Applications of Number Theory and Algebraic Geometry to Cryptography

Karl Rubin

Department of Mathematics
UC Irvine

October 28, 2006 / Global KMS Day
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 $a$, $1 \leq a \leq p - 1$.
   Bob's secret information: an integer $b$, $1 \leq b \leq p - 1$.

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 $g^{ab}$.

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

**Discrete Log Problem**

Given $g$ and $g^\lambda$, compute $\lambda$.

What about the converse? Is the Diffie-Hellman Problem easier than the Discrete Log Problem?
Suppose $G$ is a finite cyclic group, and $g$ is a generator. Given $g^\lambda$, one can compute $\lambda$, the discrete log:

Naïve method: in at most $|G|$ steps

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

(If we can factor $|G|$, and $\ell$ 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 $\ell > 2^{160}$. 
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 \( > 2^{1024} \).
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 $p > 2^{512}$.  

Karl Rubin (UC Irvine)  
Number Theory and Cryptography  
October 2006  
KMS Day 8 / 51
The $T_2$ 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 $T_2$ cryptosystem

This is the “$T_2$” cryptosystem of Rubin & Silverberg (2003).

Using a different map $G \rightarrow F_p$, 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 $T_2$: the map $G \rightarrow F_p$ is (almost) a bijection
- advantage of $T_2$: it can be generalized, to achieve even greater efficiency
Algebraic tori

**Definition**

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

**Definition**

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

\[
(\text{Res}^L_F \mathbb{G}_m)(K) = (L \otimes_F K)^\times
\]

for every field $K$ containing $F$.

In particular, $(\text{Res}^L_F \mathbb{G}_m)(F) = L^\times$. 
Algebraic tori

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

**Example**
$$\text{Res}_F^L \mathbb{G}_m \cong \mathbb{G}_m^{[L:F]}$$ over $L$,
so $\text{Res}_F^L \mathbb{G}_m$ is an algebraic torus of dimension $[L : F]$. 
Fix a prime $p$. Then

\[(\text{Res}_{F_p}^{F_p^n} G_m)(F_p) \cong F_p^n\]

If $d \mid n$ there is a norm map $N_{n/d} : \text{Res}_{F_p}^{F_p^n} G_m \rightarrow \text{Res}_{F_p}^{F_p^d} G_m$ such that

\[
\begin{array}{ccc}
(\text{Res}_{F_p}^{F_p^n} G_m)(F_p) & \xrightarrow{\sim} & F_p^n \\
\downarrow N_{n/d} & & \downarrow N_{n/d} \\
(\text{Res}_{F_p}^{F_p^d} G_m)(F_p) & \xrightarrow{\sim} & F_p^d \\
\end{array}
\]

commutes.
Algebraic tori

Definition

\[ T_n := \ker \left( \operatorname{Res}_{\mathbb{F}_p}^{\mathbb{F}_p^n} \mathbb{G}_m \oplus \mathbb{N}_{n/d} \to \bigoplus_{d \mid n, d \neq n} \operatorname{Res}_{\mathbb{F}_p}^{p^d} \mathbb{G}_m \right). \]

- \( T_1 = \mathbb{G}_m \)
- \( T_n(\mathbb{F}_p) \cong \{ x \in \mathbb{F}_p^{\times} : N_{n/d}(x) = 1 \text{ for every } d \mid n, d \neq n \} \)
  \[ = \{ x \in \mathbb{F}_p^{\times} : x^{\Phi_n(p)} = 1 \} \]
  where \( \Phi_n \) is the \( n \)-th cyclotomic polynomial (the monic polynomial of degree \( \varphi(n) \) whose roots are the primitive \( n \)-th roots of unity; \( \varphi \) is the Euler \( \varphi \) function). Thus \( |T_n(\mathbb{F}_p)| = \Phi_n(p) \approx p^{\varphi(n)} \).
- \( T_2(\mathbb{F}_p) \cong \{ x \in \mathbb{F}_p^{\times} : x^{p+1} = 1 \} \)
  the group we saw earlier in the \( T_2 \) cryptosystem.
Algebraic tori

Theorem

1. \( \text{Res}_{\mathbb{F}_p}^{\mathbb{F}_p^n} \mathbb{G}_m \) is isogenous over \( \mathbb{F}_p \) to \( \bigoplus_{d|n} T_d \)
2. \( T_n \) is an algebraic torus of dimension \( \varphi(n) \).

Conjecture (Voskresenskiĭ)

The algebraic torus \( T_n \) is birationally isomorphic to \( \mathbb{A}^{\varphi(n)} \) over \( \mathbb{F}_p \).

Here \( \mathbb{A}^{\varphi(n)} \) 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 \( T_n \) and “almost all” of \( \mathbb{A}^{\varphi(n)} \).
If Voskresenskiǐ’s Conjecture is true, then elements of $T_n(\mathbb{F}_p)$ can be \textit{compressed}, using the birational isomorphism $T_n \sim A^\varphi(n)$ to represent elements of $T_n(\mathbb{F}_p) \subset \mathbb{F}_p^n$ with only $\varphi(n)$ elements of $\mathbb{F}_p$, rather than $n$ elements of $\mathbb{F}_p$.

Thus for security we need

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

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 $T_n(\mathbb{F}_p)$. 
## Algebraic tori

Minimum sizes of $p$ to ensure security:

<table>
<thead>
<tr>
<th>$n$</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>...</th>
<th>30</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\log_2(p)$</td>
<td>1024</td>
<td>512</td>
<td>342</td>
<td>256</td>
<td>205</td>
<td>171</td>
<td>...</td>
<td>35</td>
</tr>
<tr>
<td>$\frac{\varphi(n)}{n}$</td>
<td>1</td>
<td>.50</td>
<td>.67</td>
<td>.50</td>
<td>.80</td>
<td>.33</td>
<td>...</td>
<td>.27</td>
</tr>
<tr>
<td>$\log_2(p^{\varphi(n)})$</td>
<td>1024</td>
<td>512</td>
<td>684</td>
<td>512</td>
<td>820</td>
<td>342</td>
<td>...</td>
<td>280</td>
</tr>
</tbody>
</table>
Conjecture (Voskresenskiĭ)

The algebraic torus \( T_n \) is birationally isomorphic to \( \mathbb{A}^{\varphi(n)} \) over \( \mathbb{F}_p \).

- Voskresenskiĭ’s Conjecture is trivially true when \( n = 1 \).

\[
T_1 = \mathbb{G}_m \hookrightarrow \mathbb{A}^1 \quad \text{by the natural injection}
\]

- Voskresenskiĭ’s Conjecture is true when \( n = 2 \).

\[
T_2 = \{(x, y) : x^2 - Dy^2 = 1\} \rightarrow \mathbb{A}^1 \quad \text{by} \quad (x, y) \mapsto (1 + x)/y
\]

This gives the \( T_2 \)-cryptosystem.
Voskresenskii’s Conjecture

Theorem (Klyachko)

*Voskresenskii’s Conjecture is true if* $n$ *is divisible by at most 2 distinct primes.*

Recall:

<table>
<thead>
<tr>
<th>$n$</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>...</th>
<th>30</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\log_2(p) &gt;$</td>
<td>1024</td>
<td>512</td>
<td>342</td>
<td>256</td>
<td>205</td>
<td>171</td>
<td>...</td>
<td>35</td>
</tr>
<tr>
<td>$\frac{\varphi(n)}{n}$</td>
<td>1</td>
<td>.50</td>
<td>.67</td>
<td>.50</td>
<td>.80</td>
<td>.33</td>
<td>...</td>
<td>.27</td>
</tr>
<tr>
<td>$\log_2(p^{\varphi(n)}) &gt;$</td>
<td>1024</td>
<td>512</td>
<td>684</td>
<td>512</td>
<td>820</td>
<td>342</td>
<td>...</td>
<td>280</td>
</tr>
</tbody>
</table>

In particular, $T_6$ is birationally isomorphic to $A^2$. This gives rise to the CEILIDH cryptosystem (Rubin & Silverberg 2003).
Using the trace map

\[ \text{Tr}_{\mathbb{F}_p^6/\mathbb{F}_p^2} : T_6(\mathbb{F}_p) \rightarrow \mathbb{F}_p^2 \cong A^2(\mathbb{F}_p) \]

instead of a birational isomorphism from \( T_6 \) to \( A^2 \) gives the XTR cryptosystem of Lenstra and Verheul (2000).
Voskresenskiĭ’s Conjecture

Open Question

Is $T_{30}$ birationally isomorphic to $A^8$?

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 $f : T_n \rightarrow A^{\varphi(n)}$, then $f$ can be used to **compress** elements of $T_n(\mathbb{F}_p) \subset \mathbb{F}_p^\times$.

This compression reduces transmission size by a factor of $\varphi(n)/n$, while still relying on the security of the Discrete Log Problem in $\mathbb{F}_p^\times$.

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 $T_{30}$ is birationally isomorphic to $A^8$.

The next useful case after that would be $n = 210$ (compression factor $8/35 \approx .23$). But this may be impractical for other reasons.
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

\[ y^2 = x^3 - x \]
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 \( \lambda := \begin{cases} \frac{y_2 - y_1}{x_2 - x_1} & \text{if } P_1 \neq P_2, \\ \frac{3x_1^2 + a}{2y_1} & \text{if } P_1 = P_2, \end{cases} \)

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)

\[ q + 1 - 2\sqrt{q} \leq |E(F_q)| \leq q + 1 + 2\sqrt{q}. \]

Therefore

\[ |E(F_q)| \approx q. \]

Theorem (Schoof 1985)

There is a polynomial-time algorithm for computing \(|E(F_q)|\).
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 $\ell$ 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 $\mu_\ell$, the group of $\ell$-th roots of unity in $\overline{\mathbb{F}}_q$.

**Definition**

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

**Fact**

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

**Theorem (Weil, Miller)**

There is a nondegenerate skew-symmetric bilinear pairing

\[ \langle \cdot, \cdot \rangle_\ell : E[\ell] \times E[\ell] \rightarrow \mu_\ell \]

that is computable in polynomial time.

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

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 \( q \mod \ell \) (Menezes, Okamoto & Vanstone 1993).
Suppose $C \subset E(\mathbb{F}_q)$ is a subgroup of order $\ell$, $P$ is a generator of $C$, and $Q \in E[\ell] - C$.

Define an injective homomorphism
\[
f : C \rightarrow \mathbb{F}_{q^k}^\times \quad \text{by} \quad f(R) = \langle R, Q \rangle_\ell \in \mu_\ell \subset \mathbb{F}_{q^k}^\times.
\]

Given $\{P, \lambda P\}$, compute
\[
\{f(P), f(\lambda P)\} = \{g, g^\lambda\}
\]
where $g = f(P)$ is a generator of $\mu_\ell \subset \mathbb{F}_{q^k}^\times$.

Compute $\lambda$ from $\{g, g^\lambda\}$, as a discrete log computation in $\mathbb{F}_{q^k}^\times$. 
Example: $y^2 = x^3 - x$

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 $\ell$ 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 $\mathbb{F}_q^\times$.

Thus to be secure in this case, we must have $q > 2^{512}$. 
Example: $y^2 = x^3 - x$

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 $p$ (mod $\ell$) is $\ell - 1$.
- The Weil pairing reduces computation of discrete logs in $E(\mathbb{F}_p)$ to computation of discrete logs in $\mathbb{F}_p^\times$.$^{\ell-1}$.

But $\ell > 2^{160}$, so we can’t even write down an element of $\mathbb{F}_p^\times$.$^{\ell-1}$, 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 $\ell$, and a point $Q \in E[\ell] - C$.
2. Alice chooses a secret integer $a$, $1 \leq a \leq \ell$.
3. Public information: $q$, $E$, $\ell$, $Q$, $aQ$.
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 $aM$. 
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 $\ell$ embeds into $\mathbb{F}_q^k$.)

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

\[
\begin{cases}
\text{supersingular} & \text{if } E[q] = 0, \\
\text{ordinary} & \text{if } E[q] \neq 0.
\end{cases}
\]
### Possible embedding degrees for supersingular elliptic curves:

<table>
<thead>
<tr>
<th>characteristic</th>
<th>embedding degrees</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>1, 2, 3, 4</td>
</tr>
<tr>
<td>3</td>
<td>1, 2, 3, 6</td>
</tr>
<tr>
<td>≥ 5</td>
<td>1, 2</td>
</tr>
</tbody>
</table>

- 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, . . . .
### 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 $\ell$) there is a Weil pairing

\[ A[\ell] \times A[\ell] \rightarrow \mu_\ell. \]
If $A$ is an abelian variety over $\mathbb{F}_q$, and $\ell$ 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 $A$.

An abelian variety over $\mathbb{F}_q$ is **supersingular** if it is isogenous over $\overline{\mathbb{F}}_q$ to a product of supersingular elliptic curves.
Theorem (Galbraith; Choie, Jeong & Lee; Rubin & Silverberg)

The largest security parameters of simple supersingular abelian varieties are:

<table>
<thead>
<tr>
<th>dimension</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
</tr>
</thead>
<tbody>
<tr>
<td>characteristic 2</td>
<td>4</td>
<td>6</td>
<td>5</td>
<td>6</td>
<td></td>
<td></td>
</tr>
<tr>
<td>characteristic 3</td>
<td>6</td>
<td>2</td>
<td>6</td>
<td>7</td>
<td>7</td>
<td></td>
</tr>
<tr>
<td>characteristic 5</td>
<td>2</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>characteristic 7</td>
<td>2</td>
<td>3</td>
<td>7</td>
<td>3</td>
<td>7</td>
<td></td>
</tr>
<tr>
<td>characteristic 11</td>
<td>2</td>
<td>3</td>
<td>3</td>
<td>2</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>characteristic $\geq 13$</td>
<td>2</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

(a blank entry means there are no simple supersingular abelian varieties of that dimension in that characteristic).
We construct supersingular abelian varieties with “optimal” security parameters in a way analogous to what we did with algebraic tori.

Recall the decomposition

$$\text{Res}_{F_p^n} G_m \sim \bigoplus_{d|n} T_d$$
Abelian varieties

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

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

Theorem

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

- $\text{Res}_{\mathbb{F}_q}^{\mathbb{F}_{q^n}} E \sim \bigoplus_{d \mid n} E_d$.
- $E_n(\mathbb{F}_q) \cong \{ P \in E(\mathbb{F}_{q^n}) : \text{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q} P = 0 \text{ for every } d \mid n, d \neq n \}$.
- $E_n$ 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 $2^{qk}$.

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

Karl Rubin (UC Irvine)  
Number Theory and Cryptography  
October 2006  
KMS Day  
44 / 51
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

- $E_5$ is a supersingular abelian variety of dimension 4
- the security parameter of $E_n$ is $6 \cdot (5/\varphi(5)) = 7\frac{1}{2}$. 
### Best supersingular security parameters

<table>
<thead>
<tr>
<th>dimension</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
</tr>
</thead>
<tbody>
<tr>
<td>characteristic 2</td>
<td>4</td>
<td>6</td>
<td>5</td>
<td>6</td>
<td></td>
<td></td>
</tr>
<tr>
<td>characteristic 3</td>
<td>6</td>
<td>2</td>
<td>6</td>
<td>7</td>
<td>7</td>
<td></td>
</tr>
<tr>
<td>characteristic 5</td>
<td>2</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>characteristic 7</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>3</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>characteristic 11</td>
<td>2</td>
<td>3</td>
<td>3</td>
<td>2</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>characteristic $\geq$ 13</td>
<td>2</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td></td>
</tr>
</tbody>
</table>

- $q = 3^d$, $d$ odd; $E : y^2 = x^3 - x \pm 1$; $n = 5$;
- $E_5$ has dimension 4 and security parameter $7\frac{1}{2}$. 
Some remarks on efficiency

\[ E_n \subset \text{Res}_{F_q}^{F_{q^n}} E, \text{ so} \]

\[ E_n(F_q) \subset E(F_{q^n}). \]

Therefore, even though \( E_n \) is a higher dimensional abelian variety, all computations in \( E_n(F_q) \) 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 $E_n(\mathbb{F}_q)$ is a proper subgroup of $E(\mathbb{F}_{q^n})$, and

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

Ideally one would like to represent an element of $E_n(\mathbb{F}_q)$ 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 $n = 2, 3, \text{ or } 5$ (Rubin & Silverberg 2002).

- The case $n = 2$ is not useful, because $E_2$ 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 $P \in E_n(\mathbb{F}_q) \subset E(\mathbb{F}_{q^n})$ by

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

- 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.)
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