = 5$;
- $\mathbf{E}_5$ has dimension 4 and security parameter $7\frac{1}{2}$.

Some remarks on efficiency

- $\mathbf{E}_n \subset \mathrm{Res}_{\mathbb{F}_q}^{\mathbb{F}_{q^n}} E$, so
$$\mathbf{E}_n(\mathbb{F}_q) \subset E(\mathbb{F}_{q^n}).$$
Therefore, even though $\mathbf{E}_n$ is a higher dimensional abelian variety, all computations in $\mathbf{E}_n(\mathbb{F}_q)$ can be done with elliptic curve arithmetic.

Some remarks on efficiency

- Normally one would represent an element of $E(\mathbb{F}_{q^n})$ by its x-coordinate, which requires n elements of $\mathbb{F}_q$. But $\mathbf{E}_n(\mathbb{F}_q)$ is a proper subgroup of $E(\mathbb{F}_{q^n})$, and

  $$|\mathbf{E}_n(\mathbb{F}_q)| \approx p^{\varphi(n)}.$$

  Ideally one would like to represent an element of $\mathbf{E}_n(\mathbb{F}_q)$ by $\varphi(n)$ elements of $\mathbb{F}_q$. This *compression* would reduce transmission sizes by a factor of $\varphi(n)/n$.
- We can do this when $n = 2, 3$, or 5 (Rubin & Silverberg 2002).
- The case $n = 2$ is not useful, because $\mathbf{E}_2$ is just the quadratic twist of E corresponding to the extension $\mathbb{F}_{q^2}/\mathbb{F}_q$, which is another elliptic curve.

Some remarks on efficiency

- We compress a point $P \in \mathbf{E}_n(\mathbb{F}_q) \subset E(\mathbb{F}_{q^n})$ by

$$\underset{\in E(\mathbb{F}_{q^n})}{P = (x, y)} \mapsto x \mapsto \underset{\in \mathbb{F}_{q^n} \times \mathbb{F}_{q^n}}{(x_0, x_1, \ldots, x_{n-1})} \mapsto \underset{\in \mathbb{F}_{q^n}}{(x_1, x_2, \ldots, x_{n-1})}$$

- If n is prime, this achieves a compression factor of $\frac{n-1}{n} = \frac{\varphi(n)}{n}$.
- If $n = 3$ or 5, we can *decompress* to recover the original point P. (Almost: the compression map is not injective, it is 8-to-1 when $n = 3$, and 54-to-1 when $n = 5$, but one can send a few extra bits with each transmission to make the decompression unique.)

Summary

- Properly chosen elliptic curves may provide the same security as a multiplicative group, with substantially smaller transmission lengths. (This is because there is no known subexponential algorithm for computing discrete logs on a general elliptic curve.)
- If the embedding degree is small, the Weil pairing can be used to reduce elliptic curve discrete logs to multiplicative group discrete logs.
- If the embedding degree is not too big, the Weil pairing on an elliptic curve or abelian variety has useful cryptographic applications, such as identity-based cryptography, innovative signature schemes, private information retrieval, non-interactive zero knowledge proofs, ...

Applications of Number Theory and Algebraic Geometry to Cryptography

Karl Rubin

Department of Mathematics
UC Irvine

October 28, 2006 / Global KMS Day