Elliptic Curves and elliptic pair of primes

Liljana Babinkostova

Boise State University
Let \( G \) be a group and \( g \in G \). The *Discrete Log Problem* for \( G \) is:

Given an element \( b \in \langle g \rangle \), find an integer \( x \) satisfying \( b = g^x \).
Let $G$ be a group and $g \in G$. The *Discrete Log Problem* for $G$ is

Given an element $b \in \langle g \rangle$, find an integer $x$ satisfying $b = g^x$. 

Liljana Babinkostova  
Boise State University  
Elliptic Curves and elliptic pair of primes
Diffie-Hellman Key exchange protocol

Let $G$ be a group and $g \in G$.

1. Alice chooses secret integer $a < |g|$
2. Bob chooses secret integer $b < |g|
Diffie-Hellman Key exchange protocol

Let $G$ be a group and $g \in G$.

1. Alice chooses secret integer $a < |g|$.
2. Bob chooses secret integer $b < |g|$.
3. Alice computes $g^a = A$ and sends to Bob.
4. Bob computes $g^b = B$ and sends to Alice.

Alice and Bob share the secret value $B^a = (g^b)^a = g^{ab} = A^b$. 
**Diffie-Hellman Key exchange protocol**

Let $G$ be a group and $g \in G$.

1. Alice chooses secret integer $a < |g|$
2. Bob chooses secret integer $b < |g|$
3. Alice computes $g^a = A$ and sends to Bob.
4. Bob computes $g^b = B$ and sends to Alice.
5. Alice computes $B^a$.

Alice and Bob share the secret value

$$B^a = (g^b)^a = g^{ab} = (g^b)^a = A^b$$
Definition

An elliptic curve $E$ over a field $\mathbb{F}$ is the set

$$\{(x, y) \in \mathbb{F}^2 : y^2 = x^3 + ax + b, \ a, b \in \mathbb{F}\} \cup \{\infty\}$$

with the restriction that $4a^3 + 27b^2 \neq 0$. Notationally, once we have specified the field $\mathbb{F}$, we refer to $E$ as $E(\mathbb{F})$. 
The group law on an Elliptic Curve

- Adding points on an Elliptic Curve

**Figure:** The curve $y^2 = x^3 - 4x + 6$
The group law on an Elliptic Curve

- Doubling point on an Elliptic Curve
The point at infinity

Vertical lines have no third intersection point. This is where $\infty$, the point at infinity, comes in.
The group law on an Elliptic Curve

Theorem (Poincaré, ~1900)

The addition law on $E$ has the following properties

1. $K + \infty = \infty + K = K$ for all $K \in E(F)$
2. $K + (-K) = \infty$ for all $K \in E(F)$
3. $K + (L + P) = (K + L) + P$ for all $K, L, P \in E(F)$
4. $P + Q = Q + P$ for all $P, Q \in E(F)$
Theorem (Cassells, 1966)

Let $E$ be an elliptic curve over the finite field $\mathbb{F}_p$. Then

$$E(\mathbb{F}_p) \cong \mathbb{Z}^n$$

or

$$E(\mathbb{F}_p) \cong \mathbb{Z}^{n_1} \times \mathbb{Z}^{n_2}$$

for some integer $n \geq 1$, or for some integers $n_1, n_2 \geq 1$ with $n_1$ dividing $n_2$. 
Theorem (Cassells, 1966)

Let $E$ be an elliptic curve over the finite field $\mathbb{F}_p$. Then

$$E(\mathbb{F}_p) \cong \mathbb{Z}_n \text{ or } E(\mathbb{F}_p) \cong \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2}$$

for some integer $n \geq 1$, or for some integers $n_1, n_2 \geq 1$ with $n_1$ dividing $n_2$. 
Theorem (Hasse, 1933)

Let $E$ be an elliptic curve over the finite field $\mathbb{F}_p$. Then the order of $E(\mathbb{F}_p)$ satisfies

$$|p + 1 - \#E(\mathbb{F}_p)| \leq 2\sqrt{p}$$
The group order of an Elliptic Curve

Theorem (Hasse, 1933)

Let $E$ be an elliptic curve over the finite field $\mathbb{F}_p$. Then the order of $E(\mathbb{F}_p)$ satisfies

$$|p + 1 - \#E(\mathbb{F}_p)| \leq 2\sqrt{p}$$

Theorem (Deuring, 1941)

For any $n$ such that $|n - p - 1| < 2\sqrt{p}$ there exists some elliptic curve $E(\mathbb{F}_p)$ such that $\#E(\mathbb{F}_p) = n$. 

Liljana Babinkostova

Elliptic Curves and elliptic pair of primes
Computing the order of $E(\mathbb{F}_p)$

- “Quadratic Residue” method
- Schoof’s algorithm
- SEA algorithm
Elliptic Pair of Primes

Definition

1. The primes $p$ and $q$ are called an **elliptic pair** if for two curves $E(\mathbb{F}_p)$ and $E(\mathbb{F}_q)$, the following is true

   $$|E(\mathbb{F}_p)| = q$$

   $$|E(\mathbb{F}_q)| = p$$

---

Elliptic curves are used in cryptography and these systems’ security often depends on the difficulty of computing the order of the elliptic curve group.
Elliptic curves are used in cryptography and these systems’ security often depends on the difficulty of computing the order of the elliptic curve group.

- Would finding the order of $|E(\mathbb{F}_p)|$ be easier if it is known that the prime $p$ form an elliptic pair?
Elliptic curves are used in cryptography and these systems’ security often depends on the difficulty of computing the order of the elliptic curve group.

- Would finding the order of $|E(\mathbb{F}_p)|$ be easier if it is known that the prime $p$ form an elliptic pair?
- Can properties of these elliptic pairs affect the security of the cryptosystems?
Elliptic curves are used in cryptography and these systems’ security often depends on the difficulty of computing the order of the elliptic curve group.

- Would finding the order of $|E(\mathbb{F}_p)|$ be easier if it is known that the prime $p$ form an elliptic pair?
- Can properties of these elliptic pairs affect the security of the cryptosystems?
- What properties do these elliptic pairs have?
The Frequency Data

10 digit primes

The 10 digit primes (all 5083 of them)
The Frequency Data

20 digit primes

Cumulative Total of Elliptic Primes

Consecutive 20-digit primes which were surveyed (19000+)}
Consider the elliptic curve $E(\mathbb{F}_p)$ where $E$ is the elliptic curve $y^2 = x^3 + b$.

**Conjecture**

If each integer $b < p$ which produces a prime order is a primitive root of $p$, then exactly two such prime orders are produced for the prime $p$.

**Conjecture**

If the primes $p, q$ form an elliptic pair, then $p$ is congruent to $q$ modulo 4.