Elliptic-curve Cryptography

Luciano Maino

University of Bristol - Advanced Cryptology

1 Why do we need elliptic curve cryptography?

In 1976, Whitfield Diffie and Martin Hellman published a paper that completely reshaped the field of cryptography [4]. In their seminal work "New Directions in Cryptography", they described a revolutionary idea that allows for secure communication over untrusted channels, laying the foundation for what is now known as *public-key cryptography*.

The world's first public-key encryption was *RSA*. Roughly speaking, the security of RSA is based on the problem of factoring large integers. It is known that this problem can be solved in subexponential time (see, for instance, [6]). This implies that to have secure RSA instances, one needs to use significantly large integers, which results in longer messages. A solution to this issue is to use the efficient arithmetic of elliptic curves.

In this lecture, we will:

1. define elliptic curves;
2. describe their group law;
3. discuss the hardness of the Elliptic Curve Discrete Logarithm Problem (ECDLP) providing an example of a secure and fast elliptic curve;
4. introduce the concept of pairing and briefly touch upon its role in elliptic-curve cryptography.

2 Elliptic curves

We first introduce the notion of an *elliptic curve*. Bear in mind that elliptic curves can be defined in several equivalent ways. Proving that such definitions are equivalent is a highly non-trivial task. In this course, we will take a "cryptographic approach", meaning that we will simplify the definitions and concentrate on their computational aspects.

Definition 1 (Simplified). *Let K be a field of characteristic $\neq 2, 3$. An elliptic curve E is a curve defined by the equation*

$$E : y^2 = x^3 + ax + b,$$

where $a, b \in K$ and $27b^2 + a^3 \neq 0$.

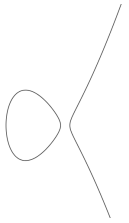

Fig. 1. The curve $E : y^2 = x^3 - x + 1$ defined over $\mathbb{Q}$.

Why do we need the condition $27b^2 + a^3 \neq 0$? This is to ensure that the curve is "smooth" and not "singular". Let's formalise this concept mathematically.

A natural way to look at elliptic curves is as curves into a projective space, the space $\mathbb{P}^2(K)$:

$$\mathbb{P}^2(K) := \{(x, y, z) \mid (x, y, z) \neq (0, 0, 0),\, x, y, z \in K\}_{/\sim},$$

where $(x, y, z) \sim (x', y', z')$ if there exists $\lambda \in K^*$ such that $x' = \lambda x$, $y' = \lambda y$ and $z' = \lambda z$.

Given the elliptic curve $E : y^2 = x^3 + ax + b$, we can *homogenise* its equation by considering $x \rightsquigarrow X/Z$ and $y \rightsquigarrow Y/Z$, i.e. we rewrite E as

$$E : ZY^2 = X^3 + aXZ^2 + bZ^3.$$

Now, let us consider the polynomial $F(X, Y, Z) = ZY^2 - X^3 - aXZ^2 - bZ^3$. The elliptic curve E is *non-singular* if Equation 1 has no solutions in $\mathbb{P}^2(K)$.

$$\begin{cases} \frac{\partial F}{\partial X}(X, Y, Z) = 0 \\ \frac{\partial F}{\partial Y}(X, Y, Z) = 0 \\ \frac{\partial F}{\partial Z}(X, Y, Z) = 0 \\ F(X, Y, Z) = 0 \end{cases} \tag{1}$$

This boils down to imposing $27b^2 + a^3 \neq 0$.

Given an elliptic curve $E : y^2 = x^3 + ax + b$, we can rewrite E in an equivalent form by performing this change of variables:

$$x \rightsquigarrow u^2x' + r, \quad y \rightsquigarrow u^3y' + su^2x' + t,$$

where $r, s, t \in K$ and $u \in K^*$.

Remark 2. After performing such a change of variable, we might end up with an elliptic curve of a form different from the one introduced in Definition 1. Elliptic curves in different forms may have some advantages compared to others with respect to certain applications.

Curves written in equivalent forms under this transformation can be identified by the notion of *j-invariant*. Given an elliptic curve $E : y^2 = x^3 + ax + b$, its j-invariant can be computed as

$$j(E) = 1728\frac{4a^3}{4a^3 + 27b^2}.$$

3 Group Law

The main reason elliptic curves are widely adopted in cryptography is because they enjoy a nice group structure. Let us briefly recall the notion of group.

Definition 3. *Let G be a non-empty set and let $*\colon G \times G \to G$ be a binary operation. The datum $(G, *)$ is a group if:*

1. *for all $a, b, c \in G$, $a * (b * c) = (a * b) * c$;*
2. *there exists an element e (called the* neutral element*) such that for all $a \in G$, $e * a = a * e$;*
3. *for each $a \in G$, there exists an element $b \in G$ such that $a * b = b * a = e$.*

Moreover, we will say that $(G, *)$ is abelian *if for all $a, b \in G$ $a * b = b * a$.*

For the rest of this section, let $E : y^2 = x^3 + ax + b$ be an elliptic curve. We will now show (without proving it) that elliptic curves are abelian groups via the *line-tangent* rule (cfr. Figures 2 and 3).

Let $P = (x_P, y_P), Q = (x_Q, y_Q) \in E$ be two distinct points such that $y_P \neq \pm y_Q$. We can "sum" P and Q as follows. We first draw the line a connecting P and Q. Such a line will intersect E at another point; define this point to be $S = (x_S, y_S)$. The point $P \oplus Q = (x_S, -y_S)$. Mathematically, we have that

$$\begin{cases} x_{P\oplus Q} = \left(\frac{y_Q - y_P}{x_Q - x_P}\right)^2 - x_P - x_Q \\ y_{P\oplus Q} = \left(\frac{y_Q - y_P}{x_Q - x_P}\right)(x_P - x_{P\oplus Q}) - y_P \end{cases}. \tag{2}$$

What happens when $y_P = -y_Q$? In this case, we necessarily have that $x_P = x_Q$. The point P is then equal to the inverse of Q. But, what's the neutral point for E? We need a distinguished point ∞. In other words $(x_P, y_P) \oplus (x_P, -y_P) = \infty$. Moreover, for all $S \in E$, $S \oplus \infty = S$.

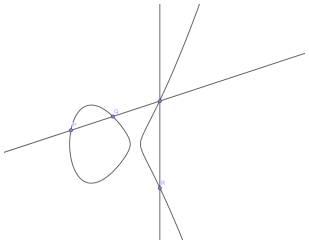

Fig. 2. Point addition. Here, we have $R = P \oplus Q$.

Remark 4. When considering the projective form of E, i.e. $E : ZY^2 = X^3 + aXZ^2 + bZ^3$, points on E are represented by projective triples (X, Y, Z). In particular, the identity element is represented by $(0, 1, 0)$.

What's the advantage of considering projective points? We can avoid inversions when summing two points. Inversions are usually very expensive operations to perform.

It remains now to deal with the case $P \oplus P$, where $y_P \neq 0$.[1] In this case, rather than having a line passing through two points, we consider the tangent line at P and repeat the same reasoning as above. Mathematically, we have

$$\begin{cases} x_{P\oplus P} = \left(\frac{3x_P^2+a}{2y_P}\right)^2 - 2x_P \\ y_{P\oplus P} = \left(\frac{3x_P^2+a}{2y_P}\right)(x_P - x_{P\oplus P}) - y_P \end{cases}. \tag{3}$$

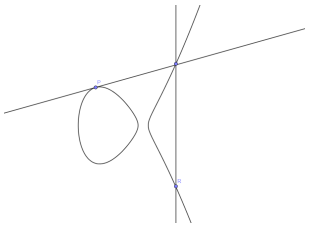

Fig. 3. Point doubling. Here, we have $R = P \oplus P$.

Remark 5. By looking at Figure 2, we could convince ourselves that $P \oplus Q = Q \oplus P$. Proving that, for all $P, Q, R \in E$, we have $P \oplus (Q \oplus R) = (P \oplus Q) \oplus R$ is a non-trivial task.

For each $n \in \mathbb{Z}$ we define $[n]P$ to be

$$\begin{cases} \underbrace{P \oplus \ldots \oplus P}_{n-\text{times}} & \text{if} \quad n > 0, \\ [-n]P & \text{if} \quad n < 0, \\ \infty & \text{if} \quad n = 0. \end{cases}$$

4 Elliptic curves defined over finite fields

We now specialise to the case where elliptic curves are defined over a finite field $\mathbb{F}_q$, where $q = p^n$ for some prime $p > 3$. Let E be an elliptic curve defined over $\mathbb{F}_q$. We define

$$E(\mathbb{F}_q) = \{(x, y) \in E \mid x, y \in \mathbb{F}_q\} \cup \{\infty\}.$$

The set $E(\mathbb{F}_q)$ enjoy a nice structure of abelian group. It is possible to prove that

$$E(\mathbb{F}_q) \simeq \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z},$$

where n_1 divides n_2 and $q - 1$ [5, §3.12]. Moreover, we have an upper bound on the cardinality of $E(\mathbb{F}_q)$:

$$\#E(\mathbb{F}_q) = q + 1 - t,$$

[1] What happens when $y_P = 0$?

where $\mid t \mid \leq 2\sqrt{q}$. The quantity t is called the *trace of Frobenius at* q [5, Thm. 3.61 (Hasse's Theorem)]. Moreover, if $\gcd(m, q) = 1$, we have that

$$E(\overline{\mathbb{F}_q})[m] := \left\{P \in E(\overline{\mathbb{F}_q}) \mid [m]P = \infty\right\} \simeq \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}.$$

Given an elliptic curve E, the group order $\#E(\mathbb{F}_q)$ can be computed efficiently. However, algorithms to do so are complicated to explain and out of scope.

5 The Elliptic Curve Discrete Logarithm Problem

Given a point $P \in E$ we say that P has *order* n if n is the smallest positive integer such that $[n]P = \infty$.

So far, we have seen that given a point $P \in E$, computing $[m]P$ can be done efficiently. However, what can we say about the converse?

Definition 6 (ECDLP). *Let E be an elliptic curve defined over $\mathbb{F}_q$ and let $P \in E(\mathbb{F}_q)$. Suppose we are given a point Q which is equal to $[m]P$ for some $m \in \mathbb{Z}$. The* Elliptic Curve Discrete Logarithm Problem (ECDLP) *asks to find any $m' \in \mathbb{Z}$ such that $[m']P = Q$.*

It is clear that the difficulty of solving this problem depends on the order of P. To be more precise, the complexity of this problem is defined by the largest prime factor dividing the order of P (cfr. Pohlig-Hellman). Therefore, the hardest instance for the ECDLP is when P has order ℓ, where ℓ is a large prime. But how large?

It turns out that the best known algorithm to attack the ECDLP takes $\approx \sqrt{\ell}$ field operations. This can be achieved using the Pollard's ρ-method.

The order of the point P must divide $\#E(\mathbb{F}_q)$. As a result, a "nice" curve for cryptographic application should have $\#E(\mathbb{F}_q) \approx \ell$. As we have seen in Section 4, we have that $\#E(\mathbb{F}_q) \approx q$. From which it follows, that a "nice" curve should have $q \approx \ell$.

Now, let's try to do some rough estimates on the size of these good elliptic curves. If we want to have an instance of the ECDLP which resist to an attack of complexity 2^{128}, we should expect to work on a base field $\mathbb{F}_q$ represented by 256 bits.

Example 7. One of the "fastest" curves to work with in elliptic-curve cryptography is *Curve25519*, which was designed by Bernstein [1]. Such a curve is defined by the equation

$$E : y^2 = x^3 + 486662x^2 + x,$$

defined over the field $\mathbb{F}_p$, where $p = 2^{255} - 19$. The points whose x-coordinates equal 9 have order

$$2^{252} + 27742317777372353535851937790883648493.$$

When instantiating concrete cryptosystems, it is usually hard to design security proofs uniquely relying on the ECDLP. This is the case for the Elliptic Curve Diffie-Hellman (ECDH). For ECDH, to prove that the key exchange is secure in the presence of an eavesdropper, we need to rely on a variant of the ECDLP.

Definition 8. *Let E be an elliptic curve defined over $\mathbb{F}_q$ and let $P \in E(\mathbb{F}_q)$. Suppose we are given a point $[m_1]P$ and $[m_2]P$, for some $m_1, m_2 \in \mathbb{Z}$. The* Computational Diffie-Hellman (CDH) *problem asks to compute $[m_1 m_2]P$.*

Clearly, if we could break the ECDLP, we could indeed break the CDH problem. What about the converse? In general, we don't know. It is believed that the best attack strategy is to indeed break the ECDLP in the first place.

6 The Weil Pairing

Elliptic curves come equipped with another useful structure, the *Weil pairing*. It was initially used as a cryptanalytic tool but later has also been employed to design more advanced cryptosystems; see, for instance the BLS signature [2].

Let E be an elliptic curve defined over $\mathbb{F}_q$ and let m be a positive integer prime to q. Let μ_m denote the group of the m-th roots of unity, i.e. for all $\sigma \in \mu_m$, we have that $\sigma^m = 1$.

The Weil e_m-pairing is a map $e_m \colon E[m] \times E[m] \to \mu_m$ that satisfies the following properties.

1. Bilinear. $e_m(S_1 \oplus S_2, T) = e_m(S_1, T) \cdot e_m(S_2, T)$, and $e_m(S, T_1 \oplus T_2) = e_m(S, T_1) \cdot e_m(S, T_2)$.
2. Alternating. $e_m(S, T) = e_m(T, S)^{-1}$.
3. Non-degenerate. If $e_m(S, T) = 1$, for all $S \in E[m]$, then $T = \infty$.

7 Additional Readings

[7] "The Arithmetic of Elliptic Curves", Silverman (especially Chapters III and V).
[5] "Elliptic curves and their applications to cryptography: an introduction", Enge.
[3] "Handbook of Elliptic and Hyperelliptic Curve Cryptography", Cohen, Frey, Avanzi, Doche, Lange, Nguyen and Vercauteren.
– CRYPTOHACK, https://cryptohack.org/.

References

1. Bernstein, D.J.: Curve25519: New Diffie-Hellman speed records. In: Yung, M., Dodis, Y., Kiayias, A., Malkin, T. (eds.) PKC 2006: 9th International Conference on Theory and Practice of Public Key Cryptography. Lecture Notes in Computer Science, vol. 3958, pp. 207–228. Springer, Heidelberg, Germany, New York, NY, USA (Apr 24–26, 2006). https://doi.org/10.1007/11745853_14
2. Boneh, D., Lynn, B., Shacham, H.: Short signatures from the Weil pairing. In: Boyd, C. (ed.) Advances in Cryptology – ASIACRYPT 2001. Lecture Notes in Computer Science, vol. 2248, pp. 514–532. Springer, Heidelberg, Germany, Gold Coast, Australia (Dec 9–13, 2001). https://doi.org/10.1007/3-540-45682-1_30
3. Cohen, H., Frey, G., Avanzi, R.M., Doche, C., Lange, T., Nguyen, K., Vercauteren, F.: Handbook of Elliptic and Hyperelliptic Curve Cryptography. Chapman & Hall/CRC (2005)

4. Diffie, W., Hellman, M.E.: New directions in cryptography. IEEE Trans. Inf. Theory **22**(6), 644–654 (1976). https://doi.org/10.1109/TIT.1976.1055638
5. Enge, A.: Elliptic curves and their applications to cryptography: an introduction. Kluwer Academic Publishers, USA (1999)
6. Pomerance, C.: Fast, Rigorous Factorization and Discrete Logarithm Algorithms. In: Discrete Algorithms and Complexity, pp. 119–143. Academic Press (1987). https://doi.org/https://doi.org/10.1016/B978-0-12-386870-1.50014-9
7. Silverman, J.H.: The arithmetic of elliptic curves. Graduate Texts in Mathematics, Springer (1986)