Ellipitic Curves and their application in Cryptography

Anna Meyer

Abstract

Cryptography is essential for safeguarding data in the contemporary digital age. The introduction of asymmetric systems in the 1970s was a significant breakthrough in this discipline. The discrete logarithm problem (DLP) is the basis for numerous cryptographic systems. This paper provides an introductory overview of elliptic curves, which possess a group structure that makes the DLP very difficult to solve. The paper shows how to use the elliptic curve discrete logarithm problem to improve established cryptographic systems, pointing out several advantages of Elliptic Curve Cryptography (ECC). By utilizing the power of elliptic curves, ECC grants better security and efficiency to protect our data in the digital age.

1. Introduction

Secure communication and confidential data transmission plays an important role in our world, in which for example online shopping and the communication via Internet is more the rule than the exception. We have to ensure that our credit card data, the potentially confidential content of our emails and much more is only transmitted to and readable by the proposed people. Cryptography is therefore a very contemporary and important field of research.
However, cryptography has played an important role for thousands of years. Even the Romans used simple methods for the secret transmission of messages. As their systems only ensured basic security requirements, the methods for encrpytion and decryption have improved a lot. In 1976, Diffie and Hellman published the paper "New Directions in Cryptographie" [2], leading to a revolution in cryptography. Until then, only symmetric cryptographic systems were used, where encryption and decryption use the same secret key. Diffie and Hellman proposed the idea of asymmetric cryptosystems which also use public keys and make a prior key exchange redundant.

Another well studied subject in mathematics are elliptic curves. They arose in the analysis of studying elliptic integrals and are used today for example in the research areas of number theory and algebraic geometry. In this paper we will show how elliptic curves can be used in cryptography, which was first proposed independently in 1985 by Neal Koblitz [5] and Victor Miller [8].
The remainder of this paper is organized as follows. In Section 2, the basic algebraic knowledge and the notation we use is introduced. Section 3 explains the necessary basic knowledge of elliptic curves to use them in cryptography. We will give a short introduction to cryptography in Section 4.1 and show how to use elliptic curves in cryptosystems in Section 4.2. Finally, Section 5 concludes the paper.

2. Preliminaries

This section introduces the necessary basic terms and algebraic objects together with their notation. Anyone familiar with the projective space may be able to skip this section and use it as a reference throughout reading.
However, before we introduce the projective space, we will recall two basic algebraic definitions.

Definition 2.1. Let K be a field.

(i) The **characteristic** of K is defined as $\mathrm{char}K := \min\{c \in \mathbb{N} : c \cdot 1 = 0\}$ or 0.

(ii) K is called **algebraically closed** if every non-constant polynomial with coefficients in K has a root in K.

Convention 2.2. In the following, unless denoted otherwise, K will always denote a fixed algebraically closed ground field.

Definition 2.3 (Projective space)**.** Let $n \in \mathbb{N}$. The **projective n-space** over K is defined as the set of all one-dimensional linear subspaces of K^{n+1}. We denote it by $\mathbb{P}^n(K)$ or just $\mathbb{P}^n$ if K is clear from the context.

Since every one-dimensional linear subspace of K^{n+1} is uniquely determined by any non-zero vector contained in it and two such vectors span the same linear subspace if and only if they are linearly dependent, i.e. if they are scalar multiples of each other, we obtain

$$\mathbb{P}^n(K) = (K^{n+1} \setminus \{0\})/\sim$$

where the equivalence relation $\sim$ is defined as

$$(x_0, \dots, x_n) \sim (y_0, \dots, y_n) :\Leftrightarrow \exists \lambda \in K \setminus \{0\} \forall i \in \{0, \dots n\} \quad x_i = \lambda y_i.$$

We denote the equivalence class of $(x_0, \dots, x_n)$ by $[x_0, \dots, x_n] \in \mathbb{P}^n$. The numbers $x_0, \dots, x_n$ are called the **homogeneous coordinates** of the point.

Remark 2.4. Consider the natural embedding

$$f : K^n \to \mathbb{P}^n, (x_1, \dots, x_n) \mapsto [x_1, \dots, x_n, 1].$$

We will usually identify K^n with $f(K^n)$ and call it the **affine part** of $\mathbb{P}^n$. The elements in the complement

$$\mathbb{P}^n \setminus f(K^n) = \{[x_1, \dots, x_n, 0] : (x_1, \dots, x_n) \in K^n \setminus \{0\}\}$$

are called **points at infinity**.

Definition 2.5 (Projective line)**.** A **projective line** in $\mathbb{P}^n(K)$ is the set of all one-dimensional linear subspaces of a two-dimensional subspace of K^{n+1}. Two distinct points $P, Q \in \mathbb{P}^n(K)$ determine a unique projective line $\overline{PQ} := \langle P, Q \rangle$ passing through both of them, where $\langle P, Q \rangle$ is the two-dimensional span of P and Q.

We can calculate the projective line explicitly. If we have to distinct points $P = [p_0, \dots, p_n], Q = [q_0, \dots, q_n] \in \mathbb{P}^n$, they correspond to the vectors $p = (p_0, \dots, p_n), q = (q_0, \dots, q_n) \in K^{n+1}$. These vectors span the two-dimensional subspace $\lambda p + \mu q$ with $\lambda, \mu \in K$. Thus, P and Q determine the projective line $[\lambda p_0 + \mu q_0, \dots, \lambda p_n + \mu q_n] \in \mathbb{P}^n$ where λ, μ are not both equal to zero.

Definition 2.6 (Zero locus)**.** Let $S \subseteq K[x_1, \dots, x_n]$ be a set of polynomials. The **zero locus** of S is defined as

$$V(S) := \{x \in K^n : f(x) = 0 \quad \forall f \in S\}.$$

If we want to transfer this concept directly to the projective n-space, we encounter difficulties. For example, take the polynomial $f = y^2 - x \in K[x, y]$. Although $[1, 1] = [-1, -1]$ in $\mathbb{P}^1$, we have $f(1, 1) = 0$ but $f(-1, -1) \neq 0$. Therefore, we have to restrict the set of polynomials S.

Definition 2.7 (Homogeneous polynomial)**.** A polynomial $f \in K[x_0, \ldots, x_n]$ of degree d is called **homogeneous** if all its monomials are of the same degree d.

In this case it holds

$$f(\lambda x_0, \ldots, \lambda x_n) = \lambda^d f(x_0, \ldots, x_n)$$

which implies in particular

$$f(\lambda x_0, \ldots, \lambda x_n) = 0 \iff f(x_0, \ldots, x_n) = 0,$$

meaning that the zero locus of homogeneous poynomials is well defined in $\mathbb{P}^n$. We further note, that every polynomial can be transformed into a homogeneous polynomial.

Definition 2.8 (Homogenization)**.** Let $f \in K[x_0, \ldots, x_{n-1}]$ be a polynomial of degree d. We define the **homogenization** $f^* \in K[x_0, \ldots, x_n]$ by $f^*(x_0, \ldots, x_n) = x_n^d f(\frac{x_0}{x_n}, \ldots, \frac{x_{n-1}}{x_n})$.

It is evident, that the homogenization is a homogeneous polynomial of degree d. Throughout this article, we will often refer to $F \in K[x, y]$ and analyse $V(F^*) \in \mathbb{P}^2$.

3. Elliptic Curves

3.1. Definition of Elliptic Curves

In this section, we will define elliptic curves. In simple terms, an elliptic curve is the solution set of a cubic equation in two variables over a field. However, to introduce them formally we need a few more definitions.

Definition 3.1 (Weierstrass equation)**.** The equation

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, a_i \in K$$

is called the **(affine) Weierstrass equation**. Its homogenization is

$$E^* : y^2z + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3.$$

The corresponding defining polynomials are

$$F := y^2 + a_1xy + a_3y - (x^3 + a_2x^2 + a_4x + a_6)$$

and

$$F^* := y^2z + a_1xyz + a_3yz^2 - (x^3 + a_2x^2z + a_4xz^2 + a_6z^3),$$

respectively. By $E(K) := V(F^*) \subseteq \mathbb{P}^2$ we denote the zero locus of F^*.

In the following, let E be a Weierstrass equation with defining polynomials F and F^*.
The Weierstrass equation can be simplified, depending on the characteristic of K.
If char$K \neq 2$, we can transform E into

$$y^2 = x^3 + ax^2 + bx + c.$$

If char$K \neq 2, 3$, we get the even simpler form

$$y^2 = x^3 + ax + b.$$

Remark 3.2. For every Weierstrass equation E, $E(K)$ contains exactly one point at infinity. This can be seen as follows. Setting $z = 0$ yields $F^*([x, y, 0]) = x^3$. Thus, $[0, 1, 0]$ is the only point of $E(K)$ at infinity and it has multiplicity 3. As this point will play an important role in Section 3.2, we introduce the notation $\mathcal{O} := [0, 1, 0]$.

Definition 3.3 (Singular)**.** Let $P \in E(K)$.

(i) P is called a **singular point (of E)** if

$$\frac{\partial F^*}{\partial x}(P) = \frac{\partial F^*}{\partial y}(P) = \frac{\partial F^*}{\partial z}(P) = 0$$

(ii) $E(K)$ (or E) is called **singular** if it contains a singular point, otherwise it is called **smooth**.

Now we can finally define elliptic curves using the notion of singularities.

Definition 3.4 (Ellpitic curve)**.** E is called an **elliptic curve** if E is smooth.

We have already seen, that the point $\mathcal{O}$ fulfills every Weierstrass equation. We will now verify that this point is not a singular point, otherwise no elliptic curve would exist. Therefore, we calculate

$$\frac{\partial F^*}{\partial z}(\mathcal{O}) = (y^2 + a_1xy + 2a_3yz - a_2x^2 - 2a_4xz - 3a_6z^2)([0, 1, 0]) = 1 \neq 0.$$

To show that E is smooth, we need to verify for every point in $E(K)$ that at least one partial derivative is not zero. As this is in general time consuming and tedious, there is another way of checking the smoothness of E by considering its discriminant.

Remark 3.5 (Discriminant)**.** The **discriminant** of a Weierstrass equation is defined as

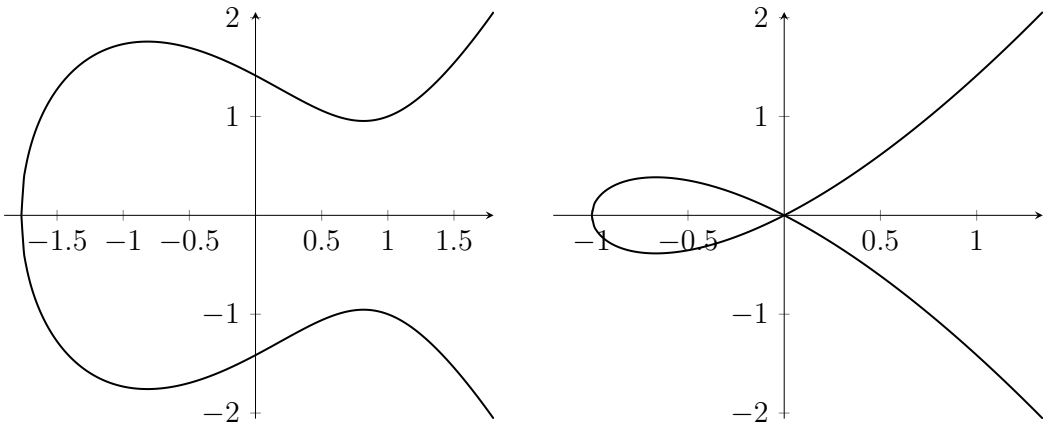
$$\Delta := -d_2^2 d_8 - 8d_4^3 - 27d_6^2 + 9d_2 d_4 d_6$$

where

$$\begin{aligned} d_2 &= a_1^2 + 4a_2, \\ d_4 &= 2a_4 + a_1 a_3, \\ d_6 &= a_3^2 + 4a_6, \\ d_8 &= a_1^2 a_6 + 4a_2 a_6 - a_1 a_3 a_4 + a_2 a_3^2 - a_4^2. \end{aligned}$$

It can be shown that E is smooth if and only if the discriminant is $\neq 0$. For example, if char$K \neq 2, 3$, i.e. we can write E as $y^2 = x^3 + ax + b$, it holds true that E is smooth iff $4a^3 + 27b^2 \neq 0$.

Using the discriminant, we know immediately that $y^2 = x^3 - 2x + 2$ is an elliptic curve since $4 \cdot (-2)^3 + 27 \cdot 2^2 = 76 \neq 0$. However, the Weierstrass equation $y^2 = x^3 + x^2$ obviously contains the singular point $(0, 0)$ and is therefore not an elliptic curve. Both curves are illustrated over $\mathbb{R}$ in Figure 1.



(a) $y^2 = x^3 - 2x + 2$ (b) $y^2 = x^3 + x^2$

Figure 1: Example of an elliptic curve and a Weierstrass equation which is no elliptic curve.

We can also consider elliptic curves over finite fields. For instance, the following Weierstrass equation, $E : y^2 = f(x) = x^3 + 2x - 1$ over $\mathbb{F}_5$, is a viable example. We already know it contains the point $\mathcal{O}$ at infinity. To determine

the affine points of $E(\mathbb{F}_5)$, we can simply evaluate f for each of the 5 values for x and check if the result is a square in $\mathbb{F}_5$. Since $f(1) = f(3) = 2$ is not a square, we get the following 6 affine points

$$\{(0,2),(0,3),(2,1),(2,4),(4,1),(4,4)\}.$$

Thus, together with the point $\mathcal{O}$ at infinity, $E(\mathbb{F}_5)$ has 7 points.

3.2. Group structure (E,+)

To be able to use elliptic curves in cryptography, we need some group structure. The key observation for defining a suitable operation on elliptic curves is the following theorem.

Theorem 3.6. Let $L \subseteq \mathbb{P}^2$ be a line. Then $|L \cap E(K)| = 3$, counted with multiplicity.

Proof. Let $L = \{[x,y,z] : ax + by + cz = 0\} \subseteq \mathbb{P}^2$ with $(a,b,c) \neq (0,0,0)$.

(i) $a = b = 0$: We have $c \neq 0$ and therefore $L = \{[x,y,0]\}$ is the line at infinity. As we have seen in the previous section in Remark 3.2, $\mathcal{O}$ is the only point in $E(K)$ with $z = 0$ and it has multiplicity 3 since $F^*([x,y,0]) = x^3$.

(ii) $a \neq 0$ or $b \neq 0$: Consider the points at infinity contained in L, i.e. $\{[x,y,0] : ax + by = 0\}$. Since we have $y = -\frac{a}{b}x$ or $x = -\frac{b}{a}y$, L only contains one point at infinity, namely $[b,-a,0]$. Thus, we get $L = \{[x,y,1] : ax + by = -c\} \cup \{[b,-a,0]\}$.

(a) $b \neq 0$: In this case $[b,-a,0] \neq [0,1,0]$, so $L \cap E(K)$ does not contain a point at infinity. Using the definition of L we can substitute $y = -\frac{ax+c}{b}$ in E. This yields a cubic polynomial in x which has 3 roots since K is algebraically closed.

(b) $b = 0, a \neq 0$: We have $[b,-a,0] = [0,1,0] \in L \cap E(K)$. To compute the affine points in $L \cap E(K)$ we substitute $x = -\frac{c}{a}$ in E which yields a quadratic polynomial in y and thus has two roots.

□

This theorem yields the following idea for defining an operation on E. If we are given two distinct points P and Q on E, we consider the unique line $\overline{PQ}$ as in Definition 2.5. Thus, we get by applying the previous theorem $\overline{PQ} \cap E(K) = \{P, Q, R\}$ and setting $P * Q := R$ is a well defined operation on $E(K)$. However, if we only consider one point, i.e. $P = Q$, we need to ensure that the chosen line meets E at P with multiplicity at least two. This is achieved by the tangenet line.

Definition 3.7 (Tangent)**.** Let $P \in E(K)$. The line

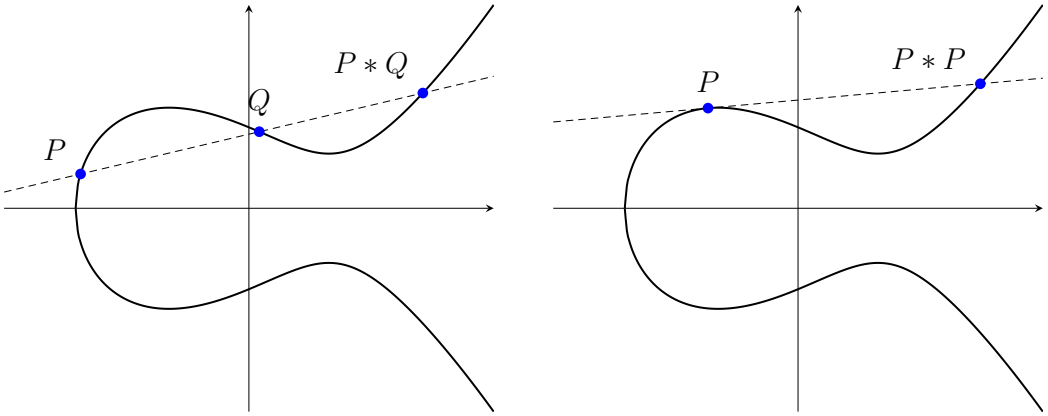
$$T_P := \{[u, v, w] \in \mathbb{P}^2 : \frac{\partial F^*}{\partial x}(P)u + \frac{\partial F^*}{\partial y}(P)v + \frac{\partial F^*}{\partial z}(P)w = 0\}$$

is called the **tangent** of E at P.

Note that elliptic curves are smooth. This means that the tangent line exists for every point in $E(K)$ and leads to a well defined operation on E. For $P, Q \in E(K)$ we define $P * Q$ by $L \cap E(K) = \{P, Q, P * Q\}$ where

$$L := \begin{cases} \overline{PQ} & \text{if } P \neq Q, \\ T_P & \text{if } P = Q \end{cases}.$$

This operation is illustrated in Figure 2.



(a) $P * Q$ if $P \neq Q$ (b) $P * P$, i.e. $P = Q$

Figure 2: Illustration of $P * Q$

To establish a group structure, however, we also need an identity element. This means, there needs to exist an element $e \in E(K)$ such that $P * e = P$

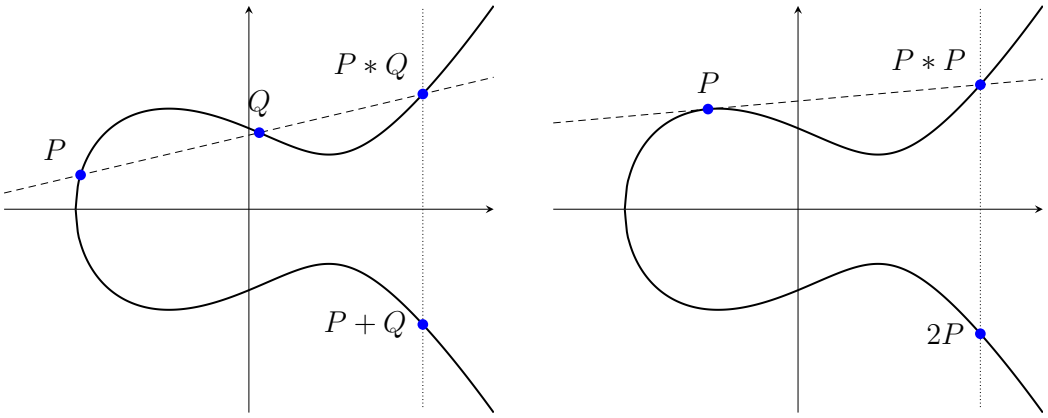
for all $P \in E(K)$. Clearly, this is unfortunately not the case. Thus, we need to come up with another operation.

Definition 3.8 (Operation " $+$ "). Let $P, Q \in E(K)$. Then,

$$P + Q := (P * Q) * \mathcal{O},$$

where $\mathcal{O}$ denotes the point at infinity $[0, 1, 0]$.

The geometrical interpretation is the following and illustrated in Figure 3. For two distinct points P and Q on the elliptic curve, we first draw the line going through both points. It intersects the curve at a third point $P * Q$. Then we draw a vertical line through $P * Q$, which is just $\overline{(P * Q)\mathcal{O}}$ by the definition of $\mathcal{O}$. The third intersection point of that line with the curve is defined as $P + Q$. If we want to add one point to itself, we consider again the tangent line.



(a) Adding two distinct points

(b) Adding the same point

Figure 3: Illustration of the operation $+$

With this new operation, we finally established a group structure on $E(K)$.

Theorem 3.9. $(E(K), +)$ is an abelian group with neutral element $\mathcal{O}$ and inverse $-P = P * \mathcal{O}$.

Proof. Let $P, Q \in E(K)$. Since $*$ is commutative by definition, we get

$$P + Q = (P * Q) * \mathcal{O} = (Q * P) * \mathcal{O} = Q + P,$$

hence + is commutative. Further we observe that

$$(P * Q) * P = Q \tag{1}$$

by the definition of $P * Q$. As $P * Q$ is the third intersection point of the line going through P and Q, the line going through $P * Q$ and P is the same line as before. Hence, the third intersection point is Q, which shows (1).
Next, we show that $\mathcal{O}$ is the identity element, i.e. $P + \mathcal{O} = P$. It holds

$$P + \mathcal{O} = (P * \mathcal{O}) * \mathcal{O} = (\mathcal{O} * P) * \mathcal{O} \overset{(1)}{=} P$$

as desired. Considering the inverse, we define $-P := P * \mathcal{O}$. Using (1) we get

$$P+(-P) = (P*(-P))*\mathcal{O}) = (P*(P*\mathcal{O}))*\mathcal{O} = ((P*\mathcal{O})*P)*\mathcal{O} \overset{(1)}{=} \mathcal{O}*\mathcal{O} = \mathcal{O}$$

where the last equality holds since an easy calculation shows that the tangent $T_{\mathcal{O}} = \{[u, v, w] : w = 0\}$ is the line at infinity. Recalling that $\mathcal{O}$ is the only point at infinity contained in $E(K)$ and has multiplicity 3, the last equality is obtained.
Proving the associativity, however, is not straightforward. One way to prove the remaining group axiom is to show that the *Abel-Jacobi map*, which is an embedding of a curve into its Jacobian, is an isomorphism for elliptic curves, as seen in e.g [11]. A lengthy computation is necessary without using more advanced algebra. Therefore, we omit this proof here and refer to the literature. □

3.3. Explicit computation formulas

In this section we want to derive explicit formulas for finding the inverse of a given point, as well as for the operations + and $*$.
In the following, we will assume char$K \neq 2$. This keeps the computations a bit simpler, but formulas for the general case can be derived by the same approach. Thus, E reduces to $y^2 = x^3 + ax^2 + bx + c$ with the defining polynomial $F(x, y) = y^2 - x^3 - ax^2 - bx - c$.

3.3.1. Formula for $-P$

It is quite easy to see that $-\mathcal{O} = \mathcal{O}$. So let $P = (x_0, y_0) = [x_0, y_0, 1] \in E(K)$ be affine. To determine the inverse geometrically, we just have to consider a

vertical line through P intersecting the elliptic curve at $P, -P$ and $\mathcal{O}$. Since the curve is symmetric around the x-axis, we obtain $-P = (x_0, -y_0)$.
As this approach does not work for the general Weierstrass equation as in Definition 3.1, we show how to derive the formula analytically. By definition of the projective line $\overline{P\mathcal{O}}$ we get

$$[x, y, 1] \in \overline{P\mathcal{O}} \iff \begin{pmatrix} x \\ y \\ 1 \end{pmatrix} \in \left\langle \begin{pmatrix} x_0 \\ y_0 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} \right\rangle \iff x = x_0.$$

So the affine points of $\overline{P\mathcal{O}}$ are $[x_0, y, 1]$. Further, we have

$$[x_0, y, 1] \in E(K) \iff F(x_0, y) = 0.$$

Since $P \in E(K)$, y_0 is a root of $F(x_0, y)$. Let y_1 be the second root. Then we get $(x_0, y_1) = P * \mathcal{O} = -P$. Thus, it remains to determine y_1. It holds

$$F(x_0, y) = (y - y_0)(y - y_1) = y^2 + (-y_0 - y_1)y + y_0 y_1 \stackrel{!}{=} y^2 - x_0^3 - ax_0^2 - bx_0 - c.$$

Coefficient matching yields $-y_0 - y_1 = 0 \iff y_1 = -y_0$. Hence, we get as before $-P = (x_0, -y_0)$.

3.3.2. Formula for $P * Q$
We already know $\mathcal{O} * \mathcal{O} = \mathcal{O}$ and $P * \mathcal{O} = -P$. Thus, it only remains to consider the case where both points are affine. Let $P = (x_0, y_0), Q = (x_1, y_1) \in E(K)$ be affine. Observe that by definition of $*$ it holds

$$P * Q = \mathcal{O} \iff P * \mathcal{O} = Q \iff -P = Q.$$

This is the case if $x_0 = x_1$ and $y_0 = -y_1$ by our calculations in the previous paragraph.
So assume $Q \neq -P$. We need to consider the line $L := \overline{PQ}$ joining P and Q. If $P \neq Q$, i.e. $x_0 \neq x_1$, the affine points of this line are given by

$$L \cap K^2 = \{(x, y) : y = \lambda x + \nu\} \text{ where } \lambda = \frac{y_1 - y_0}{x_1 - x_0} \text{ and } \nu = y_0 - \lambda x_0.$$

To get the third intersection point of L and $E(K)$, we replace $y = \lambda x + \nu$ in F. As before, we know that $F(x, \lambda x + \nu)$ has the roots x_0 and x_1 and the third root x_2 will be the x-coordinate of $P * Q$. Thus, we get

$$-(x - x_0)(x - x_1)(x - x_2) = F(x, \lambda x + \nu) = (\lambda x + \nu)^2 - x^3 - ax^2 - bx - c.$$

Coefficient matching of the quadratic terms yields $x_0 + x_1 + x_2 = \lambda^2 - a$. This yields

$$x_2 = \lambda^2 - a - x_0 - x_1 \quad \text{and} \quad y_2 = \lambda x_2 + \nu = \lambda(x_2 - x_0) + y_0$$

If $P = Q$, we need to consider the tangent line

$$T_P \cap K^2 = \left\{ (x, y) : \frac{\partial F^*}{\partial x}(P) \cdot x + \frac{\partial F^*}{\partial y}(P) \cdot y + \frac{\partial F^*}{\partial z}(P) \cdot 1 = 0 \right\}.$$

As before, we can write this as $\{(x, y) : y = \lambda x + \nu\}$ in which ν is defined as before. For the slope we get

$$\lambda = -\frac{\frac{\partial F^*}{\partial x}(P)}{\frac{\partial F^*}{\partial y}(P)} = -\frac{-3x_0^2 - 2ax_0 - b}{2y_0}.$$

Note that our assumption $P \neq -P$ ensures $y_0 \neq 0$. With these λ and ν we continue as before.

3.3.3. Formula for $P + Q$

Combining the results of the previous two sections, we finally get a formula for $P + Q$. Since $\mathcal{O}$ is the neutral element, we only have to consider the case where $P = (x_0, y_0)$ and $Q = (x_1, y_1)$ are affine. Further, we assume $-P \neq Q$ as this leads to $P + Q = \mathcal{O}$, which we have shown in the previous section. Putting the above formulas together, we get for $P + Q = (x_2, y_2)$:

$$x_2 = \lambda^2 - a - x_0 - x_1 \quad \text{and} \quad y_2 = -\lambda(x_2 - x_0) - y_0$$

where

$$\lambda = \frac{y_1 - y_0}{x_1 - x_0} \text{ if } P \neq Q \quad \text{or} \quad \lambda = -\frac{-3x_0^2 - 2ax_0 - b}{2y_0} \text{ if } P = Q.$$

We conclude the section by applying these formulas on a small example. Let us consider the elliptic curve $E : y^2 = x^3 + 4x + 20$ defined over $\mathbb{R}$. Using the discriminant as in Remark 3.5 we verify $4 \cdot 4^3 + 27 \cdot 20^2 \neq 0$, so E is indeed an elliptic curve. It contains the integral points $P = (-2, 2)$ and $Q = (1, 5)$.We want to calculate $P + Q$ and $2P$. Therefore we start by calculating the slope of the line going through both points and of the tangent line:

$$\lambda_{PQ} = \frac{5 - 2}{1 - (-2)} = 1 \quad \text{and} \quad \lambda_{T_P} = -\frac{-3 \cdot (-2)^2 - 4}{2 \cdot 2} = 4$$

Thus, we get by using our formula from the previous section for $P + Q$:

$$x_2 = 1^2 - (-2) - 1 = 2 \quad \text{and} \quad y_2 = -1 \cdot (2 - (-2)) - 2 = -6.$$

So $P + Q = (2, -6)$. Using the slope of the tangent line, we get similarly $2P = (20, -90)$.
As a second example, we consider the same curve over $\mathbb{F}_{29}$. The discriminant is also not zero modulo 29, thus, E is over this field an elliptic curve, too. One can verify that it contains the points $P' = (5, 22)$ and $Q' = (16, 27)$. Calculating the slope yields

$$\lambda = (27 - 22)(16 - 5)^{-1} = 5 \cdot 11^{-1} = 5 \cdot 8 = 40 \equiv 11 \mod 29.$$

This yields

$$x_2 = 11^2 - 5 - 16 = 121 - 21 = 100 \equiv 13 \mod 29$$

and

$$y_2 = -11(13 - 5) - 22 = -110 \equiv 6 \mod 29.$$

Hence, $P' + Q' = (13, 6)$.

4. Application in Cryptography

In this section, we will show how elliptic curves are used in cryptography. Therefore we will first introduce the necessary basic knowledge about cryptography and the public Diffie-Hellmann key exchange in Section 4.1.

4.1. Introduction to Cryptography

The goal of cryptography is to create systems which allow secure communication between two parties, typically called *Alice* and *Bob*, such that a present third party (*Eve*) cannot interfere this information exchange and is unable to eavesdrop the conversation. To accomplish this, Alice encrypts her message, sends this so-called ciphertext, which should be indecipherable to Eve, over an insecure channel to Bob, who decrypts it to recover the original message again. This basic model is shown in Figure 4. The primary security objectives are to secure confidentiality, maintain data integrity and ensure authenticity.
Nowadays, there are two general types of cryptosystems: symmetric and assymmetric. Until the 1970s, only symmetric systems were known. In these

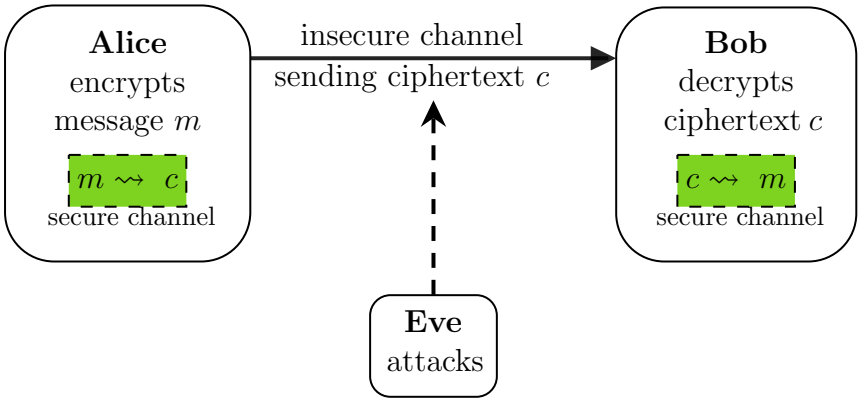


Figure 4: Basic model for secure communication in cryptography

systems, Alice and Bob agree on one secret key. Alice can then use this secret key to encrypt the message she is sending to Bob. Using the same key, Bob can decrypt the message and Eve is not able to read the message without knowing the secret key. However, Alice and Bob need to exchange the key securely before they can communicate securely. But how do they do this, if they have never met? This is one of the main drawbacks of the symmetric systems.
In 1976, Whitfield Diffie and Martin Hellman introduced the idea of public key cryptosystems, leading to assymmetric systems. Here, Alice and Bob both have a private key and a public key. To encrypt, Bob uses Alice's public key, but only Alice can decrypt it by using her secret private key. Of course, it must be very hard to determine the private key from knowing the public key. Thus, the keys are chosen in such a way, that deriving the private key solely from the public key is equivalent to solving an intractable mathematical problem.
One of these problems, which is believed to be hard to solve, is the *Discrete Logarithm Problem*.

Definition 4.1 (Discrete Logarithm Problem)**.** Let p be a prime and $g, y \in \{1, \ldots, p-1\}$ be two numbers modulo p. The **Discrete Logarithm Problem (DLP)** is finding a minimal $x \in \mathbb{N}$ such that $g^x \equiv y \mod p$.

Modern cryptography makes the assumption that the DLP cannot be solved by a probabilistic algorithm with polynomial runtime, offering a potential solution for creating a public-private key pair. To do this, Alice and Bob publicly agree on a large prime p and a non-zero integer g modulo p. Alice

chooses an integer a, computes $A := g^a$, which she sends to Bob. Bob chooses a random integer b and sends $B := g^b$ to Alice. Next, Alice calculates $A' := B^a$ and Bob calculates $B' := A^b$. This is in fact the same as

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

and now A' can be used as the secret key. Figure 5 illustrates the key exchange.

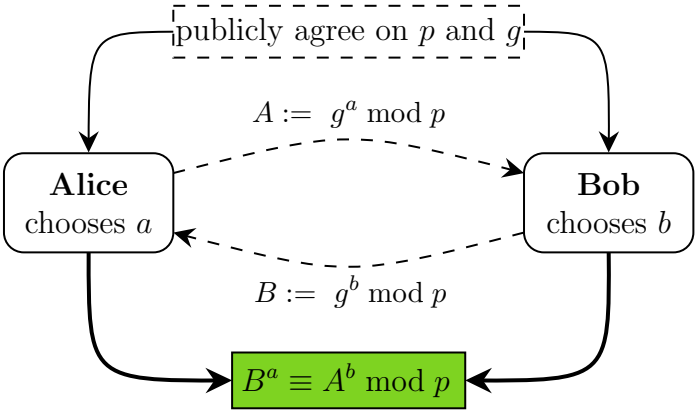


Figure 5: Diffie-Hellman key exchange

Note that although Eve knows p, g, A and B, she needs to compute a or b to get the secret key A'. In other words, if Eve could solve the DLP, she could easily derive the secret key. However, this is assumed to be hard. Nevertheless, there may be another way of solving the potentially easier problem of computing g^{ab} given g^a and g^b, which is referred to as the **Diffie-Hellman Problem (DHP)**. It is not known if it is equivalent to the DLP, i.e. if an efficient algorithm for solving the DHP leads to an efficient algorithm solving the DLP.

To conclude this section, we present the well-known *El Gamal* cryptosystem that is based on the DLP and closely related to the Diffie-Hellman key exchange. It is depicted in Figure 6. Alice chooses a prime p and an integer g modulo p. Further, she determines a number a, computes $A := g^a$ and publishes p, g and A. To send a message to Alice, Bob selects a random number b modulo p and encrypts his message x, which is without loss of generality assumed to be a number, by using the encryption function

$$e(x) = (g^b, A^b x).$$

For decryption, Alice uses her private key a in the decryption function

$$d(y, z) = y^{-a}z.$$

This does, in fact, result in a well-defined cryptosystem as one can easily check

$$(d \circ e)(x) = d(g^b, A^b x) = (g^b)^{-a}(g^a)^b x = g^{-ba+ab}x = x.$$

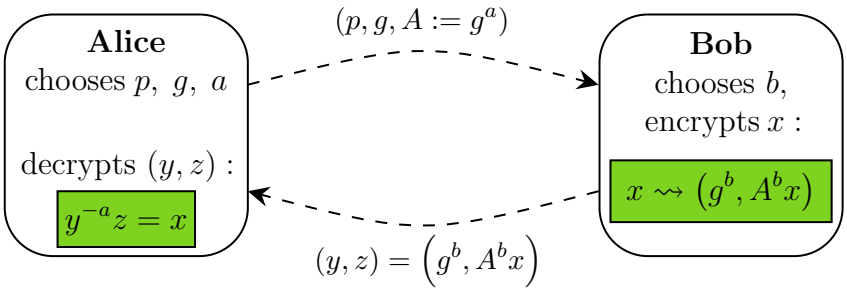


Figure 6: El Gamal cryptosystem

It appears that the cryptosystem can only be broken by Eve if she manages to solve the DLP or the DHP.

4.2. Elliptic Curve Cryptography

Although we only defined the DLP for the group $\mathbb{F}_p^*$, it exists in almost any group and the hardness of solving it depends on the way the group is represented. For instance, it is known that $\mathbb{F}_p^* \cong (\mathbb{Z}/(p-1)\mathbb{Z}, +)$, but the DLP is assumed to be hard in the first case and trivial in the latter. The DLP variant for elliptic curves is as follows.

Definition 4.2 (Elliptic Curve Discrete Logarithm Problem)**.** Let p be a prime and E an elliptic curve over the finite field $\mathbb{F}_p$. Let $P, Q \in E(\mathbb{F}_p)$. The **Elliptic Curve Discrete Logarithm Problem (ECDLP)** consists in finding an integer n such that $Q = nP$.

Thus, any cryptosystem based on the DLP, such as the El Gamal system described in the previous section, or the Diffie-Hellman key exchange, can be used with elliptic curves. In the latter scenario, Alice and Bob agree publicly on a prime p, an elliptic curve E over $\mathbb{F}_p$ and a point $P \in E(\mathbb{F}_p)$. For their private keys, they choose integers n_a and n_b respectively. Using these, they compute the public keys $Q_a = n_a P$ and $Q_b = n_b P$, which are then

exchanged. Now, Alice can compute $n_a Q_b$, while Bob can obtain the same key by computing $n_b Q_a$. The key exchange using Elliptic Curve Cryptography is illustrated in Figure 7a.
The Elliptic El Gamal cryptosystem can be obtained in a very similar manner. Alice selects a prime p, an elliptic curve E over $\mathbb{F}_p$ and a point $P \in E(\mathbb{F}_p)$. She publishes them along with her public key $Q_a := n_a P$, where n_a is her private key. In order to encrypt a message, Bob chooses a number n_b and calculates

$$e(x) = (n_b P, x + n_b Q_a).$$

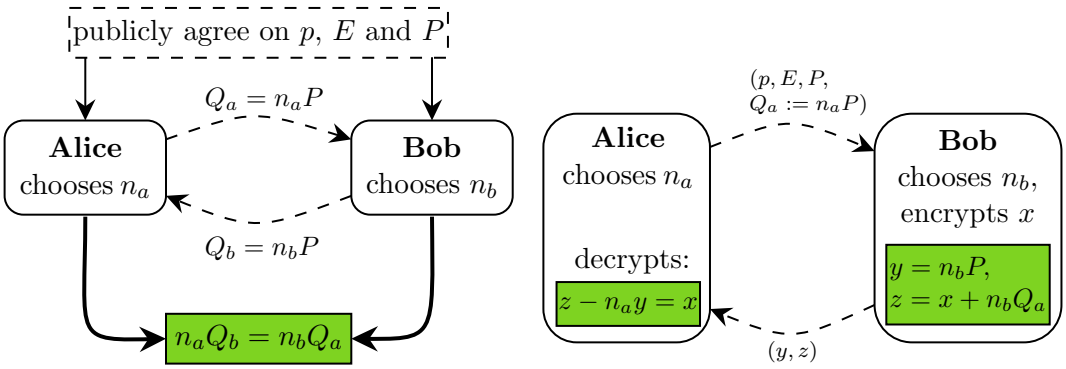
Alice can decrypt this message with the decryption function

$$d(y, z) = z - n_a y$$

to retrieve x once again because

$$(d \circ e)(x) = d(n_b P, x + n_b Q_a) = x + n_b n_a P - n_a n_b P = x.$$

This is illustrated in Figure 7b.



(a) Elliptic key exchange

(b) Elliptic El Gamal

Figure 7: Elliptic Curve Cryptography

But why should we use Elliptic Curve Cryptography with its complicated addition? It actually offers several benefits. Firstly, it enhances security as all known attacks for DLP, such as the index calculus, quickly lose their strength. The fastest known algorithm available to solve the ECDLP is in $\mathcal{O}(\sqrt{p})$, whereas for DLP, it is in $\mathcal{O}(p^\varepsilon)$ for every $\varepsilon > 0$. This also implies that we can reduce the key size (i.e. the chosen primes) when working with elliptic curves instead of other DLP-based cryptosystems, while sustaining

the same security. Thus, fewer bits need to be stored and transmitted, which is favourable as their storage and transmission is expensive. Further, some calculations can be done ahead, making Elliptic Curve Cryptography computationally faster than conventional cryptographic algorithms. However, one should also note that the security depends on the chosen elliptic curve, since there are classes of curves which are more susceptible to attacks. For further information on the security and the benefits of using Elliptic Curve Cryptography, we refer to the references such as [4] and [6].

5. Conclusion

In this paper, elliptic curves are precisely defined and a group structure is developed upon them. This enabled us to define the Elliptic Curve Discrete Logarithm Problem, which is very hard to solve. Currently, no subexponential algorithms have been found to solve the ECDLP. Hence, it is feasible to convert any cryptographic system based on the Discrete Logarithm Problem into an Elliptic Curve Cryptographic System by replacing the DLP with the ECDLP. This modification, as discussed in the previous section, offers numerous benefits, the most significant of which are enhanced security and reduced key size.

Before implementing Elliptic Curve Cryptography, however, several choices must be made. The security of the system is impacted by various factors, such as the finite field $\mathbb{F}_p$ and its representation, the elliptic curve over $\mathbb{F}_p$, and the point P. It is crucial to consider all these factors together to determine the optimal solution for each specific case since there is no universal best choice. An additional disadvantage of Elliptic Curve Cryptography is the limited research available on the topic. Other frequently used cryptographic systems, such as RSA, have been extensively researched. This exhaustive research into the security of Elliptic Curve Cryptography is still missing.

Despite being a relatively new technology, Elliptic Curve Cryptography holds significant promise as one of the most crucial cryptosystems in the future.

References

[1] Mohamed Barakat, Christian Eder, Timo Hanke, and Max Horn. An introduction to cryptography. 2023.

[2] Whitfield Diffie and Martin E Hellman. New directions in cryptography. *IEEE Transactions on Information Theory*, 1976.

[3] Andreas Gathmann. Algebraic geometry. 2021.

[4] Darrel Hankerson and Alfred Menezes. Elliptic curve cryptography. In *Encyclopedia of Cryptography, Security and Privacy*, pages 1–2. Springer, 2021.

[5] Neal Koblitz. Elliptic curve cryptosystems. *Mathematics of computation*, 48(177):203–209, 1987.

[6] Neal Koblitz, Alfred Menezes, and Scott Vanstone. The state of elliptic curve cryptography. *Designs, codes and cryptography*, 19:173–193, 2000.

[7] Thomas Krämer. Lectures on elliptic curves. 2020.

[8] Victor S Miller. Use of elliptic curves in cryptography. In *Conference on the theory and application of cryptographic techniques*, pages 417–426. Springer, 1985.

[9] Joseph H Silverman, Jill Pipher, and Jeffrey Hoffstein. *An introduction to mathematical cryptography*, volume 1. Springer, 2008.

[10] Joseph H Silverman and John Torrence Tate. *Rational points on elliptic curves*, volume 9. Springer, 1992.

[11] Robin Visser. The abel-jacobi map.