0.1 Introduction to cryptography

The discipline devoted to the study of secrecy systems is called crittology. It is divided into two main branches which are cryptography, i.e. the design and implementation of secrecy systems, and criptoanalysis, which is aimed to breaking such systems in order to test them. In this thesis we will focus on the cryptographic ascpects of crittology.
Some fundamental definitions we need in this branch of study are the following:

Definition 0.1.1. We call plaintext a message that is to be altered into a secret form, called cyphertext.

Definition 0.1.2. A cypher is a method to alter such plaintext into cyphertext.

Definition 0.1.3. A cryptosystem consists of a finite set P of possible plaintexts, a set C of possible cypertext messages, a space K of possible keys and, for every $k \in K$, an ecription function E and a decription function D such that $D(E(x)) = x$.

Cryptography as a way to encode messages is not a recent discovery: we have proof of the existence of cyphers already in roman times. A famous one is Caesar's Cypher, which consisted in replacing every letter of the alphabet by the letter three spots further, in a cyclic way:

$$C = P + 3(mod 26)$$

This is just one example of a larger class of cyphers we calll monographic, which consist in replacing each letter of the alphabet with another trough some algorithm. The monographic encryptions can however be easily broken using the frequency of letters in a given language. For this reason modern cryptosystems are based on more complicated mathematical methods.

0.1.1 The Pohling-Hellman exponentiation cyphre

Let p be a prime number and let k be an encryption key that is an integer coprime to $p-1$. The Pohling-Hellman algorithm encription of a plaintext $P < p$ works as follows: We compute the cyphertext

$$C = P^k \mod p.$$

In order to decrypt such a message we need a decryption key d such that $dk \equiv 1 \mod p-1$. Then the original plaintext can be easily found as

$$P = C^d \mod p.$$

proof:
$C^d = (P^k)^d = P^{kd}$, but since p is prime and does not divide P, we have that $P^{p-1} \equiv 1 \mod p$ by Fermat's Little Theorem. On the other hand $dk \equiv 1 \mod p-1$, so $dk = q(p-1)+1$. Therefore $C^d = P^{kd} = P^{q(p-1)+1} \equiv P \mod p$, and we have succesfully decrypted the message.

The security of such a code consists in the fact that even if someone were to intercept an encrypted message $C = P^k \mod p$, finding k (and therefore d) would still be a difficoult probelm even if they knew the value of p. This is because the exponential encryption function is believed to be a one-way function, i.e. a function that can be computed in polynomial time, however is "hard to invert" in the average-case. Modern cryptography is based on the belief that there exist functions with such property. There is however no canonical proof to of this, as it would imply $P \neq NP$ which is a long-standing open problem.

Let's now take a closer look at the inverse of the exponentiation function used in the Pohling-Hellman exponentiation cyphre:

0.1.2 The Discrete Logarithm Problem

Definition 0.1.4. Let G be a cyclic group of cardinality n and α a generator of G, β an element of G. Then we say that x is a Discrete Logarithm of β to the base α in G if $0 \leq x \leq n-1$ and x is the solution to the equation $\alpha^x = \beta$.

Definition 0.1.5. The Discrete Logaritm problem consists in finding the Discrete Logarithm of an element $\beta \in G$ to the given base α.

The Discrete Logarithm Problem is not polynomial, it depends on the cardinality n of the group G and the naive alghorithm for it requires exponential running time, while faster algorithms- such as the "Baby-step giant-step" algorithm- reduce running time up to $\sqrt{n}$.
There is however a class of groups for which the Pohling-Hellman alghorithm provides a quicker solution: the cyclic groups of order $n = \Pi p_i^{e_i}$ such that p_i are small primes. In this particular instance the computational complexity of solving DLP is $\mathcal{O}(\sum e_i(logn + \sqrt{p_i}))$ group operations.
Because of this, in order to efficiently encrypt information using cyphres based on the DLP, it is required for the group order to have at least one large prime factor. In the case of the multiplicative group $G = \mathbb{Z}_p^\star$ it is convenient to consider p a prime such that $p = 2q + 1$ where q is a large prime. This will make sure that $p - 1$ has a large prime factor.
Finally, we also have to mention the Index-calculus algorithm, which is a probabilistic algorithm collecting relations among the Discrete Logarithms of small primes, computes them and then expresses the desired Discrete Logarithm with respect to the ones of small primes. This method is subexponential, however it does not work on all grups, for example it does not work on the group of points of an elyptic curve.

Going back to the Pohling-Hellman exponentiation cyphre we see that the DLP ensures that given a wise choice of a prime number p, breaking such cyphre requires exponential time. But a great problem still persist: in order to encrypt and decrypt our messege we need to recieve the encryption key, without it being intercepted by anyone trying to attack our system. This issue can however be resolved with public key cryptography.

0.1.3 Public key cryptography

In the 1970's new cryptosystems were developed in which encryption keys could be made public. Suppose Alice (A) announced a key K so that anyone, say Bob (B) could send her an encrypted message using such key. In order to assure such message were actually kept secret decryption must require some additional information which only Alice has. This idea was first proposed by Diffle and Hellman in 1976, however its first implementation was later developed by Rivest, Shamir and Adleman in 1977, and is still known as the RSA cryptosystem.

The Diffle-Hellman key- exchange protocol

The Diffle-Hellman key-exchange protocol allows two parties- say Alice and Bob- to exchange a secret key through a possibly not secure comunication link. This cryptosystem is based on the discrete logarithm problem, therefore its unbreakability
The algorithm works as follows:
Let p be a large prime number and let r be a primitive root modulo p, i.e. a generator of the multiplicative group $Z_p^\star$. Both Alice and Bob pick an integer between 2 and $p-2$, say k_A and k_B, then Alice sends Bob

$$x \equiv r^{k_A} \mod p$$

so then Bob can generate the common key

$$K = x_B^k = r^{k_A k_B} \mod p$$

Similarly, Bob sends Alice $y \equiv r^{k_B} \mod p$ so she can also generate the common key K.

The RSA cryptosystem

Let us first give two useful notions:

Definition 0.1.6. Euler's phi function $\phi(n)$ gives the number of positive integers smaller or equal to n which are coprime to n.

Theorem 0.1.7. ***Euler theorem:*** *If a and m are coprime, then $a^{\phi(m)} \equiv 1 \mod m$.*

Suppose that Alice wants to generate a public key so that Bob - or anyone else - can send her encrypted messages using the RSA cypher. To do so Alice chooses two large (different) prime numbers p and q and computes their product $pq = R$. Then she also selects a large integer e which is coprime to $\phi(R) = (p-1)(q-1)$, and makes the pair $K = (R, e)$ public.
Bob can now encrypt his plaintext P in the following way:

$$C \equiv P^e \mod R,$$

and send it to Alice.
Finally, Alice can decrypt the message using her secret decryption key d which is the

solution of the equation $de \equiv 1 \mod \phi(R)$, and is therefore easily computed by Alice who knows $\phi(R)$.
Using Euler's theorem it is easy to check that d decrypts the message:
$C^d \equiv P^{ed} \mod R$, but $ed \equiv 1 \mod \phi(R)$, and $P^{\phi(R)} \equiv 1 \mod R$; so $P^{ed} \mod R \equiv P \mod R$.

What guarantees the security of the RSA cyphre?
Security of the RSA is based on the difficulty of:

- factorising large numbers: from R finding p and q;
- the discrete logarithm problem: finding d from $K = (R, e)$;

The two problems above are actually not proven to be equivalent. The implication is

$$factorisation \Rightarrow DLP.$$

Reference

The ElGamalov cyphre

The El Gamalov cyphre, named after Taher ElGamal who designed it in 1985, is a public key cryptographic system. It can be divided into three main steps:

- Alice and Bob exchange a secret key K using the Diffle-Hellman key-exchange protocol.
- Alice sends Bob a message P by encrypting it:
$$C = KP \mod p$$
- Bob camputes
$$P = K^{-1}C \mod p$$

An advantege of this algorithm are the fact that for every comunication Alice and Bob can generate a different key K using the Diffle-Hellman algorithm, so the same plaintext can be coded differently every time.

The ElGamalov system is actually not that used as an encryption method but more as a way to tackle the following problem that all of the above cyphers share: the lack of authentication. Suppose Alice recieves a message that she believes is from Bob. She actually has no proof that the sender really is Bob, therefore the security of the comunication is at risk.

0.1.4 Digital signature

A digital signature is a way of proving the identity of the sender of a digital encrypted message. In general, a digital signature procedure can be divided into three steps:

- an algorithm to generate the key;

- a polynomial algorithm to generate the digital signature that applies the senders signature to a message;
- a polynomial algorithm that checks the digital signature and has two possible outputs: "valid" or "invalid".

.

0.1.5 The ElGamal signature scheme

Let p be a large prime number and r a generator of the multiplicative group $Z_p^\star$. Suppose Alice and Bob both have private keys k_A and k_B that they used to exchange the key $K = r^{k_A k_B}$ using the Diffle-Hellman protocol. To sign her message m, Alice can use the pair (t, s) such that

$$r^m = y_A^t t^s \mod p, \qquad (\star)$$

where $y_A = r^{k_A} \mod p$.
To verify the signature Bob computes both sides of $(\star)$ and checks that they are the same. This is a scheme is once again based on the unbreakability of the DLP.
But how does Alice find such a pair (t, s)? She chooses a random $0 < x < p - 1$ and then sets $t = r^x \mod p$.
Then

$$r^m = y_A^t r^{xs} = r^{k_A t} r^{xs}$$

Which allows her to compute s,

$$m = k_A t + xs \Rightarrow s = (m - k_A t)x^{-1}.$$

We observe that the digital signature is tied to the message we are sending. This is to prevent an impostor from copying the signature and applying it to different content.

0.1.6 Hash functions and DSA

Definition 0.1.8. A hash function is a function h that can send arbitrarily long data into a string of fixed length:

$$h : \{0,1\}^\star \longrightarrow \{0,1\}^n$$

In order for a hash function to be useful for cryptographic use the following properties are desirable:

- given an input x, the value of $h(x)$ must be easy to compute;
- its output should look like a random number and if two messages differ by even only one entry the relative function values should appear two uncorrelated random numbers;
- it is a one-way function: given a string z it is infeasible to find x such that $h(x) = z$;
- given a plaintext P it is infeasible to find another P_1 such that $h(P) = h(P_1)$;

- it is deterministic: the same input always yields the same output.

Now, let h be a hash function, which does not need to be kept secret. Again Alice wants to prove her identity to Bob by applying a singnature. However this time, to add another layer of security, she will sign the hash funchion of her message $h(m)$.

The digital signature (t, s) can be applied in the following way:

- pick two prime numbers p, q such that $p = 1 \mod q$. When making such choices we want the length L (in bits) of q to be less or equal to the length of the output of the hash function.
- pick a genetator g of the subgroup of order q of $\mathbb{Z}_p^\star$. A way to generate g that works most of the times is to pick a random $1 < r < p-1$ and set $g = r^{(p-1)/q} \mod p$(in the case that we get $g = 1$ we repeat the step by selecting a different r). The triplet (p, q, g) is public.
- As in Diffle-Hellman, Alice has a private key $0 < k_A < q$ and she computes $y_A = g^{k_A} \mod p$.
- Alice than chooses a random $0 < x < q-1$ and computes $t = (g^x \mod p) \mod q$
- finally she finds s by solving $s = (h(m) + k_A t)x^{-1}$. The pair (t, s) is the wanted digital signature.

In order to verify the signature Bob then needs check the correctness of the equation

$$t \equiv g^{s^{-1}h(m) \mod q}(y_A)^{s^{-1}t \mod q} \mod p \mod q.$$

which by ommitting the $\mod q$ in the exponents becomes

$$t \equiv g^{s^{-1}(h(m)+k_A t)} \mod p \mod q.$$

Bob has all the information he needs to make this computation.

Observation 0.1.9. In the equation above we have $\mod q$ in the exponents which we have then ommited. This is because of thw way we have chosen $g : g = r^{\frac{p-1}{q}}$. Indeed, suppose $x \neq y$ but $x \equiv y \mod q$. Then $x = kq + y$ and

$$g^x = g^{kq} g^y \equiv g^y \mod p$$

because $g^q = r^{\frac{p-1}{q}q} \equiv 1 \mod p$ by Fermat's little theorem.

A more recent approach to cryptography involves elliptic and hyperelliptic curves. The idea is to substitute the classic groups $\mathbb{Z}_p$ with a different kind, related to such curves. A good reason for such change is that elliptic curve cryptography requires smaller keys to provide equivalent security, and is therefore used today in many online comunications. Hyperelliptic curves are on the other hand not wildely used today, even though they require even smaller keys than ECC, because the implemenation of the arithmetic of such systems is not very efficient.
In the next chapters we introduce some theoretic geometric notions regarding these two classes of curves which will give us some insight into how we can associate them with groups and what is their role in modern cryptography.

0.2 Elliptic curves

Definition 0.2.1. An elliptic curve E over a filed K is a curve that is projectively equivalent to a projective smooth cubic in $\mathbb{P}^2_K$ which consists of a point at infinity $\infty = [0:1:0]$ and affine points (x, y) satisfying what we call the generalised Weierstrass equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

This equation can be further reduced into different formulas which depend on the characteristic of the filed K. In particualr we distinguish three cases:

- if $char(K) = 2$ the formula remains as above.
- if $char(K) = 3$ the formula can be reduced to:

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

proof:
Let's apply the affine trasformation

$$(x, y) \to (x, y - \frac{a_1x + a_3}{2}).$$

Then the left side of the generalised Weierstrass equation becomes:

$$\left(y - \frac{a_1x + a_3}{2}\right)^2 + a_1x\left(y - \frac{a_1x + a_3}{2}\right) + a_3\left(y - \frac{a_1x + a_3}{2}\right) =$$

$$= y^2 - y(a_1x + a_3) + \frac{a_1^2x^2 + 2a_1a_3x + a_3^2}{4} + a_1xy - \frac{a_1^2x^2}{2} - \frac{a_1a_3x}{2} + a_3y - \frac{a_1a_3x}{2} - \frac{a_3^2}{2}$$

$$= y^2 - \frac{a_1^2x^2}{4} - \frac{a_3^2}{4} - \frac{a_1a_3x}{2}$$

So the whole equation is now

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

which we can simplify as

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

- if $char(K) \neq 2, 3$ the elliptic curve E can be written as

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

We call this equation the Weierstrass form of the elliptic curve.

proof:

First we reduce the cubic to the equation $y^2 = x^3 + a'x + b'x + c'$ as we did for the field of characteristic 3. Then it is enough to apply the transformation

$$(x, y) \to (x - \frac{1}{3}a', y)$$

and the right side of the equation becomes

$$x^3 + (\frac{1}{3}(a')^2 + b')x + (c' - \frac{1}{27}(a')^3)$$

which, after renaming the constants, is our formula.

Observation 0.2.2. A natural question is whether every cubic of the form $y^2 = x^3 + Ax + B$ is an elliptic curve. The answer is no, as we also have to satisfy the smoothnes hypothesis, which can be expressed in the form of $\Delta = 4A^2 + 27B^2 \neq 0$.

Let's prove this observation:
A curve is smooth when there is no point in which all the partial derivatives are null.
We first look at the affine part of the curve, and we compute the partial deirvative by y and obtain $2y$ which of course is zero iff $y = 0$. On the other hand the partial derivative by x is zero iff x is a root of $x^3 + Ax + B$ at least twice. This is true if and only if $\Delta = 4A^2 + 27B^2 = 0$.* So this part of the curve does not have a singular point only in the case that $\Delta \neq 0$.
We now need to prove that also the point $\infty = [0 : 1 : 0]$ is not singular. We homogenise the equation and get

* Indeed, Δ is the discriminant of such a polynomial, that is $\Delta = \mathrm{Res}(p(x), p'(x))$ is the resultant between $p(x)$ and its derivative.

$$F(x_0, x_1, x_2) = x_0^3 + Ax_0x_2^2 + Bx_2^3 - x_1^2x_2$$

$$\frac{\partial F}{\partial x_0}(\infty) = 0$$

$$\frac{\partial F}{\partial x_1}(\infty) = 0$$

$$\frac{\partial F}{\partial x_2}(\infty) = -1$$

So the smoothness condition is satisfied.

Observation 0.2.3. All cubics in Weierstrass form have a flex in $\infty = [0 : 1 : 0]$.

Corollary 0.2.4. *Every elliptic curve E over an algebraically closed field K with $char(K) \neq 2, 3$ is projectively equivalent to an affine cubic*

$$y^2 = x(x - 1)(x - c)$$

for some $c \in \mathbb{C} - \{0, 1\}$.
We call this the Legendre form of the elliptic curve.

Another way to look at elliptic curves which is often found in literature is the following:

Definition 0.2.5. An elliptic curve is an algebraic projective smooth curve of genus one with a specified point ∞.

A very useful theorem when working with genuses is the following:

Theorem 0.2.6. *Given a non singular curve $C \in \mathbb{P}^2$ of degree d we can express its genus as*

$$g = \frac{1}{2}(d-1)(d-2).$$

An immediate consequence is that smooth curves of genus one must be smooth cubics in $\mathbb{P}^2$.

We will mostly work with elliptic curves over finite fields, the points of which form an abelian group. It is however interesting to note the case $K = \mathbb{C}$, where every elliptic curve is isomorphic to a torus. Indeed in $\mathbb{C}$ a torus can be constructed as $T = \mathbb{C}/L$ from a lattice $L = \{z_1 w_1 + z_2 w_2, z_1, z_2 \in \mathbb{Z}\}$, where w_1, w_2 are two linearly indipendent complex numbers. The canonical sum of complex numbers induces a group structure on T and there is group isomorphism between each such torus to an elliptic curve E.

Observation 0.2.7. It is easy to see that

$$P = (x_1, y_1) \in E \Rightarrow P' = (x_1, -y_1) \in E.$$

0.2.1 The group law

Theorem 0.2.8. *Let E be an elliptic curve in Weierstrass form over an algebraically closed field K. The set of points of E can be endowed with the structure of a group. First consider an operation*

$$* : E \times E \to E$$

$$(P, Q) \to P * Q$$

where $P * Q = R$, the unique third point of intersection between E and the line through P and Q.

In the case that $P = Q$ such line is the tangent to the curve.

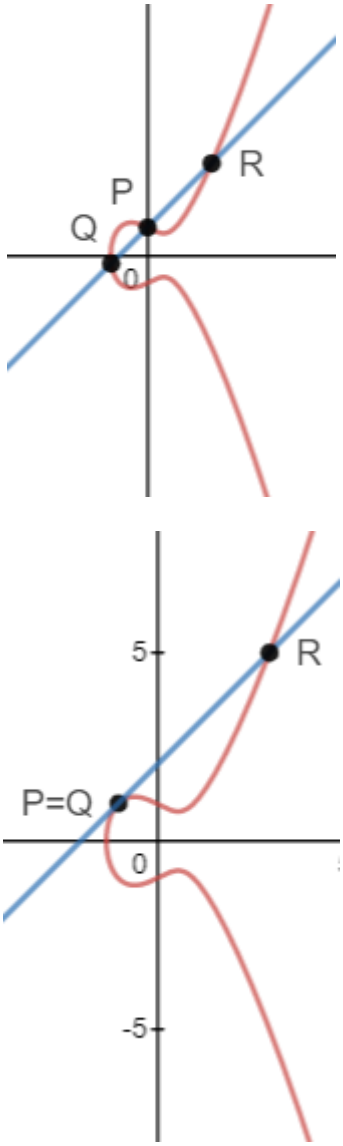
We can then define

$$+ : E \times E \to E$$

$$(P, Q) \to P + Q = P * Q * \infty$$

The elliptic curve E, together with the operation $+$ forms an additive group, with neutral element $\infty = [0 : 1 : 0]$.

proof:

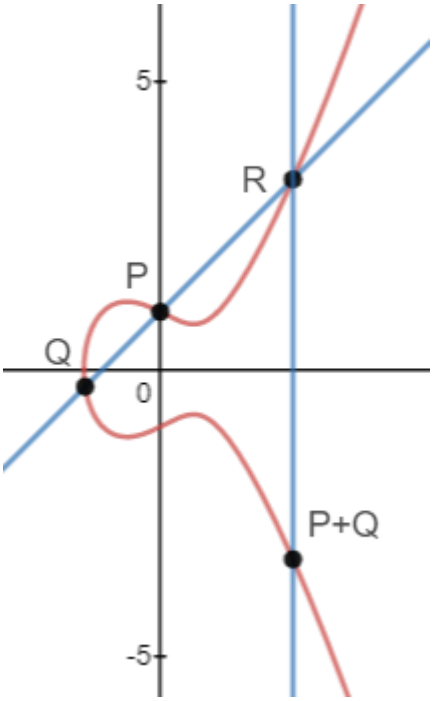


- The existence and unicity of $P * Q$ is given by Bezut's theorem, which tells us that the intersection between a line and a curve of degree three consists of three points (counted with their multeplicity, so it is possible to have just one point with multeplicity three). Therefore, the existence and well-definition of $P + Q$ is guaranteed.

- It is also clear that $*$ is a commutative operation, therefore $+$ is.

- The neutral element of the group is ∞.
  Indeed, ∞ is the only flex of the curve, so the only point with multeplicity three, which implies $\infty \star \infty = \infty$, and therefore $\infty + \infty = \infty$.
  On the other hand let $P \in E$ and $P * \infty = R$. Then $P + \infty = R * \infty = P$.

- It is easy to see that if $P = (x_1, y_1) \in E$, then $P' = (x_1, -y_1) \in E$ and $P + P' = \infty$, so each element has an opposite.



- The sum + is associative. We ommit this proof, which can be found in (insert reference).

0.2.2 Equations for the sum of points on an elliptic curve

Proposition 0.2.9. *Let K be a field of $char(K) \neq 2, 3,$, and let $P = (x_1, y_1), Q = (x_2, y_2) \in E$ elliptic curve. The coordinates of the point $P + Q = (x_3, y_3)$ are:*

- *if $P \neq Q$:*

$$x_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - x_1 - x_2$$

and

$$y_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)(x_1 - x_3) - y_1$$

- *if $P = Q$:*

$$x_3 = \left(\frac{3x_1^2 + a}{2y_1}\right)^2 - 2x_1$$

and

$$y_3 = \left(\frac{3x_1^2 + a}{2y_1}\right)(x_1 - x_3) - y_1.$$

Proposition 0.2.10. *If $char(K) = 3$, then*

- *if $P \neq Q$:*

$$x_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - a - x_1 - x_2$$

- *if* $P = Q$*:*

$$y_3 = \left(\frac{2ax_1 + b}{2y_1}\right)(x_1 - x_3) - y_1$$

If $char(K) = 2$*, then the formulas are a little more complicated and we need to distinguish four cases*

- *if* $a_1 \neq 0$ *and* $P \neq Q$

$$x_3 = \left(\frac{y_1 + y_2}{x_1 + x_2}\right)^2 + \frac{y_1 + y_2}{x_1 + x_2} + x_1 + x_2$$

$$y_3 = \left(\frac{y_1 + y_2}{x_1 + x_2}\right)(x_1 + x_3) + x_3 + y_1$$

- *if* $a_1 \neq 0$ *and* $P = Q$

$$x_3 = x_1^2 + \frac{a_6}{x_1^2}$$

$$y_3 = x_1^2 + (x_1 + \frac{y_1}{x_1} + 1)x_3$$

- *if* $a_1 = 0$ *and* $P \neq Q$

$$x_3 = \left(\frac{y_1 + y_2}{x_1 + x_2}\right)^2 + x_1 + x_2$$

$$y_3 = \left(\frac{y_1 + y_2}{x_1 + x_2}\right)(x_1 + x_3) + y_1 + a_3$$

- *if* $a_1 = 0$ *and* $P = Q$

$$x_3 = \frac{x_1^4 + a_2^2}{a_3^2}$$

$$y_3 = \left(\frac{x_1^2 + a_2}{a_3}\right)(x_1 + x_3) + y_1 + a_3$$

For the computations that yield to these results we refer to referencexy

Observation 0.2.11. If the coordinates of P and Q are elements of a field K, then also $P + Q$ has coordinates in K, so the hypothesis of having an algebraically closed field is actually not necessary to form a group with the points of an elliptic curve.

0.2.3 Divisors

Definition 0.2.12. Let C be a curve. A divisor D is a linear combination

$$D = \sum_{P \in C} a_p \cdot P$$

with only a finite number of $a_P \neq 0$.

It is important to note that this is a purely formal sum, that we do not actually compute.
On the other hand we can also consider the actual sum of points, which is given by the function:

$$sum : Div(C) \to C$$
$$D = \sum a_p \cdot P \to \sum a_p P.$$

Definition 0.2.13. We define a sum of two divisors $D = \sum a_p \cdot P$ and $E = \sum b_P \cdot P$ as

$$D + E = \sum (a_P + b_P) \cdot P.$$

The divisors on a curve C together with the sum $+$ form an abelian group $(Div(C), +)$ with neutral element $0 = \sum 0 \cdot P$.

Definition 0.2.14. We define the degree of a divisor $D = \sum a_p \cdot P$ as

$$deg(D) = \sum a_p;$$

and we define its support as the set of all points P such that $a_P \neq 0$.

Observation 0.2.15. The class of degree zero divisors of a curve C forms a subgroup $Div^0(C) \subset Div(C)$.

We now want to define a particular class of divisors called principal divisors, for which we need the notion of valuation that we briefly introduce here.
Let E be an elliptic curve, embedded into the projective plane $\mathbb{P}^2_K$, with K algebraically closed. Then, as an algebraic variety, it is associated to a homogeneous ideal $I_H(E)$. We can then define

$$S(E) = K[x_0, x_1, x_2]/I_H(E)$$

and since elliptic curves are irreducible, we have that $I_H(E)$ is a prime ideal and $S(E)$ is a domain. We can therefore consider the quotient field

$$Q(S(E)) = \{\frac{\overline{f}}{\overline{g}} \ for \ \overline{f}, \overline{g} \in S(E) \ and \ \overline{g} \notin I_H(E)\}.$$

This is however not really well defined in the projective space, as we also need to add the condition that nominator and denominator are polynomials of the same degree. With this adjustment we can then obtain a well defined field, called the field of rational functions:

$$K(E) = \{\frac{\overline{f}}{\overline{g}} \ for \ \overline{f}, \overline{g} \in Q(S(E)) \ and \ deg(\overline{f}) = deg(\overline{g})\}.$$

Finally, we can also define the following structure:

$$\mathcal{O}_{E,P} = \{h \in K(E) | \exists \overline{f}, \overline{g} \in Q(S(E)^{(d)}) \ such \ that \ h = \frac{\overline{f}}{\overline{g}} \ and \ \overline{g}(P) \neq 0\}$$

This is a local ring, with maximal ideal $\mathcal{M}_P = \{h = \frac{\overline{f}}{\overline{g}} \in \mathcal{O}_{E,P} | \overline{f}(P) = 0\}$.

Definition 0.2.16. Let R be a local ring that is a domain and let its maximal ideal $\mathcal{M} =< t >$ for some $t \in R$. Then R is a discrete valuation ring (briefly DVR) if every element of the ring can be written as ut^n for some invertible element u and some integer $n \leq 0$. We call the element t uniformizing element or uniformiser.

Proposition 0.2.17. *$\mathcal{O}_{E,P}$ is a DVR.*

Proof. In order to prove this proposition we need the following lemma and corollary, the proof of which can be founf in referencexy

Lemma 0.2.18. *(Nakayama)*
Let R be a local ring with maximal ideal $\mathcal{M}$. Then if M is a finitely generated R-module and $\mathcal{M}M = M$, then $M = 0$.

Corollary 0.2.19. *Let R be a local ring with maximal ideal $\mathcal{M}$ and M a finitely generated R-module. Consider the $K = R\backslash\mathcal{M}$ vector space:*

$$< \overline{m_1}, \dots \overline{m_r} >= M/\mathcal{M}M.$$

Then $M =< m_1, \dots, m_r >$.

Let us now use the above results to prove that $\mathcal{O}_{E,P}$ is a DVR.
First, we need to show that the maximal ideal $\mathcal{M}_P$ is generated by one element t.
Let's consider the tangent space to the curve at the point P.

$$T_pE = \left(\mathcal{M}_P/\mathcal{M}_P^2\right)^* = Hom\left(\mathcal{M}_P/\mathcal{M}_P^2, K\right)$$

We know that if P is a nonsingular point the dimension of the tangent space at the point is the dimension of the projective variety. In our case the elliptic curve is smooth, so every point is nonsingular, and we get

$$dim(\left(\mathcal{M}_P/\mathcal{M}_P^2\right)) = dim(\left(\mathcal{M}_P/\mathcal{M}_P^2\right)^*) = dim(T_PE) = dim(E) = 1.$$

Therefore $(\mathcal{M}_P/\mathcal{M}_P^2) =< \bar{t} >$ as a vector space. But $\mathcal{M}_P$ is a finitely generated $\mathcal{O}_{E,P}$-module ($\mathcal{O}_{E,P}$ is noetherian, so every ideal of this ring is finitely generated). So by the corollary above we obtain $\mathcal{M}_P =< t >$.
Secondly, we show that every element $a \in \mathcal{O}_{E,P}$ can be written as $a = ut^n$ for some u invertible element.
We define

$$M = \cap\mathcal{M}^n.$$

Again, M is a finitely generated ideal because $\mathcal{O}_{E,P}$ is noetherian. However it is easy to see that $\mathcal{M}M = M$, so by Nakayama's lemma $M = 0$. Now, if a is inveritble, we simply have $a = at^0$, while if a is not invertible, $a \in M$ and more specifically, $a \in \mathcal{M}^n\backslash\mathcal{M}^{n+1} =< t^n > \setminus < t^{n+1} >$ for some n. So $a = ut^n$ for some $u \in \mathcal{O}_{E,P}$ invertible.

□

We can now canonically define a function on $\mathcal{O}_{E,P}$ called valuation.

Definition 0.2.20. A valuation on the local ring $\mathcal{O}_{E,P}$ is a function

$$v_P : \mathcal{O}_{E,P} \backslash \{0\} \to \mathbb{Z}_+$$

$$f = ut^n \to n$$

It is easy to see that the following hold:

- $v_P(fg) = v_P(f) + v_P(g)$;
- $v_P(f+g) \geq min(v_P(f), v_P(g))$;
- $f \notin \mathcal{M}$ iff $v_P(f) = 0$.

Observation 0.2.21. From the third property it is clear that $n = v_P(f) > 0$ if and only if f is not invertible which in the local ring $\mathcal{O}_{E,P}$ implies $f(P) = 0$. In particular, n is the multeplicity of the zero P.

We can then extend the valuation to the whole field of rational functions. If $h \in K(C)$ is a rational function which can be represented around P as $h = \frac{f}{g}$, then

$$v_P : K(E) \to \mathbb{Z}$$

$$v_P(h) = v_P\left(\frac{f}{g}\right) = v_P(f) - v_P(g).$$

We therefore have $v_P(h) = a_P > 0$ iff P is a zero of h of multeplicity a_P and $v_P(h) = b_P < 0$ iff P is a pole of multeplicity b_P.

Let now h be a rational function over a closed field K. We can associate a divisor to h as

$$(h) = \sum_{P \in C} v_P(h) \cdot P$$

where $v_P(h)$ is the valuation of h in P. In the case that the field we are working in is not algebraically closed, we can still generate a divisor in this way by considering the field of rational functions $K(C)$ over its algebraic closure.

Observation 0.2.22. Sometimes we will denote the divisor of a rational function h as $div(h)$ as it will facilitate reading.

Example 0.2.23. *Let's consider the elliptic curve $E : y^2 = x^3 - x$ and the rational function $f = \frac{x}{y}$. We want to compute $v_P(f)$ for the point $P = (0,0)$.*
We consider $\mathcal{O}_{E,P}$ and its maximal ideal $\mathcal{M}_P$ which contains all non invertible elements of the local ring. We need to compute the uniformiser t, i.e. an element of the ring such that $< t >= \mathcal{M}_P$ and $\forall a \in \mathcal{O}_{E,P}, a = t^n u$ with $u \notin \mathcal{M}_P$.
Since $P = (0,0)$, $\mathcal{M}_P =< x, y >$. We are however working on the elliptic curve $y^2 = x(x^2-1)$, where $x = y^2 \cdot \frac{1}{x^2-1}$. So $\mathcal{M}_P =< y >$ and y is uniformising element.
We can now easily compute $v_P(f)$:

$$\frac{x}{y} = y \cdot \frac{1}{x^2-1},$$

so $v_P(f) = 1$.

Observation 0.2.24. In general if $P = (\alpha, 0)$ then y is uniformising element, wherease if $P = (\alpha, \beta)$ with $\beta \neq 0$ then $x - \alpha$ is uniformiser.

Definition 0.2.25. All divisors D for which there exists a rational function h such that $(h) = D$ are called principal divisors.

Proposition 0.2.26. *The set of principal dicisors of a curve C forms a subgroup $P(C)$ of $Div(C)$. In particular, $P(C) \subset Div^0(C)$ as all principal divisors have degree zero.*

The first part of the proposition can be easily proved, as we can construct a group homomorphism:

$$(K(C)\backslash 0, \cdot) \to (P(C), +)$$
$$f \cdot g \to (f \cdot g) = \sum (v_P(f) + v_P(g)) \cdot P.$$

The second part, a proof that all principal divisors have degree zero we give the reference of [6], chapter 2, corollary 6.10.

Definition 0.2.27. We define Picard group $Pic(C)$ of a curve C the quotient group

$$Pic(C) = \frac{Div(C)}{P(C)}.$$

Proposition 0.2.28. *Let E be an elliptic curve and $Pic^0(E) = \frac{Div^0(E)}{P(E)}$. Then there exists a bijective map, called the Abel Jacobi map,*

$$\sigma : Pic^0(E) \to E$$
$$[D] \to P$$

where P is the unique point such that $[D] = [P - \infty]$, i.e. $D - P - \infty$ is principal. Furthermore, if E is given by the Weierstrass equation, the geometric group law we saw in the previous chapter and the group law induced on $Pic^0(E)$ as a quotient group are the same, so σ is also a group isomorphism.

Proof. We refer to [3].

□

Corollary 0.2.29. *Let E be an elliptic curve and $D \in Div^0(E)$. Then D is principal iff $sum(D) = \infty$.*

Proof. Let $D = \sum a_P \cdot P$ be principal. Then in $Pic^0(E)$ we have

$$[D] = [0] \Rightarrow \sigma([D]) = \sigma([0]) = \infty.$$

But since D is a divisor of degree zero we can also rewrite it as $D = \sum a_P \cdot (P - \infty)$. By applying again the function σ which is also a group homomorphism we obtain

$$\sigma([D]) = \sigma([\sum a_P \cdot (P - \infty)] = \sum a_p \sigma([P - \infty]) = \sum a_p P = sum(D).$$

Therefore $sum(D) = \infty$.
In order to proove the converse we just need to reverse the implication arrows.

□

Example 0.2.30. *If $P \neq \infty$, then $D = P - \infty$ is not a principal divisor.*

0.3 Elliptic curves over a finite field

In order to use elliptic curve groups in cryptography, we need to consider them over a finite field as this makes computations feasible. This means that given a curve in Weierstrass form

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

we take $A, B \in \mathbb{F}_q$, where $\mathbb{F}_q$ is a finite field of cardinality q.

Example 0.3.1. *Consider the curve in Weierstrass form*

$$y^2 = x^3 - 2x + 2$$

Who is $E(\mathbb{F}_5)$?
The choices for x are $0, 1, 2, 3, 4$. We now just need to check which of the $f(x)$ are squares in this field. So let's first observe that in $\mathbb{F}_5$ all possible squares are:

$$0^2 \equiv 0,\ 1^2 \equiv 1,\ 2^2 \equiv 4,\ 3^2 \equiv 4,\ 4^2 \equiv 1.$$

Now we compute:
$f(0) \equiv 2$
$f(1) \equiv 1$
$f(2) \equiv 1$
$f(3) \equiv 3$
$f(4) \equiv 3$
and we get that the points of the curve are $(1, 1),\ (1, 4)\ (2, 1,)\ (2, 4),\ \infty$, i.e $E(\mathbb{F}_5) = \mathbb{Z}_5$.

In the case that the cardinality of the group that we obtain is not a prime we could have more choices. For example if $\#E(\mathbb{F}_q) = 9$ we could have either $\mathbb{Z}_9$ or $\mathbb{Z}_3 \times \mathbb{Z}_3$. We then look at the order of some elements to understand which group is the right one.

Let's now recall some properties of finite fields that will be useful in future computations:

- Given a finite field $\mathbb{F}_q$ we have that $q = p^n$ for some prime p and integer n. The characteristic of such field is p;
- All finite fields of order q are isomorphic;
- given a finite field $\mathbb{F}_q$, its' algebraic closure is a countable union of finite fields $\overline{\mathbb{F}}_q = \cup \mathbb{F}_{q^n}$;
- $\mathbb{F}_q = \{roots\ of\ x^q - x\}$
- When $q = p$ the sum and multiplication are the classic ones, modulo p;
- When $q = p^n$ for $n > 1$ we do not represent the field elements with numbers any more as the sum and product operations are not the modular ones. We can however represent the elements as polynomials of degree smaller then n. We then sum them as polynomials, and reduce the coefficients modulo p. The product is constructed by multilpying them as polynomials, and then taking the remander of a division by an irreducible polynomial of degree n.

Example 0.3.2. *Elements of* $\mathbb{F}_9$*:*

$$0, x, 2x, 1, x+1, 2x+1, 2, x+2, 2x+2.$$

sum of two elements:

$$(2x+1)+2x = 4x+1 = x+1$$

product of two elements:

$$(2x+1)(x+2) = 2x^2+5x+2$$

As $2x^2+5x+2$ *is not one of the elements of our field we need to divide this polynomial by an irreducible one in* $Z_3[x]$*, say* x^2+1*. We then get* $2x$*.*

0.3.1 Torsion points

Suppose first the field K of charcteristic not 2, and E an elliptic curve over it. We will consider the curve in the Legendre form, with a point ∞ which is the neutral element of the ellipric curve group.

Definition 0.3.3. We define

$$E[n] = \{P \in E(\overline{\mathrm{K}}) \text{ such that } nP = \infty\}$$

the (sub)group of n- torsion points of the curve.

Example 0.3.4.

$$E[2] \simeq Z_2 \oplus Z_2$$

indeed, E *can be put in the form* $y^2 = x(x-1)(x-c)$ *and a point* P *is of torsion with* $n = 2$ *if and only if* $P + P = \infty$*, i.e the tangent line at* P *is vertical. In an elliptic curve this means* $y = 0$*, so* $E[2] = \{\infty, (0,0), (1,0), (c,0)\}$*.*

Theorem 0.3.5. *If the characteristic of* K *does not divide* n *(or is* 0*),then*

$$E[n] \simeq Z_n \oplus Z_n$$

If the characteristic p *divides* n*, we can write* $n = p^r m$ *with* p *not dividing* m*. Then*

$$E[n] \simeq Z_m \oplus Z_m$$

or

$$E[n] \simeq Z_n \oplus Z_m$$

(insert proof)

In order to study the torsion subgroups, it is useful to introduce the following maps:

Definition 0.3.6. Let $y = x^3 + Ax + B$ be an elliptic curve in Weierstrass form. Then we can recursively define the following maps, called division polynomials

$$\psi_n \in \mathbb{Z}[x, y, A, b] :$$

- $\psi_0 = 0$
- $\psi_1 = 1$
- $\psi_2 = 2y$
- $\psi_3 = 3x^4 + 6Ax^2 + 12Bx - A^2$
- $\psi_4 = 4y(x^6 + 5Ax^4 + 20Bx^3 - 5A^2x^2 - 4ABx - 8B^2 - A^3)$
- $\psi_{2n} = (2y)^{-1}(\psi_n)(\psi_{n+2}\psi_{n-1}^2 - \psi_{n-2}\psi_{n+1}^2)$
- $\psi_{2n+1} = \psi_{n+2}\psi_n^3 - \psi_{n-1}\psi_{n+1}^3$

We observe that the division polynomial ψ_n is a function of x when n is odd.

Theorem 0.3.7. *Consider the polynomials:*

$$\phi_n = x\psi_n^2 - \psi_{n+1}\psi_{n-1}$$

and

$$\omega_n = (4y)^{-1}(\psi_{n+2}\psi_{n-1}^2 - \psi_{n-2}\psi_{n+1}^2).$$

Then the endomorphism of an elliptic curve $E(\mathbb{F}_q)$ (with q odd) that given a point $P = (x, y) \in E$ returns nP can be expressed as

$$(x, y) \to (\frac{\phi_n(x)}{\psi_n^2(x)}, \frac{\omega_n(x, y)}{\psi_n(x, y)^3}).$$

proof: (insert reference (Ellicptic curves number theory)).

Observation 0.3.8. Given $P = (x, y) \in E(\overline{\mathbb{F}}_q)$ and n odd, then $P \in E[n]$ iff $\psi_n(x) = 0$.

Lemma 0.3.9. *ψ_n^2 is always a polynomial only in x and*

$$\psi_n^2 = n^2 x^{n^2-1} + \text{ lower degree terms.}$$

(insert proof)

Proposition 0.3.10. *Let n be an odd prime. Then*

$$\{x \text{ coordinates of points of } E[n]\} = \{\text{roots of } \psi_n\}$$

Proof. Since n is prime $E[n] \simeq Z_n \oplus Z_n$, so $\#E[n] = n^2$. This means that $\#E[n] - \infty = n^2 - 1$, so as $n \neq 2$, there are $\frac{n^2-1}{2}$ distinct first coordinates in $E[n]$. But, by the previous lemma, ψ_n is a polynomial in x (n is odd) of degree $\frac{n^2-1}{2}$. and all of its roots are in $E[n]$, so we get the equality.

□

0.3.2 Order of the group and order of a point

The concepts of order (cardinality) of a group and order of one of its points are quite correlated. Indeed, let P be a point on an elliptic curve over a finite field $E(\mathbb{F}_q)$, and let n be its order (the smallest integer such that $nP = \infty$). We know from Lagerange's theorem that given an element of a group, its order divides the cardinality of the group, so $n|\ \#E(\mathbb{F}_q)$.
Renè Schoof first proposd in 1985 a way to calculate such cardinality in polynomial time, the Schoof algorithm, which is based on Hesse's theorem and on the Chinese Remainder theorem. Before analysing the algorithm let's first look at some results that will prove useful for its understanding.

Theorem 0.3.11. *Hesse theorem*

$$q + 1 - 2\sqrt{q} \leq \#E(\mathbb{F}_q) \leq 2\sqrt{q} + q + 1$$

(insert proof of Hesse theorem)

Observation 0.3.12. In the case that we are not interested in the exact cardinality of $\#E(\mathbb{F}_q)$ but just its approximation, Hesse's theorem tells us that it is not very far from q.

Corollary 0.3.13. *The probability that an $x \in \mathbb{F}_q$ is the absciss of a point $P \in E(\mathbb{F}_q)$ is close to $\frac{1}{2}$ for a large q.*

Proof. The number of such x is approximately $\frac{\#E(\mathbb{F}_q)}{2}$ since for almost every (x, y) on the curve, also $(x, -y)$ is. But then by Hesse's theorem

$$\frac{1}{2} + \frac{1}{2q} - \frac{1}{\sqrt{q}} \leq \frac{\#E(\mathbb{F}_q)}{2q} \leq \frac{1}{2} + \frac{1}{2q} + \frac{1}{\sqrt{q}}$$

Where $\frac{\#E(\mathbb{F}_q)}{2q}$ is the probability that a random $x \in \mathbb{F}_q$ is the first coordinate of a point of the curve.

□

This is very useful for cryptographic purposes, as it allowes us to easily pick a random point on an elliptic curve.

Definition 0.3.14. The Frobenius endomorphism on a finite field $\mathbb{F}_q$ is a map

$$\phi_q : \overline{\mathbb{F}}_q \to \overline{\mathbb{F}}_q$$

$$x \to x^q$$

In particular, if $E(\mathbb{F}_q)$ is an elliptic curve, ϕ_q acts on the coordinates of a point in the following way:

$$\phi_q(x, y) = (x^q, y^q)$$

and

$$\phi_q(\infty) = \infty.$$

Definition 0.3.15. We call the trace of a Frobenius endomorphism ϕ_q

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

It is easy to observe that by Hesse's theorem $|a_q| \leq 2\sqrt{q}$.

Proposition 0.3.16.

$$\phi_q^2 - a_q\phi_q + q = 0$$

(insert proof)

0.3.3 Schoof's algorithm

Let $E(\mathbb{F}_q)$ be our elliptic curve over a finite field $\mathbb{F}_q$ of $char \neq 2, 3$ with $q = p^n$. Let the following be its Weierstrass equation

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

The idea behind Schoofer's algorithm is quite simple: to count the points on the elliptic curve we first calculate the number of points modulo $l_1, \ldots, l_k$ and then use the chinese remainder theorem to get $\#E(\mathbb{F}_q) \mod l_1 \ldots l_k$. Finally we can get rid of the modulo by using the range given by Hesse's theorem.

Let S be a set of primes such that its product is larger then $4\sqrt{q}$, assume that p is not one of them and let a_q be the trace of the Frobenius endomorphism. We calculate $a_q \mod l_i$:

Proposition 0.3.17. $a_q \equiv 0 \mod 2$ *iff* $x^3 + Ax + B$ *has a root in* $\mathbb{F}_q$.

Proof. "⇒"
If $x^3 + Ax + B$ has a root $\tilde{x} \in \mathbb{F}_q$, the point $(\tilde{x}, 0)$ is on the curve, and since the second coordinate is 0 it has order two. By Lagrange's theorem we then have that $\#E(\mathbb{F}_q) = q + 1 - a_q$ is even, i.e $q + 1 - a_q \equiv 0 \mod 2$. But since we supposed q odd, this implies $a_q \equiv 0 \mod 2$.
"⇐"
If $a_q \equiv 0 \mod 2$, then the group order is $\equiv 0 \mod 2$. But, by Cauchy's theorem, for every prime dividing the order of the group there exists an element of that order. So in our case we have that $\exists(\tilde{x}, \tilde{y})$ of order two, which in an elliptic curve group implies $\tilde{y} = 0$, i.e. $\tilde{x}$ is a root of the equation.

□

But when does the equation above have a root? Whenever $gcd(x^3+Ax+B, x^q-x) \neq 1$.

From this proposition we see that the case $l_i = 2$ is quite simple.

If $l_i \neq 2$, the computations are more complex:
Let us now use a instead of a_q, l instead of l_i and note the following property that will

be useful for notation purposes: $(x^q, y^q) = \phi_q$ and $(x^{q^2}, y^{q^2}) = \phi_q^2$.

Let $P = (x, y) \in E[l]$ be a torsion point, and $q_l \equiv q \mod l$, with $|q_l| \leq \frac{1}{2}l$. Then, from proposition xy,

$$(x^{q^2}, y^{q^2}) + q_l(x, y) = a(x^q, y^q)$$

We can use this relation to find $a \mod l$, since (x^q, y^q) is also a point of order l.
We can now distinguish three cases:

- If $(x^{q^2}, y^{q^2}) = -q_l(x, y)$, then $a(x^q, y^q) = \infty$, so $a \equiv 0 \mod l$.
- If $(x^{q^2}, y^{q^2}) = q_l(x, y)\ \forall (x, y) \in E[l]$, then $a \equiv +(-)\omega \mod l$, with $\omega^2 \equiv q \mod l$: Since from the hypothesis we have $\phi_q^2(x, y) = q_l(x, y)$, we get $a\phi_q(x, y) = 2q_l(x, y)$. But then:

  $$a^2 q_l(x, y) = a^2\phi_q^2(x, y) = a^2\phi_q(x^q, y^q) =$$
  $$= a2q_l(x^q, y^q) = a2q_l\phi_q(x, y) = 4q_l^2(x, y)$$

  So

  $$a^2 q_l = 4q_l^2 \mod l$$

  In order for this equation to have a solution we need q_l to be a square $\mod l$, so let $w^2 = q_l \mod l$. Now, for any $P \in E[l]$,

  $$(\phi_q + w)(\phi_q - w)P = (\phi_q^2 - q)P = \infty$$

  So then there are two options, either

  $$(\phi_q - w)P = \infty$$

  or $P' = (\phi_q - w)P \neq \infty$,but $(\phi_q + w)P' = \infty$.
  In the first case we obtain $\phi_q P = \omega P$, which implies

  $$\infty = (\phi_q^2 - a\phi_q + q_l)P = (2q_l - a\omega)P$$

  so $aw \equiv 2q \equiv 2\omega^2 \mod l$ and we finally get

  $$a \equiv 2\omega \mod l$$

  In the second case, we have $\phi_q P' = -\omega P'$, and we get

  $$a \equiv -2\omega \mod l.$$

- otherwise, $\exists P = (x, y) \in E[l]$ such that $P' = \phi_q^2(P) + q_l P \neq \infty$, and the line used to sum these two points is not a tangent to the curve.
  We use the following notation:

  $$k(x, y) = (x_k, y_k).$$

  We will then compute (x_{q_l}, y_{q_l}) and then test for all integers $0 < k < l$ if they frullfil the formula

  $$\phi_q^2(x, y) + (x_{q_l}, y_{q_l}) = (x_k^q, y_k^q).$$

But since $x_k = x_{-k}$, the algorithm it is actually convenient to check the property for $0 < \pm k < \frac{l-1}{2}$. Observe that if we get a match $\pm k$ for which the formula holds, then it will hold for all points of the elliptic curve, not only P. So we will obtain

$$a \equiv k \mod l$$

or

$$a \equiv -k \mod l.$$

Let $\phi_q^2(x,y) + (x_{q_l}, y_{q_l}) = (x', y')$, and let's first look at the first coordinate. Using the addition formulas of an elliptic curve group and the equation $y^2 = x^3 + Ax + B$ we can express x' as a rational function $G(x)$, indeed:

$$x' = (\frac{y^{q^2} - y_{q_l}}{x^{q^2} - x_{q_l}}) - x^{q^2} - x_{q_l}$$

but since $y_{q_l} = yr(x)$ for some rational function r, we get

$$(y^{q^2} - y_{q_l}) = y^2(y^{q^2-1} - r(x))^2 = (x^3 + Ax + B)((x^3 + Ax + B)^{\frac{q^2-1}{2}} - r(x))^2.$$

So the k that fullfills the condition on the first coordinate is the one such that

$$x_k^q = G(x).$$

From Propositionxy we know that $\{x\ coordinates\ of\ E[l]\} = \{roots\ of\ \psi_l\}$, so the condition above is satisfied iff

$$x' = G(x) \equiv x_k^q \mod \psi_l$$

If we have found such a k, then

$$(x', y') = \pm(x_k^q, y_k^q) = (x_k^q, \pm y_k^q).$$

To determine the correct sign we look at the second coordinates. We can express $\frac{y'}{y}$ and $\frac{y_k^q}{y}$ as functions of x, so if we have $\frac{(y'-y_k^q)}{y} \equiv 0 \mod \psi_l$, then $a \equiv k \mod l$, otherwise $a \equiv -k \mod l$.

Now to conclude Schoof's algorithm we conside $a \mod l\ \forall l \in S$ and apply the Chinese remainder theorem, obtaining $a \mod \Pi l$. Since by hypothesis we have chosen S so that the product of all its elements is bigger than $4\sqrt{q}$ we can then use Hesse theorem to find the unique a such that $|a| \leq 2q$.

Running time of the algorithm and its implementation:(da completare)

Observation 0.3.18. This algorithm was later refined by Atkin and Elkies, for more information see (insert reference).

Observation 0.3.19. As noted in the beginning of this chapter, if $\#E(\mathbb{F}_q) = n$, then the order of any point $P \in E(\mathbb{F}_q)$ is a divisor of n. This means the relation can be used to restrict the options for a points order, but also the other way around: we can use some large order of a point to find n.

Example 0.3.20. *Let* $y^2 = x^3 - 10x + 21$ *be an elliptic curve in Weierstrass form over the finite field* $\mathbb{F}_{557}$. *Then it is possible to show that the point* $(2, 3)$ *has order* 189, *so* $\#E(\mathbb{F}_{557})$ *is a multiple of* 189 *in the range given by Hesse's theorem* $511 \leq \#E(\mathbb{F}_{557}) \leq 605$. *The only integer satisfying both requirements is* 567.

Observation 0.3.21. Knowing the order of an elliptic curve over a finite field can be crucial in choosing the curve we want to use for our cryptographic incription. Indeed, there are some requirements on the cardinality of the group we are using, such as for example that it should have at least one large prime factor. So even if we do not need to know $\#E(\mathbb{F}_q)$ in order to encrypt and decrypt the message, the security of the system depends on some group cardinality properties.

0.3.4 Supersingular elliptic curves

Definition 0.3.22. Let $E(\mathbb{F}_q)$ be an elliptic curve over a finite field of order $q = p^n$. Let a_q be the trace of the Frobenius endomorphism ϕ_q, so $\#E(\mathbb{F}_q) = q + 1 - a_q$. We say that E is supersingular if p divides a_q, i.e. if $a_q \equiv 0 \mod p$.

It is important to note that supersingular elliptic curves are not singular curves, as by definition of elliptic curves. The term refers to the fact that this group of curves has a "large" endomorphism ring.

Observation 0.3.23. All elliptic curves of cardinality $\#E(\mathbb{F}_q) = q+1$ are supersingular.

Proposition 0.3.24. *If the elliptic curve* E *is defined over* $\mathbb{F}_p$ *for a prime* $p > 3$, *then* E *is supersingular iff* $\#E(\mathbb{F}_q) = p + 1$.

Proof. Let E be supersingular, then $a_q \equiv 0 \mod p$ so if $a_q \neq 0$, then $|a_q| \geq p$. But by Hesse's theorem $|a_q| \leq 2\sqrt{p}$, so we would get $p \leq 2\sqrt{p}$ which is only possible for $p \leq 4$.

□

(possibilmente capitolo da espandere)

0.4 Pairings

0.4.1 The Weil Pairing

Let E be an elliptic curve over a field K and let n be an integer that cannot be divided by $p = char(K)$. Then we know that

$$E[n] = \{P \in E(\overline{\mathrm{K}}) \text{ such that } nP = \infty\} \simeq Z_n \oplus Z_n.$$

We set

$$\mu_n = \{x \in \overline{\mathrm{K}} | x^n = 1\}.$$

Since $p = char(K)$ does not divide n, the equation does not have multiple solutions, so there are exactly n distinct roots of x^n in $\overline{\mathrm{K}}$ and therefore μ_n is a cyclic group of order n, i.e. $\mu_n \simeq \mathbb{Z}_n$.

Definition 0.4.1. We call any generator of the group μ_n n-th primitive root of unity.

Supposing n as above we can now define the Weil Pairing as follows:

Definition 0.4.2. The Weil Pairing is a map

$$e_n : E[n] \times E[n] \to \mu_n$$

such that:

- it is bilinear in each variable
  $e_n(S + R, T) = e_n(S, T)e_n(R, T)$ and $e_n(S, T + Q) = e_n(S, T)e_n(S, Q)$;
- it is nondegenerate in each variable
  if $e_n(S, T) = 1 \quad \forall S \Rightarrow T = \infty$, and if $e_n(S, T) = 1 \quad \forall T \Rightarrow S = \infty$;
- $e_n(T, T) = 1$
- $e_n(S, T) = e_n(T, S)^{-1}$
- $e_n(\sigma S, \sigma T) = \sigma(e_n(S, T))$ for any automorphism σ of $\overline{\mathrm{K}}$ such that it is the identity map on all the coeficients of E;
- $e_n(\alpha(S), \alpha(T)) = (e_n(S, T))^{deg\alpha}$ for every(separable?) endomorphism of E.

Observation 0.4.3. For practical cryptographic uses of pairings it is also required for the map e_n to be easily computable (i.e. in polynomial time).

We now briefly describe one way of constructing the Weil pairing map. We however do not show that all the properties listed above hold for our map, a computation which can be found in [1] III, Proposition 8.1.

Again, let E be an elliptic curve over a field K and let n be an integer that cannot be divided by $p = char(K)$. We pick a point $T \in E[n]$ and consider the divisor

$$D = n \cdot T - n \cdot \infty.$$

Since $deg(D) = 0$ and $sum(D) = \infty$ Corollary 0.2.29 states that D is a principal divisor. Therefore

$$\exists f \in \overline{K}(E) \; such \; that \; (f) = D.$$

We now consider $T' \in E(\overline{K})$ such that $nT' = T$. Such a T' exists because

$$T \in E[n] \Rightarrow T \in E[n^2] \simeq Z_{n^2} \oplus Z_{n^2}.$$

So, as an element of $Z_{n^2} \oplus Z_{n^2}$, T can be written as

$$T = (\alpha + kn, \beta + ln)$$

with $0 \leq \alpha, \beta \leq n - 1$, $k.l \in \mathbb{Z}$. But the order of T is n, so $T = (kn, ln)$. We then just take $T' = (k, l) \in Z_{n^2} \oplus Z_{n^2}$ and $nT' = T \in Z_{n^2} \oplus Z_{n^2} \simeq E[n^2] \subset E(\overline{K})$.

Now take the divisor

$$D' = \sum_{R \in E[n]} (T' + R) - R.$$

Again, D' is a principal divisor, so

$$\exists g \in \overline{K}(E) \; such \; that \; (g) = D'.$$

Now since the divisor of the product of two rational functions is the sum of their individual divisors we can compute (g^n) as:

$$(g^n) = \sum_{R \in E[n]} n \cdot (T' + R) - n \cdot R.$$

On the other hand, if we call $[n]$ the map that given a point multiplies it by n using the elliptic curve group addition, then the divisor

$$(f \circ [n]) = \sum_{R \in E[n]} n \cdot (T' + R) - n \cdot R.$$

This is because we know that f has a unique zero in T of multiplicity n, but then $\forall R \in E[n]$,

$$f(T) = f(nT') = f(nT' + \infty) = f(nT' + nR) = (f \circ n)(T' + R) = 0,$$

so $(f \circ n)$ has zeros of multipicity n in $T' + R$. Similarly, f has a unique n pole at ∞ and therefore $(f \circ n)$ has a n-pole at R for every $R \in E[n]$.
We now see that g^n and $f \circ [n]$ have the same divisors. Furthermore, we can actually easily show that they differ only by a constant as maps, indeed the map

$$(\overline{K}(E), \cdot) \to (P(C), +)$$

is a group homomorphism, and it is easy to see that its kernell consists of all constant functions. This implies that, up to constant multiplication, two rational functions with same principal divisors are the same. Therefore we can assume

$$f \circ [n] = g^n.$$

Now let $S \in E[n]$ and $X \in E(\overline{K})$,

$$g(X + S)^n = (f \circ [n])(X + S) = f(nX + nS) = f(nX) = (f \circ [n])(X) = g^n(X).$$

so

$$\left(\frac{g(X + S)}{g(X)}\right)^n = 1,$$

i.e. for every $S \in E[n]$, $\frac{g(X+S)}{g(X)}$ is a root of unity, and we can define a map

$$e_n : E[n] \times E[n] \to \mu_n$$
$$(S,T) \to \frac{g(X+S)}{g(X)}.$$

We observe that the map does not depend on the choice of X. Indeed let's fix S and write

$$\tilde{g} : E(\overline{K}) \to \overline{K}(E)$$
$$X \to \frac{g(X+S)}{g(X)}.$$

Consider the morphism of varieties

$$\phi : E(\overline{K}) \to \mathbb{P}'$$
$$X \to [\tilde{g}(X) : 1] \; if \; \tilde{g} \; is \; regular \; in \; X$$
$$X \to [1 : 0] \; if \; \tilde{g} \; has \; a \; pole \; in \; X.$$

Since $E(\overline{K})$ is a projective variety over a closed field it is complete, and therefore $\phi(E)$ is closed in $\mathbb{P}'$ with the Zariski topology. But all closed varieties in $\mathbb{P}'$ are points, finite unions of points or $\mathbb{P}'$ itself. $E(\overline{K})$ is irreducible, so $\phi(E)$ is irreducible and cannot be union of finitely many points. Also the map ϕ is not surjective as $\tilde{g}(X)$ can only take finitely many values (the n-roots of unity), so $\phi(E) \neq \mathbb{P}'$. This leaves only the option of ϕ being constant and therefore so is $\tilde{g}$.

We can also give another equivalent construction of the Weil pairing,

Proposition 0.4.4. *Given $P, Q \in E[n]$ choose divisors $D_P \sim P - \infty$ and $D_Q \sim Q - \infty$ such that the two have disjoint supports. It can easily be checked that nD_P and nD_Q are principal divisors, and if we call f_P and f_Q their associated rational functions, then the map*

$$\tilde{e}_n : E[n] \times E[n] \to \mu_n$$
$$\tilde{e}_n(P,Q) = \frac{f_P(D_Q)}{f_Q(D_P)}$$

is equivalent to the Weil pairing e_n as constructed above.

Observation 0.4.5. Given a divisor $D = \sum a_P \cdot P$ we define

$$f(D) = \Pi f(P)^{a_P}.$$

Observation 0.4.6. As we have already mentioned, two functions with the same divisor can differ by constant multiplication. So if we wish to define f_P (and f_Q) in a canonical way we can choose them to be normalised, i.e. such that they satisfy

$$u_R f_P^{-v_R(f)}(R) = 1,$$

where R is a fixed poinft on E of our choice, u_R is the uniformising element at R and $v_R(f)$ the valuation of f_P in that same point.

Proof. First we must show that the map $\tilde{e}_n$ is well defined and does not depend on our choice of divisor D_P. In order to do so we will need use the Weil reciprocity law, which states that for every $f, g \in \overline{K}(E)$

$$f(div(g)) = g(div(f)).$$

Now, let us consider another divisor of the class of D_P, which we can express as $\tilde{D} = D_P + (g)$ for some rational function g, which we can normalise. Let us also suppose f_P to be chosen normalised, then the normalised function with divisor $m\tilde{D} = n \cdot D_P + n \cdot (g)$ is $\tilde{f} = f_P g^n$, so

$$\tilde{e}_n(P,Q) = \frac{\tilde{f}(D_Q)}{f_Q(\tilde{D})} = \frac{f_P(D_Q)g^n(D_Q)}{f_Q(D_P)f_Q(div(g))} = \frac{f_P(D_Q)g^n(D_Q)}{f_Q(D_P)g(div(f_Q))} =$$

$$= \frac{f_P(D_Q)g^n(D_Q)}{f_Q(D_P)g(nD_Q)} = \frac{f_P(D_Q)g^n(D_Q)}{f_Q(D_P)g^n(D_Q)} = \frac{f_P(D_Q)}{f_Q(D_P)}.$$

We therefore see that the result is the same whether we use D_P or $\tilde{D}$ for the computation. The same reasoning can be applied for D_Q, so our map $\tilde{e_n}$ is well defined.

The next step of the proof is to verify that $e_n(P,Q) = \tilde{e}_n(P,Q)$. We choose P', Q' and R such that $P' \neq \pm Q'$ and

$$mP' = P, \quad mQ' = Q, \quad 2R = P' - Q'.$$

We also choose

$$D_P = P - \infty, \quad D_Q = (Q + nR) - nR.$$

We then consider the rational functions f_P and f_Q selected as explained above and using the same reasoning as seen in the previous Weil pairing construction we can claim that there exist functions g_P, g_Q:

$$f_P \circ [n] = g_P^n \quad f_Q \circ [n] = g_Q^n.$$

Now,

$$\tilde{e}_n(P,Q) = \frac{f_P(D_Q)}{f_Q(D_P)} = \frac{f_P(Q+nR)f_Q(\infty)}{f_P(nR)f_Q(P)} =$$

$$= \frac{f_P(nQ'+nR)f_Q(n\infty)}{f_P(nR)f_Q(nP')} = \left(\frac{g_P(Q'+R)g_Q(\infty)}{g_P(R)g_Q(P')}\right)^n.$$

It can be show that the divisor of the following two functions is 0;

$$\phi(X) = \frac{g_P(X+Q'+R)g_Q(X)}{g_P(X+R)g_Q(X+P')}, \qquad \psi(X) = \Pi_{i=0}^{n-1} g_Q(X+iQ');$$

so having no zeros or poles they must both be constant.
We can now continue our computations:

$$\tilde{e_n}(P,Q) = \left(\frac{g_P(Q'+R)g_Q(\infty)}{g_P(R)g_Q(P')}\right)^n = (\phi(\infty))^n =$$

$$= \Pi_{i=0}^{n-1} \phi(iQ') = \Pi_{i=0}^{n-1} \frac{g_P((i+1)Q'+R)g_Q(iQ')}{g_P(R+iQ')g_Q(P'+iQ')} =$$

$$= \Pi_{i=0}^{n-1} \frac{g_P((i+1)Q'+R)}{g_P(R+iQ')} \Pi_{i=0}^{n-1} \frac{g_Q(iQ')}{g_Q(P'+iQ')} =$$

$$= \frac{g_P(R+mQ')}{g_P(R)} \Pi_{i=0}^{n-1} \frac{g_Q(iQ')}{g_Q(P'+iQ')} =$$

$$= \frac{g_P(R+Q)}{g_P(R)} \Pi_{i=0}^{n-1} \frac{g_Q(P'+iQ')}{g_Q(P'+iQ')} =$$

$$= \frac{g_P(R+Q)}{g_P(R)} = e_n(P,Q).$$

□

We now have two equivalent formulas for the Weil pairing, however we are still missing an algorithm to efficiently compute it. The Miller algorithm provides a solution to such problem, so we will briefly describe how it works. We will start by defining a group of functions $f_{n,P}$ which have some properties that allow them to be easily computed in a recursive way with respect to n. We will then show that we can use such functions to compute the Weil pairing, and finally we will state the (Miller) algortihm that actually computes the mentioned functions in polynomial time. The following computations are mainly an extract of [5].

Let E be an elliptic curve, $P, Q \in E$. We call $L_{P,Q}$ the line through P, Q which intersects E also in $-(P+Q)$. Define

$$G_{P,Q} = \frac{L_{P,Q}}{L_{P+Q,-(P+Q)}}.$$

Since $(L_{P,Q}) = P + Q + (-(P+Q)) - 3 \cdot \infty$, we obtain

$$(G_{P,Q}) = P + Q - (P+Q) - \infty.$$

Now we can recusively define the set of functions $f_{n,P}$ im the following way:

$$f_{0,P} = f_{1,P} = 1$$

$$f_{n+1,P} = f_{n,P} G_{P,nP}$$

$$f_{-n,P} = \frac{1}{f_{n,P} G_{nP,-nP}}.$$

Proposition 0.4.7. *The functions $f_{n,P}$ satisfy:*

1. $(f_{n,P}) = n \cdot P - (n-1) \cdot \infty - nP$
2. $f_{n+m,P} = f_{n,P} f_{m,P} G_{mP,nP}$
3. $f_{nm,P} = f_{m,P}^n f_{n,mP} = f_{n,P}^m f_{m,nP}$

Proof. 1. We procede by induction. The thesis is easily verifyed for $n = 0, 1$. Then, assuming the property tohold for n,

$$(f_{n+1,P}) = (f_{n,P}) + (G_{P,nP}) = n \cdot P - (n-1) \cdot \infty - nP + P + nP - (P + nP) - \infty =$$

$$= (n+1) \cdot P - (n+1-1) \cdot \infty - (n+1)P.$$

$$f_{-n,P} = -(f_{n,P}) - (G_{nP,-nP}) = -n \cdot P + (n-1) \cdot \infty + nP - nP - (-nP) + (nP + (-nP)) + \infty =$$

$$= -n \cdot P - (-n-1) \cdot \infty - (-nP).$$

2. Using the formula 1. we can explicitly compute the divisors of $f_{n,P} f_{m,P} G_{mP,nP}$ and $f_{n+m,P}$) which turn out to be the same. Being all the functions normalised the equality follows.
3. We use the same reasoning as in 2.

□

Proposition 0.4.8. *Let E be an elliptic curve, n be an integer coprime with $char(K)$ and $P, Q \in E[n]$. Then for all $T \neq \infty, Q, -PQ - P$,*

$$e_n(P, Q) = \frac{f_{n,Q}(T) f_{n,P}(Q - T)}{f_{n,P}(-T) f_{n,Q}(P + T)}.$$

Proof. We recall that $e_n(P, Q) = \frac{f_P(D_P)}{f_Q(D_Q)}$ where $D_P \sim P - \infty$ and $D_Q \sim Q - \infty$, they have disjoint support and $(f_P) = nD_P, (f_Q) = nD_Q$.
Since $(G_{P,T}) = P + T - (P + T) - \infty$, we have that $P - \infty \sim (P + T) - T$ so we can choose $D_P = (P + T) - T$, and $D_Q = Q - \infty$. Since $T \neq \infty, Q, -P, Q - P$ we have that D_Q and D_P satisfy the disjoint support condition.
Consider now the function

$$\tau : E \to E$$
$$R \to R - T$$

From the previous proposition we have the formula for $div(f_{n,P})$ which we apply to obtain

$$div(f_{n,P} \circ \tau) = n \cdot (P - T) - (n-1) \cdot (-T) - (nP - T) =$$

$$= n \cdot (P - T) - n \cdot (-T) = div(f_P) = nD_P.$$

On the other hand

$$(f_{n,Q}) = n \cdot Q - (n-1) \cdot \infty - nQ = nD_Q = (f_Q).$$

So we simply take $f_P = f_{n,P} \circ \tau$ and $f_Q = f_{n,Q}$ and we get a Weil pairing

$$e_n(P, Q) = \frac{f_P(Q)}{f_P(\infty)} \cdot \frac{f_Q(T)}{f_Q(P + T)} = \frac{f_{n,P} \circ \tau(Q)}{f_{n,P} \circ \tau(\infty)} \cdot \frac{f_{n,Q}(T)}{f_{n,Q}(P + T)} = \frac{f_{n,P}(Q - T) f_{n,Q}(T)}{f_{n,P}(-T) f_{n,Q}(P + T)}.$$

□

In particular, if $P \neq Q \in E[n]$ the formula can even be reduced to

$$e_n(P,Q) = (-1)^n \frac{f_{n,P}(Q)}{f_{n,Q}(P)},$$

for the proof of which we refer to [5].

The above proposition shows how we can compute the Weil pairing using the functions we constructed recursively $f_{n,P}$. What makes this particular set of functions useful is property 2. of Proposition 0.4.7, as it allowes effective recursion computation.
Indeed, for example to compute $f_{4,P}$ we can procede as follows: set $f_{1,P} = 1$ and then $f_{2,P} = f_{1,P}^2 \cdot G_{P,P}$, $f_{4,P} = f_{2,P}^2 \cdot G_{2P,2P}$.

Theorem 0.4.9. ***Miller's algorithm***
input: P, n
output: $f_{n,P}$

Let $n = \sum_{k=0}^{t} n_k \cdot 2^k$ *with* $t = 1$ *be the binary expansion of* n. *Then:*
. *Set* $T = P$ *and* $f = 1$;
. *for* $i = t - 1$ *to* 0:
. $f = f \cdot G_{T,T}$
. $T = 2T$
. *if* $n_i = 1$:
. *set* $f = f \cdot G_{T,P}$
. $T = T + P$
. *return* f

(ancora un po' da completare, spiegare meglio)

Miller's algorithm running time is $\mathcal{O}(logn)$.

Proposition 0.4.10. *If* $\{T_1, T_2\}$ *are a base of* $E[n]$, *then* $e_n(T_1, T_2)$ *is an* n*-th primitive root of the unity.*

Proof. $e_n(T_1, T_2) = \xi$ is a generator of μ_n if the order of ξ is n. So, suppose $ord(\xi) = d$, then by the bilinearity of the pairing $e_n(T_1, dT_2) = e_n(T_1, T_2)^d = 1$. Let now $T_3 \in E[n]$, then $T_3 = aT_1 + bT_2$ and

$$e_n(T_3, dT_2) = e_n(aT_1, dT_2)e_n(bT_2, dT_2) = e_n(T_1.dT_2)^a e_n(T_2, dT_2)^b = 1$$

This implies

$$dT_2 = \infty$$

but since $T_2 \in E[n]$ we have $n|d$, so $ord(\xi) = n$ and ξ is an n-th root of unity.

□

Corollary 0.4.11. *If* $E[n] \subset E(K)$, *then* $\mu_n \subset K$.

for the proof of this corollary see referencexy(it requires galois theory)

0.4.2 The Tate-Linchtenbaum pairing

(da scrivere)

0.5 Elliptic curve cryptography- ECC

(capitolo solo iniziato, appena da scrivere)

0.5.1 Diffle-Hellman key-exchange protocol

Let $E(\mathbb{F}_q)$ be a large, known, elliptic curve group over a finite field. Let also $R \in E(\mathbb{F}_q)$ be an element of order a large prime p. In order to determine a common secret key K, Alice and Bob each indipendently pick a random integer $1 \leq k_A \leq p-1$ and $1 \leq k_B \leq p-1$, which will be their private secret key.
Then Alice sends Bob

$$P = k_A R$$

and Bob sends Alice

$$Q = k_B R.$$

Now, using their private keys, they can both easily find the common key $K = k_A k_B R$. The security of the system is based on the unbreakability of the ECDLP:

Definition 0.5.1. Elliptic Curve Discrete Logarithm Problem:
Consider a group G of points of an elliptic curve and $R \in G$ an element of the group with order a large prime number. Then given a point $P \in G$ the ECDLP consists in finding a k such that $P = kR$ on the curve.

0.5.2 Encoding a message on an elliptic curve

Let m be the message we want to encrypt using elliptic curve cryptography, and $E(\mathbb{F}_q)$ be the curve we want to use. In order to use any of the previously described cyphres(che sono appena da scrivere) we need to represent m as a point $P \in E(\mathbb{F}_q)$. There are various ways to do so: (da scrivere)

0.6 Elliptic Curve Cryptography and pairings

For many years the additional structure of elliptic curve groups was not really considered for cryptographic purposes. The finding of pairings changed that, introducing both new cryptographic opportunities as well as further limitations on “good” curve choices.

0.6.1 The MOV attack

One crucial application of pairings in cryptography is to use them to reduce the ECDLP in a large group into DLP in smaller ones. This is the idea behind the MOV(Menezes, Okamoto, Vanstone) cryptographic attack.
Le e be a Weil pairing of an ellicptic curve over a finite field $\mathbb{F}_q$, and let P and $Q = kP$ be two points on such curve. Suppose also that P has order n and that such order is coprime with q. We want to solve the ECDLP, i.e. find k.
We will do so by reducing the ECDLP in $E(\mathbb{F}_q)$ to the DLP in $\mathbb{F}_{q^m}$, a finite field on which we can use the subexponential index calculus method. This way, if q^m is not much larger than q we can solve the new problem much faster then the original one.

Let us first observe that given two points P and Q on the elliptic curve $E(\mathbb{F}_q)$, the k for which $Q = kP$ does not necessarily exist, indeed the following property holds:

Proposition 0.6.1. *Let P and Q be points of an elliptic curve of order n. Then there exists k such that $Q = kP$ if and only if $e_n(P, Q) = 1$.*

Proof. "$\Rightarrow$"

$$e_n(P, Q) = e_n(P, kP) = e_n(P, P)^k = 1$$

"$\Leftarrow$"
Since $gcd(n, q) = 1$ we know that $E[n] \simeq Z_n \oplus Z_n$. We can now find a point R such that $\{P, R\}$ is a basis of $E[n]$, and we then know by proposition(xy) that $e_n(R, P)$ is a generator of μ_n. We now have that

$$Q = xP + yR,$$

and

$$1 = e_n(P, Q) = e_n(P, xP + yR) = e_n(P, P)^x e_n(P, R)^y = e_n(P, R)^y.$$

But since $e_n(P, R)$ is an n-th root of unity it has order n, and so we get $y \equiv 0 \mod n$. But then $yR = \infty$, which leaves us with $Q = xP$. We now have our $k = x$.

□

By slightly adjusting this proof we obtain the MOV attack:

Let us choose an m such that $E[n] \subset E(\mathbb{F}_{q^m})$. This is possible since $E[n] \subset \overline{F_q}$, and $\overline{F}_q = \cup^i F_{q^i}$.
Then we repeat the following steps unitil the least common multipe of the tuple $(d_1, \ldots, d_k)$ is n.

- choose a random point $T_i \in E(\mathbb{F}_{q^m})$ and compute its order n_i;
- let $d_i = gcd(n, n_i)$ and $\tilde{T_i}' = (n_i/d_i)T_i$. Now $\tilde{T}_i$ has order d_i, which divides n. This implies $\tilde{T}_i' \in E[n]$.
- compute the Weil pairing $\xi_i = e_n(\tilde{T_i}', P)$, and $\xi_i' = e_n(\tilde{T_i}', Q) = e_n(\tilde{T_i}', P)^k = \xi_i^k$;

- from corollary(xy) we have that $\mu_n \subset \mathbb{F}_{q^m}$, so $\xi_i, \xi_i^k \in \mathbb{F}_{q^m}^*$. So we can now try to solve the DLP
$$\xi_i' = \xi_i^k$$
in the multiplicative group $\mathbb{F}_{q^m}^*$.
- this way we obtain $k_i = k \mod d_i$. But since we repeat the algorithm untill the least common multiple of the d_i's is n (i.e. the d_i are "parwise coprime"), we can then use the chinese remainder theorem to find $k \mod n$.

Time analysis:
Weil pairings and the chinese remainder theorem can be computed quickly, so the running time really depends on finding the k_i's and on their number. The number of k_i's we need is again not very high, so in the end all that is left is computing the k_i's, which is the classic discrete logarithm problem and depends of course on how large m is, since we are working in $\mathbb{F}_{q^m}^\star$.

In conclusion, when using elliptic curve cyphres we need to take into consideration the limitations on the curve choices given by the MOV attack. Usually an elliptic curve for which the smallest m such that $E[n] \subset E(\mathbb{F}_{q^m})$ is bigger than 20 is considered safe. Most of elliptic curves satisfy such condition, but not all. In particular the MOV attack is really effective on supersingular elliptic curves. Indeed in this case if $\exists P \in E[n]$, then $E[n] \subset E(\mathbb{F}_{q^2})$ when the field characteristic is not 2 or 3, in which cases we however still get $m \leq 4$ and $m \leq 6$. For more about this topic we refer to Alfred J. Menzenes, T. Okamoto, and Scott A. Vanstone; Reducing elliptic curve logarithms to logarithm in a finite field.

(espandere e spiegare bene se decidiamo di inserire le supersingular curves)

0.6.2 Weil pairing and the Decision Diffle Hellman Problem

Given a group with a known Weil pairing e the Decision Diffle Hellman Problem can become easy.

Definition 0.6.2. Decision Diffle Hellman Problem- DDHP:
Given a point $P \in E(\mathbb{F}_q)$, aP, bP and another point Q in the same elliptic curve, determine whether or not $Q = abP$.

(da scrivere)

0.6.3 The Frey-Ruck attack

0.6.4 A cyphre based on the Weil pairing

0.7 Hyperelliptic curves

Definition 0.7.1. Let X and Y be two curves. Consider for any two open subsets U and V of X and morphisms $\phi_u : U \to Y, \phi_v : V \to Y$ the equivalence realtion:
$$(U, \phi_u) \equiv (V, \phi_v) \iff \phi_u|_{U \cap V} = \phi_v|_{U \cap V}.$$

We define a rational map $\phi : X - - - > Y$ is an equivalence class $[(U, \phi_u)]$ under this relation.
In particular, a rational map is called dominant if $\phi_u(U)$ is dense in Y.

Observation 0.7.2. In general the composition of two rational maps can be not well defined,as we could have that the image of first map does not intersect the domain of the second. However if we consider the first map to be dominant we avoid this problem.

Definition 0.7.3. Two curves are said to be birationally equivalent if there exists a birational map between them, i.e a dominant rational map $f : X - - - > Y$ such that there exists $g : Y - - - > X$ dominant and $f \circ g = id_X, g \circ f = id_Y$.

Definition 0.7.4. A hyperelliptic curve of genus g over a field K is a curve that is birationally equivalent to the affine curve

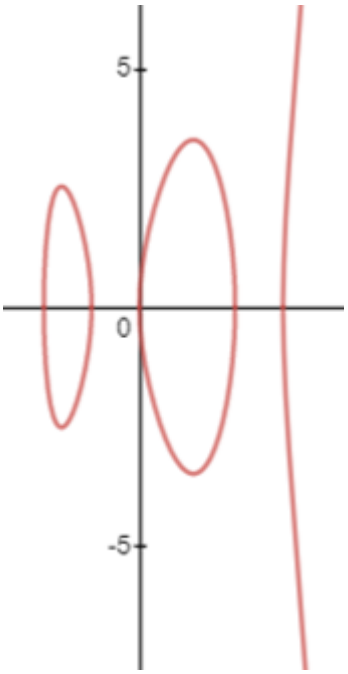
$$y^2 + h(x)y + f(x) = 0$$

with $f \in K[x]$ monic of degree $n = 2g + 1$ or $n = 2g + 2$ and $h(x) \in K[x]$ of degree $\leq g$. We also require for all (x, y) to be nonsingular points on the affine curve, so we do not allow the case $2y + h(x) = 0 = f'(x)$.
In particular, if $char(K) \neq 2$ we can further simplify the equation to

$$y^2 = f(x).$$

In this case we ask for f not to have zeroes of multeplicity more than one.

Example 0.7.5. $y^2 = x^5 - 2x^4 - 7x^3 + 8x^2 + 12x$ *is a hyperelliptic curve of genus* 2.



Observation 0.7.6. A more formal definition of hyperelliptic curves states that any curve of genus $g \geq 2$ is hyperelliptic if there exists a finite morphism of degree two $\pi : C \to \mathbb{P}'$. When this is the case we have that $[K(\mathbb{P}') : K(C)]$ is a field extension of degree two. We also observe that denoting the morphism with π is an indicator of the fact that usually the finite morphism is exactly the projection on $\mathbb{P}'$.

The above formula gives us a very simple way to represent hyperelliptic curves, however by homegenising the equation we can easily see that it has a singularity at the point ∞. We can however get rid of such singularity (i.e. find a non singular curve birationally equivalent to the first one) by considering the blow up at the singular point, possibly more than once. For more details we refer to referencexy(tesi manuela).

Observation 0.7.7. The behaviour of principal divisors and rational functions on a (hyper)elliptic curve $y^2 = f(x)$ is "forced" at infinity. Let for example $h = x - a$ for some constant $a \in K$ be our function. It is clear that h does not have poles in the affine plane but has two zeroes in $\overline{K}$: $(a, \sqrt{f(a)}$ and $(a, -\sqrt{f(a)})$ (or a single double zero if $f(a) = 0$) . But the principal divisor associated to h has degree zero, so we need to "compensate" with two poles at infinity;

$$(h) = (a, \sqrt{f(a)}) + (a, -\sqrt{f(a)}) - 2\infty.$$

In order to use hyperellptic curves in cryptography we need a group structure. Unfortunately the construction used on elliptic curves cannot be applied in this case, we can however use divisors to define a different group correlated to the curve. In particular, we will only use hyerelliptic curves for which the polynomial f has degree $2g + 1$, so we will consider only such ones from now forth.

0.7.1 The Jacobian variety

As mentioned before, we are looking for a group structure to associated to a hyperelliptic curve. This will be the Jacobian variety.

Definition 0.7.8. Let C be a hyperelliptic curve. We define its Jacobian variety as

$$J(C) = Div^0(C)/P(C)$$

where $P(C)$ is the subgroup of principal divisors of C.

The jacobian has the structure of a quotient group.

Observation 0.7.9. It can be shown that if E is an elliptic curve, then

$$J(E) = Div^0(E)/P(E) = E.$$

Let C be a hyperelliptic curve over a filed K. We can define a map ω that works in the following way:

- if $char(K) \neq 2$

$$\omega : C \to C$$
$$(x, y) \to (x, -y)$$
$$\infty \to \infty$$

- if $char(K) = 2$

$$\omega : C \to C$$
$$(x, y) \to (x, -y - h(x))$$
$$\infty \to \infty$$

This is an involution, i.e. $\omega \circ \omega = id$.
Given a divisor $D \in Div^0(C), D = \sum c_j(P_j - \infty)$ we write $\omega(D) = \sum c_j \omega(P_j)$.

Proposition 0.7.10. *If $D \in Div^0(C), D = \sum c_j \cdot (P_j - \infty)$, then $D + \omega(D)$ is a principal divisor.*

proof:
$D + \omega(D) = \sum c_j \cdot (P_j + \omega(P_j) - 2\infty)$. We want to show that this is a principal divisor. We do this by showing it is the divisor of the polynomial $A(x) = \Pi(x - a_j)^{c_j}$.
If the field we are working with is not of characteristic two we can write $C : y^2 = f(x)$, and $P_j = (a_j, \pm\sqrt{(f(a_j))})$ for some a_j. Then $D + \omega(D)$ is the divisor of the polynomial $A(x) = \Pi(x - a_j)^{c_j}$, indeed, for every a_j, $P_j = (a_j, \sqrt{f(a_j)}$ and $\omega(P_j) = (a_j, -\sqrt{f(P_j)})$ are zeroes of order c_j of $A(x)$, while all the poles are at ∞.
If the field has characreristic two, $C : y^2 + h(x)y = f(x)$, and for every a_j, $P_j = \left(a_j, \frac{-h(a_j)+\sqrt{h(a_j)^2+4f(a_j)}}{2}\right)$ and $\omega(P_j) = \left(a_j, \frac{-h(a_j)-\sqrt{h(a_j)^2+4f(a_j)}}{2}\right)$ are the points on the curve corresponding to the zeroes of $A(x)$ of order c_j, while again, all poles are at ∞.

As a consequence of this proposition, we see that we can obtain the opposite element of a divisor class $[D] \in J(C)$ by using the omega function:

$$[D + \omega(D)] = [0] \Rightarrow [\omega(D)] = [-D].$$

Suppose now that we are working with a field K of characteristic not 2. We want to describe the algorithmic way we endowe $J(C)$ with the structure of a group. In order to do so we introduce the Mumford representation which gives us a very concrete representation of the points of the Jacobian. We will just give an idea of how this group structure is obtained, without proving most of the statements. In order to have a more complete explanation we refer to [3] and [2] (inserire i capitoli delle citazioni).

Theorem 0.7.11. *There is a one-to-one correspondence between elements of $J(C)$ and pairs of polynomials $[u, v]$ such that:*

- *u is monic;*
- *$deg(v) < deg(u) \leq g$;*
- *$v^2 - f(x)$ is a multiple of u.*

Definition 0.7.12. The pair $[u.v]$ as above is called the Mumford representation of the corresponding class in $J(C)$.

As mentioned above we now give just an idea of how this correspondence is constructed.

Definition 0.7.13. Let $D = \sum c_j \cdot (P_j - \infty)$ with $P_j = (a_j, b_j)$ be a divisor of degree zero. We say it is semi-reduced if:

- $c_j \geq 0 \ \forall j$;
- if $b_j = 0$ then $c_j = 0, 1$;
- if $b_j = 0$ then $\omega(P_j)$ does not appear in the sum.

In the case that we also have $\sum c_j \leq g$ we say the divisor is reduced.

Given a dvisor $D \in Div^0(C)$, we can easily find a semi-reduced divisor in its same class, which we will still call D. So let's now consider the semi-reduced divisor $D = \sum c_j \cdot (P_j - \infty)$ where $P_j = (a_j, b_j)$. We take

$$u(x) = \Pi_j (x - a_j)^{c_j}.$$

Then there exists a unique $v(x)$ such that

- $\forall j \ v(a_j) = b_j$;
- $deg(v) \leq deg(u)$;
- u divides $f - v^2$;
- $D = MCD(((u(x)), (y - v(x)))$.

Conversely, if $u, v \in K[x]$ satisfy $deg(v) < deg(u)$ and u divides $f - v^2$, then $D = MCD(((u(x)), (y - v(x)))$ is a semi-reduced divisor.

Observation 0.7.14. By MCD of two divisors $D_1 = \sum d_j \cdot (Q_j - \infty)$, $D_2 = \sum e_j \cdot (Q_j - \infty)$ we mean

$$MCD(D_1, D_2) = \sum min(d_j, e_j) \cdot (Q_j - \infty).$$

Let's now consider the map

$$\phi : [u(x), v(x)] \to D = MCD((u(x)), (y - v(x))).$$

The map ϕ is actually a bijection between polynomials in the Mumford representation and reduced divisors and since it can also be shown that for every class $[D] \in J(C)$ there is a unique representative $\tilde{D}$ which is reduced, ϕ gives us the one to one correspondence with $J(C)$ we were looking for.

The theorem is also valid if the hyperelliptic curve is defined over a field with characteristic 2 ($C : y^2 = h(x)y + f(x)$) and the proof is very similar to the one above, so we will not write it down expliciltly.

Example 0.7.15. *The divisor* $0 = \sum 0 \cdot P_j$ *is reduced, and its Mumford representation is* $[1, 0]$.

Observation 0.7.16. In practice in order to get the Mumford representation of a semi-reduced divisor D of degree zero we can find the reduced divisor in its same class and then apply ϕ, or use another method which we now describe:
First, associate polynomials u,v to D as above, i.e. so that $u(x) = \Pi(x - a_j)^{c_j}$ and $v(x)$ satisfies $\forall j, \quad v(a_j) = b_j, deg(v) \leq deg(u)$ and $f - v^2$ is a multiple of u. Even if this requirement is fullfilled what we obtain is still not necessarily the Mumford representation yet, as we can still have $deg(u) > g$. However we can then just apply the reduction procedure described below and get the $[\tilde{u}, \tilde{v}]$ associated to the reduced divisor.

Reduction procedure:

input: $[u, v]$ representing the semi-reduced divisor

- set $\tilde{u} = (f - v^2)/u$;
- set $\tilde{v} = -v \mod \tilde{u}$;
- multiply $\tilde{u}$ by some constant to make it monic;
- if $deg(\tilde{u}) > g$ go back to the first step.

output: $[\tilde{u}, \tilde{v}]$

Example 0.7.17. *Let* $C : y^2 = x^5 - 3x^3 + 2x - 1$ *be a hyperelliptic curve over* $\mathbb{F}_5$ *of genus* 2. *Let's find the Mumford representation of*

$$D = (0, 3) + (1, 3) + (2, 1) - 3 \cdot \infty.$$

First we observe that D *is semi-reduced as* $\sum c_j = 3 > g = 2$. *Then we find the polynomials* u, v

$$u(x) = x(x - 1)(x - 2) = x^3 - 3x^2 + 2x$$

and $v(x)$ *of degree less than* $deg(u)$ *(so* $v(x) = ax^2 + bx + c$ *) such that* $v(0) = 3, v(1) = 3, v(2) = 1$, *i.e.*

$$v(x) = -x^2 + x + 3$$

We check that u *divides* $f - v^2$*:*

$$f(x) - v^2(x) = x^5 - x^4 - x^3 - 4x = (x^3 - 3x^2 + 2x)(x^2 + 2x + 3) = u(x)(x^2 + 2x + 3).$$

Finally, we apply the reduction procedure described above

$$\tilde{u} = \frac{(f - v^2)}{u} = (x^2 + 2x + 3);$$

$$\tilde{v} = -v \mod \tilde{u} = x^2 - x - 3 \mod \tilde{u} = 2x + 4$$

and we are done since $deg(\tilde{u}) = 2 \leq g$. *The Mumford representation of* D *is*

$$D = [x^2 + 2x + 3, 2x + 4].$$

We now use the Mumford representation to define a sum and inverse on $J(C)$ where $C : y^2 = h(x)y + f(x)$.

Theorem 0.7.18. ***(Inverse algorithm)***
input:$D = [u, v]$
Take $v' = v - h$
output: $-D = [u, v']$

The original algorithm for the addition of two divisors in Mumford representation was originally given by Cantor for the case $h(x) = 0$ and then extended by Neal Koblinz so it can be used also on C defined over a field of characteristic two.

Theorem 0.7.19. ***(Cantor algorithm)***
input: $D_1 = [u_1, v_1]$ *e* $D_2 = [u_2, v_2]$

- *set* $d = MCD(u_1, u_2, v_1 + v_2 + h)$ *and find* h_1, h_2, h_3 *such that*
$$d = u_1h_1 + u_2h_2 + (v_1 + v_2 + h)h_3;$$
- *set* $v_0 = (v_2u_1h_1 + v_1u_2h_2 + (v_1v_2 + f)h_3)/d;$
- *set* $u = u_1u_2/d^2$ *and* $v \equiv v_0 \mod u;$
- *set* $u' = (f - vh - v^2)/u$ *and* $v' = -h - v \mod u'$
- $u = u'$ *and* $v = v'$
- *make* u *monic by dividing it by some number;*
- *if* $deg(u) > g$ *go back to the fourth step;*

output: $D_1 + D_2$

Example 0.7.20. *Le* $C : y^2 = x^5 - 3x^3 + 2x - 1$ *be the same hyperelliptic curve over* $\mathbb{F}_5$ *as in the previous example. We show how to sum the divisors* $D_1 = (0, 3) + (1, 3) + (2, 1) - 3 \cdot \infty$ *and* $D_2 = (0, 2) + (2, 4) - 2 \cdot \infty$ *using the Cantor algorithm.*
We have already calculated the Mumford representation od $D_1 = [x^2 + 2x + 3, 2x + 4]$. D_2 *is a reduced divisor with*$u_2(x) = x(x - 2) = x^2 - 2x$ *ans* $v_2(x)$ *of degree less than two such that* $v_2(0) = 2$ *and* $v_2(2) = 4$, *i.e.* $v_2(x) = x + 2$. *So*

$$D_1 + D_2 = [x^2 + 2x + 3, 2x + 4] + [x^2 - 2x, x + 2].$$

- $d = MCD(x^2 + 2x + 3, x^2 - 2x, 3x + 1) = 1$, *so we need to find* $h_1, h_2, h_3 \in \mathbb{F}_5[x]$ *such that*
$$d = (x^2 + 2x + 3)h_1 + (x^2 - 2x)h_2 + (3x + 1)h_3.$$
By taking $h_1 = 0, h_2 = 2, h_3 = x + 1$ *we obtain the desired equation.*
- *Now we compute*
$$v_0 = (2x + 4)(x^2 - 2x)2 + ((2x + 4)(x + 2) + x^5 - 3x^3 + 2x - 1)(x + 1) =$$
$$= x^6 + x^5 - 3x^4 + 3x^3 + 2x^2 + x + 2.$$

- *we set*

$$u = (x^2 + 2x + 3)(x^2 - 2x) = x^4 - x^2 - x$$

$$v = v_0 \mod u = x^2 - x + 2$$

- *finally,*

$$u' = \frac{x^5 - 3x^3 + 2x - 1 - (x^2 - x + 2)^2}{x^4 - x^2 - x} = x - 1$$

$$v' = -(x^2 - x + 2) \mod (x - 1) = 2$$

Since u' is monic and of degree less than $g = 2$ we are done;

$$D_1 + D_2 = [x - 1, 2].$$

Observation 0.7.21. The Cantor algorithm holds for any hyperelliptic curve, whatever its genus or whatever the field it is defined over. It is however not very efficient in general, as it requires the Euclidean agorithm to solve the first step. However once we have fixed the genus g of the curve we can implement it to be more efficient. In particular, for curves of genus 2 and 3 we have polynomials u and v of small degrees, so we can even get explicit addition formulas which are very fast. (espandere?)

For hyperelliptic curves of genus 2 we can also give a geometric idea of the sum operation, as we did for elliptic curves, only we now use polynomials of degree three instead of lines.
Indeed, let $C : y^2 + h(x)y = f(x)$ and consider $J(C)$ and $D_1 = P_1 + P_2 - 2 \cdot \infty$, $D_2 = Q_1 + Q_2 - 2 \cdot \infty$ two canonical representatives of equivalence classes in $J(C)$. There is exactly one polynomial of degree three containing the four points P_1, P_2, Q_1, Q_2, let's call it $v(x)$.
In order to find $C \cap \{y = v(x)\}$ we solve $v(x)^2 + h(x)v(x) = f(x)$ which has degree six, so besides the points we already had we also get other two x_5 and x_6 and then $y_5 = v(x_5)$ and $y_6 = v(x_6)$. Therefore we have other two points $R_1 = (x_5, y_5)$ and $R_2 = (x_6, y_6)$ that belong to the intersection of the curve with the polynomial v.
The divisor $(y - v)$ of the curve C is then:

$$(y - v) = P_1 + P_2 + Q_1 + Q_2 + R_1 + R_2 - 6 \cdot \infty = D_1 + D_2 + R_1 + R_2 - 2 \cdot \infty.$$

$(y - v)$ is associated to a rational function and therefore it is a principal divisor. So

$$(y - v) = D_1 + D_2 + R_1 + R_2 - 2 \cdot \infty = 0;$$

but in then

$$D_1 + D_2 = w(R_1 + R_2 - 2 \cdot \infty) = w(R_1) + w(R_2) - 2 \cdot \infty$$

0.7.2 Hyperelliptic curves over finite fields

Let's first start with a finite field $\mathbb{F}_q$ for some q odd. Then the curve is of the form $C : y^2 = f(x)$ with coefficients in $\mathbb{F}_q$ and no multiple roots in $\overline{\mathbb{F}}_q$. Let $n = 2g + 1$ be the degree of f.

The hyperelliptic equivalent of Hesse's theorem is called Weil theorem, and it gives us an aproximation of the cardinality $\#J_C(\mathbb{F}_q)$ of $J(C)$.

Theorem 0.7.22. *(Weil) Let C be a hyperelliptic curve of genus g. Then*

$$(\sqrt{q} - 1)^{2g} \leq \#J_C(\mathbb{F}_q) \leq (\sqrt{q} + 1)^{2g}.$$

(insert proof?)

Bibliography

[1] J. Silvermann, *The Arithmetic of Elliptic Curves, Second edition,* Springer-Verlag (2009).

[2] L. C. Washington, *Elliptic Curves: Number Theory and Cryptography, Second Edition,* Chapman and Hall/CRC, 2008 (2008).

[3] M. Vidoni, *Aspetti algebrici e geometrici della Crittografia* Master thesis, University of Trieste, (2016-2017).

[4] A. Alvarado, *An exposition of Schoff's Algorithm*, *https* : $//mathpost.asu.edu/\ sjgm/issues/2005_spring/SJGM_alvarado.pdf(2005)$

[5] V. Miller, *The Weil Pairing, and Its Efficient Calculation.*J Cryptology 17, 235–261 (2004).

[6] R. Hartshorne, *Algebraic Geometry*, Springer-Verlag New York (1977).