CS 355: Topics in Cryptography **Spring 2019**

Lecture 12: Elliptic Curves

Dima Kogan

1 Why Elliptic Curves?

We use discrete log based assumptions such as DLog, CDH, and DDH all over cryptography. 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. 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 $2^{\widetilde{O}(\sqrt[3]{\log p})}$. 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.

Since Diffie and Hellman published their papers, people started searching for other groups to use for the Diffie-Hellman protocol. They were looking for groups for which: (i) the group elements have compact representation ;(ii) the group operation can be implemented efficiently, and (iii) the discrete-log problem is hard. Ideally, the best discrete-log algorithm on the group should be no better than the generic algorithms (e.g., Pollard Rho).

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 $\mathbb{F}_p^*$.

In 1985 Neal Koblitz [1] and Victor S. Miller [2], inspired by an earlier work by Lenstra[1], independently suggested using the group of points on an elliptic curve as an alternative to $\mathbb{F}_p^*$ for key exchange.

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

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

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

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

where $\mathcal{O}$ is a special point called *point in infinity* (we will see why). 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 $O(\sqrt{p})$. 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.

2 Where do Elliptic Curves come from?

Throughout history, mathematicians have been interested in finding solutions to equations (or points on *curves*) of certain properties:

[1] Lenstra used elliptic curves for cryptanalysis: he gave a new factoring algorithm for $\mathbb{F}_p^*$ using elliptic curves [3].

- 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 last question gives rise to the theory of elliptic curves, but for simplicity, let's look at the first question, which is simpler but conveys some of the ideas.

2.1 A Simpler Analogue: The Group of Rational Points on The Unit Circle

Observe that the rational points on the unit circle are in correspondence with Pythagorean triples:

$$a^2 + b^2 = c^2 \iff \left(\frac{a}{c}\right)^2 + \left(\frac{b}{c}\right)^2 = 1\,.$$

Given two rational points (a, b), (c, d) on the unit circle, we can obtain a new point as following:

$$(a, b) \boxplus (c, d) = (ac - bd, ad + bc)\,,$$ [2]

and one can easily verify that $e^2 + f^2 = 1$. The point $(1, 0)$ is an identity element:

$$(a, b) \boxplus (1, 0) = (a, b)\,,$$

and each element has an inverse:

$$(a, b) \boxplus (a, -b) = (a^2 + b^2, -ab + ab) = (1, 0)\,.$$

This group operation also has a geometric construction, as it corresponds to angle addition (see Figure 1), and the addition law then follows from sine and cosine addition formulas.

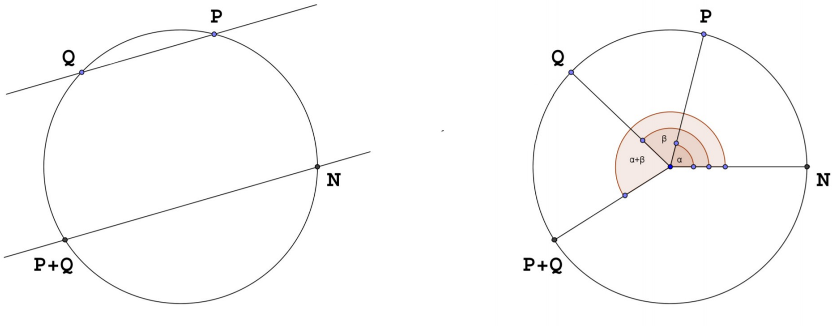


Figure 1: The group of rational point on the unit circle.
Image from: F. Lemmermeyer, Pell Conics,
https://www.mathi.uni-heidelberg.de/~flemmermeyer/pell/bfc02.pdf

[2] We use a the $\boxplus$ symbol to emphasize that this is not addition in $\mathbb{Q}^2$.

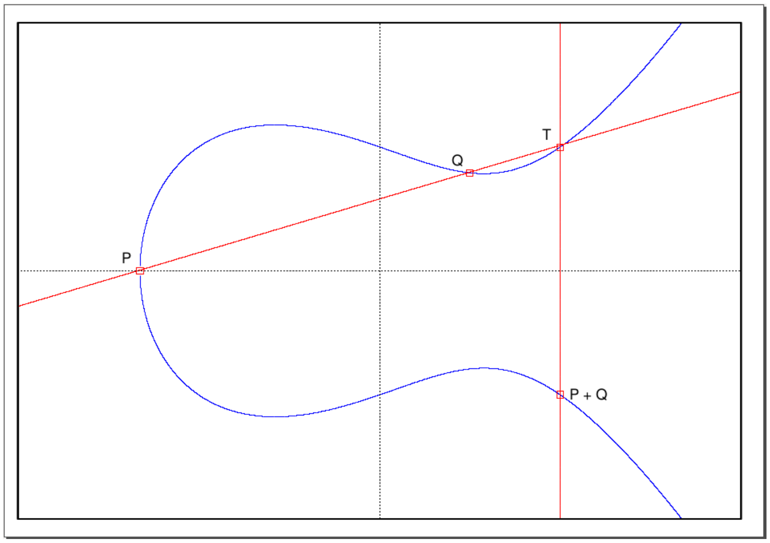
3 Elliptic curves over $\mathbb{Q}$

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 $y^2 = x^3 - x + 9$, or more generally $y^2 = x^3 + Ax + B$. Consider then the addition operation $\boxplus : \tilde{E}(\mathbb{Q}) \times \tilde{E}(\mathbb{Q}) \to \tilde{E}(\mathbb{Q})$, defined as (1) "draw line"

+ (2) “flip y” . Then, it is natural to ask then whether the set $\tilde{E}(\mathbb{Q})$ under this addition operation forms a group.

It turns out that it almost does, but we are missing the identity element. If you add a special point $\mathcal{O}$ called the point at ∞, then $E(\mathbb{Q}) = \tilde{E}(\mathbb{Q}) \cup \{\mathcal{O}\}$ forms a group.

- Identity element: by definition, for any point $P \in E(\mathbb{Q})$, we have $\mathcal{O} \boxplus P = P \boxplus \mathcal{O} = P$.
- Inverses: for every point $P = (x, y) \in E(\mathbb{Q})$, we define $-P = (x, -y)$, and extend our addition rule such that $P \boxplus (-P) = \mathcal{O}$. (Indeed our “draw line & flip” rule is not well-defined for $P \boxplus (-P)$ since the line between P and $-P$ does not intersect the curve at a third point.)
- Associativity: it can be shown that for every $P, Q, R \in E(\mathbb{Q})$, it holds $P \boxplus (Q \boxplus R) = (P \boxplus Q) \boxplus R$.

The geomtric addition rule can also be expressed algebraically. For example for $P = (x_1, y_1), Q = (x_2, y_2) \in E(\mathbb{Q})$ such that $P \neq \pm Q$ and $P, Q \neq \mathcal{O}$, the slope of the line between P and Q is

$$m = \frac{y_2 - y_1}{x_2 - x_1}, \tag{1}$$

and the equation of the line is

$$y = m(x - x_1) + y_1 .$$

To find the intersection with E, substitute into the curve equation:

$$(m(x - x_1) + y_1)^2 = x^3 + Ax + B .$$

This can be rearranged as:

$$0 = x^3 - m^2 x^2 + \cdots .$$

This is not easy to solve, but we know two out of the three roots of this degree-three polynomial, namely P and Q (since they are by definition on the intersection of the line with the curve). And therefore

$$x^3 - m^2 x^2 + \cdots = (x - x_1)(x - x_2)(x - x_3) = x^3 - (x_1 + x_2 + x_3)x^2 \ldots ,$$

so

$$x_3 = m^2 - x_1 - x_2$$

and

$$\tilde{y}_3 = m(x_3 - x_1) + y_1 .$$

Reflecting across the x-axis, we get that

$$P \boxplus Q = (x_3, y_3) \quad \text{where} \quad x_3 = m^2 - x_1 - x_2 \quad \text{and} \quad y_3 = m(x_1 - x_3) - y_1 . \tag{2}$$

The other cases can be handled similarly. For example for $P \boxplus P$ we need to take the tangent to the curve instead of the chord between P and Q.

4 Elliptic Curves Over Finite Fields

Similarly to $E(\mathbb{Q})$, we can consider all points on the curve

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

over the finite field $\mathbb{F}_p$. This gives rise to the *finite* group $E(\mathbb{F}_p)$.

For example, consider the curve $E\colon\ y^2 = x^3 + x + 1$ over $\mathbb{F}_5$. Recall that since 5 is a prime, $\mathbb{F}_5$ is the set $\{0, 1, 2, 3, 4\}$ with addition and multiplication modulo 5.

x	$x^3 + x + 1$	y	Points
0	1	± 1	$(0,1), (0,4)$
1	3	$-$	$-$
2	1	± 1	$(2,1), (2,4)$
3	1	± 1	$(3,1), (3,4)$
4	4	± 2	$(4,2), (4,-2)$
∞		∞	$\mathcal{O}$

Thus, $E(\mathbb{F}_5)$ has order 9. We denote $|E(\mathbb{F}_5)| = 9$ (or sometimes $\#E(\mathbb{F}_5) = 9$). We can use the addition formula from Equations 1 and 2 to compute $(3,1) \boxplus (2,4)$ on E:

$$m = \frac{4-1}{2-3} = \frac{3}{-1} = -3 = 2 \pmod 5$$

$$x_3 = 2^2 - 3 - 2 = 4 \qquad y_3 = 2(3-4) - 1 = 2,$$

so $(3,1) \boxplus (2,4) = (4,2)$.

5 Some important properties

1. The general case we consider is a curve

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

where $4A^3 + 27B^2 \neq 0$. If this condition does not hold, then the curve has a multiple root, and the curve is called singular.

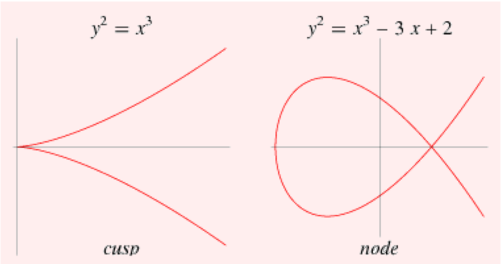


Figure 2: Singular Elliptic Curves. From: http://mathworld.wolfram.com/EllipticDiscriminant.html

2. The group $E(\mathbb{F}_p)$ is commutative (aka Abelian): $P \boxplus Q = Q \boxplus P$ for every $P, Q \in E(\mathbb{F}_p)$.

3. Hasse's Theorem: the order of $E(\mathbb{F}_p)$ satisfies:

$$|E(\mathbb{F}_p)| = p + 1 - t\,,$$

where $|t| \leq 2\sqrt{p}$. Moreover, it is possible to efficiently compute the order $|E(\mathbb{F}_p)|$ using an algorithm by Schoof.

4. The interesting case from a cryptographic perspective is when $|E(\mathbb{F}_p)|$ has a large prime factor and thus contains a large cyclic subgroup. Such curves can in fact be efficiently generated.

5. For $\alpha \in \mathbb{N}$ and a point $P \in E(\mathbb{F}_p)$, we denote $\alpha P := \underbrace{P \boxplus P \boxplus \ldots \boxplus P}_{\alpha \text{ times}}$.

6 Elliptic-Curve Cryptography

Public Parameters. A prime p, parameters $A, B \in \mathbb{F}_p$ such that $E\colon\ y^2 = x^3 + Ax + B$ is an elliptic curve, a point $P \in E(\mathbb{F}_p)$ of large prime order q (i.e., $qP = \mathcal{O}$), the order q.

Elliptic-Curve Discrete Log. Given $P, \alpha P \in E(\mathbb{F}_p)$ where $\alpha \xleftarrow{R} \mathbb{Z}_q$, find α. For most elliptic curves, the best known algorithm for this problem runs in time $\Omega(\sqrt{q})$. There are exceptions, so to avoid the pitfall of choosing an insecure curve, many implementations use a fixed set of curves.

DH Key Exchange. Alice chooses $\alpha \xleftarrow{R} \mathbb{Z}_q$, computes and sends $Q_A = \alpha P$. Bob chooses $\beta \xleftarrow{R} \mathbb{Z}_q$, computes and sends $Q_B = \beta P$. The shared secret is $\alpha\beta P$.

7 Examples of Elliptic Curves Used in Practice

The NIST Curve P256. Standardized by NIST in 1999. All implementations of TLS 1.3 are required to support this curve for DH key exchange. The curve P256 is defined over the prime $p := 2^{256} - 2^{224} + 2^{192} + 2^{96} - 1$. The curve has the form $y^2 = x^3 - 3x + b$ where

$$b := \text{5ac635d8 aa3a93e7 b3ebbd55 769886bc 651d06b0 cc53b0f6 3bce3c3e 27d2604b}.$$

The standard also specifies a generator point. The parameter b was generated using some public deterministic algorithm run on a seed S. We don't know how S was selected, which some people find worrying.

Curve 25519. This is another popular curve designed by Dan Bernstein to have additional security properties. It is defined over the prime $p := 2^{255} - 19$, hence its name. This p is the largest prime less than 2^{255}. The curve has the form:

$$y^2 = x^3 + 486662x^2 + x\,.$$

Notice that this is not in the standard form we have discussed (it has a x^2 term). It is called Montgomery form which is useful for implementation.

References

[1] N. Koblitz, “Elliptic curve cryptosystems,” *Mathematics of computation*, vol. 48, no. 177, pp. 203–209, 1987.

[2] V. S. Miller, “Use of elliptic curves in cryptography,” in *CRYPTO ’85*, 1985.

[3] H. W. Lenstra, “Factoring integers with elliptic curves,” *The Annals of Mathematics*, vol. 126, no. 3, p. 649, nov 1987. [Online]. Available: https://doi.org/10.2307%2F1971363

[4] S. Kim, “CS355 lecture notes,” 2018, https://crypto.stanford.edu/cs355/18sp/lec14.pdf.

[5] D. Boneh and V. Shoup, “A graduate course in applied cryptography,” 2019. [Online]. Available: https://crypto.stanford.edu/~dabo/cryptobook/

[6] D. Hankerson, A. J. Menezes, and S. Vanstone, “Guide to elliptic curve cryptography,” *Computing Reviews*, vol. 46, no. 1, p. 13, 2005.

[7] T. R. Shemanske, *Modern Cryptography and Elliptic Curves: A Beginner’s Guide*. American Mathematical Soc., 2017, vol. 83.

[8] S. D. Galbraith, *Mathematics of Public Key Cryptography*. Cambridge University Press, 2012. [Online]. Available: https://www.math.auckland.ac.nz/~sgal018/crypto-book/crypto-book.html

[9] A. Sutherland, “Lecture notes on elliptic curves,” 2019, https://math.mit.edu/classes/18.783/2019/LectureNotes10.pdf.