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.

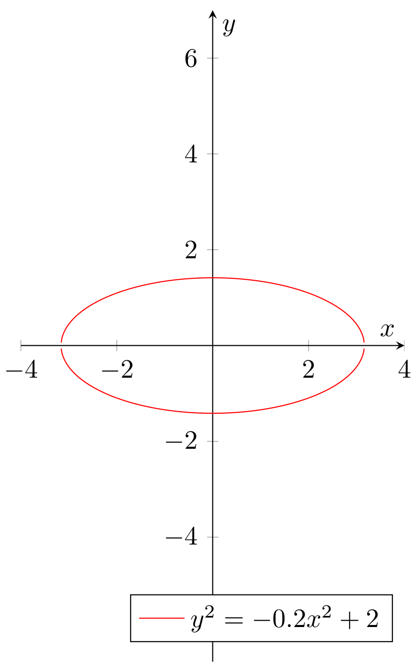
Algorithm Family	Cryptosystems	Security Level (bit)			
		80	128	192	256
Integer Factorization	RSA	1024	3072	7680	15360
Discrete Logarithm	DH, DSA, Elgamal	1024	3072	7680	15360
Elliptic Curves	ECDH, ECDSA	160	256	384	512
Symmetric key	AES, 3DES	80	128	192	256

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

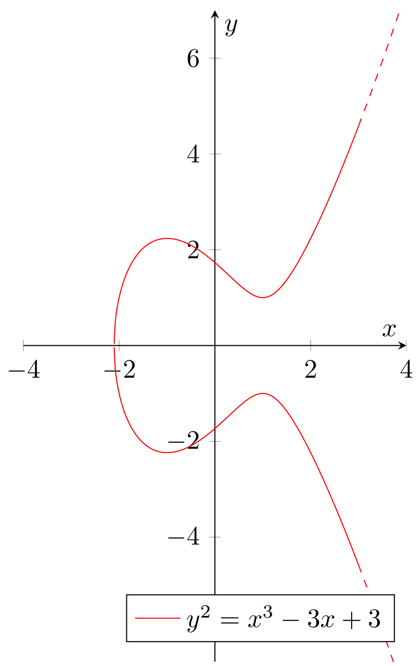
The bare minimum number of bits is defined by the symmetric key encryption scheme, we cannot have a smaller key with respect to the symmetric case and have the same level of security; then asymmetric schemes need, in general, a large number of bits to guarantee the same level of security, the fact is 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

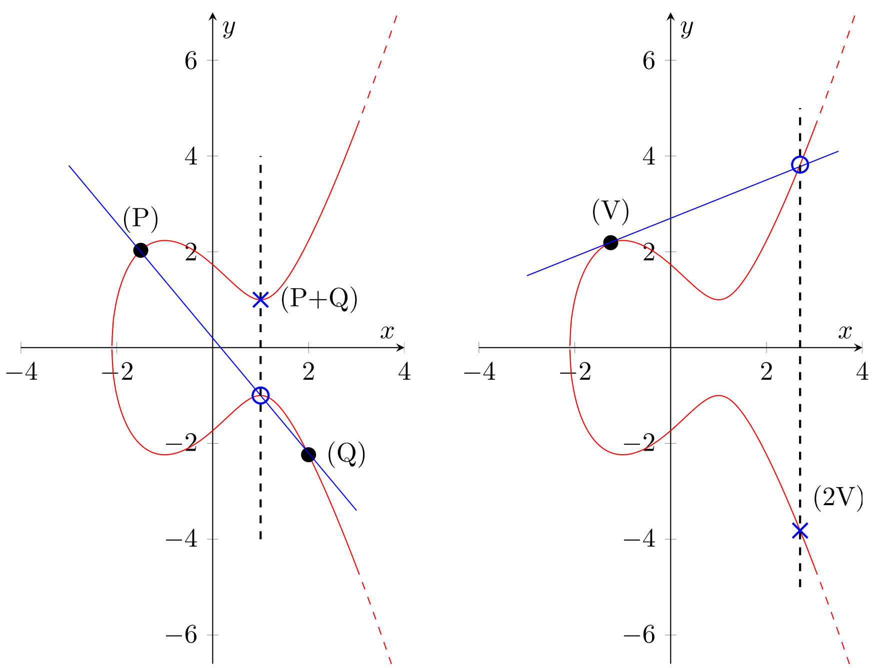


(b) Elliptic Curve

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 $modp$, and the coefficient 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, $\mathscr{O}$.
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 analytical interpretation of this operator; here we start with the geometrical one since it is easier to understand and more explicative.



(a) Point addition (b) Point doubling

Figure 2: Graphical interpretation of group operator

4 Discrete Logarithm Problem with Elliptic Curves

(a) Core (b) Preprocessing

Figure 3: Mix columns base functions

5 Use of Elliptic Curves in Cryptography

6 Conclusion