Homework #4
Elliptic Curves

CNS Course Sapienza

Riccardo Prinzivalle, 1904064

November 20, 2020

1 Homework Goal

This homework contains a basic introduction on Elliptic Curves (EC), the general idea on the math basis, the Discrete Logarithm Problem with EC and the practical utilize of EC in cryptography.

2 Elliptic Curves Motivation

Elliptic Curves are the main trend in asymmetric encryption today: why is their usage so spread? This question has a simple answer: it is sufficient to look at table 1, where there is a comparison of the key length needed to guarantee the same level of security.

Algorithm Family	Cryptosystems	Security Level (bit)			
		80	128	192	256
Integer Factorization	RSA	1024	3072	7680	15360
Discrete Logarithm	DH, DSA, Elgamal	1024	3072	7680	15360
Elliptic Curves	ECDH, ECDSA	160	256	384	512
Symmetric key	AES, 3DES	80	128	192	256

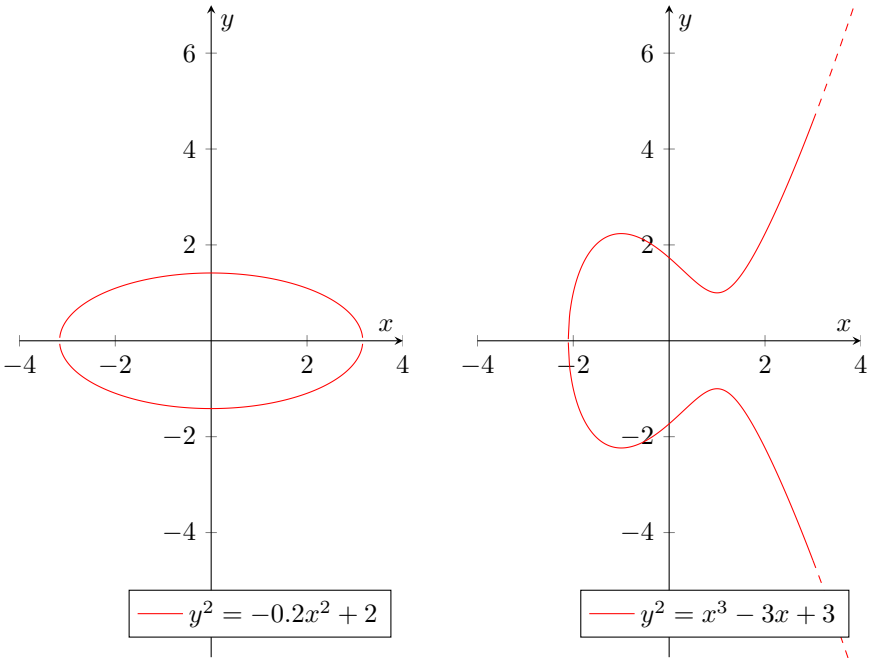
Table 1: Key length comparison in public key and symmetric key algorithm

The bare minimum number of bits is defined by the symmetric key encryption scheme, we cannot have a smaller key with respect to the symmetric case and

have the same level of security; then asymmetric schemes need, in general, a large number of bits to guarantee the same level of security, the fact is that elliptic curves cryptography needs less than $\frac{1}{10}$ of the bits needed for another asymmetric scheme supposed the same level of security, and this relationship become smaller as the level of security grows. Indeed, if one wants to use a public key cryptography scheme, elliptic curves are the suggested choice to guarantee security without using much computational effort.

3 Mathematical background

The base idea besides elliptic curves lies on common calculus background: everyone knows the circumference equation, isn't it? It is $x^2 + y^2 = r^2$, but what if we add coefficients in front of the variables? We end up with an ellipse: $ax^2 + by^2 = r^2$, whose graph can be seen in Fig. 1a.

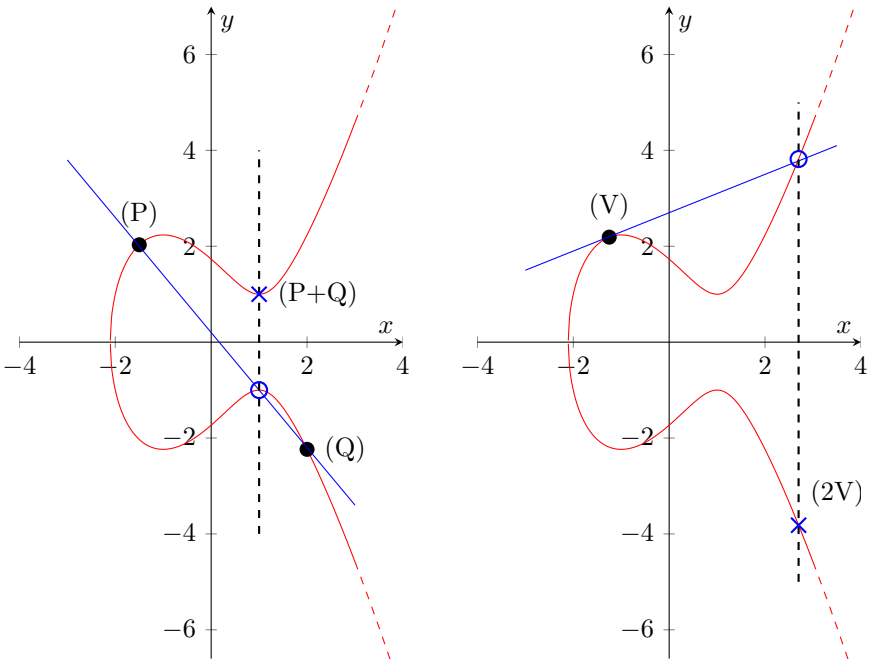


(a) Ellipse (b) Elliptic Curve

Figure 1: Graphical comparison of ellipse and elliptic curve

Well, an elliptic curve is something much similar: the general equation is $y^2 = x^3 + ax + b$, and an example of it can be seen in Fig. 1b. We can easily see from the plot that this family of curves has symmetry with respect to x axis.

In order to perform cryptography with elliptic curves, we need to reduce their usage to a special family of them: instead of defining them over the real domain $\mathbb{R}$, we use the integer group $\mathbb{Z}_p$ (which is a set of integer numbers with a group operator and is closed w.r.t. this operation), with $p > 3$. In addition, the elliptic curve equation is reduced in $\mod p$, and the coefficients must satisfy the following equation to remove useless or too easy to break curves: $4a^3 + 27b^2 \neq 0$. To fulfill the group operation, we need to add an imaginary point at infinity, $\mathcal{O}$. Now that we have defined the elliptic curves of interest, we need to define a group over them, which is the basis of cryptography: in order to fulfill this task, we need a set of elements, which are the points belonging to the elliptic curves, and then we need a group operator to fulfill the group law. It is possible to have both a geometrical and analytical interpretation of this operator; here we start with the geometrical one since it is easier to understand and more explicative. The geometric interpretation starts by drawing the elliptic curve without modulo reduction and defined on $\mathbb{R}$, so we can easily visualize the curve in a 2D graph as those in Fig. 2. The group operation can be divided into 2 simpler case: the addition of two different point and the addition of the same point, called also *doubling*.



(a) Point addition (b) Point doubling

Figure 2: Graphical interpretation of group operator

The first situation is represented in Fig. 2a: we want to sum points P and Q, we draw the secant line passing through this two points, then, due to the particular

form of the elliptic curve, we are able to find a new intersection between the EC and the secant other than the two point to be summed, this new point is highlighted by a circle in the figure, finally this point is mirrored w.r.t. the x axis and the resulting point is the sum between P and Q, and it is denoted by an **x** in the plot.
In the other case, we need to develop something different: since we are adding the same point, we cannot define a secant line, but, if we think at point Q of Fig. 2a and we try to move it along the EC towards V, we easily see that the secant becomes the tangent to the EC in point V as in Fig. 2b. Given this mind set, it is easy to apply the same reasoning as in the previous case: we seek for the intersection between the tangent line and the EC, then project this point mirroring it w.r.t. the x axis and we end up with the point 2V. All this is represented in Fig. 2b.
The geometrical interpretation is fine to visualize the reasoning and the idea, but what if we want to use this mind set in practice? We need to develop an analytical formulation: take the idea in the case of addition, then with doubling it's similar. We start from the EC equation $EC : y^2 = x^3 + ax + b$ and we define the secant passing through points P and Q as $\mathscr{L} : y = sx + m$, whose coefficient can be easily found once we have the values of the two points to be added. We want to find the point to be mirrored, so we solve the system between EC and $\mathscr{L}$, which simply is $s^2x^2 + m^2 + 2smx = x^3 + ax + b$, whose only unknown is the variable x (the other parameters are determined once we have the practical problem). This system admits 3 different solution: two of them are the points to be added and the third one is the point to be added. With some computations, we end up with the addition formula:

$$s = \frac{y_2 - y_1}{x_2 - x_1} \mod p \tag{1}$$

Equation 1 gives us the slope of the secant line. A little extension to this formula: in implementation we use $(y_2 - y_1)(x_2 - x_1)^{-1} \mod p$ since inversion is easier to compute than division (multiplicative inverse can be computed by means of Extended Euclidean Algorithm). Similar reasoning and computation drive us to the formula of the slope in the case of doubling:

$$s = \frac{3x_1^2 + a}{2y_1} \mod p \tag{2}$$

Now we are finishing our journey, but we still need one more thing: to define a group, it is necessary to have a neutral element for the group operator; something such that $P+? = P$. If we understood correctly the addition mechanism, to end in P, we need to obtain a secant whose third intersection point with the EC is the mirror of P w.r.t. the x axis: so we need a vertical secant line, which is obtainable only by using an artificial point defined before as $\mathscr{O}$. This point is not a real point, we just created it to be at $+\infty$ or at $-\infty$ on y axis in order to obtain a vertical secant line. This behavior can be seen in Fig. 3.

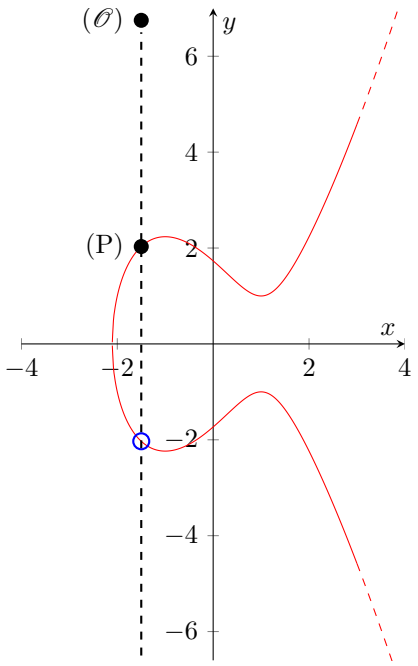


Figure 3: Group operator neutral element

The introduction of $\mathscr{O}$ allows to fulfill two different group properties:

- $P + \mathscr{O} = P \quad \forall P \in EC$
- $P + (-P) = \mathscr{O} \quad \forall P \in EC$

The second property needs some more explanation: $-P$ is the mirror of the point P w.r.t. the x axis, so $-P = (x_p, -y_p)$, where the minus in front of P comes from the group operator, while the minus in front of y_p is the typical minus operation used in $\mathbb{R}$. With these properties the mathematical background comes to an end, we must only add a theorem without proof, which is the following:

Theorem. *The points on an EC, including $\mathscr{O}$, have a cyclic subgroup. Under certain conditions, all points on an EC form a cyclic group.*

This theorem comes in handy when dealing with cryptography, since we need a cyclic subgroup to guarantee that a computation is easy to do in one way but hard to reverse. A cyclic subgroup is such that, if we apply repeatedly the group operation to a generator of the group, we will end up with generator itself after some number of iteration depending on the nature of the cyclic group.

4 Discrete Logarithm Problem with EC

Once we have a cyclic group, it is useful to use it for the Discrete Logarithm Problem (DLP). This idea is also suggested by the previous analysis of tab. 1.

We can synthesize the DLP problem on elliptic curve with the following definition:

Definition. *Given an elliptic curve E, if we consider a generator P of the cyclic subgroup derived from E and another element T, the discrete logarithm problem is finding the integer d, where $1 \leq d \leq \#E$ (where $\#E$ is the cardinality of the cyclic subgroup generated by E), such that $d \cdot P = T$. For $d \cdot P$ it is intended the sum of P by itself d times.*

It is possible to give a geometrical interpretation of the just given definition: we start from the point P on the curve E, and we hop on it d times til we get in point T. Note that T is a point, while d is a integer: that is true for every DLP, no matter what is the cyclic group on which we define the problem. As the DLP has been defined, it is possible to use T as public key, and d as private key. That is due to the nature of the DLP: even if we leave both P and T public, it is difficult to compute the corresponding d if the curve E has been chosen wisely. To correctly choose an elliptic curve, it is necessary to know the cardinality of the cyclic group it generates: thanks to **Hasse's theorem**, it is possible to have a range of the cardinality of the cyclic group, $p+1-2\sqrt{p} \leq \#E \leq p+1+2\sqrt{p}$, where p is the argument of the modulo reduction. The **Hasse's theorem** can be approximated as follows: the cardinality is simply approximated with p, this can be seen in Fig. 4, if p has 160 bits, $\sqrt{p}$ has 80 bits and $2\sqrt{p}$ has 81 bits, when we sum p and $2\sqrt{p}$ we are dealing only with the 81 rightest bit, the least significative, so $2\sqrt{p}$ may seem a huge number, but in comparison with p is just small and we can obtain this approximation.

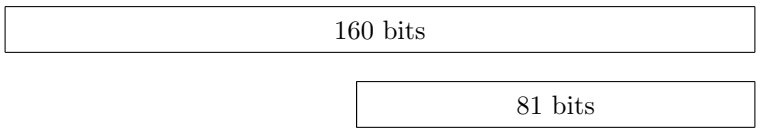


Figure 4: Visualization of Hasse's theorem approximation

In a real implementation, it is necessary to know the exact cardinality of E to avoid specific attacks, so people tends to adopt some standardized elliptic curves, such that specified from NIST or BSI, on these organization websites , it is possible to obtain the parameters a and b and the generator of the cyclic group.
To quantify the security of a well chosen elliptic curve, it is possible to say that the best known algorithm to compute the DLP on elliptic curves requires approximately $\sqrt{p}$ steps, so if we use 192 or 256 bits, an attacker needs 2^{96} or 2^{128} steps respectively.

5 Use of Elliptic Curves in Cryptography

One of the first use of EC in cryptography is to perform Diffie-Helman key exchange, the algorithm is the same as for another cyclic group, so in this case

we define it over elliptic curves but it resembles DH defined in the case of DLP on $\mathbb{Z}_p^*$.
This protocol can be divided into two major phases:

1. The two interlocutors chose the common elliptic curve $E : y^2 = x^3 + ax + b \mod p$ and the primitive element $P = (X_p, Y_p)$
2. TODO

(a) Core (b) Preprocessing

Figure 5: Mix columns base functions

6 Conclusion