CS 355 – Topics in Cryptography May 16, 2018

Lecture 14: Elliptic Curves Cryptography

Instructors: Henry Corrigan-Gibbs, Sam Kim, David J. Wu

1 Why Elliptic Curves?

We use discrete log based assumptions such as DLog, CDH, and DDH all over cryptography. However, unlike factoring based problems, the discrete log based problems are defined with respect to *some* cyclic group of prime order $\mathbb{G}$. There are definitely some groups for which the discrete log problem is easy. For instance, consider the *additive* prime ordered group $\mathbb{G} = (\mathbb{F}_q, +)$ for q prime. Given a generator $x \in \mathbb{F}_q$, and a random element $y \in \mathbb{F}_q$, it is easy to compute $c \in \mathbb{F}_q$ for which $c \cdot x = y$ by simply computing $c = x^{-1} \cdot y \mod q$.

When Diffie and Hellman first proposed the Diffie-Hellman key exchange protocol, the group that they proposed was the *multiplicative* group $\mathbb{G} = (\mathbb{F}_p^*, \times)$ for p prime. More precisely, if p is a special prime of the form $p = 2q + 1$ where q is prime, then the order of $\mathbb{F}_p^*$ is $p - 1 = 2q$. Hence, $\mathbb{F}_p^*$ contains a subgroup $\mathbb{G}'$ of order q, which is the actual prime ordered group that one would use. For simplicity, let's just refer to this group as $\mathbb{F}_p^*$ without worrying about subgroups.

The group $\mathbb{F}_p^*$ is very simple and the discrete log problem is conjectured to be hard. However, the discrete log problem is not as hard as we would like in that there are *subexponential* time algorithms that solve discrete log in $\mathbb{F}_p^*$ in time roughly $2^{\widetilde{O}(\sqrt[3]{\log p})}$.[1] Hence, to get $\lambda = 128$ bits of security, NIST proposes people to use 3092 bit modulus p. This means that the representation of each group element must be at least 3092 bits, and the algebraic operations must operate on 3092 bit numbers, which is not ideal.

Hence, we can ask the following question:

> **Question**: Are there other groups with more efficient group representations/operations where discrete log is hard?

Since Diffie and Hellman published their papers, people started searching for more efficient groups to use for the Diffie-Hellman protocol. Most groups that people came up with either had easy discrete log problem or did not provide any real advantage in terms of efficiency over $\mathbb{F}_p^*$. One exception was the *elliptic curve groups*, which were proposed in the mid 1980's.

An elliptic curve is basically a formula of the following form:

$$y^2 = x^3 + Ax + B.$$

Let $\mathbb{F}_q$ be a finite field. Then, the elliptic curve group that people use for cryptography is the set

$$E_{A,B}(\mathbb{F}_p) = \left\{(x, y) \in \mathbb{F}_p : y^2 = x^3 + Ax + B\right\} \cup \{\infty\}.$$

We can define a suitable group operation such that the set above is a group. In this group, the best attack on the discrete log problem runs in *exponential time* $O(2^{\frac{1}{2}\log p})$. Hence, to get $\lambda = 128$ bits of security, we just need to use a 256 bit prime. Note that each group element consists of two field elements $x, y \in \mathbb{F}_p$, which means that it only requires 512 bits to represent them. With optimization, each group element can be represented by ≈ 256 bits.

[1] The notation $\widetilde{O}(\cdot)$ is the same as the big-O notation $O(\cdot)$ but without any log terms.

2 Where do Elliptic Curves come from?

In mathematics, there are a couple of number systems $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$. Since the Greek era, mathematicians are interested in finding solutions to equations (equations are sometimes called *curves*) over a specific number system.

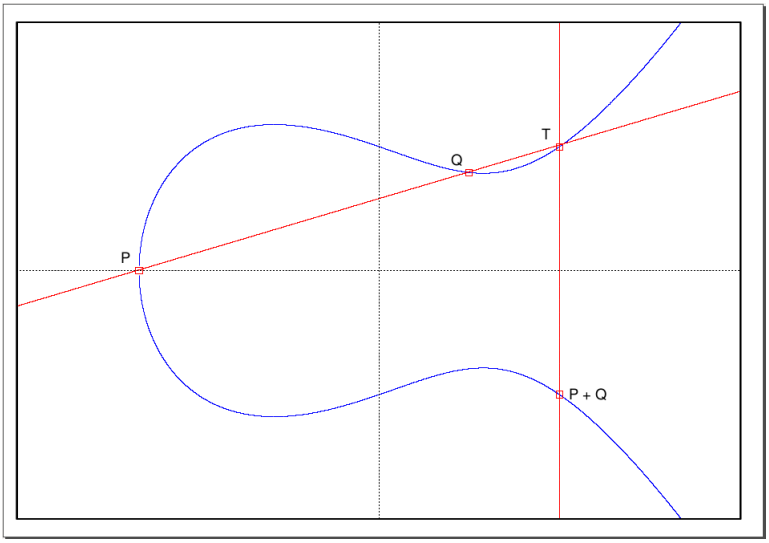
- Find rational solutions $(x, y) \in \mathbb{Q} \times \mathbb{Q}$ such that $x^2 + y^2 = 1$. This question was studied by Pythagoras.
- Find integer solutions $(x, y, z) \in \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}$ such that $x^3 + y^3 = z^3$. The famous *Fermat's Last Theorem* says that there does not exist any positive integer solutions to this equation.
- Find rational solutions $(x, y) \in \mathbb{Q} \times \mathbb{Q}$ such that $y^2 = x^3 - x + 9$. This question was studied by Diophantus.

The equation $y^2 = x^3 - x + 9$ that Diophantus studied is an example of an elliptic curve. Let's convince ourselves that finding rational solutions to this equation is not trivial. To find rational solutions to this equation, the most obvious thing to try is to randomly plug in rational values of x and see if we get rational values of y.

- If we set $x = 0$, then we have $y^2 = 9$. Hence, $(0, 3)$ and $(0, -3)$ are rational solutions to this equation.
- If we set $x = 1$, then again, we have $y^2 = 9$. Hence, $(1, 3)$ and $(1, -3)$ are rational solutions to this equation.
- If we set $x = 2$, then we have $y^2 = 15$. However, $\sqrt{15}$ is not a rational number.

In fact, it is easy to check that $(-1, \pm 3)$, $(0, \pm 3)$, $(1, \pm 3)$ are rational solutions to $y^2 = x^3 - x + 9$, but it is not clear how to get more rational solutions to this equation. Diophantus asked the following question: Is there a more systematic way of enumerating all solutions in $\mathbb{Q} \times \mathbb{Q}$ for the equation $y^2 = x^3 - x + 9$?

Let's just draw out the curve $y^2 = x^3 - x + 9$. Elliptic curves generally have the following form.



Diophantus made the following observation:

1. **Observation 1**: Say you know 2 rational points $(x_0, y_0), (x_1, y_1) \in \mathbb{Q} \times \mathbb{Q}$ on the curve. Then, it is possible to get a third rational point on the curve by drawing a line that intersects the curve at the two points $(x_0, y_0), (x_1, y_1)$, and finding a third intersecting point (x_2, y_2) on the curve. It turns out that (x_2, y_2) is also a rational solution contained in $\mathbb{Q} \times \mathbb{Q}$.

2. **Observation 2**: Say you know 1 rational point $(x, y) \in \mathbb{Q} \times \mathbb{Q}$ on the curve. Then, the point $(x, -y)$ is also a rational point on the curve.

Diophantus observed that starting from a finite set of points on the curve like $(-1, \pm 3)$, $(0, \pm 3)$, $(1, \pm 3)$, by incorporating observation 1 and observation 2, one can get many more rational solutions to the equation.

Let us denote $\tilde{E}(\mathbb{Q}) \subset \mathbb{Q} \times \mathbb{Q}$ to be the set of all rational solutions to $y^2 = x^3 - x + 9$. What Diophantus observed was that combining (1) "draw line" + (2) "flip y" gives a "mapping" $* : \tilde{E}(\mathbb{Q}) \times \tilde{E}(\mathbb{Q}) \to \tilde{E}(\mathbb{Q})$. Then, it is natural to ask then whether the set $\tilde{E}(\mathbb{Q})$ along with the mapping $*$ forms a group.

It turns out that $\tilde{E}(\mathbb{Q})$ and $*$ almost forms a group. If you add a special point called the point at ∞, then $E(\mathbb{Q}) = \tilde{E}(\mathbb{Q}) \cup \{\infty\}$ forms a group with operation $*$. We add the point at infinity ∞ because the slope between two points in $\tilde{E}(\mathbb{Q})$ might not be well defined.

Therefore, we define the group operation $* : E(\mathbb{Q}) \times E(\mathbb{Q}) \to E(\mathbb{Q})$ as follows:

- Say $(x_0, y_0), (x_1, y_1) \in E(\mathbb{Q}) \setminus \{\infty\}$, then
    1. If slope between the these two points are well-defined, we apply the (1) "draw line" + (2) "flip y".
    2. If slope is not well-defined, then output the special point at infinity ∞.
- For any point $(x, y) \in E(\mathbb{Q}) \setminus \{\infty\}$,
    1. Define $\infty * (x, y) \to (x, y)$
    2. Define $(x, y) * \infty \to (x, y)$
    3. Define $\infty * \infty \to \infty$

Then, the set $E(\mathbb{Q})$ and the mapping $*$ forms an abelian group.

General elliptic curves. We define an elliptic curve

$$y^2 = x^3 + Ax + B$$

where $4a^3 + 27b^2 \neq 0$. It turns out that the observation that Diophantus made applies to general elliptic curves.

Fact 2.1. The set $E_{A,B}(\mathbb{Q}) = \left\{(x, y) \in \mathbb{Q} \times \mathbb{Q} : y^2 = x^3 + Ax + B\right\} \cup \{\infty\}$ and the operation $*$ forms an abelian group.

The fact above, in fact, generalizes when we switch $\mathbb{Q}$ to a finite field $\mathbb{F}_p$.

Fact 2.2. The set $E_{A,B}(\mathbb{F}_p) = \left\{(x, y) \in \mathbb{F}_p \times \mathbb{F}_p : y^2 = x^3 + Ax + B\right\} \cup \{\infty\}$ and the operation $*$ forms an abelian group.

The operation $*$ has to be slightly modified since we are not working over $\mathbb{Q}$, but the main ideas remains unchanged.

Remarks. Let us conclude with some remarks:

- Given a curve $y^2 = x^3 + Ax + B$ and $\mathbb{F}_p$, it is possible to efficiently compute the order $|E_{A,B}(\mathbb{F}_p)|$. This is related to the Hasse-Weil bound, and Schoof's algorithm.
- We can generate A, B, p such that $|E_{A,B}(\mathbb{F}_p)| \approx p$.
- There are lots of ways to optimize the group representation and group operation.

3 Additional Structure on Elliptic Curves: Pairings

We will talk more about pairings next lecture.