Università degli Studi di Padova

DIPARTIMENTO DI MATEMATICA "TULLIO LEVI-CIVITA"
Corso di Laurea Magistrale in Matematica

Tesi di Laurea Magistrale

Security evaluation of a key management scheme based on bilinear maps on elliptic curves

Relatore:
Prof. Riccardo Colpi
Correlatori:
Prof. Nicola Laurenti
Dr.ssa Silvia Ceccato
Dr.ssa Anna Poltronieri

Laureando:
Luca Parolini
Matricola 1148702

19 Aprile 2019

Contents

Introduction

Elliptic curves have been an important research topic of number theory and geometry throughout the 20th century; their structure and properties have been widely studied in mathematics. In recent years, many applications of elliptic curves to cryptography have been developed. Cryptosystems based on groups of rational points on elliptic curves allow more efficient alternatives to finite field cryptography, which usually requires groups with larger cardinality and lower efficiency. The existence of bilinear pairings raises even more interest in this research area. These are non-degenerate, bilinear maps that were first applied in the attack of cryptographic hard problems, such as the discrete logarithm and its variants. Later, many efficient cryptosystems based on pairings have been developed; however, their security must be carefully studied. Among the various applications that came out, we are interested in the broadcast encryption scheme, that was introduced by Boneh, Gentry and Waters in 2005 [15]. Besides its feature of having constant size private keys, it can be applied to manage revocation of users, as in [18]. Its security is based on the decisional version of the ℓ-BDHE problem, which is a variant of the classical Diffie-Hellman problem, specifically constructed for pairing-based cryptography. Its hardness, is still a research topic and only some theoretical evidence exists. The aim of this work is to investigate the security of this broadcast encryption system, taking in account a model that proves the hardness of the ℓ-BDHE problem, under strong assumptions. Drawbacks of this approach will be discussed: its main weakness is the system's behaviour during attack simulations, which is far from real. The main result is Theorem 4.13, which is applied to find an asymptotic lower bound on the running time of an adversary. Also the elliptic curve choice, when implementing an encryption scheme, could affect its security. We will review the main criteria for this choice and we will investigate the existence of elliptic curves suitable for the system of our interest. This thesis has the following outline.

- *Chapter 1* gives the mathematical background of elliptic curves, where the group structure of the set of points is introduced. We study an algorithm for square roots computation in finite fields, which allows to efficiently find affine coordinates of points.
- *Chapter 2* introduces the Weil maps, together with a proof of their bilinearity and other properties.
- *Chapter 3* contains an overview of hard cryptographic problems and their connections. We define symmetric, asymmetric and general pairings. Then we show how the Weil maps fit these definitions, introducing distortion maps for the symmetric case.
- *Chapter 4* is about the security analysis of the broadcast encryption scheme. After the definition of the generic group model, we present a bound on the adversary's advantage in solving the ℓ-BDHE problem, which can be applied to the case of the encryption scheme in [15]. Eventually, we examine other security issues and propose a family of elliptic curves suitable for implementing that cryptosystem.

Chapter 1

Elliptic Curves

This chapter contains an overview of basic facts about elliptic curves needed to define the Weil pairing, a bilinear map that is useful in cryptographic applications. We show that the set of points on an elliptic curve has a natural group structure and then we see that it is possible to find, in probabilistic polynomial time, a random point on a given curve over a finite field. This is a key point when we want to use elliptic curves cryptography.

1.1 Definitions

For our purposes, we define an elliptic curve as the locus of some cubic equation, avoiding a more general definition like the one introduced in algebraic geometry. We prefer that approach because the final aim of this work is to apply such curves to cryptography rather than to study their abstract properties. A more general approach can be found in [52]. Hence we give the following definition.

Definition 1.1. An *elliptic curve* E over a field K, denoted by E/K, is the locus in $\mathbb{P}^2_K$ of the following cubic equation, called *generalized (projective) Weierstrass equation*:

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3, \tag{1.1}$$

where $a_1, \ldots, a_6 \in K$.

We will often refer to the affine equation, which can be obtained using the non-homogeneous coordinates $x = X/Z$ and $y = Y/Z$ and which is

$$E: \; y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6; \tag{1.2}$$

where we just need to remember that there is an extra point $O = [0, 1, 0]$ out at infinity. We also remark that this is the unique point at infinity of E, relative to the dehomogeneization with respect to Z. Indeed, recall that given $[x, y, z] \in \mathbb{P}^2_K$ with $z \neq 0$, then $[x, y, z] = [x/z, y/z, 1]$ and we call these points "*finite*". The set of all such points can be identified with the affine plane $\mathbb{A}^2_K$. On the contrary, we call $[x, y, 0]$ "*points at infinity*" in $\mathbb{P}^2_K$. Hence, consider the generalized projective Weierstrass equation and set $Z = 0$: this leads to the equation $X^3 = 0$, which gives a unique point $\mathbb{P}^2_K \ni [0, y, 0] = [0, 1, 0]$ on the curve. Under further assumptions on the field we get more compact equations; firstly suppose that $\mathrm{char}(K) \neq 2$, so that we can complete the square:

$$\left(y + \frac{a_1x}{2} + \frac{a_3}{2}\right)^2 = x^3 + \left(a_2 + \frac{a_1^2}{4}\right)x^2 + \left(a_4 + \frac{a_1a_3}{2}\right)x + \left(\frac{a_3^2}{4} + a_6\right).$$

Hence we can write the equation as

$$y'^2 = x^3 + b_2x^2 + b_4x + b_6, \tag{1.3}$$

where

$$\begin{aligned} y' &= y + \frac{a_1x}{2} + \frac{a_3}{2}, \\ b_2 &= a_2 + \frac{a_1^2}{4}, \\ b_4 &= a_4 + \frac{a_1a_3}{2}, \\ b_6 &= \frac{a_3^2}{4} + a_6. \end{aligned}$$

As shown in [52, III.3.1b], given an elliptic curve, any two Weierstrass equations for it are related by a change of variable of the form:

$$x' = u^2x + r, \qquad y' = u^3y + su^2x + t,$$

with $u, r, s, t \in K,\ u \neq 0$. Then 1.3 is a new Weierstrass equation for the same elliptic curve.
Finally if $\mathrm{char}(K) \neq 2, 3$ we can also write the right hand side of the previous equation as

$$y'^2 = \left(x + \frac{b_2}{3}\right)^3 + \left(b_4 - \frac{b_2^2}{3}\right)x + b_6 - \frac{b_2^3}{27}.$$

Without loss of generality, we assume for our purposes that $\mathrm{char}(K) \neq 2, 3$ and hence consider throughout this thesis elliptic curves E/K as the locus of a (cubic) *Weierstrass equation* of the form

$$y'^2 = x'^3 + ax' + b \tag{1.4}$$

for some $a, b \in K$, that come from the previous equalities, and letting $x' = x + b_2/3$. Elliptic curves in characteristic 2 or 3 suffer from specialized discrete log attack [21] thus they should generally be avoided. Moreover, given r_1, r_2, r_3 the roots of the above cubic, then it can be shown that the *discriminant* of the curve is

$$\Delta = \prod_{i<j}(r_i - r_j)^2 = -(4a^3 + 27b^2).$$

We also do not allow E to have multiple roots, which is equivalent to require that $\Delta \neq 0$ and we call curves with this property *non-singular*. Under this hypothesis all points are non-singular; indeed, at first we see that O is so differentiating the short homogeneous equation $E(X, Y, Z) = Y^2Z - X^3 - aXZ^2 - bZ^3 = 0$ with respect to Z:

$$\frac{\partial E}{\partial Z}(O) = 1 \neq 0.$$

Now assume by contradiction that E has a singular point at $P_0 = (x_0, y_0)$ and note that the substitution

$$x = x' + x_0 \qquad y = y' + y_0$$

leaves Δ invariant. Therefore, without loss of generality, we assume that E is singular at $(0, 0)$ and we consider the affine equation $E(x, y)$, of the form 1.4. Differentiating we have

$$E(0,0) = b = 0, \qquad \frac{\partial E}{\partial x}(0,0) = a = 0, \qquad \frac{\partial E}{\partial y}(0,0) = 0.$$

Hence the discriminant of E is $\Delta = 0$, which contradicts the initial hypothesis.

Next we define an important family of sets. Unless otherwise specified, we will always consider points on elliptic curves by means of their affine coordinates, adding the unique extra point O.

Definition 1.2. Let E/K be an elliptic curve defined over K and let L be a field such that $K \subseteq L$; we define the *L-rational points of E* by

$$E(L) = \{O\} \cup \{(x, y) \in L \times L \mid y^2 = x^3 + ax + b\}.$$

We simply denote by E the set $E(\overline{K})$ of the rational points on the algebraic closure of the field over which the curve is defined.

Thus different fields give different sets of points on the elliptic curve. We focus on the case when the definition field is a finite field $K = \mathbb{F}_{p^k}$, p prime; this is the usual setting of cryptographic applications that we would like to investigate.

1.2 Group law

The sets of rational points of E are rather interesting, because we can define a group law on each of them, which is the aim of this section. These groups are useful for the implementation of elliptic curve cryptosystems. Let E/K be an elliptic curve and let $L \in \mathbb{P}^2_K$ be a line. As a consequence of Bezout's Theorem [45] the intersection $E \cap L$, which are loci of some degree 3 and 1 polynomials respectively, contains three points, not necessarily distinct, and taken with their multiplicity. We first need an auxiliary operation:

Definition 1.3. Let $P, Q \in E$ and let L_{PQ} be the line connecting P and Q (the tangent line through P if $P = Q$). Then we define $P * Q$ as the third point of intersection of L_{PQ} with E.

We first state a Lemma by Chasles about cubic curves, that can be found in [22]. It will be useful in next proposition's proof.

Lemma 1.4 (Chasles)**.** *Let $\mathcal{C}_1, \mathcal{C}_2 \subseteq \mathbb{P}^2_K$ be cubic plane curves that have 9 points of intersection. If $\mathcal{C} \subseteq \mathbb{P}^2_K$ is any cubic curve containing 8 of those points, then it contains the ninth one as well.*

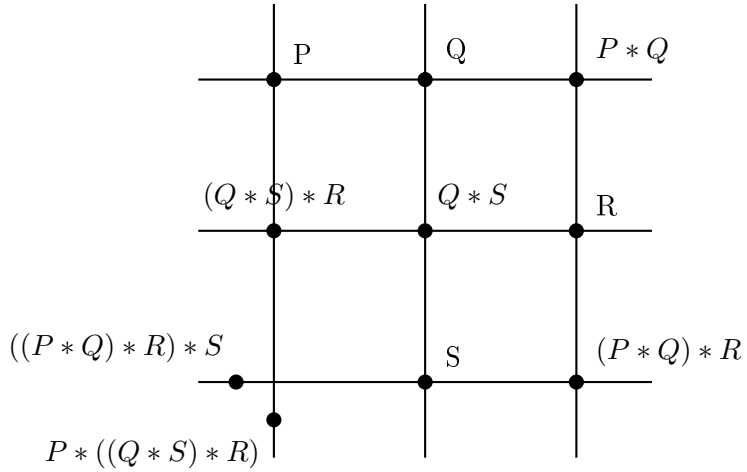
We are now ready to prove the following properties of the operation defined above.

Proposition 1.5. *Let E be an elliptic curve, then $\forall P, Q, R, S \in E$ the following hold:*

1. $P * Q = Q * P$;
2. $(P * Q) * P = Q$;
3. $P * Q = P$ *if the line L_{PQ} connecting P, Q is tangent to the curve at P;*
4. $((P * Q) * R) * S = P * ((Q * S) * R)$.

Proof. 1. The lines L_{PQ} and L_{QP} coincide.

2. Take $P, Q, R \in L_{PQ} \cap E$, the three points of intersection of L_{PQ} with E. Then $(P * Q) * P = R * P = Q$.



3. If L_{PP} is the tangent line to E at P, the only other intersection point in $L_{PP} \cap E$ is Q.

4. P, Q, $P * Q$, $(Q * S) * R$, $Q * S$, R, S, $(P * Q) * R$, $P * ((Q * S) * R)$ are 9 points of intersection of E and the cubic curve generated by the vertical lines in the above figure. Then, by Lemma 1.4, the cubic curve generated by the horizontal lines, containing 8 of the 9 previous points, must pass also through $P * ((Q * S) * R)$. As the intersection of E and the horizontal lines must contain at most 9 points by Bezout's Theorem [45], $((P * Q) * R) * S$ must coincide with $P * ((Q * S) * R)$. □

We use the previous operation to define a composition law on the group of point of E.

Definition 1.6. Let O be the point at infinity of an elliptic curve E, then we define the following composition law:

$$\begin{aligned} \oplus : \quad & E \times E \longrightarrow E \\ & (P, Q) \longmapsto P \oplus Q := O * (P * Q). \end{aligned} \tag{1.5}$$

We first prove that the above definition is actually a group law, then we give explicit formulae to compute this by means of affine coordinates for a curve with equation 1.4.

Theorem 1.7. *The composition law 1.5 has the following properties:*

1. *If a line L intersects E at the points P, Q, R (not necessarily distinct), then:*

$$(P \oplus Q) \oplus R = O;$$

2. *(identity element) $P \oplus O = P, \qquad \forall P \in E;$*

3. *(commutativity) $P \oplus Q = Q \oplus P, \qquad \forall P, Q \in E;$*

4. *(inverse) $\forall P \in E$ there is a point denoted by $\ominus P$ such that $P \oplus (\ominus P) = O;$*

5. *(associativity) $(P \oplus Q) \oplus R = P \oplus (Q \oplus R), \qquad \forall P, Q, R \in E.$*

In other words, $(E, \oplus)$ is an abelian group with identity element O. Moreover, if we assume that E is defined over K, then $E(L)$ is a subgroup of $E = E(\bar{K})$ for every field L such that $K \leq L \leq \bar{K}$.

Proof. We prove all parts mainly using properties of Proposition 1.5.

1. $(P \oplus Q) \oplus R = O * ((O * (P * Q)) * R) = O * ((O * R) * R) = O * O = O$.
2. $P \oplus O = O * (P * O) = O$.
3. Follows directly from the commutativity of the operation $*$ and the definition of 1.5.
4. Consider $\ominus P = P * O$ and check that it is the inverse element of P; indeed $P \oplus (P * O) = (P \oplus O) \oplus (P * O) = O$, where the two equalities follow from (1) and (2)
5. $(P \oplus Q) \oplus R = O * (((P * Q) * O) * R) = O * (P * ((Q * R) * O)) = O * (P * (Q \oplus R)) = P \oplus (Q \oplus R)$.

Finally, if P, Q have coordinates in L, then the equation of L_{PQ} has coefficients in L. If further E is defined over K, then the third point of intersection must have coordinates given by a rational combination of the coefficients of both the line and the curve and hence in L. This proves that $E(L) \leq E$. □

We will use only $+$ and $-$ instead of $\oplus$ and $\ominus$ to ease the notation. We also define for each $m \in \mathbb{Z}$ a *scalar multiplication* function $[m] : E \longrightarrow E$:

$$P \longmapsto [m]P := \begin{cases} \underbrace{P + P + \ldots + P}_{m \text{ times}} & \text{if } m \geq 0, \\ \underbrace{(-P) + (-P) + \ldots + (-P)}_{-m \text{ times}} & \text{if } m < 0. \end{cases} \tag{1.6}$$

Next we can find explicit formulae for the group law, assuming to have an elliptic curve defined by the affine equation $y^2 = x^3 + ax + b$; note that one can also derive the formulae for a general Weierstrass equation [52] with a similar approach. Given $P_1, P_2 \in E(K)$, to apply the Definition 1.5 we need to compute $P = P_1 * P_2$ and then $O * P$. We will use projective coordinates to easily interpret lines that contain O.

Lemma 1.8. *Let $P = \left[x, y, 1\right] \in \mathbb{P}^2_K$ such that $P \in E$, then $O * P = \left[x, -y, 1\right]$.*

Proof. The line connecting P with O has points given by the following equation:

$$\left[x, y, 1\right] + \alpha \left[x, y - 1, 1\right] = \left[(\alpha + 1)x, (\alpha + 1)y - \alpha, \alpha + 1\right].$$

By substitution in the curve's homogeneous equation $Y^2Z = X^3 + aXZ^2 + bZ^3$ we get:

$$\begin{aligned} & y^2(\alpha+1)^3 + \alpha^2(\alpha+1) - 2y\alpha(\alpha+1)^2 = x^3(\alpha+1)^3 + a(\alpha+1)^3x + b(\alpha+1)^3 \\ \Leftrightarrow \quad & (y^2 - x^3 - ax - b)(\alpha+1)^2 + \alpha^2 - 2y\alpha(\alpha+1) = 0 \\ \Leftrightarrow \quad & \alpha(\alpha(1-2y) - 2y) = 0, \end{aligned}$$

where the first left hand side term in the second equation vanishes since $\left[x, y, 1\right]$ belongs to the curve. Thus a solution is $\alpha = 0$, which gives P, and the other is $\alpha = 2y/(1-2y)$, so that

$$O * P = \left[\tfrac{x}{1-2y}, \tfrac{-y}{1-2y}, \tfrac{1}{1-2y}\right] = \left[x, -y, 1\right]. \qquad \square$$

If, in the previous Lemma, we consider the affine coordinates, then given $P = (x, y)$, it holds $O * P = (x, -y)$.
It only remains to compute $P_1 * P_2$, where $P_i = \left[x_i, y_i, 1\right]$ $i = 1, 2$. We assume $P_1 \neq P_2$ and also $P_1, P_2 \neq O$; then we compute the connecting line $L_{P_1P_2}$ in the projective plane.

$$L_{P_1P_2} : \qquad 0 = \begin{vmatrix} X & x_1 & x_2 \\ Y & y_1 & y_2 \\ Z & 1 & 1 \end{vmatrix} = X(y_1 - y_2) - Y(x_1 - x_2) + Z(x_1y_2 - y_1x_2)$$

Assuming that $x_1 \neq x_2$, the previous equation becomes

$$Y = mX + qZ,$$

with

$$m = \frac{y_1 - y_2}{x_1 - x_2}, \qquad q = \frac{x_1 y_2 - y_1 x_2}{x_1 - x_2}.$$

The unique point at infinity of the curve is $O = \big[0, 1, 0\big]$, which does not lay on the line, hence we can now look at $L_{P_1P_2}$ by means of affine coordinates. The dehomogenisation with respect to Z gives $y = mx + q$ and by substitution in the affine equation of E, we get the cubic equation

$$x^3 - m^2x^2 + (a - 2mq)x + b - q^2 = 0.$$

Note that two distinct roots of this equation, namely x_1, x_2, are already known since $P_1, P_2 \in L_{P_1P_2} \cap E$. Denoting by t the third one, we can write the cubic as

$$(x - x_1)(x - x_2)(x - t) = x^3 - (x_1 + x_2 + t)x^2 + \dots.$$

Therefore, the corresponding degree 2 terms must be equal and we have

$$x_1 + x_2 + t = m^2 \implies t = m^2 - x_1 - x_2.$$

Using the line's equation we find the coordinates of $P_1 * P_2$ and according to Lemma 1.8 it suffices to change the second coordinate sign to get

$$P_1 + P_2 = (m^2 - x_1 - x_2; -m^3 + mx_1 + mx_2 - q). \tag{1.7}$$

Next assume $x_1 = x_2 = \overline{x}$ and $y_1 \neq y_2$, so that the points are still distinct. We can find the line connecting them as before, getting $L_{P_1P_2} : \ X = Z\overline{x}$. This equation is satisfied by O which must be the third point in $L_{P_1P_2} \cap E$. Then note that $O * O = O$ and hence $P_1 + P_2 = O$.
The last case left is when $P_1 = P_2 = \big[\bar{x}, \bar{y}, 1\big]$; we take as connecting line the tangent line to E at $P_1 = P_2 = P$. Note that, as we proved in our general hypotheses, all points of E are non-singular, thus L_{PP} is given by

$$\frac{\partial E}{\partial X}(\bar{x}, \bar{y}, 1)X + \frac{\partial E}{\partial Y}(\bar{x}, \bar{y}, 1)Y + \frac{\partial E}{\partial Z}(\bar{x}, \bar{y}, 1)Z = 0,$$

which gives the equation

$$(-3\bar{x}^2 - a)X + 2\bar{y}Y + (\bar{y}^2 - 2a\bar{x} - 3b)Z = 0.$$

If $\bar{y} = 0$ the line becomes $(-3\bar{x}^2 - a)X - (2a\bar{x} + 3b)Z = 0$ and O belongs to it; this shows that the third point of $L_{PP} \cap E$ is O and $P_1 + P_2 = O$.
Otherwise, if $\bar{y} \neq 0$ we can work on the affine equation for L_{PP}:

$$y = mx + q.$$

where

$$m = \frac{3\bar{x}^2 + a}{2\bar{y}}, \qquad q = \frac{-\bar{y}^2 + 2a\bar{x} + 3b}{2\bar{y}}$$

and hence we can apply the same procedure as in the first case. Substituting in the curve's equation we get again a cubic equation in the indeterminate x, of which we know the

double root $\bar{x}$. Comparing the degree two term of that equation with the corresponding one in

$$(x-\bar{x})^2(x-t)=0 \qquad \Longleftrightarrow \qquad x^3-(2\bar{x}+t)x^2+(\bar{x}^2+2\bar{x}t)x-\bar{x}^2t=0,$$

we find out that

$$t=m^2-2\bar{x}.$$

Hence substituting in the equation for L_{PP} and changing the second coordinate sign we have

$$P+P=(m^2-2\bar{x},-m^3+2m\bar{x}-q)$$

To sum up we state the following theorem.

Theorem 1.9 (Group law formulae)**.** *Let $E:\ y^2=x^3+ax+b$ be an elliptic curve and $P_i=(x_i,y_i)\neq O$, with $i=1,2$. Define $P=P_1+P_2$, then:*

1. *If $x_1\neq x_2$ we have*

$$P=(m^2-x_1-x_2;-m^3+mx_1+mx_2-q),$$

with

$$m=\frac{y_1-y_2}{x_1-x_2}, \qquad q=\frac{x_1y_2-y_1x_2}{x_1-x_2}.$$

2. *If $x_1=x_2$, but $y_1\neq y_2$, we have $P=O$.*

3. *If $P_1=P_2$ and $y_1=0$, we have $P=O$.*

4. *If $P_1=P_2=(\bar{x},\bar{y})$ and $\bar{y}\neq 0$, we have*

$$P=(m^2-2\bar{x},-m^3+2m\bar{x}-q),$$

with

$$m=\frac{3\bar{x}^2+a}{2\bar{y}}, \qquad q=\frac{-\bar{y}^2+2a\bar{x}+3b}{2\bar{y}}.$$

These formulae show that the operation + can be computed in polynomial time, since all the expressions found contain only sums, multiplications and fractions. As we can see, the group law formulae are more complicated than operations on integers modulo n, classically used in cryptography. However, the important fact is the existence of such a group law that makes subgroups of the points of E appropriate also for cryptographic purposes.

1.3 Finding points on elliptic curves

The existence of a group structure in every set $E(L)$ is certainly a nice property, but it should be stressed that it is useful in cryptography only in case we are able to efficiently find random points on the curve. A procedure that would give such a point on $E:\ y^2=x^3+ax+b$, with $a,b\in K$, is the following:

1. given a field $L\supseteq K$, randomly choose $x\in L$;

2. solve $y^2=x^3+ax+b$ for y; if there are no solutions, then go to step (1),

3. if the solution is unique then set $P=(x,y)$, otherwise set $P=(x,y_j)$, where j is randomly chosen in $\{1,2\}$ and y_1,y_2 are the two distinct solutions to the curve equation in the variable y.

In this way, we have established a possible method that has few acceptable drawbacks; firstly, it is not possible to find O, but this is not cryptographically interesting, since it is the identity of the group and hence not relevant. Secondly, points $(x, 0)$ on the x-axis have slightly more probability to be found since that result does not lead to the final random choice between two different solutions. If the group is sufficiently large, the difference from uniform distribution is small, because there are at most three such points (intersections between the x-axis line and E).
The efficiency of the previous procedure depends on methods used in finding square roots in a field. We will show that this is possible in whatever finite field with probabilistic polynomial time, applying a variant of the Tonelli-Shanks algorithm [3]. One can find faster algorithms in [9], which are beyond the aim of this thesis.

1.3.1 Tonelli-Shanks Algorithm

Let $q = p^k$ with p an odd prime and consider the finite field $\mathbb{F}_q$. Let first show some preliminary results.

Proposition 1.10. *Let $\mathbb{F}_q$ be the finite field with q elements. There are $q-1$ squares in $\mathbb{F}_q$ if q is even and $\frac{1}{2}(q-1)$ squares if q is odd.*

Proof. Recall that the multiplicative group $\mathbb{F}_q^*$ of a finite field is cyclic. Hence define the map

$$\begin{aligned} \sigma : \quad \mathbb{F}_q^* &\longrightarrow \mathbb{F}_q^* \\ x &\longmapsto x^2, \end{aligned} \tag{1.8}$$

which is a group homomorphism. Its kernel is

$$\ker(\sigma) = \{1\} \cup \{g \in \mathbb{F}_q^* \mid \mathrm{ord}(g) = 2\};$$

and has cardinality

$$|\ker(\sigma)| = \begin{cases} 1 & \text{if } q \text{ is even;} \\ 2 & \text{if } q \text{ is odd.} \end{cases}$$

Indeed, if q is odd then $2 \mid (q-1)$ and so there exists a unique element of order 2. Otherwise, if q is even, then $2 \nmid q-1$ and $\mathbb{F}_q^*$ contains no elements of order 2. Hence, by isomorphism theorems:

$$\frac{\mathbb{F}_q^*}{\ker(\sigma)} \cong \mathrm{Im}(\sigma) \implies |\mathrm{Im}(\sigma)| = \begin{cases} q-1 & q \text{ even;} \\ \frac{1}{2}(q-1) & q \text{ odd.} \end{cases}$$ □

The next result shows how to find square roots in a particular case.

Proposition 1.11. *Let G be a group of odd order m and let $a \in G$, then $x^2 = a$ has a unique solution in G, which is $a^{(m+1)/2}$.*

Proof. Note that if we set $x := a^{(m+1)/2}$, we have $x^2 = a^{m+1} = a^m a = a$. To prove the uniqueness, let us consider the map 1.8 and note that it is injective. Indeed, being m odd we can write $m + 1 = 2k$ and, assuming $x^2 = y^2$, we have:

$$x = x^{2k} = y^{2k} = y.$$

Since G is finite the map is also surjective and hence a bijection. □

Keeping the previous results in mind, we see what happens in general; at first, we can easily write $q-1 = 2^s t$ for some t odd dividing by 2 as many times as possible. By the structure theorem for cyclic abelian groups we know that

$$\mathbb{F}_q^* \cong \mathbb{Z}_{2^s} \times \mathbb{Z}_t$$

Thus we have $H = \{(1,h) : h \in \mathbb{Z}_t\}$, the unique subgroup of order t of the cyclic group $\mathbb{F}_q^*$. Next, if $\mathbb{Z}_{2^s} = \langle k \rangle$, we build a chain of subgroups

$$H = G_0 \subseteq G_1 \subseteq \ldots \subseteq G_{s-1} \subseteq G_s = \mathbb{F}_q^*, \tag{1.9}$$

with $|G_{s-i}| = 2^{s-i}t$ and $|\frac{G_i}{G_{i-1}}| = 2$. To get each subgroup of the chain it suffices to take $G_j \coloneqq \langle k^{2^{s-j}} \rangle \times \mathbb{Z}_t$ for all $j = 1, \ldots, s$. Next, consider the quotient G_s/H and the projection map:

$$G_s \xrightarrow{\pi} \frac{G_s}{H} \cong \mathbb{Z}_{2^s}.$$

Proposition 1.12. *If $g \in \mathbb{F}_q^*$ is not a square, then $\pi(g) = gH$ is a generator of G_s/H.*

Proof. By contradiction we assume that gH does not generate G_s/H and we show that it must be $g = a^2$, with $a \in \mathbb{F}_q^*$. As $\mathbb{F}_q^* \cong \mathbb{Z}_{2^s} \times H \cong \langle k \rangle \times \langle h \rangle$, we can write $g = (k^a, h^b)$ with $1 \leq a \leq 2^s$ and $1 \leq b \leq t$. By Proposition 1.11, we know that $\left(h^b\right)^{(t+1)/2}$ is a square root of $h^b \in \mathbb{Z}_t$. It remains to check if k^a is a square too; we see that

$$\mathrm{ord}(k^a) = \frac{\mathrm{ord}(k)}{(\mathrm{ord}(k), a)} = \frac{2^s}{(2^s, a)} = 2^s \quad \Leftrightarrow \quad (2^s, a) = 1.$$

By the initial hypothesis, k^a cannot have order 2^s, thus a must be even. This shows that $k^a = (k^{a/2})^2$. □

Note that, assuming q odd, it exists a non-square element, because in this case only half of the elements in $\mathbb{F}_q^*$ are squares by 1.10. We do not know a deterministic algorithm that finds a non-square element, so we will pick $g \in \mathbb{F}_q^*$ at random and Proposition 1.10 gives probability $\frac{1}{2}$ to find a non-square. This property can be tested efficiently by the following Proposition.

Proposition 1.13. *A non zero element $a \in \mathbb{F}_q$ is a square (respectively non-square) if and only if:*

$$a^{\frac{q-1}{2}} = 1 \qquad \textit{(respectively -1).}$$

Proof. Consider the polynomial $f(x) = x^{q-1} - 1$ in $\mathbb{F}_q[x]$ and let $a \in \mathbb{F}_q^*$. As $a^q = a$ holds in $\mathbb{F}_q^*$, we see that every element of the group is a root of $f(x)$. Therefore, the polynomial has exactly $q-1$ roots; moreover

$$f(x) = \left(x^{\frac{q-1}{2}} + 1\right)\left(x^{\frac{q-1}{2}} - 1\right), \tag{1.10}$$

because $q-1$ is even. Since in $\mathbb{F}_q$ there are no zero divisors and we know $f(a) = 0$, then either $a^{\frac{q-1}{2}} = -1$ or $a^{\frac{q-1}{2}} = 1$ for all $a \in \mathbb{F}_q^*$. Both the polynomials in the product have exactly $\frac{1}{2}(q-1)$ roots and note that if $a = b^2$, $b \in \mathbb{F}_q^*$ then $a^{\frac{q-1}{2}} = b^{q-1} = 1$. We conclude that the square elements on $\mathbb{F}_q$ are exactly the roots of the second factor in 1.10 and the non-square ones are roots of the first. □

The previous results allow us to find a generator gH of G_s/H; therefore, it is always possible to write every element $a \in \mathbb{F}_q^*$ in the form $g^e h$, for some $h \in H$. The idea is to find the square root of a computing it separately for g^e and h. The latter has an easy square root provided by Proposition 1.11; for the first one we should use the above construction. We look at the chain 1.9 and we start from the top, since we are given $a \in G_s$; we want to descend the chain multiplying a by powers of the non-square element, which we can write as $g = (k^{2\gamma+1}, h^\delta)$. Initialize an exponent counter $e_1 \coloneqq 0$ and let $a = (k^{2\alpha}, h^\beta)$ be a square; we check it applying Proposition 1.13. It follows that $a \in \langle k^2 \rangle \times \langle h \rangle = G_{s-1}$.
We now examine the first step of the algorithm, where we check if $a \in G_{s-2}$: this happens if and only if $a^{\frac{q-1}{2^2}} = a^{2^{s-2}t} = 1$, because:

- $|G_{s-2}| = 2^{s-2}t$ gives that $a \in G_{s-2} \Rightarrow a^{2^{s-2}t} = 1$;
- on the contrary, $1 = a^{2^{s-2}t} = (k^{2^{s-1}\alpha t}, h^{2^{s-2}bt}) \Leftrightarrow 2^s | (2^{s-1}\alpha t)$; since t is odd, we have that $2 \mid \alpha$ and $a \in \langle k^4 \rangle \times \langle h \rangle = G_{s-2}$.

If that condition is true we set $e_2 \coloneqq e_1$, otherwise, if $a^{\frac{q-1}{4}} \neq 1$, it is easy to see that α is odd, as before. Thus we consider ag^{-2} and we show that it is contained in G_{s-2}:

$$\begin{aligned}\left(ag^{-2}\right)^{2^{s-2}t} &= \left(k^{2\alpha-2(2\gamma+1)}, h^{\beta-2\delta}\right)^{2^{s-2}t} \\ &= \left(k^{-2^s t\gamma + 2^{s-1}t(\alpha-1)}, h^{(\beta-2\delta)2^{s-2}t}\right) = (1,1),\end{aligned}$$

because $\alpha - 1$ is even and so 2^s divides the exponent of k. Thus we update the exponent counter for g setting $e_2 \coloneqq e_1 + 2^{2-1}$.
In general, given e_{i-1} such that $ag^{-e_{i-1}} \in G_{s-i+1}$, we want to define e_i such that $ag^{-e_i} \in G_{s-i}$.

- If $\left(ag^{-e_{i-1}}\right)^{\frac{q-1}{2^i}} = 1$, we have

  $$\left(k^{2\alpha - e_{i-1}(2\gamma+1)}, h^{\beta - e_{i-1}\delta}\right)^{2^{s-i}t} = (1,1) \quad \Rightarrow \quad 2^s \mid 2^{s-i}t(2\alpha - e_{i-1}(2\gamma+1)).$$

  Therefore $2^i \mid 2\alpha - e_{i-1}(2\gamma+1)$ and hence $ag^{-e_{i-1}} \in G_{s-i} = \langle k^{2^i} \rangle \times \langle h \rangle$. We set $e_i \coloneqq e_{i-1}$.

- Otherwise, observe that $ag^{-e_{i-1}-2^{i-1}} \in G_{s-i}$. First, we remark that it easy to see by construction that $2 \mid e_{i-1}$ and, as before, we find out that $2^i \nmid 2\alpha - e_{i-1}(2\gamma+1)$, but 2^{i-1} divides it by definition of e_{i-1}. Then we have

  $$\left(ag^{-(e_{i-1}+2^{i-1})}\right)^{2^{s-i}t} = \left(k^{2^{s-i+1}t\alpha - (2^{s-i}e_{i-1}+2^{s-1})(2\gamma+1)t}, h^{(\beta - e_{i-1}\delta - 2^{i-1}\delta)2^{s-i}t}\right),$$

  where the second component is 1 because $t = \mathrm{ord}(h)$ divides the exponent, so the previous identity becomes, after few calculations,

  $$k^{-2^s\gamma t} \cdot k^{2^{s-1}t\left(\frac{2\alpha-(2\gamma+1)e_{i-1}}{2^{i-1}} - 1\right)} = 1.$$

  Indeed, as seen before, $2 \mid \left(\frac{2\alpha-(2\gamma+1)e_{i-1}}{2^{i-1}} - 1\right)$. In this case we set $e_i \coloneqq e_{i-1} + 2^{i-1}$.

We apply the previous steps for $i = 2, \ldots, s$ and output $g^{\frac{e_s}{2}} h^{\frac{t+1}{2}}$; this process is known as *randomized Tonelli-Shanks* algorithm.

Theorem 1.14. *The randomized Tonelli-Shanks algorithm on $\mathbb{F}_q^*$, with q an odd prime power, fails with probability $1/2$; if it does not fail it returns a square root of a, provided that $a \in \mathbb{F}_q^*$ is a square.*

Proof. A random choice for the non-square element g will succeed with probability $1/2$, then after Tonelli-Shanks loop we end up with $ag^{-e_s} \in H$ and $2 \mid e_s$ We conclude that $g^{\frac{e_s}{2}} h^{\frac{t+1}{2}}$ is actually the square root of a. □

To sum up, we write down the algorithm.

Algorithm 1 Tonelli-Shanks Algorithm - computes $b = \sqrt{a}$ with $a \in \mathbb{F}_q^*$ and q odd.

Require: q odd, $a \in \mathbb{F}_q^*$.
Ensure: $b = \sqrt{a}$
$A \leftarrow a$
$Z \leftarrow g \overset{\text{R}}{\in} \mathbb{F}_q^*$
if $Z^{\frac{q-1}{2}} = 1$ **then**
  fail
else $\{Z$ in a non-square$\}$
  let $q - 1 = 2^s t$
  $e \leftarrow 0$
  for $i = 2$ to s **do**
    if $(AZ^{-e})^{\frac{q-1}{2^i}} \neq 1$ **then**
      $e \leftarrow e + 2^{i-1}$
    end if
  end for
  $h \leftarrow AZ^{-e}$
  return $b \leftarrow Z^{\frac{e_s}{2}} h^{\frac{t+1}{2}}$
end if

This proves that it is possible to efficiently find random points on the set of rational points of an elliptic curve over a finite field.

Chapter 2

The Weil pairing

The aim of this chapter is to define the Weil pairing, that is a bilinear map defined on the product of two subgroups of an elliptic curve's group of points. This provides an example of a map for the pairing based cryptography. We need, at first, to generalize the definition of elliptic curve, in order to introduce some tools that are necessary to define the Weil pairings.

2.1 Algebraic varieties and curves

A slightly more general approach to elliptic curves involves some algebraic geometry tools. We briefly introduce affine and projective algebraic varieties and see how general curves, and more specifically elliptic ones, are defined as some of them. Then we will give some definitions related to varieties, before introducing the Weil map. We denote by $K[X] = K[X_1, \dots, X_n]$ the ring of n-variate polynomials over the field K and by $\mathbb{A}^n$, $\mathbb{P}^n$ the affine and projective spaces over the algebraic closure $\bar{K}$ of the field K.

Definition 2.1. Given an ideal $I \subset \bar{K}[X]$, we say that the *affine algebraic set* relative to I is the set:

$$V_I = \{P \in \mathbb{A}^n : f(P) = 0,\ \forall f \in I\}.$$

Moreover, if V is an affine algebraic set, the associated ideal $I(V)$ is the ideal of $\bar{K}[X]$ given by

$$I(V) = \{f \in \bar{K}[X] :\ f(P) = 0\ \forall P \in V\}.$$

We say that an affine algebraic set V is defined over K, and we denote it by V/K, if $I(V)$ is generated by polynomials in $K[X]$. Its set of *K-rational points* is

$$V(K) = V \cap \mathbb{A}^n_K.$$

Eventually, we say that V is an *affine variety* when $I(V)$ is a prime ideal in $\bar{K}[X]$.

We see that every ideal of $K[X]$ and $\bar{K}[X]$ is finitely generated, since every field is Noetherian and thus Hilbert's basis theorem applies, showing that these polynomial rings are Noetherian. An important consequence is that every affine algebraic set V is the zero set of a finite set of polynomials. Therefore, an algebraic set is defined over the field K if and only if there exist a finite set $\{f_1, \dots, f_s\} \subseteq K[X]$ such that for every $f \in I(V)$ we have $f = f_1 r_1 + \cdots + f_s r_s$ for some $r_1, \dots, r_s \in \bar{K}[X]$.

Remark 2.2. Let V be an affine algebraic set and define $I(V/K) \coloneqq I(V) \cap K[X]$. Then V is defined over K if and only if:

$$I(V) = I(V/K)\bar{K}[X].$$

Indeed, if we assume the previous equality, we see that for every $f \in I(V)$ we have $f = \sum_{i=0}^{l} g_i r_i$, where $g_i \in I(V/K) \subseteq K[X]$ and $r_i \in \bar{K}[X]$ for $i = 0, \ldots, l$. Thus, $I(V)$ is generated by polynomials of $K[X]$. The converse follows from the definition of ideal.

Definition 2.3. The *affine coordinate ring* of an affine variety V/K is the quotient ring

$$K[V] \coloneqq \frac{K[X]}{I(V/K)} = \frac{K[X]}{I(V) \cap K[X]}.$$

We also call its field of fractions $K(V)$ the *function field* of V/K. We similarly define $\bar{K}[V]$ and $\bar{K}(V)$.

To justify the previous definition we remark that $K[V]$ is a commutative integral domain, because V is an affine variety, thus $I(V)$ is a prime ideal and so $I(V) \cap K[X]$ is a prime ideal in $K[X]$. Recall that the quotient of a ring by a prime ideal is an integral domain. Moreover, the affine coordinate ring is Noetherian since it is the quotient of a Noetherian ring.

Definition 2.4. Let V be an affine variety and $P \in V$. We define the following ideal in $\bar{K}[V]$:

$$M_P \coloneqq \{f \in \bar{K}[V] : \ f(P) = 0\},$$

which is maximal since the map

$$\frac{\bar{K}[V]}{M_P} \longrightarrow \bar{K} \qquad f \mapsto f(P)$$

is an isomorphism. Indeed, it is clearly a ring homomorphism, which is surjective because any $k \in \bar{K}$ it is the image of the coset $f(X) = k + M_P$. It is also injective, since distinct cosets $f + M_P, g + M_P \in \bar{K}[V]/M_P$ are such that $f - g \notin M_P$, or equivalently $f(P) - g(P) \neq 0$. Then the quotient ring is a field, M_P is maximal and thus prime. Notice also that M_P/M_P^2 is a finite dimensional $\bar{K}$-vector space.

Proposition 2.5. *The local ring of the affine variety V at P*

$$\bar{K}[V]_P \coloneqq \left\{ f \in \bar{K}(V) : \ f = \frac{g}{h}, \textit{ with } g, h \in \bar{K}[V],\ h(P) \neq 0 \right\}.$$

is Notherian and local.

Proof. We claim that $\bar{K}[V]_P$ is the localization of $\bar{K}[V]$ at M_P. Indeed, the set $S \coloneqq \bar{K}[V] \setminus M_P$ is multiplicatively closed and it gives the localization $S^{-1}\bar{K}[V] =: A$. The set:

$$\widetilde{M_P} \coloneqq \left\{ \frac{f}{s} : f \in M_P,\ s \in S \right\}$$

is a well-defined ideal of A and for every $g/t \in A \setminus \widetilde{M_P}$ we have that $g \in S$ and hence g/t is a unit of A. It follows that $\widetilde{M_P}$ is the unique maximal ideal of A and so that A is local. To conclude, it is well-known that the localization of a Noetherian ring is still Notherian. □

Therefore, the evaluation at P of every quotient of polynomials $f = g/h \in \bar{K}[V]_P$ is well defined. Moreover, the functions in $\bar{K}[V]_P$ are said to be *regular* (or *defined*) at P.

Definition 2.6. Let V be an affine variety: we say that its dimension, denoted by $\dim_{\mathbb{A}^n}(V)$, is the transcendence degree of $\bar{K}(V)$ over $\bar{K}$.

Definitions and results about transcendence degree can be found for example in [58], [37] and we do not study this topic here, because it's beyond the aim of this work.

These definitions can be stated also in the projective case with few differences; the two cases are related, as usual, by the homogeneization and dehomogeneization mappings. We say that an ideal $I \subset \bar{K}[X]$ is homogeneous if it is generated by homogeneous polynomials. We associate to every such ideal a subset of the projective space by means of the following definition.

Definition 2.7. Given a homogeneous ideal $I \subset \bar{K}[X]$ we say that its associated *projective algebraic set* is:

$$V_I = \{P \in \mathbb{P}^n : f(P) = 0,\ \forall f \in I\}.$$

Moreover, if V is a projective algebraic set, the associated homogeneous ideal $I(V)$ is the ideal of $\bar{K}[X]$ generated by

$$\{f \in \bar{K}[X] : f \text{ homogeneous},\ f(P) = 0\ \forall P \in V\}.$$

We say that such a V is defined over K, denoting it by V/K, if $I(V)$ can be generated by homogeneous polynomials in $K[X]$. Its set of *K-rational points* is

$$V(K) = V \cap \mathbb{P}^n_K.$$

Eventually, we say that V is a *projective variety* if $I(V)$ is a prime ideal in $\bar{K}[X]$.

Same properties as before hold for projective varieties defined over the field K and similarly it is possible to construct the coordinate ring and the function field of a projective variety V/K as $K[V \cap \mathbb{A}^n]$ and $K(V \cap \mathbb{A}^n)$ respectively. Notice that different choices of the affine space $\mathbb{A}^n \subset \mathbb{P}^n$ give different projective function fields, but they are all canonically isomorphic [52]. In general, we say that functions $f \in \bar{K}(V)$ are *regular* or *defined* at P if they are in the local ring $\bar{K}[V]_P$, which is still defined in the projective case as the (affine) local ring of $V \cap \mathbb{A}^n$.

Remark 2.8. In particular, if we consider an elliptic curve E/K with Weierstrass equation 1.4 and we set $f(X,Y) = Y^2 - X^3 - aX - b$, with $a, b \in K$, then the relative function field is

$$K(E) = \mathrm{Frac}\left(\frac{K[X,Y]}{\langle f(X,Y)\rangle}\right).$$

Similarly as before, the projective dimension of a variety V is defined as:

$$\dim_{\mathbb{P}^n}(V) = \dim_{\mathbb{A}^n}(V \cap \mathbb{A}^n).$$

With all this new notions we can work on elliptic curves in a more general context. They were defined, in the first chapter, as the zero loci of the Weierstrass equations as 1.4. In general, we can define a curve to be a projective variety of dimension 1. This means that we have the same definitions that we have just studied in this section also in the case of elliptic curves. Next, we give some other definitions about curves in general. We assume for our purpose that curves are non-singular, because we focus on elliptic curves that are so. Recall that in this general context we define a *smooth* or *non-singular* point P of a variety V as a point such that

$$\left(\frac{\partial f_i}{\partial X_j}(P)\right)_{1 \le i \le m,\, 1 \le j \le n}$$

has rank $n - dim(V)$, where $f_i \in \bar{K}[X]$ for $i = 1, \ldots, m$ are generators for $I(V)$. A variety is said to be *smooth* or *non-singular* if all its points are smooth.
The local ring of a curve $\mathcal{C}$ at P is a Noetherian local domain by Proposition 2.5. It follows, by [2, Proposition 9.2], that it is a discrete valuation ring, because one can show:

$$\dim_{\bar{K}}(\widetilde{M}_P/\widetilde{M}_P^2) = 1.$$

We have the following discrete valuation map.

Definition 2.9. Let $\mathcal{C}$ be a curve and $P \in \mathcal{C}$; the *normalized valuation* on $\bar{K}[\mathcal{C}]_P$ is the following map:

$$\begin{aligned} &\mathrm{ord}_P : \bar{K}[\mathcal{C}]_P \longrightarrow \{0, 1, \ldots\} \cup \{\infty\} \\ &\mathrm{ord}_P(f) \coloneqq \sup\{d \in \mathbb{Z} : \ f \in M_P^d\}. \end{aligned}$$

Note that it is a discrete valuation since:

- $\mathrm{ord}_P(fg) = \mathrm{ord}_P(f) + \mathrm{ord}_P(g)$, for every $f, g \in \bar{K}[\mathcal{C}]_P$;
- $\mathrm{ord}_P(f + g) \geq \min(\mathrm{ord}_P(f), \mathrm{ord}_P(g))$, for every $f, g \in \bar{K}[\mathcal{C}]_P$.

From the definition it easily follow that $\mathrm{ord}_P(f/g) = \mathrm{ord}_P(f) - \mathrm{ord}_P(g)$, hence the map ord_P can be extended to $\bar{K}(\mathcal{C})$:

$$\mathrm{ord}_P : \bar{K}(\mathcal{C}) \longrightarrow \mathbb{Z} \cup \{\infty\}.$$

Functions in $\bar{K}(\mathcal{C})$ are quotients of polynomials $f(X) = g(X)/h(X)$; we say that roots of the polynomial g are *zeros* of the function and roots of h are *poles* of f. It clearly follows by definition of the mapping ord_P relative to $P \in \mathcal{C}(\bar{K})$ that:

- if $k = \mathrm{ord}_P(f) > 0$ then f has a zero at P of multiplicity k;
- if $k = \mathrm{ord}_P(f) < 0$ then f has a pole at P of multiplicity $-k$;
- if $k = \mathrm{ord}_P(f) \geq 0$ then f is *regular* (or defined) at P.

This last condition agrees with the definition of regular (or defined) function that we gave above, when we first defined the function fields.
To keep track of zeros and poles of a function we introduce divisors. We say that the *divisor group* $\mathrm{Div}(\mathcal{C})$ of a curve is the free abelian group generated by the points of $\mathcal{C}$. So a divisor $D \in \mathrm{Div}(\mathcal{C})$ is a formal sum:

$$D = \sum_{P \in \mathcal{C}} n_p \, (P),$$

with $n_P \in \mathbb{Z}$ and $n_P = 0$ for almost every $P \in \mathcal{C}$. We call the sum $\deg(D) \coloneqq \sum_{P \in \mathcal{C}} n_p$ *degree* of the divisor D. It is possible to associate to every function $f \in \bar{K}(C)^*$ its divisor

$$\mathrm{div}(f) = \sum_{P \in \mathcal{C}} \mathrm{ord}_P(f) \, (P).$$

Note that $\mathrm{div}(f) \in \mathrm{Div}(\mathcal{C})$ since, by [52, Proposition II,1.2], there are only finitely many points of $\mathcal{C}$ that are zeros or poles of f, thus the previous sum has just finitely many terms. We say that a divisor $D \in \mathrm{Div}(\mathcal{C})$ is *principal* if $D = \mathrm{div}(f)$ for some $f \in \bar{K}(C)^*$. Moreover, two divisors $D_1, D_2 \in \mathrm{Div}(\mathcal{C})$ are called *linearly equivalent* if $D_1 - D_2$ is principal. We will apply [52, Propositions III,3.3-3.5], that are the following results about divisors on elliptic curves.

Proposition 2.10. *Let E/K an elliptic curve and $D = \sum_{P\in E} n_P(P) \in Div(E)$, then D is principal if and only if $\sum_{P\in E} n_P = 0$ and $\sum_{P\in E}[n_P]P = O$, where we denote by $[\cdot]$ the scalar multiplication map 1.6.*

Proposition 2.11. *Let E/K be an elliptic curve and let $P, Q \in E$. Then, (P) and (Q) are linearly equivalent if and only if $P = Q$.*

2.2 Maps between curves

After some basic definitions and properties about curves we examine maps between them, first in general and then for elliptic ones. The main reference here is [52] too. We begin giving a couple of definitions about maps and morphisms.

Definition 2.12. Let $V_1, V_2 \subseteq \mathbb{P}^n$ projective varieties. A *rational map* from V_1 to V_2 is a map

$$\varphi : V_1 \longrightarrow V_2$$
$$\varphi = [f_0, \ldots, f_n],$$

such that $f_0, \ldots, f_n \in \bar{K}(V_1)$ are defined on every $P \in V_1$ and whose images give a point of V_2:

$$\varphi(P) = [f_0(P), \ldots, f_n(P)] \in V_2.$$

Definition 2.13. A rational map of projective varieties $\varphi = [f_0, \ldots, f_n]$ from V_1 to V_2 is *regular* at $P \in V_1$ if it exists $g \in \bar{K}(V_1)$ such that:

1. $gf_0, \ldots, gf_n$ are regular at P,
2. $(gf_j)(P) \neq 0$ for some $j \in \{1, \ldots, n\}$.

If such a g exists we set $\varphi(P) = [gf_0(P), \ldots, gf_n(P)]$. If, moreover, the map is regular at every point of V_1 we say that it is a *morphism*.

Note that the function g in Definition 2.13 depends on the point $P \in V_1$. Morphisms have the following property.

Proposition 2.14. *Let $\varphi : \mathcal{C}_1 \to \mathcal{C}_2$ be a morphism of curves, then φ is either constant or surjective.*

Moreover, the following result gives conditions for a rational map to be a morphism.

Proposition 2.15. *Let $\mathcal{C}$ be a curve, $V \subseteq \mathbb{P}^n$ a projective variety, $P \in \mathcal{C}$ a smooth point and $\varphi : \mathcal{C} \to V$ a rational map. Then φ is regular at P and, moreover, if $\mathcal{C}$ is smooth then φ is a morphism.*

Next, consider two curves $\mathcal{C}_1/K$, $\mathcal{C}_2/K$ and $\varphi : \mathcal{C}_1 \to \mathcal{C}_2$ a non-constant rational map defined over K. Composition with φ induces an injection of function fields fixing K:

$$\varphi^* : K(\mathcal{C}_2) \longrightarrow K(\mathcal{C}_1) \qquad \varphi^* f = f \circ \varphi. \tag{2.1}$$

Indeed, applying the above results we know that φ needs to be surjective, so if $f \circ \varphi(P) = g \circ \varphi(P)$, $\forall P \in \mathcal{C}_1$, then f and g coincide on $\mathcal{C}_2$. We say that a rational map of curves is *separable*, *inseparable* or *purely inseparable* if the extension field $K(\mathcal{C}_1)/\varphi^* K(\mathcal{C}_2)$ has the same property.
Proposition 2.15 can be applied to elliptic curves, which are smooth, and to the rational maps canonically associated to them, which have explicit formulae given by Theorem 1.9. This gives the following result.

Proposition 2.16. *Let E/K be an elliptic curve, the maps giving the group law on E:*

$$\begin{aligned} +: E \times E &\to E \\ (P_1, P_2) &\mapsto P_1 + P_2 \end{aligned} \qquad \text{and} \qquad \begin{aligned} -: E &\to E \\ P &\mapsto -P. \end{aligned}$$

are morphisms of curves.

2.2.1 Isogenies

When studying elliptic curves it is useful to describe a particular case of maps between them, that are *isogenies*.

Definition 2.17. Let E_1, E_2 be two elliptic curves. An *isogeny* between E_1 and E_2 is a morphism of curves

$$\varphi : E_1 \longrightarrow E_2,$$

such that $\varphi(O) = O$. E_1 and E_2 are *isogenous* if there exists an isogeny φ between them, such that $\varphi(E_1) \neq \{O\}$.

Note that by 2.14 we see that every isogeny φ satisfies either $\varphi(E_1) = \{O\}$ or $\varphi(E_1) = E_2$. Let

$$\mathrm{Hom}(E_1, E_2) \coloneqq \{\text{isogenies } \varphi : E_1 \to E_2\}.$$

We prove that $\mathrm{Hom}(E_1, E_2)$ is a group under the addition law:

$$(\varphi + \psi)(P) = \varphi(P) + \psi(P).$$

Indeed, by Proposition 2.16, the map $\varphi + \psi$ given by:

$$E_1 \xrightarrow{\varphi \times \psi} E_2 \times E_2 \xrightarrow{+_{E_2}} E_2$$

$$P \longmapsto (\varphi(P), \psi(P)) \longmapsto \varphi(P) + \psi(P),$$

is a composition of morphisms and thus a morphism. Moreover, it clearly maps O to itself and hence it is an isogeny. As $+_{E_2}$ is a group law for the group of points of the elliptic curve E_2, it follows that the addition between isogenies defines a group law for the set $\mathrm{Hom}(E_1, E_2)$. Since isogenies are maps between the groups of points of elliptic curves it seems natural to focus our attention on isogenies that are group homomorphisms. It turns out that all of them have this property.

Theorem 2.18. *Let E_1, E_2 be elliptic curves and $\varphi : E_1 \to E_2$ an isogeny. Then:*

$$\varphi(P + Q) = \varphi(P) + \varphi(Q),$$

for all $P, Q \in E_1$.

Therefore, $\mathrm{Hom}(E_1, E_2)$ is exactly the group of those morphisms of curves that are group homomorphisms. The *endomorphism ring* of an elliptic curve E is defined as $\mathrm{End}(E) = \mathrm{Hom}(E, E)$. It actually has a ring structure setting:

$$(\varphi\psi)(P) = \varphi \circ \psi(P).$$

The distributive law follows from Proposition 2.18:

$$(\alpha + \beta) \circ \gamma(P) = (\alpha + \beta)(\gamma(P)) = \alpha(\gamma(P)) + \beta(\gamma(P)) = \alpha \circ \gamma(P) + \beta \circ \gamma(P).$$

The invertible elements of the endomorphism ring form the *automorphism group* of E, denoted by $\mathrm{Aut}(E)$. We implicitly worked on groups of rational points over $\bar{K}$, but clearly if the curves are defined over a field K we can look at isogenies defined over K. Their collection is the group $\mathrm{Hom}_K(E_1, E_2)$ and consequently we define the endomorphism ring $\mathrm{End}_K(E)$ and the automorphism group $\mathrm{Aut}_K(E)$ over K.

Next, we focus on three particularly useful maps. The first one is the *translation-by-Q* map:

$$\tau_Q : E \longrightarrow E, \qquad \tau_Q(P) = P + Q. \tag{2.2}$$

It follows from the addition formulae 1.9 that it is a rational map and so a morphism, thanks to Proposition 2.15 and smoothness of elliptic curves. For every $Q \in E$ the map τ_{-Q} provides an inverse for the translation-by-Q map, thus every such morphism is actually an isomorphism. Clearly τ_Q is not an isogeny, unless $Q = O$. It is interesting to notice, here, that any morphism of elliptic curves is the composition of an isogeny and a translation.

Proposition 2.19. *Let $F : E_1 \to E_2$ be any morphism of elliptic curves. Then $F = \tau \circ \varphi$, where τ is a translation map as 2.2 and $\varphi \in \mathrm{Hom}(E_1, E_2)$ is an isogeny.*

Proof. The map

$$\varphi = \tau_{-F(O)} \circ F$$

is a composition of morphisms, such that $\varphi(O) = F(O) - F(O) = O$. Hence φ is an isogeny and we get $F = \tau_{F(O)} \circ \varphi$, as wanted. □

Therefore, it follows immediately from Proposition 2.18 that every morphism is the composition of a group homomorphism and a translation.
Secondly, we study the family of multiplication maps $[m]$, with $m \in \mathbb{Z}$, acting on points of elliptic curves as defined in 1.6. Recall that if a curve is defined over K, then also $[m]$ is so.

Proposition 2.20. *For each $m \in \mathbb{Z}$ the map $[m] : E \to E$ defined by 1.6 is an isogeny. Moreover, if $m \neq 0$ then it is non-constant.*

Proof. For every $m \in \mathbb{Z}$, arguing by induction on m, we get from Proposition 2.16 that the repeated sum is an isogeny.
To prove that $[m]$ is non-constant, we first study the case $m = 2$. Consider an elliptic curve given by the equation 1.4 and let $P = (x, y) \in E$; from the explicit addition formulae 1.9 we get that the x-coordinate of $[2]P$ is:

$$\frac{x^4 - 2ax^2 - 8bx + a^2}{4(x^3 + ax + b)}.$$

Since $\mathrm{char}(K) \neq 2, 3$, if P has order 2, then it satisfies the identity

$$x^3 + ax + b = 0.$$

Hence only finitely many points of E have order 2 and so $[2] \neq [0]$. Now, since $[mn] = [m] \circ [n]$, applying the previous claim, we are reduced to considering the case of odd m. Dividing the numerator by the denominator with the division algorithm for polynomials we get $-3ax^2 - 9bx + a^2$ as residue. If it vanishes, then also the discriminant of the curve must vanish, as can be easily checked. So the denominator does not divide the numerator and we can find x_0 such that the former vanishes for $x = x_0$, but not the latter. Choosing y_0 such that $P_0 = (x_0, y_0) \in E$, then P_0 is a non-trivial point of order 2, since $[2]P_0 = O$. For an odd m we have $[m]P_0 = P_0 \neq O$, that concludes the proof. □

An important consequence of this result is that all the maps $[m]$, for $m \in \mathbb{Z}$, $m \neq 0$, are surjective, because they are non-constant morphisms of curves.
Eventually, assume the elliptic curve E/K is defined over a field with $\text{char}(K) = p$, with $p > 0$. Let $q = p^k$ and recall that the q-th power map $K \to K$ is a homomorphism, that acts as the identity on $\mathbb{F}_q$; more precisely, $x \in \mathbb{F}_q$ if and only if $x^q = x$. Then, if E is the zero locus of $f(x, y) = y^2 - x^3 - ax - b$ (1.4), let $E^{(q)}$ be the curve generated by $f^{(q)}(x, y) = y^2 - x^3 - a^q x - b^q$. Note that $E^{(q)}$ is an elliptic curve too, being the zero locus of a Weierstrass equation, and it is non-singular, since by means of an easy computation it holds $\Delta(E^{(q)}) = \Delta(E)^q \neq 0$. The *q-th Frobenius morphism* is the map:

$$\Phi_q : E \longrightarrow E^{(q)} \qquad \Phi_q(x, y) = (x^q, y^q). \tag{2.3}$$

Indeed, for every point $P = (x, y) \in E$, it holds:

$$f^{(q)}(\Phi_q(P)) = f^{(q)}(x^q, y^q) = f(x, y)^q = 0.$$

The map is actually a morphism, since Proposition 2.15 applies; furthermore, having $\Phi_q(O) = O$, Φ_q is an isogeny. In particular, if $K = \mathbb{F}_q$, then $E = E^{(q)}$ and so the q-th Frobenius map is an endomorphism of $E/\mathbb{F}_q$, whose set of fixed points is exactly $E(\mathbb{F}_q)$.

2.3 Weil pairing

We finally have the background to construct the Weil pairing. First, we need to define an important subgroup of points on an elliptic curve. From now on all the curves E/K are defined over a finite field $K = \mathbb{F}_{p^k}$ of characteristic p. Let $n = |E(K)|$ and assume without loss of generality that $(n, p) = 1$ since, on the contrary, one can set the anomalous attack [57], which breaks the discrete logarithm problem in linear time.

Definition 2.21. Let $r \in \mathbb{N}$, $r \neq 0$; the subgroup of $E(L)$, with $L \supseteq K$, given by

$$E(L)[r] = \{P \in E(L) : [r]P = O\},$$

is called the *$r-$torsion subgroup*. Its elements are all points whose order divides r. We simply denote by $E[r]$ the subgroup $E(\bar{K})[r]$.

The $r-$torsion subgroup is the kernel of the scalar multiplication map $[r]$. Clearly it exists some integer $m \geq 1$ such that $E(\mathbb{F}_{p^m})[r] = E[r]$ and then for all $m' > m$ we have $E\left(\mathbb{F}_{q^{m'}}\right)[r] = E[r]$. Next theorem describes the structure of $E[r]$; its proof follows from theorems about isogenies, that we do not study.

Theorem 2.22. *Let E/K be an elliptic curve and let $r \in \mathbb{N}$, $r \neq 0$. Then it holds:*

1. *if either* $\text{char}(K) = 0$ *or* $\text{char}(K) = p > 0$, *with* $(p, r) = 1$, *then:*

$$E[r] = \mathbb{Z}_r \times \mathbb{Z}_r;$$

2. *if* $\text{char}(K) = p > 0$, *then one of the following holds:*

   (a) $E[p^j] = \{O\}$, *for all* $j = 1, 2, 3 \ldots$
   (b) $E[p^j] = \mathbb{Z}_{p^j}$, *for all* $j = 1, 2, 3 \ldots$

This result leads to the following classification of elliptic curves.

Definition 2.23. An elliptic curve E/K, defined over a field K of characteristic $p > 0$, is called *supersingular* if $E[p] = \{O\}$ and *ordinary* otherwise.

Now, we can actually construct the Weil pairing; we denote by $r \geq 2$ an integer prime to p. Let $T \in E[r]$ and consider the divisor $D = r(T) - r(O)$. This is principal thanks to Proposition 2.10, i.e. $D = \mathrm{div}(f)$ for some function $f \in \bar{K}(E)$. Next, it exists $T' \in E$ such that $[r]T' = T$, because the multiplication map is surjective. Applying again 2.10, we get that it exists a function $g \in \bar{K}(E)$ such that:

$$\mathrm{div}(g) = \sum_{R \in E[r]} (T' + R) - (R).$$

Indeed, it suffices to note that the coefficients of the divisors sum to zero and

$$\sum_{R \in E[r]} T' + R - R = [r^2]T = [r]T = O,$$

because the $r-$torsion group $E[r]$ contains r^2 elements. The function g does not depend on the choice of T', since varying $R \in E[r]$, all the points $P = T' + R$ are such that $[r]P = T$. Therefore, we could write:

$$\mathrm{div}(g) = \sum_{[r]P = T} (P) - \sum_{R \in E[r]} (R).$$

Then, zeros and poles of the composite function $f \circ [r]$ are points such that multiplied by r give T and O respectively, or in other words they are zeros and poles of f. So we have:

$$\mathrm{div}(f \circ [r]) = r \left(\sum_{[r]P = T} (P) \right) - r \left(\sum_{R \in E[r]} (R) \right) = r \, \mathrm{div}(g) = \mathrm{div}(g^r).$$

Therefore we can assume, multiplying by a suitable constant, that $g^r = f \circ [r]$. Next, let $S \in E[r]$ and $P \in E$ (it could be $P = T$ too); we have:

$$g(P + S)^r = f([r](P + S)) = f([r]P) = g(P)^r.$$

This proves that $g(P + S)/g(P) \in \mu_r$ is an r-th root of unity. So we can define a map, which is called *Weil e_r-pairing*, by:

$$\begin{aligned} e_r &: E[r] \times E[r] \longrightarrow \mu_r \\ e_r(S, T) &= \frac{g(P + S)}{g(P)}, \end{aligned} \tag{2.4}$$

where $P \in E$ is any point such that both $g(P + S)$ and $g(P)$ are defined and non-zero. Note that although g is defined up to multiplication by an element of $\bar{K}^*$, the Weil map does not depend on it.
Before investigating the connection between the Weil map and cryptographic pairings, we need to prove some properties. We start with a lemma on Galois theory on elliptic function fields, that we will apply in the next proof. $\mathrm{Aut}(L/K)$ denotes the group of automorphisms of the extension field L/K that fix elements of K.

Lemma 2.24. *If $\varphi : E_1 \to E_2$ is an isogeny, then the map:*

$$\begin{aligned} \ker\varphi &\longrightarrow \mathrm{Aut}\left[\bar{K}(E_1)/\varphi^*\bar{K}(E_2)\right] \\ T &\longmapsto \tau_T^* \end{aligned}$$

is a group isomorphism, where τ_T denotes the translation-by-T map 2.2 and τ_T^* the automorphism induced on $\bar{K}(E_1)$ as in 2.1. Moreover, if φ in separable, then $[\bar{K}(E_1)/\varphi^*\bar{K}(E_2)$ is a Galois extension.

The proof of this fact is part of [52, Theorem III,4.10]. From Galois theory, the last part of the statement is equivalent to say that $\varphi^*\bar{K}(E_2)$ contains exactly the elements which are fixed by the automorphisms of $\bar{K}(E_1)$, i.e. it is the *fixed field* of the group of automorphisms.

Theorem 2.25. *The Weil e_r-pairing defined by 2.4 is:*

1. *bilinear:* $e_r(S_1+S_2,T) = e_r(S_1,T)e_r(S_2,T)$;
   $e_r(S,T_1+T_2) = e_r(S,T_1)e_r(S,T_2)$
2. *alternating:* $e_r(S,T) = e_r(T,S)^{-1}$;
3. *non-degenerate: if $e_r(S,T) = 1$ for all $S \in E[r]$, then $T = O$;*
4. *compatible: if $Q \in E[rs]$ and $T \in E[r]$, then $e_{rs}(S,T) = e_r([s]Q,T)$.*

Proof. 1. As in the previous construction, let $P \in E$; linearity in the first factor of the map follows immediately from the definition:

$$e_r(S_1+S_2,T) = \frac{g(P+S_1+S_2)}{g(P+S_1)} \cdot \frac{g(P+S_1)}{g(P)} = e_r(S_2,T)e_r(S_1,T).$$

For the second factor let $f_1, f_2, f_3 \in \bar{K}(E)$ and $g_1, g_2, g_3 \in \bar{K}(E)$ the functions defined above, relative to points T_1, T_2 and $T_3 \coloneqq T_1 + T_2$ respectively. By Proposition 2.10, it exists a function $h \in \bar{K}(E)$, with divisor

$$\mathrm{div}(h) = (T_1+T_2) - (T_1) - (T_2) + (O).$$

Moreover, we have:

$$\mathrm{div}\left(\frac{f_3}{f_1 f_2}\right) = r(T_1+T_2) - r(O) - r(T_1) + r(O) - r(T_2) + r(O) = r\,\mathrm{div}(h).$$

This proves that it exists a constant $c \in \bar{K}^*$ such that $f_3 = cf_1f_2h^r$. Then, if we compose with the map $[r]$ and recall that $f_i \circ [r] = g_i^r$ for $i = 1,2,3$, we get:

$$g_3^r = f_3 \circ [r] = c(f_1f_2h^r) \circ [r] = c(f_1 \circ [r])(f_2 \circ [r])(h \circ [r])^r = cg_1^r g_2^r (h \circ [r])^r.$$

So it exists another constant $c' \in \bar{K}^*$ such that $g_3 = c'g_1g_2(h \circ [r])$ and hence:

$$\begin{aligned} e_r(S,T_1+T_2) &= \frac{g_3(P+S)}{g_3(P)} \\ &= \frac{g_1(P+S)g_2(P+S)h([r]P+[r]S)}{g_1(P)g_2(P)h([r]P)} \\ &= e_r(S,T_1)e_r(S,T_2), \end{aligned}$$

because $[r]S = O$ and thus the factors with h simplify.

2. From (1) we get the identity:

$$e_r(S+T,S+T) = e_r(S,S)e_r(S,T)e_r(S,T)e_r(T,T).$$

So, if we show that $e_r(T,T) = 1$ for all $T \in E[r]$, the identity (2) follows immediately from the above equation.
For every point $Q \in E$, consider the translation-by-Q map τ_Q 2.2. It holds:

$$\operatorname{div}\left(\prod_{i=0}^{r-1} f \circ \tau_{[i]T}\right) = \sum_{i=0}^{r-1} \operatorname{div}\left(f \circ \tau_{[i]T}\right) = \sum_{i=0}^{r-1} r([1-i]T) - r([-i]T) = 0.$$

Indeed, if f has a zero at T of multiplicity r, then $f\left(\tau_{[i]T}([1-i]T)\right) = f(T) = 0$. So $[1-i]T$ is a zero of $f \circ \tau_{[i]T}$, with the same multiplicity r; the same idea applies for the pole. This equality proves that $\prod_{i=0}^{r-1} f \circ \tau_{[i]T}$ is constant. Then, we choose $T' \in E$ such that $[r]T' = T$, whose existence is provided by the surjectivity of the map $[r]$. The product $\prod_{i=0}^{r-1} g \circ \tau_{[i]T'}$ is also constant, because for every $P \in E$:

$$\begin{aligned}\left(\prod_{i=0}^{r-1} g \circ \tau_{[i]T'}(P)\right)^r &= \prod_{i=0}^{r-1} f\left([r](P+[i]T')\right) \\ &= \prod_{i=0}^{r-1} f\left([r]P+[i]T\right) \\ &= \prod_{i=0}^{r-1} f \circ \tau_{[i]T}([r]P),\end{aligned}$$

where we know that the last product is constant. Its evaluation at P and $P+T'$, gives:

$$\prod_{i=0}^{r-1} g(P+[i]T') = \prod_{i=0}^{r-1} g(P+[i+1]T').$$

When we simplify likewise terms on both sides of this equation, it remains the identity $g(P) = g(P+[r]T') = g(P+T)$. We conclude that:

$$e_r(T,T) = \frac{g(P+T)}{g(P)} = 1.$$

3. $e_r(S,T) = 1$ for all $S \in E[r]$ implies that $g(P+S) = g(P)$ for every $S \in E[r]$. Recall that $[r] : E \to E$ is a non constant isogeny with $\ker[r] = E[r]$ and it induces the map $[r]^* : \bar{K}(E) \to \bar{K}(E)$ on the function field. It can be proved that if $\operatorname{char}(K) \nmid r$, as this is the case, then the map $[r]$ is separable and hence, setting $\varphi = [r]$, the automorphism group of Lemma 2.24 is a Galois group. Note that τ_S^* fixes g for all $S \in E[r] = \ker[r]$, since:

$$g(P) = g(P+S) = g(\tau_S(P)) = (\tau_S^* g)(P).$$

Thus, g is contained in the fixed field $[r]^*\bar{K}(E)$ and we have $g = h \circ [r]$, for some $h \in \bar{K}(E)$. Therefore

$$(h \circ [r])^r = g^r = f \circ [r],$$

so that f and h^m are equal up to multiplication by a constant. Finally, since $m \operatorname{div}(h) = \operatorname{div}(f)$, we get $\operatorname{div}(h) = (T) - (O)$ and so we conclude that $T = O$, by Proposition 2.11.

4. Consider the functions $f, g \in \bar{K}(E)$, as defined above, and note that $\mathrm{div}(f^s) = rs(T) - rs(O)$. Then, recalling the above expression for $\mathrm{div}(g)$, we have:

$$\begin{aligned}\mathrm{div}\,(f \circ [rs])^s &= rs\left(\sum_{[rs]P=T}(P)\right) - rs\left(\sum_{R\in E[rs]}(R)\right)\\ &= rs\left(\sum_{[r]([s]P)=T}(P)\right) - rs\left(\sum_{([s]R)\in E[r]}(R)\right) = \mathrm{div}\left((g\circ[s])^{rs}\right).\end{aligned}$$

Therefore, it exists a constant $c \in \bar{K}^*$ such that $(g \circ [s])^r s = c(f \circ [rs])^s$. Following the procedure that defines the Weil pairing we get:

$$e_{rs}(Q,T) = \frac{g\circ[s](P+Q)}{g\circ[s](P)} = \frac{g(P'+[s]Q)}{g(P')} = e_r([s]Q,T),$$

where $P' = [s]P$. □

Recall that, assuming $(\mathrm{char}(K), r) = 1$, the r-th roots of unity form a cyclic group of order r and, thanks to Theorem 2.22, $E[r]$ has $\mathbb{Z}_r$-vector space structure.

Corollary 2.26. *There exist points $S, T \in E[r]$ such that $e_r(S,T)$ is a primitive r-th root of unity.*

Proof. Let $\mu_d = \{e_r(S,T) : S, T \in E[r]\}$, with $d \mid r$, and note that μ_d is a subgroup of μ_r, since the Weil pairing is bilinear and alternating. Thus, for all $S, T \in E[r]$, it holds:

$$1 = e_r(S,T)^d = e_r([d]S, T).$$

Non-degeneracy implies that $[d]S = O$ and since this holds for every $S \in E[m]$, which contains also some element of order m, it must be $d = m$. □

Remark 2.27. It also possible to prove that if $E[r] \subset E(K)$, then $\mu_r \subset K^*$ (see [52]).

Corollary 2.28. *Let $S, T \in E[r]$, such that $e_r(S,T)$ is a primitive r-th root of unity. Then the map:*

$$f : \langle S\rangle \longrightarrow \mu_r \qquad f(R) = e_r(R,T) \tag{2.5}$$

is a group isomorphism.

A proof follows immediately from properties in 2.26.

Chapter 3

Cryptographic pairings

3.1 Security problems

We have examined some basic facts about elliptic curves, because of their importance in cryptography. They provide an alternative to the common choice of finite groups $\mathbb{F}_q^*$, for some integer q, in cryptographic applications. One of the earliest works on elliptic curves cryptography (ECC) was proposed by Koblitz [35] in 1987; the group of points $E(\mathbb{F}_p)$, on some elliptic curve, can be used to construct cryptosystems and this approach gives an advantage in terms of group size. For example, when working on multiplicative groups of finite fields we need to consider, for security's sake, finite fields that have 1024-bit size. Elliptic curves group law needs more complex formulae to be computed and this leads to a higher computational cost. However, it is often sufficient to take smaller groups, of about 160-bit size, in order to guarantee the same security level. This because, at the moment, there is no known specialized algorithm to solve the discrete logarithm problem 3.1 on elliptic curves: the most efficient ones do not apply to the case of elliptic curves, as discussed in [43]. The best generic methods are based on the birthday paradox and have $O(\sqrt{n})$ expected running time, where n is the group order. For this reason we can work on elliptic curves defined on smaller finite fields than those used in the common multiplicative group case. This compensates for the increased complexity of the group operations, because the underlying field arithmetic is faster. Though, one should be careful about the choice of elliptic curves and security parameters, because of improvements in the efficiency of algorithms solving the discrete logarithm problem on finite fields. This induces a modification of these parameters; some comments and up-to-date information can be found in [46].
We define the discrete logarithm problem (DLP), that is of great importance in cryptography, since the security of many cryptosystems rely on its hardness and on related problems. The choice of its additive formulation is due to the additive structure of the group of points on an elliptic curve.

Definition 3.1 (DLP)**.** Let $G = \langle P \rangle$ be an additive group of order n. An instance of the *discrete logarithm problem (DLP)* on G is the problem, given $P, Q \in G$, of computing the integer $x \in \{0, \dots, n-1\}$ such that $Q = xP$.

The corresponding problem on elliptic curves has an analogue definition, which uses the multiplication maps 1.6. This problem is believed to be intractable for certain groups [41], including the multiplicative group of a finite field and the group of points of an elliptic curve. A second crucial problem, which has been studied since the beginning of modern cryptography is the following.

Definition 3.2 (CDHP)**.** Let $G = \langle P \rangle$ be an additive cyclic group of order n. An instance of the *computational Diffie-Hellman problem (CDHP)* on G is the problem, given $P, aP, bP \in G$, of computing abP.

Notice that the DHP easily reduces in polynomial time to the DLP. There are many problems related to DHP; one of its most studied weaker versions is the following.

Definition 3.3 (DDHP)**.** Let $G = \langle P \rangle$ be an additive group of order n. An instance of the *decisional Diffie-Hellman problem (DDHP)* on G is the problem, given $P, aP, bP, cP \in G$, of verifying whether $cP = abP$ holds in G.

Of course, being able to solve the CDHP allows immediately to solve the DDHP. We will examine some variants of these problems in chapter 4.
We show an approximate comparison of ECC on $E(\mathbb{F}_p)$ and "conventional" cryptography on $\mathbb{F}_q^*$. Denote by $n = \lceil \log_2 p \rceil$ and $N = \lceil \log_2 q \rceil$ the approximate sizes of field elements in the different cases. Algorithms solving the DLP on elliptic curves generally have complexity proportional to

$$C_{\mathrm{EC}}(n) = 2^{n/2},$$

as can be found in [10]. Then let:

$$L_q(\mu, c) = \exp\left(c(\ln q)^{\mu}(\ln \ln q)^{1-\mu}\right) \tag{3.1}$$

be a complexity function, dependent on the parameters μ, c. When $\mu = 1$ the function L_q is exponential in $\ln q$, while for $\mu = 0$ it is polynomial in $\ln q$. If $0 < \mu < 1$ the behaviour is strictly between polynomial and exponential and it is usually called *sub-exponential*. Algorithms solving the DLP on elliptic curves have exponential complexity in n, while sub-exponential algorithms solving the same problem in $\mathbb{F}_q^*$ are available. Indeed, discrete logarithms in such groups can be found in time proportional to $L_q(1/3, c_0)$; for example, there exist algorithms that achieve $c_0 \approx 1.92$. Under certain assumptions on the characteristic of the field, this parameter has been lowered [5, 33]. These new parameters are more suitable for the implementation of cryptosystems, but they do not change the ideas of this comparison. In terms of N and neglecting constant factors, we find that the complexity in the "conventional" case is proportional to:

$$C_{\mathrm{conv}}(N) = \exp\left(c_0 N^{1/3}(\ln(N \ln 2))^{2/3}\right).$$

Equating $C_{\mathrm{EC}}(n)$ and $C_{\mathrm{conv}}(N)$ and neglecting constant factors, it follows that in order to achieve a similar level of security in both cases, it results:

$$n = c_1 N^{1/3}(\ln(N \ln 2))^{2/3},$$

where $c_1 \approx 4.91$. The constants n, N can be interpreted as key sizes, expressed in bits, for cryptosystems in the two cases. One can find a detailed discussion on some well-known modern algorithms and their complexities in [20, ch. 19-20].

A classical example in cryptography is the Diffie-Hellman key exchange protocol, which is computationally secure if the CDHP hardness holds. Let $G = \langle P \rangle$ be an additive cyclic group of order n; the users Alice and Bob want to share a common secret key without any handshake procedure. Assume that P and n are publicly known. The communication channel between the users is public and adversaries could get the information shared through it. The protocol consists of the following steps:

1. Alice chooses a secret random integer $a \in \{0, \ldots, n-1\}$ and sends aP to Bob;
2. Bob chooses a secret random integer $b \in \{0, \ldots, n-1\}$ and sends bP to Alice;
3. both Alice and Bob compute abP, which will be their common secret key.

If an adversary, that collects n, P, aP, bP, tries to compute the secret key it would have to solve an instance of the CDHP. This protocol has only one exchange round, since the messages are independent and can be exchanged at the same time. Moreover, we can easily extend this procedure to the case of three users: they choose the secret personal parameters a, b, c and, after two exchange rounds, they agree on the common key $abcP$. An adversary that is able to compute it from the knowledge of $n, P, aP, bP, cP, abP, acP, bcP$ could get the final secret key. This problem is believed to be not easier than CDHP [41]. It remains to understand whether it is possible to find a one-round key exchange protocol, secure against an attacker that observes the communications. Joux in 2000 was able to apply bilinear pairings, that will be introduced in the next section, to construct such a protocol. There are many other examples of pairing-based cryptography, such as identity-based encryption, by Boneh and Franklin [14], and the short signature scheme by Boneh, Lynn and Shacham [17], that arise interest in studying those maps. Further information and bibliography can be found in [41]. A more recent work by Boneh, Gentry and Waters exploits bilinear pairings to construct a broadcast encryption scheme, which is proved fully collusion secure [15]. An interesting feature of elliptic curves, which allows their application to pairing-based cryptography, is the existence of bilinear pairings defined on some subgroups the rational points group. The Weil pairing 2.4, is an easy example of such maps.

3.2 Cryptographic bilinear pairings

In the remainder of this chapter, we give three different definitions of cryptographic pairings and we prove, in the end, that the Weil map fits them. We consider maps defined on additive groups in analogy to the elliptic curves case. We denote by aP the sum of $a \in \mathbb{Z}$ times the group element P and we write 0 for the zero in additive groups or 1 for the identity in multiplicative groups.

Definition 3.4 (Symmetric bilinear pairing)**.** Let G, H be respectively an additive and a multiplicative cyclic group of prime order r and let P be a generator of G. A *symmetric bilinear pairing* or *type-1 pairing* is an efficiently computable map

$$e : G \times G \longrightarrow H$$

such that it is:

1. *non-degenerate*: $e(P, P) \neq 1$;
2. *bilinear*: $e(aS, bT) = e(S, T)^{ab}$, for all $a, b \in \mathbb{Z}$ and $S, T \in G$.

The properties of Definition 3.4 imply that when P is a generator of G, then $e(P, P)$ is a generator of H. Indeed, by bilinearity $e(P, P)^r = e(0, P) = 1$. Moreover, if $e(P, P)^h = 1$ for some $h < r$, then $e(hP, P) = 1$ and hence, by bilinearity, $e(hP, t) = 1$ for all $t \in G$. We conclude, since non-degeneracy gives $hP = 0$, while $\mathrm{ord}(P) = r$.
It follows that a symmetric bilinear pairing is completely determined by the value it takes at $e(P, P)$. Besides the degenerate map, given by $e(P, P) = 0$, there are other $r - 1$ ones

that are all equivalent up to a constant. If e_1, e_2 are symmetric pairings, then it exists $c \in \mathbb{Z}$ such that for all $P_1, P_2 \in G$:

$$e_1(P_1, P_2) = e_1(aP, bP) = e_1(P, P)^{ab} = (e_2(P, P)^c)^{ab} = e_2(P_1, P_2)^c,$$

Furthermore, these maps are symmetric, since:

$$e(aP, bP) = e(P, P)^{ab} = e(bP, aP).$$

Remark 3.5. The non-degeneracy condition of the symmetric pairing is equivalent to:

$$e(P_1, P_2) = 1 \quad \forall P_1 \in G \Leftrightarrow P_2 = 0 \qquad \text{and} \qquad e(P_1, P_2) = 1 \quad \forall P_2 \in G \Leftrightarrow P_1 = 0$$

Indeed, assuming the conditions of Definition 3.4 and the identities $e(aP, bP) = 1$, for all $b \in \mathbb{Z}$, then $e(b(aP), P) = 1$ for every $b \in \mathbb{Z}$. Thus if, by contradiction, $aP \neq 0$, then aP must be a generator of G, that has prime order r. Hence $b(aP) = P$ for some $b \in \{0, \ldots, r-1\}$ and so we get a contradiction. On the other hand, $e(0, xP) = e(P, P)^{xr} = 1$ for all $P_2 = xP \in G$. The same proof holds for the second variable.
Conversely if, by contradiction, $e(P, P) = 1$, then it holds $e(aP, P) = 1$ for all $a \in \mathbb{Z}$ and hence it would be $P = 0$.

Note that the efficient computability is a strong requirement of Definition 3.4.

In order to get more general definitions, one can loose a bit the symmetry requirement, allowing maps defined on the product of different groups.

Definition 3.6 (Asymmetric bilinear pairing)**.** Let G_1, G_2 be additive cyclic groups and let H be a multiplicative cyclic group, all of prime order r. Assume that there exists an efficiently computable isomorphism of groups $\varphi : G_2 \to G_1$, such that its inverse $\varphi^{-1} : G_1 \to G_2$ is not. An *asymmetric bilinear pairing* or *type-2 pairing* is an efficiently computable map

$$e : G_1 \times G_2 \longrightarrow H$$

such that it is:

1. *non-degenerate*: $e(P_1, P_2) = 1$ for all $P_2 \in G_2$ if and only if $P_1 = 0$ and $e(P_1, P_2) = 1$ for all $P_1 \in G_1$ if and only if $P_2 = 0$;
2. *bilinear*: $e(aS, bT) = e(S, T)^{ab}$, for all $a, b \in \mathbb{Z}$ and $S, T \in G$.

The existence of an efficiently computable isomorphism with non efficient inverse has many consequences. In particular, one can analyse the pairings performance, vulnerabilities of cryptosystems due to the application of different types of pairing and the influence of the isomorphism on relations between cryptographic problems, like Diffie-Hellman and its variants. We do not focus on these topics: some comments on them can be found in [53, 55] and related works. If $\varphi : G_2 \to G_1$ had an efficiently computable inverse, then type-2 pairings would essentially be the same as type-1 ones. Indeed, consider e as in 3.6 and the symmetric bilinear pairing $\sigma : G_2 \times G_2 \to H$, defined by the choice of $\sigma(P_2, P_2) \coloneqq e(\varphi(P_2), P_2)$, where P_2 is a generator of G_2. Note that $\varphi(P_2)$ is a generator of G_1 and hence, for every $S \in G_1$ and $T \in G_2$:

$$\begin{aligned} e(S, T) &= e(a\varphi(P_2), bP_2) \\ &= e(\varphi(P_2), P_2)^{ab} \\ &= \sigma(P_2, P_2)^{ab} \\ &= \sigma(aP_2, P_2) = \sigma(\varphi^{-1}(S), T). \end{aligned}$$

Thus, the asymmetric pairing can be viewed as a symmetric one. In general, even if φ^{-1} is not efficiently computable, one can define from the asymmetric pairing a symmetric one:

$$\begin{aligned}\tilde{e}: \quad & G_2 \times G_2 \longrightarrow H \\ & (aP_2, bP_2) \longmapsto e(\varphi(aP_2), bP_2) = e(\varphi(P_2), P_2)^{ab},\end{aligned}$$

with $a, b \in \{0, \ldots, r-1\}$. Note that we can prove, similarly to the symmetric case, that when $G_2 = \langle P_2 \rangle$, then $e(\varphi(P_2), P_2)$ is a generator of H. Moreover, assuming that the hypotheses in Definition 3.6 hold, we can still require DDHP to be hard in G_1, but not in G_2 any more. Indeed, it is possible to check, by means of an efficient computation, whether $e(\varphi(aP_2), bP_2) = e(\varphi(P_2), cP_2)$. If this holds, then $e(\varphi(P_2), P_2)^{ab} = e(\varphi(P_2), P_2)^c$; it follows that $ab \equiv c \mod r$ and hence $abP_2 = cP_2$ in G_2. Given the inefficient computability of φ^{-1}, it is not possible to apply the same idea to solve the DDHP on G_1. Eventually, we can make the previous definition even more general.

Definition 3.7. Let G_1, H be an additive and a multiplicative cyclic group of order r, respectively, and let G_2 be an additive group where each element has order dividing r. If there exist no efficiently computable homomorphism neither from G_1 to G_2 nor in the other direction, then we call *general pairing* the non-degenerate, bilinear map defined at 3.6.

Here the integer r needs not to be prime and the group G_2 needs not to be cyclic. However, if no efficiently computable homomorphism exists, the definition gives a *type-3 pairing*, according to literature. We give this general definition, as in [39, ch. 1], since in some works on pairing-based cryptography are considered groups of composite orders and type-3 pairings [13, 16].

Remark 3.8. Assume that the hypotheses in Definition 3.7 hold and let $P_1 \in G_1$ and $P_2 \in G_2$, both elements of order r; then $\langle e(P_1, P_2) \rangle = H$: this can be proved using non-degeneracy and the fact that $\langle P_1 \rangle = G_1$.
The converse does not hold in general: for example, if $G_1 \cong \mathbb{Z}_{\ell^2}$, with ℓ prime, and $G_2 \cong \mathbb{Z}_\ell \oplus \mathbb{Z}_\ell$, there are no elements of order ℓ^2 in G_2. However, the converse holds if the order is a prime number r, because every non-trivial group G_2 is cyclic of prime order. So if $e(P_1, P_2)$ generates H, then both P_1 and P_2 cannot be 0, and by non-degeneracy it follows immediately that $rP_1 = 0, rP_2 = 0$. Eventually, if $hP_1 = 0$ for some $h < r$, then we come to a contradiction:

$$1 \neq e(P_1, P_2)^h = e(hP_1, P_2) = e(0, P_2) = 1.$$

The same happens if $hP_2 = 0$ for some $h < r$.

Remark 3.9. The non-degeneracy (1) in Definition 3.7 is equivalent to the following conditions:

- $\forall P \in G_1,\ P \neq 0,\ \exists Q \in G_2$ such that $e(P, Q) \neq 1$;
- $\forall Q \in G_2,\ Q \neq 0,\ \exists P \in G_2$ such that $e(P, Q) \neq 1$.

The proof is straightforward.

These pairings differ from the previous ones: in particular, they are not all equivalent up to exponentiation by a constant. This follows from the next proposition.

Proposition 3.10. *Let G_1, H be two cyclic groups of composite order r, with additive and multiplicative notation respectively. Then it exists a bilinear, non-degenerate pairing*

$$\begin{aligned} e : G_1 \times G_2 &\longrightarrow H \\ (P_1, P_2) &\longmapsto h, \end{aligned}$$

where G_2 is an additive group of order $d \mid r$, $P_1 \in G_1, P_2 \in G_2$ are generators and $h \in H$ is such that $h^d = 1$.

Proof. Pick $h \in H$ of order $d \mid r$; then the map defined extending by linearity the identity $e(P_1, P_2) = h$ is non-degenerate. Indeed, if $b \in \{0, \dots, d-1\}$ and

$$e(aP_1, bP_2) = e(P_1, P_2)^{ab} = h^{ab} = 1 \qquad \forall a \in \{0, \dots, r-1\},$$

then $d \mid ab$ for all $a \in \{0, \dots, r-1\}$; thus $d \mid b$ and so $bP_2 = 0$. The same argument applies to the second variable. Furthermore we have:

$$e(aP_1, 0) = e(P_1, P_2)^{ad} = h^{ad} = 1,$$

for all $a \in \{0, \dots, r-1\}$. Similarly $e(0, bP_2) = 1$, for all $b \in \{0, \dots, d-1\}$. □

3.3 Applying the Weil pairing to cryptography

After having examined the various types of cryptographic bilinear pairings, we show that suitable restrictions of the Weil maps produce examples of pairings for elliptic curves cryptography. In this case, given an elliptic curve $E/\mathbb{F}_q$, we can construct pairings from products of additive subgroups of the rational points $E(\mathbb{F}_{q^k})$, for some extension field $\mathbb{F}_{q^k} \supseteq \mathbb{F}_q$, to the multiplicative group $\mathbb{F}^*_{q^k}$. We remark that the Weil map is efficiently computable, thanks to Miller algorithm [57].
It is interesting to look for information on the smallest extension of $\mathbb{F}_q$, such that $E[r] \subset E(\mathbb{F}_{q^k})$; the aim is to reduce as much as possible the size of the field where arithmetic operations are performed, in order to drop their computational cost. To this purpose, we define the *embedding degree* as the integer k that produces this inclusion. It turns out that if $E[r] \subset E(\mathbb{F}_{q^k})$, then $r \mid (q^k - 1)$; however, it may happen that for a certain smaller extension field $\mathbb{F}_{q^h}$ it holds that $r \mid (q^h - 1)$, but $E[r] \nsubseteq E(\mathbb{F}_{q^h})$. Only under certain assumptions the previous condition is also sufficient for this inclusion to hold, as the following theorem proves.

Theorem 3.11 (Balasubramanian-Koblitz [4])**.** *Let E be an elliptic curve defined over $\mathbb{F}_q$ and suppose that r is a prime divisor of $N = |E(\mathbb{F}_q)|$, such that $r \nmid q - 1$. Then $E(\mathbb{F}_{q^k})$ contains r^2 points of order r if and only if $r \mid (q^k - 1)$.*

Proof. Whenever $E[r] \subset E(\mathbb{F}_{q^k})$, by 2.27 one gets $\mu_r \leq \mathbb{F}^*_{q^k}$ and so $r \mid (q^k - 1)$. Conversely, there exists a point $P \in E(\mathbb{F}_q)$ of order r, because $r \mid N$ and groups of points are finite abelian. If $r \mid (q^k - 1)$, then $r \nmid q$ and hence $E(\mathbb{F}_{q^m})$ contains r^2 points of order r, for some m (2.22). Let $Q \in E(\mathbb{F}_{q^m})$, such that P, Q form a basis for the $\mathbb{Z}_r$-vector space $E[r] \cong \mathbb{Z}_r \times \mathbb{Z}_r$. Let Φ_q denote the q-th Frobenius endomorphism 2.3 on points of $E(\mathbb{F}_{q^m})$. Since Φ_q acts as a $\mathbb{Z}_r$-linear map on points of order r, [57, Theorem 4.10] states that its characteristic polynomial modulo r is:

$$X^2 - tX + q \in \mathbb{Z}_r[X],$$

with $t = q+1-N$. Let λ_1, λ_2 be the eigenvalues and note that Φ_q fixes $P \in E[r] \cap E(\mathbb{F}_q)$. Therefore, $\lambda_1 = 1$ and then $\lambda_2 = q$; indeed, by substitution in the characteristic polynomial:

$$q^2 - tq + q = Nq \equiv 0 \mod r.$$

Moreover, as $r \nmid (q-1)$, we see that $q \not\equiv 1 \mod r$ and so the eigenvalues are distinct. Thus the action of Φ_q on $E[r]$ is diagonalizable and hence Φ_q^k is diagonalizable too. The latter turns out to be the identity matrix; therefore all points P, Q are fixed by Φ_q^k, which implies that all r-torsion points are fixed. We conclude that $E[r] \subset E(\mathbb{F}_{q^k})$. □

This leads naturally to the following definition.

Definition 3.12. Let $E/\mathbb{F}_q$ be an elliptic curve and let r be a prime divisor of $|E(\mathbb{F}_q)|$, coprime to q. The *embedding degree* of E, with respect to r (or to a subgroup of $E(\mathbb{F}_q)$ of order r), is the smallest integer k such that r divides $q^k - 1$.

The choice of points when executing some protocol implicitly defines cyclic subgroups generated by the points themselves. However, they might change at every execution of the algorithm and we should avoid this situation. For example, to enhance efficiency during computations of Miller's algorithm, the pairing should act on subgroups G_1, G_2 of $E[r]$ defined over fields whose cardinality should be as small as possible. We usually assume, for cryptographic applications, to deal with subgroups whose order gives embedding degree $k > 1$. We further suppose that $|E(\mathbb{F}_{q^k})|$ and $p = \mathrm{char}(\mathbb{F}_{q^k})$ are relatively prime, as in section 2.3. In the following analysis, the first group is always defined as:

$$G_1 \coloneqq E(\mathbb{F}_q)[r] = E[r] \cap E(\mathbb{F}_q),$$

while the second one is chosen each time in order to fit the different settings. Thus we will obtain pairings of the form:

$$e_{r|_{G_1 \times G_2}} : G_1 \times G_2 \longrightarrow \mu_r.$$

We first prove another important result about the structure of the r-torsion subgroup, which will be useful in the proof of 3.15.

Lemma 3.13. *Given an elliptic curve $E/\mathbb{F}_q$, with $N = |E(\mathbb{F}_q)|$, and given a large prime $r \mid N$, let k be the embedding degree of E relative to r and assume that $k > 1$. Then $E[r] = G_1 \oplus G_q \subset E(\mathbb{F}_{q^k})$, where:*

$$G_1 = E(\mathbb{F}_q)[r] = \{P \in E[r] : \Phi_q(P) = P\} \quad \textit{rational subgroup} \tag{3.2}$$

$$G_q = \{P \in E[r] : \Phi_q(P) = [q]P\} \quad \textit{trace-zero subgroup} \tag{3.3}$$

and Φ_q denotes the q-th Frobenius endomorphism 2.3.

Proof. Following the proof of Theorem 3.11, we can prove that Φ_q has two eigenvalues $\lambda_1 = 1, \lambda_2 = q$ as a $\mathbb{Z}_r$-linear map over $E[r]$. They are distinct modulo r, since from $k > 1$ it follows that $q \not\equiv 1 \mod r$; thus the r-torsion subgroup decomposes as:

$$E[r] = \ker(\Phi_q - \mathrm{Id}) \oplus \ker(\Phi_q - q\,\mathrm{Id}) = G_1 \oplus G_q.$$ □

Now we introduce a crucial map for the implementation of type-2 pairings. Let $E/\mathbb{F}_q$ be an elliptic curve, and let assumptions in the previous lemma hold. The *trace map* is defined as:

$$\mathrm{Tr} : E(\mathbb{F}_{q^k}) \longrightarrow E(\mathbb{F}_q) \qquad R \longmapsto \sum_{i=0}^{k-1} \Phi_q^i(R).$$

We have $\mathrm{Tr}(R) \in E(\mathbb{F}_q)$, since $\Phi_q(\mathrm{Tr}(R)) = \mathrm{Tr}(R)$ for all $R \in E(\mathbb{F}_{q^k})$. Being the q-th Frobenius map a group homomorphism, it easily follows that also the trace map is so.

Remark 3.14. As every $Q \in G_1$ is fixed by Φ_q, then the Frobenius trace obviously acts on G_1 as multiplication by k. Moreover, it acts on G_q as multiplication by $(q^k-1)/(q-1)$. Indeed, given $S \in G_q$ we have:

$$\mathrm{Tr}(S) = S + [q]S + [q^2]S + \cdots + [q^{k-1}]S = \left[\sum_{i=0}^{k-1} q^i\right] S = \left[\frac{q^k-1}{q-1}\right] S.$$

If we assume, as in Lemma 3.13, that the embedding degree is $k > 1$, then we have that $r \mid (q^k - 1)$ and $r \nmid (q-1)$, hence $r \mid \frac{q^k-1}{q-1}$. Therefore $\mathrm{Tr}(S) = O$ and we have:

$$\ker\left(\mathrm{Tr}_{|_{E[r]}}\right) = G_q \qquad \mathrm{im}\left(\mathrm{Tr}_{|_{E[r]}}\right) = G_1.$$

It follows from the structure of the r-torsion subgroup $E[r]$ (2.22), that both the rational and the trace zero subgroups have order r, since they are both non-trivial.

Theorem 3.15. *In the same hypotheses of Lemma 3.13, the restriction of the Weil pairing $e_{r|_{G_1\times G_q}}$ (or $e_{r|_{G_q\times G_1}}$) is non-degenerate. More generally, if $G_2 \neq G_1, G_q$ is any cyclic subgroup of $E[r]$, then the Weil pairing restricted to $G_1\times G_2, G_2\times G_1, G_q\times G_2$ or $G_2\times G_q$ is non-degenerate.*

Proof. The Weil pairing e_r is non-degenerate on $E[r]$, but it is trivial on $G_1 \times G_1$ and $G_q \times G_q$, since both G_1, G_q are cyclic and the map is alternate. Thus we can show that for every $O \neq P \in G_1$ it exists $Q \in G_q$, such that $e_r(P,Q) \neq 1$. Indeed, assume by contradiction that all $Q \in G_q$ give $e_r(P,Q) = 1$ and note that, being $E[r] = G_1 \oplus G_q$, every point in $E[r]$ can be written as $[a]S+[b]T$, with S, T generators of G_1, G_q respectively. Thus the equality

$$e_r(P, [a]S + [b]T) = e_r(P,S)^a e_r(P,T)^b = e_r([c]S, S)^a e_r(P,T)^b = 1$$

gives a contradiction with the non-degeneracy condition on $E[r]$. This proves the non-degeneracy of $e_{r|_{G_1\times G_q}}$ and the same idea applies for $e_{r|_{G_q\times G_1}}$.
Moreover, let G_2 be a cyclic subgroup: for every $O \neq P \in G_1$, if $Q \in G_q$ is such that $e_r(P,Q) \neq 1$, then it exists $R \in G_1$ such that $R + Q \in G_2$. Therefore we get the non-degeneracy of the restriction $e_{r|_{G_1\times G_2}}$, since:

$$e_r(P, R+Q) = e_r(P,R)e_r(P,Q) = e_r(P,Q) \neq 1.$$

The other cases can be similarly proved. □

Now, suppose that P, Q are generators of the groups G_1 and G_q respectively, so that $E[r] = \langle P\rangle \oplus \langle Q\rangle$. We shall assume, in addition, that $\mathrm{Tr}(P) = [k]P \neq O$, since in a cryptographic context r is much bigger than k [23].

Lemma 3.16. *Let $\{P, Q\}$ be a basis of $E[r]$, as stated above. Then $e_r(P,Q)$ is a primitive r-th root of unity.*

Proof. Suppose $e_r(P,Q) = \zeta$, with $\zeta^d = 1$ for some $d \mid r$. Thus $e_r(P, [d]Q) = 1$, by bilinearity, and $e_r(Q, [d]Q) = 1$, since e_r is also alternating. We can write any $R \in E[r]$ as $[a]P + [b]Q$, for some integers a, b. Therefore for every $R \in E[r]$:

$$e_r(R, [d]Q) = e_r(P, [d]Q)^a e_r(Q, [d]Q)^b = 1.$$

Now, non-degeneracy implies that $[d]Q = O$ and thus $r \mid d$. □

We begin studying type-2 pairings (3.6); first of all, note that given $R = [a]P + [b]Q \in E[r]$ for some integers a, b, then $\mathrm{Tr}(R) = [ak]P$. The point

$$T \coloneqq [k]R - \mathrm{Tr}(R) = [bk]Q$$

is a generator of G_q, unless $R \in G_1$, that would give $T = O$. In applications, one can use the generators P, T, since they can both be efficiently found. For the latter we can construct an efficient randomized algorithm by extracting random points until one is not in G_1. We refer to [46, ch. 8] for comments on the problem of hashing to subgroups of elliptic curves. Next, it is possible to choose $R \in E[r]$, such that it belongs to neither $\langle P \rangle$ nor $\langle T \rangle$. This can be checked with the Weil pairing, since $R \in \langle P \rangle$ if and only if $e_r(P, R) = 1$. Indeed, assume the latter condition and note that:

$$e_r(P, R) = e_r(P, [a]P + [b]Q) = e_r(P, P)^a e_r(P, Q)^b = e_r(P, Q)^b = 1.$$

As $e_r(P, Q)$ is a primitive r-th root, by Lemma 3.16, then $b \equiv 0 \mod r$. This proves that $R = [a]P + O$ must be in $\langle P \rangle$; the converse is straightforward. Similarly, $R \in \langle T \rangle$ if and only if $e_r(R, T) = 1$. Therefore set $G_2 \coloneqq \langle R \rangle$ and note that $e_{r|_{G_1 \times G_2}}$ is bilinear and still non-degenerate, by Theorem 3.15. Moreover, the trace map restricted to G_2 gives an efficiently computable isomorphism $\mathrm{Tr}_{|_{G_2}} : G_2 \to G_1$. Indeed, it is a non-trivial homomorphism of groups, because $R \notin \langle T \rangle$, and we have:

$$\mathrm{Tr}([h]R) = \mathrm{Tr}([ha]P + [hb]Q) = [ha]\,\mathrm{Tr}(P) + [hb]\,\mathrm{Tr}(Q) = [hak]P \in \langle P \rangle.$$

It is also injective, since $\mathrm{Tr}([h_1]R) = \mathrm{Tr}([h_2]R)$ implies that $[h_1]\,\mathrm{Tr}(R) = [h_2]\,\mathrm{Tr}(R)$ and so $h_1 \equiv h_2 \mod r$. Note also that, assuming $r \neq \mathrm{char}(\mathbb{F}_{q^k})$, Theorem 2.22 shows that the group $E[r]$ is not cyclic; thus $\langle R \rangle$ cannot be the whole r- torsion subgroup and, unless trivial, it must be a cyclic subgroup of prime order r. Then, $\mathrm{Tr}_{|_{G_2}}$ is also surjective and so it is an isomorphism; this proves that $e_{r|_{G_1 \times G_2}}$, for the above choice of subgroups, is a type-2 pairing. Restricting the Weil map to $G_1 \times G_q$ we obtain also an example of type-3 pairing, where no efficiently computable, non-trivial isomorphism exists.

3.3.1 Distortion maps for the symmetric pairings

Eventually, we examine the case of symmetric pairings. However, recalling that the Weil pairing is alternate, we have to face the problem that e_r is trivial when restricted to products $G \times G$ of cyclic subgroups of $E[r]$. Following the ideas in [56], we need to introduce a particular map that modifies the points of G.

Definition 3.17. Let $E/\mathbb{F}_q$ be an elliptic curve and let $R \in E(\mathbb{F}_q)$ be a point of prime order $r \mid |E(\mathbb{F}_q)|$. A *distortion map*, defined over a field $K \supseteq \mathbb{F}_q$, with respect to the cyclic group $G = \langle R \rangle$, is an endomorphism $\psi \in End_K(E)$ such that for every $Q \in \langle R \rangle$, $Q \neq O$, it holds $\psi(Q) \notin \langle Q \rangle$.

Let

$$\psi_{|_{G_1}} : E(\mathbb{F}_q)[r] \longrightarrow E[r] \setminus G_1$$

be a distortion map with respect to the group G_1; it allows us to construct a symmetric bilinear pairing as follows:

$$\tilde{e}_r : G_1 \times G_1 \longrightarrow \mu_r \qquad \tilde{e}_r(P, Q) \coloneqq e_r(P, \psi(Q)). \tag{3.4}$$

This map is bilinear, since the Weil pairing is so and the distortion map is a group homomorphism. Moreover, it is also non-degenerate; to prove it, we first show that the group $G = \{\psi(T) : T \in G_1\}$ is cyclic of order r. Indeed, if $G_1 = \langle P \rangle$, then $[r]\psi(P) = \psi([r]P) = O$. In addition, if we assume $[h]\psi(P) = O$ for some $h < r$, we get a contradiction with Definition 3.17, since $\psi([h]P) = O \in \langle P \rangle$. Therefore, Theorem 3.15 applies, proving the non-degeneracy of $\tilde{e}_r$.
Next, we investigate on conditions for the existence of distortion maps on elliptic curves, because of their importance in applications. Since a non-zero point $T \in G_1$ gives an image $\psi(T) \neq O$, a distortion map exists only in case $E[r]$ is not a cyclic group. Otherwise there would be a contradiction, because both Q and $\psi(Q)$ would generate the unique cyclic subgroup of order r in $E[r]$. Then, by Theorem 2.22, we get as a first condition $r \neq \mathrm{char}(\mathbb{F}_q)$, that is generally assumed to hold in applications. Consider any extension L of the field $\mathbb{F}_q$, then the ring $\mathrm{End}_L(E[r])$ of endomorphisms restricted to $E[r]$ can be viewed as the subgroup of all $\mathbb{Z}_r$-linear maps on $\mathbb{Z}_r \times \mathbb{Z}_r$. Clearly, the distortion maps with respect to $\langle P \rangle$ correspond to those linear maps that do not have P as an eigenvector. It turns out that they always exist when the curves are supersingular.

Theorem 3.18. *Let $E/\mathbb{F}_q$ be a supersingular elliptic curve, with embedding degree k and let $L = \mathbb{F}_{q^k}$. If $P \in E(\mathbb{F}_q)$ has prime order r, such that $(r, \mathrm{char}(\mathbb{F}_q)) = 1$, then $\mathrm{End}_L(E[r])$ is isomorphic to the ring of all 2×2 matrices over $\mathbb{Z}_r$. In particular, there exist distortion maps over L, with respect to $\langle P \rangle$.*

For a proof of this theorem we refer to [56]; moreover, a complete characterisation of the embedding degrees for supersingular elliptic curves can be found in [11, Theorem IX.20]. It is interesting to notice that these curves have embedding degree $k \leq 6$. Then, it remains to understand what happens in case of ordinary curves. Surprisingly, in most cases, there are no distortion maps on such curves.

Theorem 3.19. *Let $E/\mathbb{F}_q$ be an ordinary elliptic curve and let $P \in E(\mathbb{F}_q)$ be a point of prime order $r \neq \mathrm{char}(\mathbb{F}_q)$. When the embedding degree of E with respect to r is $k > 1$, no distortion map with respect to $\langle P \rangle$ exists.*

Proof. Assume that $\psi \in \mathrm{End}(E)$ is a distortion map with respect to $\langle P \rangle$ and recall that the endomorphism ring of an ordinary curve is commutative ([52]). Thus, the identity

$$\Phi_q(\psi(P)) = \psi(\Phi_q(P)) = \psi(P),$$

holds, since $P \in E(\mathbb{F}_q)$. We know from 3.13 that, being $k > 1$, $E[r] \cap E(\mathbb{F}_q) = \langle P \rangle$ is the eigenspace of Φ_q with eigenvalue 1. Then $\Phi_q(R) \neq R$ for every $R \in E[r] - \langle P \rangle$; in particular, since $\psi(P) \notin \langle P \rangle$ by definition 3.17, we get a contradiction with the previous identity. □

The case of ordinary elliptic curves with embedding degree $k = 1$ is studied in [56, Theorem 7]. However, we do not consider it, since we previously remarked that in cryptographic applications it is usually assumed $k > 1$.
As a conclusion, we propose an easy example of distortion map in the case of supersingular elliptic curves over prime fields. Consider the curve $E/\mathbb{F}_p$, for some prime $p \equiv 2 \mod 3$, of equation $y^2 = x^3 + b$. First, we compute the cardinality of $E(\mathbb{F}_p)$.

Lemma 3.20. *Given the prime $p \equiv 2 \mod 3$, let $E/\mathbb{F}_p$ be the elliptic curve of equation $y^2 = x^3 + b$; then $|E(\mathbb{F}_p)| = p + 1$.*

Proof. Consider the homomorphism

$$\begin{aligned} \varphi : \mathbb{F}_p^* &\longrightarrow \mathbb{F}_p^* \\ x &\longmapsto x^3. \end{aligned}$$

Since $3 \nmid (p-1)$, there are no elements of order 3 in $\mathbb{F}_p^*$ and so $\ker(\varphi) = \{1\}$. Thus the homomorphism is injective, and clearly also surjective. It follows that every element in $\mathbb{F}_p$ has a unique cube root in this field. Therefore, given $y \in \mathbb{F}_p$, it exists unique $x = \sqrt[3]{y^2 - b}$ such that $(x, y) \in E(\mathbb{F}_p)$. Having p distinct possible values for y, and counting the point at infinity, we conclude the proof. □

Therefore, by [57, Proposition 4.29], these elliptic curves are supersingular; we focus on the case of $b = 1$. Let $\zeta \in \mathbb{F}_{p^2}$ be a primitive third root of unity (note that $(p^2 - 1) \equiv 0 \mod 3$) and define the function:

$$\begin{aligned} \psi : E(\overline{\mathbb{F}_p}) &\longrightarrow E(\overline{\mathbb{F}_p}) \\ (x, y) &\longmapsto (\zeta x, y) \\ O &\longmapsto O. \end{aligned} \tag{3.5}$$

It can be proved that ψ is a group homomorphism, by means of the explicit formulae for the group law 1.9. More precisely, it is an automorphism, since it is an injective homomorphism of $E(\overline{\mathbb{F}_p})$ to itself. We prove that ψ is a distortion map.

Proposition 3.21. *Let $E/\mathbb{F}_p$ be the elliptic curve defined above and let $P \in E(\mathbb{F}_p)$ a point of order $r \mid (p+1)$. Then ψ, defined by 3.5, is a distortion map with respect to $G_1 = \langle P \rangle$.*

Proof. Assume that the equality $\psi(P) = [u]P$ holds for some integer u. The point $[u]P$ belongs to $E(\mathbb{F}_p)$, but we note that $\psi(P) \in \mathbb{F}_{p^2} \setminus \mathbb{F}_p$ and this proves that $\psi(P) \notin \langle P \rangle$. Indeed, if $P = (x, y)$ with $x, y \in \mathbb{F}_p$, then $\psi(P) = (\zeta x, y)$ and assuming $(\zeta x)^p = \zeta x$, we have $\zeta^{p-1} = 1$. Since ζ has order 3, it holds $3 \mid (p-1)$, which is a contradiction with the hypothesis $p \equiv 2 \mod 3$. □

The distortion map allows to modify the Weil pairing e_r in order to get a symmetric bilinear pairing, as seen before.

Chapter 4

Security analysis of a pairing-based broadcast encryption scheme

Pairings have turned out to be very useful in many protocols of modern cryptography. We focus on an application of symmetric bilinear pairings: the broadcast encryption system introduced by Boneh, Gentry and Waters [15], that we denote by $\mathfrak{B}$. Its security is based on the so called ℓ-BDHE problem, which will be defined later as a variant of standard cryptographic problems 3.1. In this context, we always assume that an attacker can compute the bilinear pairing or, at least, to ask for its computation to an oracle. From now on, pairings $e : G \times G \to H$ are supposed to be symmetric (3.4), since $\mathfrak{B}$ is implemented by means of this type of maps. Assume, as usual, that G, H are both cyclic groups of prime order r, with multiplicative and additive notation respectively. We denote these groups and the relative pairing as (G, H, e). Notation will always be similar to the elliptic curve case, where elements of G are points and H is a subgroup of a finite field. The non-degeneracy of e allows to solve DDHP instances in G using the pairing. Indeed, if $P \in G^*$, then $e(P, P)$ must be a generator of H; thus given $aP, bP, cP \in G$, for some integers a, b, c, it holds:

$$abP = cP \quad \Leftrightarrow \quad e(aP, bP) = e(P, cP).$$

A direct consequence for pairing-based cryptography is the impossibility of building secure cryptosystems on (G, H, e) based on the hardness of DDHP.

4.1 MOV reduction

A well known technique for the solution of DLP on elliptic curves was pointed out in 1993 by Menezes, Okamoto and Vanstone in [42]. The MOV attack, called after their names, reduces the DLP computation from groups of rational points on elliptic curves to finite fields. We outline the main idea of this algorithm, since it is crucial for the security analysis. Suppose that an attacker knows $P_1, P_2 \in G$; so its aim is to find the integer $x \in \{0, \ldots, r-1\}$ such that $P_2 = xP_1$ in G. When those points are non-trivial, they both have order r; therefore $g = e(P_1, P_1) \in H$ and $h = e(P_1, P_2) \in H$ have order r too. Since the equality $g = h^x$ holds, solving DLP in H gives the solution of the original DLP instance. Thus to guarantee hardness of this problem on G, its counterpart on H should be hard. The MOV attack uses a similar technique, adapted to the specific elliptic curves case. Assume to use pairings $\tilde{e}_r$, obtained form a Weil pairing and a distortion map as in 3.4, and let $E/\mathbb{F}_q$ be an elliptic curve. We refer to [42] for details in the case of a general elliptic curve; here suppose that E is supersingular, since we are concerned with this case.

It can be proved [49,52] that for a supersingular curve it holds:

$$E(\mathbb{F}_q) \cong \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2}$$

for some integers n_1, n_2, such that $n_2 \mid n_1$. In particular, applying [49, Theorems 4.2, 4.8], the supersingular case has $n_1 = n_2 = cN$, for appropriate integers c, N. A DLP instance on E is given by $P \in E(\mathbb{F}_q)$ of known order $n \mid |E(\mathbb{F}_q)|$, not necessarily prime, and a second point $R \in \langle P \rangle$. The MOV reduction algorithm works as follows.

Algorithm 2 Supersingular MOV reduction - Given $P \in E(\mathbb{F}_q)$ of order n on a supersingular elliptic curve and $R \in \langle P \rangle$, computes $x \in \{0, \ldots, n-1\}$ such that $R = [x]P$.

Require: $P \in E(\mathbb{F}_q)$, $R \in \langle P \rangle$, $n = \text{ord}(P)$
Ensure: x, such that $R = [x]P$
1: compute k, the embedding degree of E with respect to n
2: determine integers c, N such that $E(\mathbb{F}_q) \cong \mathbb{Z}_{cN} \oplus \mathbb{Z}_{cN}$
3: pick $Q' \in E(\mathbb{F}_q)$ at random
4: set $Q = [cN/n]Q'$
5: compute $\alpha = \tilde{e}_n(P, Q)$
6: compute $\beta = \tilde{e}_n(R, Q)$
7: compute x such that $\beta = \alpha^x$ in $\mathbb{F}_{q^k}$
8: **if** $R = [x]P$ **then**
9: **return** x
10: **else**
11: go to step 3
12: **end if**

The algorithm outputs the correct answer, since

$$\beta = \tilde{e}_n(R, Q) = \tilde{e}_n([x]P, Q) = \alpha^x$$

In [42] the authors show that algorithm 2 terminates in probabilistic polynomial time; it may happen that the point Q, defined at step 4, does not produce an element α with order n. Note that the supersingular case is peculiar, because one can efficiently compute the embedding degree at step 1, thanks to the small bound $k \leq 6$ and Theorem 3.11. Clearly, the MOV attack allows to apply faster methods for the DLP solution, available in the case of finite fields, to solve an instance of this problem on elliptic curves.

4.2 Variants of the Diffie-Hellman problem

A variant of the computational Diffie-Hellman problem 3.2, is its bilinear version, which is specifically built for the pairing-based case.

Definition 4.1. An instance of the *bilinear Diffie-Hellman problem (BDHP)* in (G, H, e) is the problem of computing $e(P, P)^{abc}$, given a generator P of G and aP, bP, cP, with a, b, c integers.

When the BDHP is supposed to be hard in (G, H, e), then the CDHP is hard in both the groups G and H. Indeed, if we assume that the CDHP can be efficiently solved in G, then it is possible to compute abP from an instance of the BDHP and hence find $e(abP, cP) = e(P, P)^{abc}$, thanks to the pairing. The same result comes from the knowledge of $e(P, P)^{ab}$ and $e(P, P)^c$, assuming that CDHP can be efficiently solved in H. Along with

the implementation of many pairing-based cryptosystems, other weakened versions of the main cryptographic problems have been developed. In particular, we define the following one, on which is based the security of the broadcast encryption system $\mathfrak{B}$.

Definition 4.2. Consider the groups with pairing (G, H, e). Let S, T be generators of G and pick an element $a \in \mathbb{Z}_r^*$. An instance of the *(computational) ℓ-bilinear Diffie-Hellman exponent problem* or *ℓ-BDHE* is the problem of computing $e(S,T)^{a^\ell}$, given S, T, $aS, a^2S, \ldots, a^{\ell-1}S, a^{\ell+1}S, \ldots, a^{2\ell}S$. In the same hypotheses, its decisional version requires to decide whether $e(S,T)^{a^\ell} = h$ holds or not in H, given $h \in H$.

Note that if an attacker is supposed to efficiently solve the CDHP in G, then it can solve the ℓ-BDHE problem too, computing $a^\ell S$ from $a^{\ell-1}S$, aS. We remark that the ℓ-BDHE problem is weaker than the BDHP too. Indeed, assuming that the latter is easy in (G, H, e), then an adversary, knowing $a^{\ell-1}S$, aS and $T = bS$, can compute $e(S,S)^{a^{\ell-1}ab} = e(S,T)^{a^\ell}$, solving the first problem.
We say that $A \prec B$ if the problem A can be solved in polynomial time, with polynomially many queries to an oracle that solves B. Then, we summarize the connections between cryptographic problems introduced before:

$$\ell - \text{BDHE} \prec BDHP \prec CDHP \prec DLP.$$

The same relations hold for the corresponding decisional versions. The common approach, when studying the hardness of such problems, is to investigate the probabilistic advantage that an adversary has in solving one of them.

Definition 4.3. A probabilistic algorithm $\mathcal{A}$, that outputs an element $h \in H$, has *advantage* ε in solving an instance of the ℓ-BDHE problem in (G, H, e) if

$$\Pr\left[\mathcal{A}\left(S, T, aS, a^2S, \ldots, a^{\ell-1}S, a^{\ell+1}S, \ldots, a^{2\ell}S\right) = e(S,T)^{a^\ell}\right] \geq \varepsilon.$$

The probability is taken over the random choice of generators $S, T \in G$, the random choice of $a \in \mathbb{Z}_r^*$ and the random bits used by $\mathcal{A}$.

There are similar definitions for all other variants of the Diffie-Hellman problem, but here we focus on the ℓ-BDHE one. Moreover, in its *decisional* version the adversary is asked to distinguish $e(S,T)^{a^\ell}$ from a random value $h \in H$. In this case, the advantage of an attacker is defined as follows.

Definition 4.4. A probabilistic algorithm $\mathcal{A}$, that outputs a bit $b \in \{0,1\}$, has *advantage* ε in solving an instance of the decisional ℓ-BDHE problem in (G, H, e) if

$$\left|\Pr\left[\mathcal{A}\left(S, T, aS, a^2S, \ldots, a^{\ell-1}S, a^{\ell+1}S, \ldots, a^{2\ell}S; t_0, t_1\right) = b\right] - \frac{1}{2}\right| \geq \varepsilon,$$

where $t_b = e(S,T)^{a^\ell}$ and $t_{1-b} = e(S,T)^t$. The probability is taken over the random bit $b \in \{0,1\}$, the random choice of generators $S, T \in G$, the random choice of $a, t \in \mathbb{Z}_r^*$ and the random bits used by $\mathcal{A}$.

This definition is based on how far the probability that $\mathcal{A}$ guesses the correct bit is from $1/2$. Note that when it is equal to $1/2$ the algorithm is choosing the output at random, so it has no advantage in solving the problem.

Definition 4.5. We say that the *(decisional) (t, ε, ℓ)-BDHE assumption* holds in (G, H, e) if no t-time algorithm has advantage at least ε in solving the (decisional) ℓ-BDHE problem in G.

4.3 Semantic security of the system $\mathfrak{B}$

In the remainder of this chapter we want to connect the security of the system $\mathfrak{B}$ to the decisional (t, ε, ℓ)-BDHE assumption, and provide a result about the hardness of the latter problem. Firstly, we need to define the chosen ciphertext security of a broadcast encryption system against a static adversary. The usual way to define it is by means of an attack simulation and the probability that it has success. Let us recall the construction of a particular case of $\mathfrak{B}$, proposed in [15, Section 3.1], since it gives an example of notation that will be used later. Consider n users and denote by S the set of recipients. The system is based on the following algorithms, that work on (G, H, e).

- *Setup(n)* picks a random generator $P \in G$ and random elements $\alpha, \gamma \in \mathbb{Z}_r^*$. Then it computes $P_i \coloneqq \alpha^i P$, for $i = 1, 2, \ldots, n, n+2, \ldots, 2n$, and $Q \coloneqq \gamma P$. The algorithm outputs the public key:

$$k_p \coloneqq (P, P_1, \ldots, P_n, P_{n+2}, \ldots, P_{2n}) \in G^{2n}$$

  and the private keys $D_i = \gamma P_i$, for all users $i \in \{1, \ldots, n\}$.

- *Encrypt(S, k_p)* picks a random $t \in \mathbb{Z}_r^*$, it sets an encryption key $k_S \coloneqq e(P_n, P_1)^t$ and it let:

$$\mathrm{Hdr} \coloneqq \left(tP \, , \, Q + \sum_{j \in S} tP_{n+1-j} \right)$$

  be an header, that will be included in the message. Then, the encryption algorithm outputs the pair (Hdr, k_S).

- *Decrypt(S, i, D_i, Hdr = (C_0, C_1), k_p)* outputs the decryption key

$$k_i \coloneqq \frac{e(P_i, C_1)}{e\left(D_i + \sum_{j \in S,\, j \neq i} P_{n+1-j+i}, C_0\right)}$$

The simulation that follows describes an attack from a set of previously authorised users, that now collude to get information on a broadcast message. The adversary chooses the set of recipients and tries to disclose the secret key relative to the message. Security is based on the indistinguishability of the secret key $k_S \in H$ from a random element of H. We denote by $\mathcal{A}$ and $\mathcal{C}$ the attacker and the challenger respectively; assume they both know the number n of users and let S denote the set of all authorised users. Then the simulation consists of the following steps.

1. **Initialization 1.** $\mathcal{A}$ chooses to attack the target set S^* of authorised users.

2. **Initialization 2.** $\mathcal{C}$ invokes *Setup(n)* and sends to $\mathcal{A}$ the resulting public key k_p and the private keys D_i, for all $i \notin S^*$.

3. **Query phase 1.** $\mathcal{A}$ adaptively issues decryption queries, $q_1, \ldots, q_m$, that are triples $q_i = (u_i, S_i, \mathrm{Hdr}_i)$, where $u_i \in S_i \subseteq S^*$ and $\mathrm{Hdr}_i \in G^2$ are valid headers. $\mathcal{C}$ invokes *Decrypt($S_i, u_i, D_i, \mathrm{Hdr}_i, k_p$)* and answers with the decryption key k_i.

4. **Challenge.** $\mathcal{C}$ runs the algorithm *Encrypt(S^*, k_p)*, that outputs (Hdr^*, k^*). Then $\mathcal{C}$ chooses a random bit $b \in \{0, 1\}$, sets $k_b \coloneqq k^* \in H$, it picks a random key $k_{1-b} \in H$ and it sends to $\mathcal{A}$ the triple $(\mathrm{Hdr}^*, k_0, k_1)$.

5. **Query phase 2.** $\mathcal{A}$ continues to adaptively issue decryption queries $q_{m+1}, \ldots, q_d$, where each query is a triple $q_i = (u_i, S_i, \mathrm{Hdr}_i)$, where $u_i \in S_i \subseteq S^*$ and $\mathrm{Hdr}_i \in G^2$ are valid headers, with the additional constraint $\mathrm{Hdr} \neq \mathrm{Hdr}^*$. Then $\mathcal{C}$ answers as in step 3.

6. **Guess.** $\mathcal{A}$ outputs the guess $b' \in \{0, 1\}$ for b and wins the challenge if $b' = b$.

We make some comments on the previous attack.

- The attacker is *static*, because the target set of users is chosen at step 1 and it is never updated during the simulation.
- $\mathcal{A}$ gets the private keys outside the set S^*, since we are assuming that users in $S \setminus S^*$ collude to attack a message directed to S^*.
- During the second query phase, we assume that the attacker cannot issue a decryption query of the form (u, S^*, Hdr^*), with $u \in S^*$, because this case would reveal the secret key.
- This simulation tests the indistinguishability of the correct couple (Hdr^*, k^*) from (Hdr^*, k), for a random $k \in H$.

Then we define security in terms of the advantage in winning against $\mathcal{C}$ in the previous simulation.

Definition 4.6. A broadcast encryption system is (t, ε, n, q_d) *chosen cyphertext secure*, or (t, ε, n, q_d) *CCA secure*, if for all t-time algorithms that make a total of q_d decryption queries it holds

$$\left| \Pr\left[\mathcal{A}(n) = b\right] - \frac{1}{2} \right| < \varepsilon, \tag{4.1}$$

where the algorithm $\mathcal{A}$ behaves as in the previous attack simulation, n is the number of users and $b \in \{0, 1\}$ is the random bit that $\mathcal{A}$ has to guess. The probability is taken over the random choices of the simulation. In particular, a broadcast encryption system is (t, ε, n) *semantically secure* when it is $(t, \varepsilon, n, 0)$ CCA secure.

The idea proposed in [15] is to prove that the ℓ-BDHE assumption implies the semantic security of the broadcast encryption system defined in [15, Section 3.2]; recall that the system depends on a parameter and on the number of users, denoted by n and B respectively.

Theorem 4.7 (Semantic security)**.** *Consider the groups with pairing (G, H, e). For any positive integers B and $n = kB$, $k \in \mathbb{N}$, the B-broadcast encryption system is (t, ε, n) semantically secure, assuming that the decisional (t, ε, B)-BDHE assumption holds in (G, H, e).*

We do not give the proof of this result, which can be found in [15, Theorem 3.1].

4.4 ℓ-BDHE problem hardness in the generic group model

Theorem 4.7 implies that we can study semantic security by means of investigating the ℓ-BDHE problem's hardness. We determine in this section an upper bound to the advantage of a generic algorithm in solving this problem, mainly following [12] and [38].

Before stating the main theorem of this section, we need to define the generic group model, introduced by Shoup in [51]. This model can deal with adversaries that do not exploit any

special feature of the group structure in their attacks. Adversaries in this setting are Turing machines dealing with bit strings instead of group elements. They can store information in their memory, but they are not able to compute group operations or pairings on their own: these operations are provided by oracles. An *encoding function* of a finite group G on the set $\{0,1\}^m$, for some integer m, is an injective map $\sigma : G \to \{0,1\}^m$. The encoding σ associates to every group element a distinct bit string. We adapt the definition of generic algorithm given in [51] to the case of pairing-based cryptography.

Definition 4.8. Consider the groups with pairing (G, H, e) and let $m \in \mathbb{N}$ be the length of encodings. A *generic pairing-based algorithm* $\mathcal{A}$ is a probabilistic algorithm that behaves as follows.

- It takes as input two encoding lists; the first one contains encodings of elements in G, denoted by $L_{G,s} = (\sigma(P_1), \ldots, \sigma(P_s))$, where $P_i \in G$ and $\sigma(P_i) \in \{0,1\}^m$ are random bit strings, for $i = 1, \ldots, s$. The second one contains encodings of elements in H, denoted by $L_{H,t} = (\varrho(h_1), \ldots, \varrho(h_t))$, where $h_j \in H$ and $\varrho(h_j)$ are random bit strings, for $j = 1, \ldots, t$.

- During the execution, it has access to three oracles. The answer to every query is appended to the appropriate list, so that after the q-th query the new lists are $L_{G,s+q_1}$ and $L_{H,s+q_2}$, with $q = q_1 + q_2$. Consider now the $(q+1)$-th query; then two oracles output random bit strings $\sigma(P_i \pm P_j)$ or $\varrho(e(P_i, P_j))$ in $\{0,1\}^m$, given $i, j \in \{1, \ldots, s + q_1\}$ and one more bit, in the first case, that specifies the group operation. The last oracle outputs random bit strings $\varrho(h_i \cdot h_j^{\pm 1}) \in \{0,1\}^m$, given $i, j \in \{1, \ldots, t + q_2\}$ and one more bit that specifies the operation. Assume that if $\mathcal{A}$ makes twice the same query, then the oracles must give twice the same answer. Suppose also that $\mathcal{A}$ and the oracles keep track of outputs during the simulation.

- It outputs a bit string, denoted by $\mathcal{A}(L_{G,s}, L_{H,t}) \in \{0,1\}^*$, in the set of binary strings of arbitrary length.

These oracles are indistinguishable from ones that encode elements by means of two random encoding functions, as long as these maps satisfy the following definition.

Definition 4.9. Consider the groups with pairing (G, H, e). The encoding functions $\sigma : G \to \{0,1\}^m$ and $\varrho : H \to \{0,1\}^m$ are *compatible* with the oracles of Definition 4.8 if there exist two sequences $P_1, \ldots, P_{s+q_G} \in G$ and $h_1, \ldots, h_{t+q_H} \in H$, such that $\sigma(P_i)$, $\varrho(h_j)$ are equal to the outputs of the corresponding queries and such that it holds:

$$P_k = P_i \pm P_j, \qquad h_k = h_i \cdot h_j^{\pm 1}, \qquad h_k = e(P_i, P_j)$$

according to the choices made in the corresponding query. Here $q = q_G + q_H$ is the total number of queries.

The main limitation of the generic approach is that it may exist some specific algorithm that exploits features of a particular group or bilinear pairing to achieve some more efficient attack. However it is possible, by means of this analysis, to get information on the hardness of a problem, at least in this abstract framework. Such techniques provide evidence that a cryptographic problem could be suitable for implementing a cryptosystem and that it should not be discarded, as long as all known algorithms for solving it are generic. When some specific one is known, the elliptic curve and other security parameters should be chosen in order to make that algorithm have no advantage on generic ones. For further comments on this model and its validity we refer to [36].

4.4.1 General Diffie-Hellman Exponent problem

Before investigating the ℓ-BDHE problem's hardness in the generic group model, we define it in a more general form, suitable for the next theorem. Let r be a prime integer and let s, t, n be positive integers. In the following part $\mathbb{Z}_r[X] = \mathbb{Z}_r[X_1, \ldots, X_n]$ will denote the ring of n-variate polynomials over the field $\mathbb{Z}_r$. Let us consider the two vectors

$$\begin{aligned} U(X) &= (u_1(X), \ldots, u_s(X)) \in \mathbb{Z}_r[X]^s, \\ V(X) &= (v_1(X), \ldots, v_t(X)) \ \in \mathbb{Z}_r[X]^t, \end{aligned}$$

and the n-variate polynomial $f \in \mathbb{Z}_r[X]$; we assume that $u_1 = v_1 = 1$. Let (G, H, e) be a pair of groups with pairing. Consider a generator $P \in G$ and set $h \coloneqq e(P, P) \in H$. The (U, V, f)-*Diffie-Hellman problem* in (G, H, e) is the problem of computing $h^{f(x)} \in H$, given

$$\left(P, u_2(x)P \ldots, u_s(x)P, h, h^{v_2(x)}, \ldots, h^{v_t(x)}\right) \in G^s \times H^t,$$

with $x \in \mathbb{Z}_r^n$. Its decisional version is the problem, given the same inputs as before, to distinguish $h^{f(x)} \in H$ from a random element $h' \in H$. The polynomials, once evaluated, give values in $\mathbb{Z}_r$ and so this new problem describes general instances of some variant of the DLP, as ones defined in Section 4.2. In particular, to get an instance of the ℓ-BDHE problem it suffices to choose:

$$\begin{aligned} U(X_1, X_2) &= (1, X_2, X_1, X_1^2, \ldots, X_1^{\ell-1}, X_1^{\ell+1}, \ldots, X_1^{2\ell}), \\ V(X_1, X_2) &= (1), \\ f(X_1, X_2) &= X_1^{\ell} X_2. \end{aligned} \tag{4.2}$$

Next, we define dependence and independence relations for polynomial vectors, in the context of pairing-based cryptography.

Definition 4.10. Let $U = (1, u_2, \ldots, u_s) \in \mathbb{Z}_r[X]^s$ and $V = (1, v_2, \ldots, v_t) \in \mathbb{Z}_r[X]^t$ be two multivariate polynomial vectors, with s, t positive integers. We say that a polynomial $f \in \mathbb{Z}_r[X]$ is *dependent* on the vectors U, V if the identity:

$$f = \sum_{\substack{i,j=1 \\ i<j}}^{s} a_{i,j} u_i u_j + \sum_{k=1}^{t} b_k v_k,$$

holds for some constants $\{a_{i,j}\}_{i<j;\, i,j=1,\ldots,s}$ and $\{b_k\}_{k=1,\ldots,t}$ in $\mathbb{Z}_r$. We say that f is *independent* on U, V if it is not dependent on them.

Furthermore, let d_f denote the total degree of $f \in \mathbb{Z}_r[X]$ and define the *total degree* of a polynomial vector $U \in \mathbb{Z}_r[X]^s$ as $d_U \coloneqq \max\{d_f | f \in U\}$. Then, next definitions are useful to deal with lists where a generic pairing-based algorithm stores information during the execution. Assume that encodings are associated to polynomials.

Definition 4.11. Let $L = \{(\sigma_i, v_i) | i = 1, \ldots, k\}$ be a list, where $(\sigma_i, v_i) \in \{0,1\}^* \times \mathbb{Z}_r[X]$ for every $i = 1, \ldots, k$. We say that there is a *collision* in L if there exist two elements (σ_i, v_i) and (σ_j, v_j) in L, with $i \neq j$, such that $\sigma_i = \sigma_j$, but $v_i \neq v_j$.

Definition 4.12. Let $L = \{(\sigma_i, v_i) | i = 1, \ldots, k\}$ be a list, where $(\sigma_i, v_i) \in \{0,1\}^* \times \mathbb{Z}_r[X]$ for every $i = 1, \ldots, k$. We say that L is *coherent*, with respect to $x = (x_1, \ldots, x_n) \in \mathbb{Z}_r^n$, if for all pairs $((\sigma_i, v_i); (\sigma_j, v_j)) \in L^2$ it holds:

$$v_i \neq v_j \quad \Rightarrow \quad v_i(x) \neq v_j(x).$$

4.4.2 An upper bound on the advantage in generic bilinear groups

This generalisation allows to find the following upper bound on the advantage that a generic algorithm has, in solving the decisional (U, V, f)-Diffie-Hellman problem in (G, H, e). In particular, it will give an upper bound for the special case of the ℓ-BDHE problem.

Theorem 4.13. *Let $U \in \mathbb{Z}_r[X]^s$ and $V \in \mathbb{Z}_r[X]^t$ be two vectors of n-variate polynomials over $\mathbb{Z}_r$. Let $f \in \mathbb{Z}_r[X]$ be an n-variate polynomial over $\mathbb{Z}_r$ and set $d \coloneqq \max\{2d_U, d_V, d_f\}$. Let G and H be cyclic groups of prime order r, with additive and multiplicative notation respectively and let $e : G \times G \to H$ a symmetric bilinear pairing. Consider a generator $P \in G$ and set $h \coloneqq e(P, P)$. If f is independent on U, V, then for any generic pairing-based algorithm $\mathcal{A}$, that makes at most q queries to the oracles, it holds:*

$$\left| \Pr\left[\mathcal{A}\begin{pmatrix} \sigma(U(x)P), \varrho(h^{V(x)}), \\ \varrho(h^{t_0}), \varrho(h^{t_1}) \end{pmatrix} = b : \begin{matrix} x \overset{R}{\in} \mathbb{Z}_r^n,\ y \overset{R}{\in} \mathbb{Z}_r,\ b \overset{R}{\in} \{0,1\}, \\ t_b \coloneqq f(x),\ t_{1-b} \coloneqq y \end{matrix} \right] - \frac{1}{2} \right| \leq \frac{d(q+s+t+2)^2}{2r},$$

where σ and ϱ are random encoding functions of G and H respectively. Here $\sigma(U(x)P)$ and $\varrho(h^{V(x)})$ denote the lists of encodings $\sigma(u_i(x)P)$, for all $i = 1, \ldots, s$, and $\varrho(h^{v_j(x)})$, for all $j = 1, \ldots, t$.

According to Definition 4.4, the left hand side of the above inequality is the advantage of an adversary, which will be denoted by $Adv_{\mathcal{A}}(q, r)$. The proof of this theorem depends on the next lemma, which follows from results in [50].

Lemma 4.14. *Let $K[X] = K[X_1, \ldots, X_n]$ be the ring of n-variate polynomials over the field K. Let $p(X) \in K[X]$ be a polynomial of total degree d and assume that p is not identically zero. Consider any finite subset S of the field K. Then, if $x_1, \ldots, x_n$ are chosen independently and uniformly from S, we get:*

$$\Pr[p(x_1, \ldots, x_n) = 0] \leq \frac{d}{|S|}$$

Proof. Arguing by induction on the number n of variables, in case of $n = 1$ the above bound holds, since the polynomial p is univariate and hence it has at most d roots. In case of $n > 1$, consider $d_1 = \deg_{X_1}(p)$ and assume, without loss of generality, that $d_1 \geq 1$. Therefore, one can write:

$$p(X_1, \ldots X_n) = \sum_{i=0}^{d_1} X_1^i q_i(X_2, \ldots, X_n).$$

By definition of d_1, the polynomial q_{d_1} cannot be identically zero and we note that its total degree is at most $d - d_1$. Thus, by inductive hypothesis, it holds:

$$\Pr[q_{d_1}(x_2, \ldots, x_n) = 0] \leq \frac{d - d_1}{|S|}.$$

Moreover, evaluating the polynomials q_i at $x_2, \ldots, x_n$ we get the univariate polynomial

$$f(X_1) = \sum_{i=0}^{d_1} X_1 q_i(x_2, \ldots, x_n).$$

Let ε_1 and ε_2 be the events that $q_{d_1}(x_2, \ldots, x_n) = 0$ and $f(x_1) = 0$ respectively. Observe that, if the event ε_1 does not occur, then $X_1^{d_1} q_{d_1}(x_2, \ldots, x_n)$ is not identically zero; this

implies that also f is not identically zero. Being f univariate, the case of $n = 1$ applies, giving the inequality $\Pr[\varepsilon_2|\neg\varepsilon_1] \leq d_1/|S|$. Eventually, since the event ε_2 occurs if and only if $p(x_1, \ldots, x_n) = 0$, we conclude as follows:

$$\begin{aligned}\Pr[\varepsilon_2] &= \Pr[\varepsilon_1 \wedge \varepsilon_2] + \Pr[\varepsilon_2 \wedge (\neg\varepsilon_1)] \\ &= \Pr[\varepsilon_1 \wedge \varepsilon_2] + \Pr[\varepsilon_2|\neg\varepsilon_1]\Pr[\neg\varepsilon_1] \\ &\leq \Pr[\varepsilon_1] + \Pr[\varepsilon_2|\neg\varepsilon_1] \\ &\leq \frac{d - d_1}{|S|} + \frac{d_1}{|S|} = \frac{d}{|S|}.\end{aligned}$$

□

Note that this bound gives non-trivial information only when $\deg(p) < |S|$.

Proof of Theorem 4.13. Consider an algorithm $\mathcal{C}$ that interacts as follows with $\mathcal{A}$. In order to deal with the decisional version of the (U, V, f)-Diffie-Hellman problem we append the polynomials $v_{t+1} \coloneqq T_0$ and $v_{t+2} \coloneqq T_1$ to the vector $V(X)$, getting $V'(X_1, \ldots, X_n, T_0, T_1)$. We will use them to model the two elements that the adversary tries to distinguish. During the whole simulation $\mathcal{C}$ updates the following lists, where it stores the initial inputs and new answers to the queries issued by $\mathcal{A}$:

$$L_{G,k} = \{(\sigma_i, u_i) : i = 1, \ldots, \tau_{G,k}\}, \qquad L_{H,k} = \{(\varrho_j, v_j) : j = 1, \ldots, \tau_{H,k}\},$$

where $u_i \in \mathbb{Z}_r[X_1, \ldots, X_n]$, $v_j \in \mathbb{Z}_r[X_1, \ldots, X_n, T_0, T_1]$ and $\sigma_i, \varrho_j \in \{0,1\}^m$, for some integer m. We associate encodings to polynomials, whose evaluation determines the group elements, up to the choice of a random generator $P \in G$. The lists $L_{G,k}, L_{H,k}$ are indexed with k, which is the number of issued queries. The constraint $\tau_{G,k} + \tau_{H,k} = k + s + t + 2$ must hold for all $k = 0, \ldots, q$. Moreover, let $\mathcal{S}_k$ and $\mathcal{R}_k$ denote the sets of encodings on G and H respectively, given by all the first entries of pairs in $L_{G,k}$ and $L_{H,k}$. The simulation consists of three parts.

Initialization. At $k = 0$ the algorithm $\mathcal{C}$ puts the input values in the lists, setting:

$$L_{G,0} = \{(\sigma_i, u_i) : i = 1, \ldots, \tau_{G,0} = s\}, \qquad L_{H,0} = \{(\varrho_j, v_j) : j = 1, \ldots, \tau_{H,0} = t + 2\},$$

with $u_i \in U(X_1, \ldots, X_n)$, $v_j \in V(X_1, \ldots, X_n, T_0, T_1)$ and σ_i, ϱ_j distinct random stings in $\{0,1\}^m$. The order r of G and the initial encodings $\mathcal{S}_0, \mathcal{R}_0$ are given to $\mathcal{A}$; without loss of generality, we further assume that $\mathcal{A}$ makes oracle queries only on strings obtained from $\mathcal{C}$.

Query phase. At each step $k = 1, \ldots, q$ the interaction between $\mathcal{A}$ and $\mathcal{C}$ consists of one of the following queries.

- Group operations in G, H. Whenever $\mathcal{A}$ asks for a group operation in G, it specifies a pair of encodings $\sigma_i, \sigma_j \in \mathcal{S}_{k-1}$ and a bit indicating the operation $\sigma_i \pm \sigma_j$. Then $\mathcal{C}$ sets $\tau_{G,k} \coloneqq \tau_{G,k-1} + 1$ and performs the polynomial operation $u_i \pm u_j =: u_{\tau_{G,k}}$. If $u_{\tau_{G,k}} = u_l$ for some $l \leq \tau_{G,k-1}$, then it defines $\sigma_{\tau_{G,k}} \coloneqq \sigma_l$; otherwise it chooses $\sigma_{\tau_{G,k}}$ as a new random bit string in $\{0,1\}^m \setminus \{\sigma_1, \ldots, \sigma_{\tau_{G,k-1}}\}$. Eventually, $\mathcal{C}$ sets $L_{G,k} = L_{G,k-1} \cup \{(\sigma_{\tau_{G,k}}, u_{\tau_{G,k}})\}$ and sends $\sigma_{\tau_{G,k}}$ to $\mathcal{A}$, that updates the encoding set relative to G as $\mathcal{S}_k = \mathcal{S}_{k-1} \cup \{\sigma_{\tau_{G,k}}\}$.
  The procedure for a group operation query in H is analogous.

- Bilinear pairing. The algorithm $\mathcal{A}$ specifies a pair of encodings $\sigma_i, \sigma_j \in \mathcal{S}_{k-1}$. Then $\mathcal{C}$ sets $\tau_{H,k} \coloneqq \tau_{H,k-1} + 1$ and performs the polynomial operation $u_i \cdot u_j =: v_{\tau_{H,k}}$. If $v_{\tau_{H,k}} = v_l$ for some $l \leq \tau_{H,k-1}$, then it defines $\varrho_{\tau_{H,k}} \coloneqq \varrho_l$; otherwise it chooses $\varrho_{\tau_{H,k}}$ as a new random bit string in $\{0,1\}^m \setminus \{\varrho_1, \ldots, \varrho_{\tau_{H,k-1}}\}$. Eventually, $\mathcal{C}$ sets $L_{H,k} = L_{H,k-1} \cup \{(\varrho_{\tau_{H,k}}, v_{\tau_{H,k}})\}$ and sends $\varrho_{\tau_{H,k}}$ to $\mathcal{A}$, that updates the encoding set relative to H as $\mathcal{R}_k = \mathcal{R}_{k-1} \cup \{\varrho_{\tau_{H,k}}\}$.

Guess. After at most q queries, $\mathcal{A}$ terminates and returns $b' \in \{0,1\}$. Then $\mathcal{C}$ chooses random $x_1, \ldots, x_n, t \in \mathbb{Z}_r$ and a random bit $b \in \{0,1\}$, setting $t_b \coloneqq f(x_1, \ldots, x_n)$ and $t_{1-b} = t$. Eventually, $\mathcal{C}$ concludes the simulation evaluating polynomials in $L_{G,q}$, $L_{H,q}$ at $X_i = x_i$, for $i = 1, \ldots, n$, $T_0 = t_0$ and $T_1 = t_1$.

Note that $L_{G,q}$, $L_{H,q}$ are collision-free, by construction. Moreover, once the polynomials are evaluated, the bit strings are associated to group elements. Thus, $\mathcal{C}$ outputs are indistinguishable from encodings by means of random encoding functions $\sigma : G \to \{0,1\}^m$ and $\varrho : H \to \{0,1\}^m$, compatible with the oracles simulated by $\mathcal{C}$, when both $L_{G,q}$, $L_{H,q}$ are coherent with respect to $x_1, \ldots, x_n, t_0, t_1$: let ε_s be such event. Otherwise an oracle would encode the same element with two different binary strings, as follows from Definition 4.12. Therefore we need to bound the probability that ε_s occurs. Firstly we consider the symbolic substitution $T_b = f(X_1, \ldots, X_n)$: we claim that it does not create new polynomial identities. Indeed, note that the variable T_b appears only in polynomials v_j and assume $v \coloneqq v_i - v_j \neq 0$. Since the queries produce only sums and product from initial polynomials, we can write v as:

$$v = \sum_{\substack{\mu,\lambda=1 \\ \mu<\lambda}}^{s} a_{\mu,\lambda} u_\mu u_\lambda + \sum_{\gamma=1}^{t} b_\gamma v_\gamma + c_0 T_0 + c_1 T_1 \tag{4.3}$$

for suitable constants $a_{\mu,\lambda}, b_\gamma, c_0, c_1 \in \mathbb{Z}_r$. From the independence assumption, it clearly follows that f is independent on U, V' in $\mathbb{Z}_r[X_1, \ldots, X_n, T_0, T_1]$. So if $v \neq 0$, but the substitution causes the right hand side of 4.3 to vanish, then the independence of f would be contradicted. Therefore we now work on polynomials in the variables $X_1, \ldots, X_n, T_{1-b}$. The probability that $u_i - u_j(x_1, \ldots, x_n) = 0$, for some $u_i \neq u_j$ in $L_{G,q}$, or $v_i - v_j(x_1, \ldots, x_n, t) = 0$, for some $v_i \neq v_j$ in $L_{H,q}$, is bounded by d/r. Indeed, Lemma 4.14 applies with $K = S = \mathbb{Z}_r$ and, by construction, d bounds the total degree of all the polynomials. Since there are at most $2\binom{q+s+t+2}{2}$ such pairs (u_i, u_j) and (v_i, v_j), we get:

$$\Pr(\neg\varepsilon_s) \leq \binom{q+s+t+2}{2} \frac{2d}{r} \leq \frac{d(q+s+t+2)^2}{r}.$$

When ε_s occurs, the simulation gives $\Pr[b' = b|\varepsilon_s] = 1/2$ and the following inequalities hold:

$$\Pr[b' = b] \leq \Pr[b' = b|\varepsilon_s](1 - \Pr[\neg\varepsilon_s]) + \Pr[\neg\varepsilon_s] = \frac{1}{2} + \frac{\Pr[\neg\varepsilon_s]}{2},$$
$$\Pr[b' = b] \geq \Pr[b' = b|\varepsilon_s](1 - \Pr[\neg\varepsilon_s]) = \frac{1}{2} - \frac{\Pr[\neg\varepsilon_s]}{2}.$$

Thus, we conclude that

$$\left|\Pr[b' = b] - \frac{1}{2}\right| \leq \frac{\Pr[\neg\varepsilon_s]}{2} \leq \frac{d(q+s+t+2)^2}{2r}. \qquad \square$$

Theorem 4.13 gives relevant information on some specific problem, since the bound adapts itself to the choice of input polynomials. In particular, Theorem 4.13 applies when such input vectors are defined as in 4.2. Indeed, $f(X_1, X_2) = X_1^\ell X_2$ is independent on U, V in $\mathbb{Z}_r[X_1, X_2]$. To prove it, assume that

$$X_1^\ell X_2 = \sum_{\substack{\mu,\lambda=1 \\ \mu<\lambda}}^{2\ell+1} a_{\mu,\lambda} u_\mu u_\lambda + b,$$

for some $a_{\mu,\lambda}, b \in \mathbb{Z}_r$. It follows that we should have the identity

$$X_1^\ell = \sum\nolimits_{\lambda \in \{1,\ldots,\ell-1,\ell+1,\ldots,2\ell\}} a_{2,\lambda} X_1^\lambda,$$

which cannot hold for any sequence $a_{2,\lambda}$ of coefficients. Recall that this choice of the inputs gives the polynomial model for the ℓ-BDHE problem in a pair of groups with pairing (G, H, e). Therefore the advantage of a generic algorithm $\mathcal{A}$ in solving the corresponding decisional problem is bounded by

$$Adv_{\mathcal{A}}(q, r, \ell) \leq \frac{2\ell(q + 2\ell + 4)^2}{r}, \tag{4.4}$$

where q is the maximum number of queries allowed to $\mathcal{A}$. This inequality implies a lower bound on the complexity of such adversary, where the time, here, is measured by the number of queries. Indeed, consider an advantage $\varepsilon \in [0, 1/2]$ and assume that $\mathcal{A}$ can issue at most q queries; then the inequality 4.4 gives, after few computations:

$$q \geq \sqrt{\frac{r\varepsilon}{2\ell}} - 2\ell - 4 =: q_{\min}(r, \varepsilon, \ell). \tag{4.5}$$

Thus $q_{\min}(r, \varepsilon, \ell)$ is the minimum number of queries needed to achieve advantage at most ε and we conclude that any generic adversary, achieving such advantage ε, must take time at least $\Omega(q_{\min}(r, \varepsilon, \ell))$. Recall that, if $f, g : \mathbb{N} \to \mathbb{R}$ are two real valued functions, the *big-omega* notation, $f(n) \in \Omega(g(n))$, means that there exist two constants $C \in \mathbb{R}$ and $N \in \mathbb{N}$, such that it holds the inequality $|f(n)| \geq C|g(n)|$, for all $n > N$. We will estimate later the complexity of each query in a specific case, in terms of finite field operations. Evidently, the lower bound grows with the group order r, so that large groups give a higher security level, as expected.

Remark 4.15. Let $\varepsilon \in [0, 1/2]$ and $n, B \in \mathbb{N}$ be some fixed parameters; then the system $\mathfrak{B}$ is (t, ε, n) semantically secure for every $t < q_{\min}(r, \varepsilon, B)$, since the decisional (t, ε, B) BDHE assumption holds in the same hypotheses and Theorem 4.7 applies. Thus we deduce information on the parameters for the semantic security of the cryptosystem $\mathfrak{B}$. The parameter t measures the number of queries issued by an adversary.

4.4.3 Limitations of the generic group model: an example case

The key point in the proof of 4.13 is the indistinguishability of the polynomial simulation from a real one. When the coherence of both encoding lists is achieved, an adversary $\mathcal{A}$ observes the same answers as those produced by a real oracle, which outputs encodings given by a specific encoding function of some group. Therefore an attacker would behave the same way in both cases; guessing on encodings of abstract polynomials, before their evaluation, the probability that $\mathcal{A}$ outputs the correct bit must be $1/2$. The assumption that all encodings are random strings is particularly strong and it restricts the significance of Theorem 4.13 for real applications, although it remains an important theoretic result. Indeed, the particular representation of real elements, such as points on elliptic curves, matters, as it could make their encodings adversarially distinguishable from uniformly distributed ones. An example is provided by the following attack from [47]. Let $E/\mathbb{F}_p$ be an elliptic curve over a prime field, for some large prime p; for every integer k, the point $(X, Y, Z) \in E(\mathbb{F}_{p^k})$ is represented by means of *projective Jacobian coordinates*, if the corresponding affine point has coordinates $\left(X/Z^2; Y/Z^3\right)$. Thus it is a homogeneous representation, where the first and second coordinates have weight 2 and 3 respectively.

Recall that Jacobian coordinates allow to construct efficient formulae for point operations. Assume to use standard algorithms for doubling, addition and scalar point multiplication, as defined in [10]. Let $T \in E(\mathbb{F}_p)$ be a point of prime order r, with affine coordinates (x_T, y_T); then pick a secret integer k and set $P \coloneqq [k]T$, represented by means of Jacobian coordinates (X_0, Y_0, Z_0). Denote by P_i, for $i = 1, \ldots, l$, the intermediate points obtained during the execution of the doubling-and-add algorithm for scalar multiplication; moreover, let (X_i, Y_i, Z_i) and (x_i, y_i) be their Jacobian and affine coordinates respectively. The binary encoding of k is given by:

$$(k)_2 = (k_m, k_{m-1}, \ldots, k_0) \quad \Leftrightarrow \quad k = \sum_{j=0}^{m} k_j 2^j,$$

with $k_j \in \{0, 1\}$, for $j = 0, \ldots, m$, and $m = \lfloor \log_2(k) \rfloor$. We claim that it is possible to guess the least significant bit k_0 with probability at least $2/3$, in the case of $p \equiv 1 \mod 3$. Indeed, let us focus on the computation of the Z-coordinate; recall that the attacker knows Jacobian coordinates for P_l and hence also its affine representation (x_0, y_0). For each bit k_j of $(k)_2$ the double-and-add algorithm performs one of the following intermediate operations:

1. if $k_j = 1$, the addition $P_j \coloneqq [2]P_{j-1} + T$, which yields:

$$Z_j'^3 = \frac{Z_j}{x_j' - x_T},$$

   where $(X_j', Y_j', Z_j') = P_j' =: [2]P_{j-1}$;

2. if $k_j = 0$, the doubling $P_j \coloneqq [2]P_{j-1}$, which yields:

$$Z_{j-1}^4 = \frac{Z_j}{2y_{j-1}}.$$

Note that, from (x_0, y_0), one can efficiently compute x_j', by summing $-T = (x_T, -y_T)$ (1.8), or y_{j-1}, by reversing the affine version of the doubling formulae (1.9). Furthermore assume, for example, $k_0 = 0$, which causes the last step in the double-and-add algorithm to be a doubling as in case 2. To briefly analyse the probability to spot the correct k_0 we use the following lemma, that follows from [31, Proposition 7.1.2].

Lemma 4.16. *Let $q = p^n$ be an odd prime power, for some integer $n \geq 1$. Assume that $r \mid (q-1)$, then the following hold:*

- *$x \in \mathbb{F}_q^*$ is an r-th power in $\mathbb{F}_q^*$ if and only if $a^{(q-1)/r} = 1$;*
- *there are exactly $(q-1)/r$ distinct r-th powers in $\mathbb{F}_q^*$.*

Therefore, since $p \equiv 1 \mod 3$, the above Lemma implies that $\frac{Z_0}{x_0' - x_T}$ is not a third power in $\mathbb{F}_p$ with probability $2/3$. In this case, the adversary would immediately understand the correct value for k_0, because the last step of the scalar multiplication could not be an addition as 1. Otherwise, there are at most three candidates for (X_1, Y_1, Z_1) and it is possible to check if halving the results is possible or not, looking again for a contradiction. By means of this backtracking technique, the adversary can guess k_0, with probability higher that $2/3$; a similar procedure works if $k_0 = 1$. To avoid this specific attack one should use projective coordinates only for internal calculations, giving outputs only by means of affine coordinates. This analysis could not be performed in the generic group model, where encodings are random bit strings, which do not take account of such vulnerabilities.

In conclusion, although the application of Theorem 4.13 produces some important information on the security level of the decisional ℓ-BDHE problem and asymptotic bounds on the parameters, one should be aware that these result does not guarantee the semantic security in all particular cases. To the best of our knowledge, only generic algorithms are available for solving this problem and so one can take advantage of the results of these section, when studying the security of the broadcast encryption system $\mathfrak{B}$.

4.5 A family of elliptic curves for the secure implementation of symmetric pairings

The hardness of the ℓ-BDHE problem in a pair of groups with pairing is not the only concern, when investigating the security of $\mathfrak{B}$. Other vulnerabilities should be taken into account: this section aims to show that there exist suitable elliptic curves for the implementation of symmetric pairings. We mainly refer to [46] for comments on topics that we do not examine in detail.

The MOV reduction, outlined in Section 4.1, allows to reduce instances of the discrete logarithm problem on an elliptic curve to instances of the same problem on a finite field, taking advantage of bilinear pairings. Pairing-based cryptography requires to choose elliptic curves that enable efficient pairing computation as well as a high security level. Usually, a suitable elliptic curve $E/\mathbb{F}_q$ should admit pairings taking values in sufficiently large finite fields, such that the MOV reduction is ineffective. In particular, the following conditions should hold:

- the DLP must be computationally infeasible in the cyclic subgroup $E(\mathbb{F}_q)[r] \leq E[r]$, for some prime number $r \mid N = |E(\mathbb{F}_q)|$ such that $(r, \mathrm{char}(\mathbb{F}_q)) = 1$;
- the DLP must be computationally infeasible in $\mathbb{F}_{q^k}^*$, where k is the embedding degree of E with respect to r (3.12).

The former requirement is achieved when r is a large prime factor of N, while the latter depends on the embedding degree, which can be studied by means of Theorem 3.11. Recall that the ℓ-BDHE problem is weaker than the DLP and so cryptosystems must be even more protected from discrete logarithm attacks. A classical result by Hasse [52, ch.V, Theorem 1.1] gives information about the number of rational points on E.

Theorem 4.17 (Hasse)**.** *Let $E/\mathbb{F}_q$ be an elliptic curve and let N denote $|E(\mathbb{F}_q)|$. Then it holds:*

$$|N - q - 1| \leq 2\sqrt{q}.$$

Thus, when q is large, N has roughly the same bit size as q, because from the above inequality we get:

$$\log(\sqrt{q} - 1)^2 \leq \log N \leq \log(\sqrt{q} + 1)^2$$
$$c_1 \log q \leq \log N \leq c_2 \log q$$

for some constants $c_1, c_2 \in \mathbb{R}$. Then, the parameter

$$\varrho \coloneqq \frac{\log q}{\log r}$$

measures the ratio between the bit sizes of N and r. In order to get the above condition on r, the ideal case is to choose a curve with $\varrho \approx 1$. Then the embedding degree k is

completely defined by ϱ and the choice of the bit sizes of r and q^k, since $\log q^k / \log r = k\varrho$. Recall also that we will always assume, as in section 2.3, that $|E(\mathbb{F}_q)|$ and $p = \mathrm{char}(\mathbb{F}_q)$ are relatively prime, to avoid the anomalous attack [57]. Common ranges for these parameters can be found in [24], where the authors define, as follows, requirements needed to get elliptic curves suitable for pairing-based cryptography.

Definition 4.18. An elliptic curve $E/\mathbb{F}_q$ is *pairing-friendly* if the following two conditions hold:

1. $\varrho \leq 2$, for some prime integer $r \mid N$;
2. the embedding degree k of E with respect to r is less than $\log_2(r)/8$.

Pairing-friendly curves must be specifically constructed, since randomly chosen ones have small probability to satisfy this definition, as shown in [4]. We refer to [46, ch. 4,10] for the construction of pairing-friendly curves. Currently, the most efficient cryptographic pairings come from elliptic curves (or higher-dimensional algebraic varieties). As explained in Section 3.3, distortion maps are needed to get non-degenerate symmetric pairings from the Weil ones. More generally, the same ideas apply also in the case of more efficient elliptic curve pairings, such as the Ate ones and their variants. Therefore, as explained in Section 3.3.1, only supersingular elliptic curves allow the construction of symmetric pairings, which are required for implementing $\mathfrak{B}$. In [24] there is a classification of these curves, which shows that they admit only embedding degrees $k \in \{1, 2, 3, 4, 6\}$. Due to results in [1,6,27], it is advised to avoid supersingular elliptic curves defined on fields of characteristic 2 and 3. This restricts significantly the choice of parameters, since the remaining cases give embedding degrees $k = 2$ or $k = 3$.

In recent years, improvements in the asymptotic complexity of the DLP computation in finite fields have been achieved, forcing to update parameters of pairing-friendly elliptic curves. In our case the best choice is a supersingular curve $E/\mathbb{F}_q$, over some field with large prime characteristic $\mathrm{char}(\mathbb{F}_q) = p > 3$, since the embedding degree is small. Medium characteristic fields should be avoided too. Indeed, authors of [6] show that there exists an algorithm solving the DLP in $\mathbb{F}_Q$, which has quasi-polynomial computational complexity $(\log Q)^{O(\log\log Q)}$, when $Q = q^{2m}$, $q \approx m$ and $m \leq q + 2$. In our case, having few choices for the embedding degree, the size of p should be decided depending on the complexity of the DLP computation in $\mathbb{F}_{q^k} = \mathbb{F}_{p^n}$, for some integer n.

Remark 4.19. For a large prime p, we have the following cases, from [46, Section 9.3.10].

1. If n is prime, then the complexity depends on whether the prime p is the root of a polynomial, i.e. $p = P(u)$ for $P(X) \in \mathbb{Z}[X]$, or it has no special form. In the former case only the generic algorithms apply, giving asymptotic complexity $L_{p^n}(1/3, 1.923)$, where the complexity function $L_q(\mu, c)$ is defined by 3.1. In the latter case, methods from [32] apply, but it holds $\deg(P) = 2$, so they give the same generic complexity, as in the former case.
2. If n is composite, we distinguish the same cases as before; new methods for the DLP computation, proposed in [7, 34, 48], apply. Therefore, if p is the root of a polynomial of degree at least 3, then the asymptotic complexity becomes $L_{p^n}(1/3, 1.56)$; otherwise, it is $L_{p^n}(1/3, 1.74)$.

According to [46], when n is composite, the field size should be enlarged, with respect to the first case, by a factor 2 or 4/3 respectively.

Next, let k be the embedding degree of $E/\mathbb{F}_q$ with respect to r. Recall that the image of every pairing, taking values in a group of order r, is a subgroup of $\mathbb{F}_{q^k}^*$. However, to better determine the security of a pairing-based cryptosystem, we point out that this is not always the minimal field containing the group μ_r of r-th roots of unity. Indeed, μ_r lies in the *minimal embedding field* $\mathbb{F}_{p^{\mathrm{ord}_r(p)}}$, where $\mathrm{ord}_r(p)$ denotes the order of p in the multiplicative group $\mathbb{Z}_r^*$. This gives an embedding into an extension of the field $\mathbb{F}_p$, which is not necessarily an extension of $\mathbb{F}_q$. The difference in size between $\mathbb{F}_{q^k}$ and the minimal embedding field can be relevant, as the following result from [30] proves.

Proposition 4.20. *Let $q = p^m$ be a prime power and let $E/\mathbb{F}_q$ be an elliptic curve; consider a prime number r, dividing $|E(\mathbb{F}_q)|$, and let k be the embedding degree of E with respect to r. Then it holds:*

$$k = \frac{\mathrm{ord}_r(p)}{\gcd(\mathrm{ord}_r(p), m)}$$

Proof. To ease the notation, set $\delta \coloneqq \mathrm{ord}_r(p)$ and $\gamma \coloneqq \gcd(\delta, m)$. By Theorem 3.11, k is the smallest integer such that $q^k \equiv 1 \mod r$; it follows that $k \mid (\delta/\gamma)$, since:

$$1 \equiv p^\delta \equiv \left(p^\delta\right)^{m/\gamma} \equiv q^{\delta/\gamma} \mod r.$$

Furthermore, the congruence $p^{mk} \equiv 1 \mod r$ implies that $\delta \mid mk$ and hence $\frac{\delta}{\gamma} \mid \frac{mk}{\gamma}$. In conclusion, it holds $\frac{\delta}{\gamma} \mid k$, because $\gcd(\frac{\delta}{\gamma}, \frac{m}{\gamma}) = 1$. □

Thus the minimal embedding field is $\mathbb{F}_{p^{\mathrm{ord}_r(p)}} = \mathbb{F}_{p^{k\gamma}}$, instead of $\mathbb{F}_{q^k} = \mathbb{F}_{p^{km}}$ and so the bit sizes of elements in these fields differ by a factor of m. Moreover, it is possible to enlarge this gap as wanted, by increasing the exponent m relatively prime to $\mathrm{ord}_r(p)$; these differences disappear when q is a prime number. In general, the elliptic curve choice for cryptographic applications should guarantee that the DLP is computationally infeasible in the minimal embedding field and not only in $\mathbb{F}_{q^k}$. It follows from [8] a characterisation of this field.

Proposition 4.21. *Assuming that the hypotheses in Theorem 4.20 hold, then the minimal embedding field of E with respect to r is $\mathbb{F}_{p^n}$ if and only if $r \mid \Phi_n(p)$, where $\Phi_n(X)$ is the n-th cyclotomic polynomial.*

After this review of the main security requirements, we introduce a family of pairing-friendly supersingular elliptic curves that satisfy them, under the choice of suitable parameters, and that admit an efficient pairing. These curves were first proposed in [54] and, in a more general fashion, in [59]. They are a valuable choice for the implementation of the broadcast encryption system $\mathfrak{B}$ and, in general, for all cryptosystems that require symmetric pairings. Take a prime $p > 3$, such that $p \equiv 5 \mod 6$, set $q \coloneqq p^2$ and let $b \in \mathbb{F}_q$ be a square, but not a cube. Then define the elliptic curves E_b by means of the affine equation

$$E_b/\mathbb{F}_q : y^2 = x^3 + b.$$

The authors of [54] suggest to use the reduced Ate paring, from [29], since they propose a faster algorithm for its computation on the curves E_b. In addition, [56, Theorem 2] provides explicit distortion maps on these elliptic curves. It can be proved that the group of $\mathbb{F}_q$-rational points on all curves E_b has cardinality

$$|E_b(\mathbb{F}_q)| = p^2 - p + 1.$$

For the sake of security and efficient pairing computation, consider the largest prime divisor r of $|E_b(\mathbb{F}_q)|$ and assume that $r^2 \nmid |E_b(\mathbb{F}_q)|$; then the pairing should be defined on the group $G = E_b(\mathbb{F}_q)[r]$. Examples of elliptic curves satisfying all previous conditions are given in the article. By Proposition 4.21, the minimal embedding field of all the curves E_b, with respect to r, is $\mathbb{F}_{p^6} = \mathbb{F}_{q^3}$, since $\Phi_6(p) = |E(\mathbb{F}_q)|$. Note that in this case the embedding degree must satisfy the inequality $2k \geq 6 = \mathrm{ord}_r(p)$ and we know that $k \in \{2, 3\}$. Thus it must be $k = 3$ and so there is no difference between the embedding field $\mathbb{F}_{q^k}$ and the minimal one.
The first concern, before considering the computational complexity of the pairing computation, is about the security of these curves. As remarked above, the large prime p should guarantee the computational infeasibility of the DLP in $\mathbb{F}_{p^6}$. In particular, since its cardinality is a prime power with composite exponent, it should be assumed that the complexity of the DLP computation is bounded as in the second case of Remark 4.19. The other security issue that could concern curves E_b is the Weil descent attack. The idea, first pointed out in [25], is to reduce the DLP from an elliptic curve over a composite finite field to the same problem on another curve over a smaller field, where more efficient methods apply. In the case of curves E_b this attack can be performed with computational complexity $\tilde{\mathcal{O}}(q)$. Recall that $f(n) \in \tilde{\mathcal{O}}(g(n))$ if there exists a constant c such that $f(n) \in O\left(g(n)\log^c(g(n))\right)$. According to [54] the prime p should be at least an integer of 200 bit length, in order to get a curve secure against the Weil descent attack.

4.5.1 Computational complexity of the group law and pairing computation: the case of curves E_b

In Section 4.4.2, Theorem 4.13 gives a lower bound for the running time of an adversary solving the decision ℓ-BDHE problem, with maximum advantage ε. Assuming that an attacker has access to oracles computing the group law, on elliptic curve points, or the bilinear pairing, then time was measured as the number of queries to these oracles. Here we collect their computational complexities in terms of finite field operations. Despite Theorem 4.13 deals with a polynomial form of such queries, a real adversary would have access to oracles that work on rational points of some elliptic curve. Consider the family of curves E_b, defined above, and the symmetric pairing of [54, Definition 1]. Assume to compute it by applying the modified Miller's algorithm [54, Algorithm 1] and suppose that points are represented by means of affine coordinates. For the study of computational complexity, denote by M_n, S_n and I_n the multiplication, squaring and inversion in $\mathbb{F}_{p^n}$ respectively. Let Π denote the computation of the p-th Frobenius map over $\mathbb{F}_{p^6}$ and assume that it has the same computational complexity as the p^3-th Frobenius map computation over the same field. Eventually, let $\exp_h$ denote the exponentiation by h in $\mathbb{F}_{p^6}$. According to [28], efficient arithmetic can be performed in the *optimal extension field* $\mathbb{F}_{p^n}$, which satisfies the following requirements:

- $p = 2^\ell - c$, for some integers ℓ, c, such that $\log_2 |c| \leq \ell/2$;
- an irreducible polynomial $f(X) = X^n - \omega \in \mathbb{F}_p[X]$ exists.

Furthermore we need to encode $p - 1$ in the following *Non-Adjacent Form (NAF)*:

$$p - 1 = \sum_{j=0}^{\ell} s_j 2^j, \tag{4.6}$$

where $s_j \in \{-1, 0, 1\}$ and $s_j s_{j+1} = 0$ for all $j = 0, \ldots, l - q$. Refer to [10, ch. IV] for an algorithm that gives this encoding. Note also that each integer has a unique NAF

representation; let w^+_{NAF} and w^-_{NAF} denote its number of 1 and -1 components respectively. All these assumptions, which are verified in the examples proposed by [54], lead to the following complexity for the pairing computation:

$$\begin{aligned}&(49+8l+8w^+_{\mathrm{NAF}}+8w^-_{\mathrm{NAF}})M_2+(9+2l+2w^+_{\mathrm{NAF}}+3w^-_{\mathrm{NAF}})M_6+\\&+(7+2l+w^+_{\mathrm{NAF}}+w^-_{\mathrm{NAF}})S_2+(2+l)S_6+\\&+(5+l+w^+_{\mathrm{NAF}}+w^-_{\mathrm{NAF}})I_2+1I_6+2\Pi+1\exp_h,\end{aligned} \tag{4.7}$$

where $h = |E(\mathbb{F}_q)|/r$. Moreover, assuming that all the previous hypotheses hold, we study also the complexity of each group operation query. Indeed, the corresponding oracle performs an addition or a subtraction of points in $E(\mathbb{F}_{p^2})$, which both require the following number of finite field operations:

$$3M_2 + 1I_2. \tag{4.8}$$

Evidently, addition queries are much less expensive that pairing ones; note also that to refine the result in 4.5 we need a lower bound on the complexity of every query. Since no information on the adversary's strategy is known, a conservative assumption is that all queries are group law computations on G. Therefore it follows that Remark 4.15 holds with

$$t_{\min}(r,\varepsilon,B) \coloneqq q_{\min}(r,\varepsilon,B)(3M_2+1I_2).$$

In this context, the time parameter in the decision ℓ-BDHE assumption measures the number of finite field operations.

Remark 4.22. The group operation query of Theorem 4.13 can be easily modified in order to allow operations such as $\alpha P_i \pm \beta P_j$, where $\alpha, \beta \in \mathbb{Z}_r$ and $P_i, P_j \in G$ are admissible query inputs. The procedure would be the same, since the new oracle would associate a bit string to the polynomials $\alpha u_i \pm \beta u_j$ in the same fashion as before. Moreover, the proof does not change, since the maximum total degree of the resulting polynomials is the same as in the original argument. However, we do not introduce such modified query in this work, because the above analysis would depend on the computational cost of scalar multiplication $[m]$ in $E(\mathbb{F}_q)$, defined by 1.6. There are many different efficient algorithms that compute it; their complexity depends on the elliptic curve specific parameters; some classical ones are proposed in [10]. The easiest method is the double-and-add algorithm [10, Algorithm IV.1]; it can be adapted to the case of multiplication for some integer m, written in NAF form, by replacing addition with subtraction in the steps corresponding to components -1 of the encoding. Its complexity becomes:

$$(w^+_{\mathrm{NAF}}+w^-_{\mathrm{NAF}})(3M_2+1I_2)+\lceil\log_2(m)\rceil(4M_2+1I_2),$$

which is still less than the paring computation's complexity examined before. Hence the analysis of the bound in the case of modified oracles would be similar as above.

4.6 Conclusions and open problems

In Chapters 1 and 2 we introduced the mathematical background of pairing-based cryptography. We mainly examined the construction of the Weil maps, which give examples of cryptographic pairings. The general definitions of the latter ones are reviewed in Chapter 3, since there are many versions of those definitions in literature. The main topic, studied in Chapter 4 is the security of the broadcast encryption system proposed in [15]. The semantic security of this cryptosystem is connected to the decisional ℓ-BDHE assumption by [15, Theorem 3.1]. In Section 4.4, we proved the hardness of the latter problem in the

generic group model, adapting [16, Theorem A.2] to the case of our interest. From this result, we deduced a lower bound 4.5 on the complexity of an adversary with advantage ε. Its running time is expressed in terms of queries to oracles computing the group law and the bilinear pairing. This result allows to give a bound on the semantic security parameters for the encryption scheme 4.15. Some drawbacks of the generic group model are examined in Section 4.4.3; in particular, there is an example from literature showing that the specific encoding of points violates, in some cases, this model's assumptions. Eventually, we analysed the main security issues of pairing-based cryptography, that can be avoided by a meaningful choice of the elliptic curve. This raises the issue of the existence of suitable curves for implementing the studied encryption system; in particular, supersingular ones are needed. In Section 4.5 is proposed a family of such curves, that admit an efficiently computable pairing. Eventually, given its computational complexity, we refined the lower bound 4.5, in terms of finite field operations.
An article by Lubicz and Sirvent [38] introduces a slightly different version of the generic group model. Recall that the original one, followed in this thesis, is based on oracles that output random bit strings, as answers to queries. These random choices correspond, at the end of simulation, to the application of random encoding functions. In contrast, in the new model two encoding functions are randomly chosen at the beginning and oracles answers follow the group law induced by these maps. Then authors study the set of group law pairs, that remain indistinguishable from the induced ones. The final probability, that gives the bound, is computed over the random choice of such pairs over this set. It could be interesting to adapt their results to the decisional ℓ-BDHE problem. This would lead to new lower bounds on the attack complexity.

Bibliography

[1] G. Adj, A. Menezes, T. Oliveira, F. Rodriguez-Henriquez. *Computing discrete logarithms in* $\mathbb{F}_{3^{(6\cdot 137)}}$ *and* $\mathbb{F}_{3^{(6\cdot 163)}}$ *using Magma.* C. K. Koc, S. Mesnager and E. Savas (eds) Arithmetic of Finite Fields (WAIFI 2014), vol. 9061, of Lectures Notes in Computer Science, pp. 3-22, Springer, 2014.

[2] M. F. Atiyah, I. G. Macdonald. *Introduction to commutative algebra.* Addison-Wesley Publishing Company, 1969.

[3] E. Bach, Jeffrey Shallit. *Algorithmic number theory.* The MIT Press, vol. 1, 1996.

[4] R. Balasubramanian, N. Koblitz. *The improbability that an elliptic curve has subexponential discrete log problem under the Menezes-Okamoto-Vanstone algorithm.* Journal of Cryptology, vol. 11, issue 2, pp. 141–145, 1998.

[5] R. Barbulescu, P. Gaudry, T. Kleinjung. *The tower number field sieve.* Advances in Cryptology, ASIACRYPT 2015, LCNS 9453, pp. 31–55, 2015.

[6] R. Barbulescu, P. Gaudry, E. Thomé, A. Joux. *A heuristic quasi-polynomial algorithm for discrete logarithm in finite fields of small characteristic.* P. Q. Nguyen, E. Oswald (eds) Advances in Cryptology – EUROCRYPT 2014, Lecture Notes in Computer Science, vol. 8441, Springer, 2013.

[7] R. Barbulescu, P. Gaudry, A. Guillevic, F. Morain. *Improving NFS for the dis-crete logarithm problem in non-prime finite fields.* M. Fischlin and E. Oswald (eds) Advances in Cryptology, Eurocrypt 2015, Lecture Notes in Computer Sciences, vol. 9056, pp.129-155, 2015.

[8] N. Benger, M. Scott. *Constructing tower extensions of finite fields for implementation of pairing-based cryptography.* M.A. Hasan, T. Helleseth (eds), WAIFI 2010. Lecture Notes in Computer Science, vol. 6087, pp. 180–195. Springer, 2010.

[9] D. J. Bernstein. *Faster square roots in annoying finite fields.*
URL: http://cr.yp.to/papers/sqroot.ps.

[10] I. Blake, G. Seroussi, N. Smart. *Elliptic curves in cryptography.* Cambridge University Press, 1999.

[11] I. Blake, G. Seroussi, N. Smart. *Advances in elliptic curve cryptography.* Cambridge University Press, 2005.

[12] D. Boneh, X. Boyen, E. Goh. *Hierarchical identity based encryption with constant size ciphertext.* Advances in Cryptology, R. Cramer editor, EUROCRYPT 2005, vol. 3493, pp. 440–456, Lecture Notes in Computer Science, Springer, 2005.

[13] D. Boneh, X. Boyen, H. Shacham. *Short group signatures.* CRYPTO 2004, Springer-Verlag, 2004.

[14] D. Boneh, M. Franklin. *Identity-based encryption from the Weil pairing.* Advances in Cryptology – CRYPTO 2001, Lecture Notes in Computer Science, vol. 2139, pp. 213–229, Springer, 2001. Full version: SIAM Journal on Computing, vol.32, pp. 586–615, 2003.

[15] D. Boneh, C. Gentry, B. Waters. *Collusion resistant broadcast encryption with short ciphertext and private keys.* Advances in cryptology—CRYPTO 2005, Lecture Notes in Computer Science, vol. 3621, pp. 258–275, Springer, 2005.

[16] D. Boneh, E.-J. Goh, K. Nissim. *Evaluating 2-DNF formulae on ciphertexts.* Theory of Cryptography '05, vol. 3378 of Lecture Notes in Computer Science, pp. 325–341, Springer-Verlag, 2005.

[17] D. Boneh, B. Lynn, H. Shacham. *Short signatures from the Weil pairing.* Advances in Cryptology – ASIACRYPT 2001, Lecture Notes in Computer Science, vol. 2248, pp. 514–532, Springer, 2001. Full version: Journal of Cryptology, vol. 17, pp. 297–319, 2004.

[18] S. Ceccato. *A key management scheme for access control to GNSS services.* Tesi di Laurea Magistrale, Dipartimento di Ing. dell'Informazione, Università di Padova, a.a. 2015-16,
URL: http://tesi.cab.unipd.it/52989/

[19] J.H. Cheon. *Security analysis of the strong Diffie-Hellman problem.* S. Vaudenay (eds) Advances in Cryptology - EUROCRYPT 2006, Lecture Notes in Computer Science, vol. 4004. Springer, 2006.

[20] H. Cohen, G. Frey, R. Avanzi, C. Doche, T. Lange, K.Nguyen, F.Vercauteren. *Handbook of elliptic and hyperelliptic curve cryptography.* Chapman & Hall/CRC, 2006.

[21] D. Coppersmith. *Fast evaluation of logarithms in fields of characteristic two.* IEEE Transactions on Information Theory, vol. 30, pp. 587–594, 1984.

[22] D. Eisenbund, M. Green, J. Harris *Cayley-Bacharach theorems and conjectures.* Bulletin of the American Mathematical Society, vol. 33, n. 3, 1996.

[23] A. Enge. *Bilinear pairings on elliptic curves.* arXiv:1301.5520, 2013
https://arxiv.org/abs/1301.5520

[24] D. Freeman, M. Scott, E. Teske. *A taxonomy of pairing-friendly elliptic curves.* Journal of Cryptology, vol. 23, issue 2, pp. 224–280, 2010.

[25] G. Frey, H. Gangl. *How to disguise an elliptic curve (Weil de-scent).* Talk at ECC '98, The 2nd Workshop on Elliptic Curve Cryptography, U. Waterloo, 1998,
URL: http://www.cacr.math.uwaterloo.ca/conferences/1998/ecc98/frey.ps

[26] S.Galbraith, K. Paterson, N. Smart. *Pairings for cryptographers.* Discrete Applied Mathematics, vol. 156, pp. 3113-3121, 2008.

[27] R. Granger, T. Kleinjung, J. Zumbragel, *Breaking 128-bit secure supersingular binary curves.* J. A. Garay and R. Gennaro (eds) Advances in Cryptology – CRYPTO 2014, part II, vol. 8617 of Lecture Notes in Computer Science, pp. 126-145, Springer, 2014.

[28] D. Hankerson, A. J. Menezes, S. Vanstone. *Guide to Elliptic Curve Cryptography.* Springer-Verlag, 2004.

[29] F. Hess, N. P. Smart, F. Vercauteren. *The eta pairing revisited.* IEEE Transactions on Information Theory, vol. 52, issue 10, pp. 4595–4602, 2006.

[30] L. Hitt *On the Minimal Embedding Field.* T. Takagi, T. Okamoto, E. Okamoto, T. Okamoto (eds) Pairing-Based Cryptography – Pairing 2007. Lecture Notes in Computer Science, vol. 4575, pp. 294–301, Springer, 2007.

[31] K. Ireland, M. Rosen. *A classical introduction to modern number theory.* Springer, 1982

[32] A. Joux, C. Pierrot. *The special number field sieve in $\mathbb{F}_{p^n}$ – application to pairing-friendly constructions.* Z. Cao and F. Zhang (eds) Pairing-Based Cryptography – Pairing 2013, vol. 8365 of Lecture Notes in Computer Science, pp. 54-61, Springer, 2014.

[33] T. Kim, R. Barbulescu. *Extended tower number field sieve: A new complexity for medium prime case.* Annual Cryptology Conference, LCNS 9814, pp. 543–571, Springer Berlin Heidelberg, 2016.

[34] T. Kim, J. Jeong. *Extended Tower Number Field Sieve with Application to Finite Fields of Arbitrary Composite Extension Degree.* S. Fehr (eds) Public-Key Cryptography – PKC 2017, Lecture Notes in Computer Science, vol. 10174. Springer, 2017.

[35] N. Koblitz. *Elliptic curve cryptosystems.* Mathematics of Computation, vol. 48, n. 177, pp. 203-209, 1987.

[36] N. Koblitz, A. Menezes. *Another look at generic groups.* Advances in Mathematics of Communications 1, pp. 13–28, 2007.

[37] H. Kredel, V. Weispfenning. *Computing dimension and independent sets for polynomial ideals.* Journal of Symbolic Computation, vol. 6, issues 2-3, pp. 231-247, 1988.

[38] D. Lubicz, T. Sirvent. *On generic groups and related bilinear problems.* Identity-Based Cryptography, M. Joye, G. Neven (eds.), IOS Press, vol. 2, pp. 169-187, Cryptology and Information Security Series, 2008.

[39] B. Lynn. *On the implementation of pairing-based cryptosystems.* URL: https://crypto.stanford.edu/pbc/thesis.html, 2007.

[40] D. Maimuţ, C. Murdica, D. Naccache, M. Tibouchi. *Fault Attacks on Projective-to-Affine Coordinates Conversion.* E. Prouff (eds) Constructive Side-Channel Analysis and Secure Design, COSADE 2013, Lecture Notes in Computer Science, vol. 7864, Springer, 2013.

[41] A. Menezes. *An introduction to pairing-based cryptography.* Contemporary Mathematics, vol. 477, pp. 47–65, American Mathematical Society, 2009.

[42] A. Menezes, T. Okamoto, S. Vanstone. *Reducing elliptic curve logarithms in a finite field.* IEEE Transactions on Information Theory, vol. IT-39, n. 5, pp. 1639-1646, 1993.

[43] V. S. Miller. *Use of elliptic curves in cryptography.* Advances in Cryptology, CRYPTO-1985 Proceedings, pp. 417-426, 1985.

[44] J. S. Milne. *Algebraic geometry.* Version 6.02.
URL: https://www.jmilne.org/math/CourseNotes/AG.pdf, 2017.

[45] R. Miranda. *Algebraic curves and Riemann surfaces.* Graduate Studies in Mathematics book 5, American Mathematical Society, 1995.

[46] N. El Mrabet, M. Joye. *Guide to pairing based cryptography.* Chapman & Hall/CRC, 2017.

[47] D. Naccache, N. Smart, J. Stern. *Projective coordinates leak.* Advances in Cryptology, Eurocrypt 2004, LNCS 3027, pp. 257-267, Springer-Verlag, 2004.

[48] P. Sarkar, S. Singh. *New complexity trade-offs for the (multiple) number field sieve algorithm in non-prime fields.* Cryptology ePrint Archive, Report 2015/944, 2015,
URL: http://eprint.iacr.org/2015/944.

[49] R. Schoof. *Nonsingular plane cubic curves defined over finite fields.* Journal of Combinatorial Theory, series A, vol. 46, issue 2, pp. 183-211, 1987.

[50] J. T. Schwartz. *Fast probabilistic algorithms for verification of polynomial identities.* Journal of the Association for Computing Machinery, vol. 27, n. 4, pp. 701-717, 1980.

[51] V. Shoup. *Lower Bounds for Discrete Logarithms and Related Problems.* Advances in Cryptology, W. Fumy (eds), EUROCRYPT 1997, Lecture Notes in Computer Science, vol. 1233, Springer, 1997.

[52] J. H. Silverman. *The arithmetic of elliptic curves.* Springer-Verlag, 1986.

[53] N.P. Smart, F. Vercauteren. *On computable isomorphisms in efficient asymmetric pairing-basedsystems.* Discrete Applied Mathematics, vol. 155, issue 4, pp. 538-547, 2007.

[54] T. Teruya, K. Saito, N. Kanayama, Y. Kawahara, T.Kobayashi, E. Okamoto *Constructing Symmetric Pairings over Supersingular Elliptic Curves with Embedding Degree Three.* Z. Cao, F. Zhang (eds) Pairing-Based Cryptography – Pairing 2013, Lecture Notes in Computer Science, vol. 8365. Springer, 2014.

[55] O. Uzunkol, M. S. Kiraz. *Still wrong use of pairings in cryptography.* Applied Mathematics and Computation, vol. 333, pp. 467-479, 2018.

[56] E. R. Verheul. *Evidence that XTR is more secure than supersingular elliptic curve cryptosystems.* Journal of Cryptology 17, n. 4, pp. 277-296, 2004

[57] L. C. Washington. *Elliptic curves. Number theory and cryptography.* Chapman & Hall/CRC, 2003.

[58] A. Wright. *Transcendence degree.*
URL: http://www-personal.umich.edu/ alexmw/TranscDeg.pdf

[59] X. Zhang, K. Wang. *Fast Symmetric Pairing Revisited.* Z. Cao and F. Zhang (eds) Pairing-Based Cryptography – Pairing 2013, Lecture Notes in Computer Science, vol. 8365, Springer, 2013.