Elliptic curves cryptography

— **Slide 1** : Hello everyone, let me introduce myself quickly. I'm Yann-Arby, I'm studying a master degree in mathematics at the University of Picardie Jules Verne. Today, I'll speak about elliptic curves and their application in cryptography. It's a 10 min presentation so please bear with me until the end to ask any question you might have during my speech. So let's just dive into it.

— **Slide 2** : Through this beamer my motivation is to answer the following questions.

They are about today's topic which is about the group of rationals points of an elliptic curve defined over a field K.

In fact, Elliptic curves are today's trend in cryptography. It's broadly use in signature authentication and key sharing protocol.

Therefore, I'd like to show you the underlying mechanism of its construction in order to give an example of one of the most use key sharing protocol which is know as the Diffie-Hellman protocol.

— **Slide 3** : In this presentation

- I'll answer the first question in section 2 and 3.
- Then I'll describe the construction of the group in section 4.
- After that I'll explain why it works and give an application in section 5 and 6.
- Finally I'll give the cons and pros of the model in section 7.

— **Slide 3** : The study of the group of rationals points of an elliptic curve, aimed towards its application in cryptography, was made in parallel between N. Koblitz and Victor S. Miller in 1985.

— **Slide 4** : To lay the foundation of the group we'd like to build. We need a couple of tools. Such as :

- The projective plane

  Indeed as we'll see by definitions elliptic curves are projective geometry's objects.
- The projective lines

  To understand projective plane we need to understand projective lines as they are what generates the projective plane.
- Straight and tangent lines

  That's the two lines that we will need to understand in order to treat each case we would stumble upon studying the binary operation of the group $(E, +)$.
- The rationals points

  They will be the elements of our group. Thanks to them we can compute additions and doubles. Which is the heart of our construction.

— **Slide 5** : The projective plane is a quotient-set define over a vector space without its origin, and define by an equivalence relation which let two vectors be the same if there are on the same line.

More precisely the projective plane is the reunion between the affine plane and the infinity line.

The affine plane is generated by the projective line. We can see an example of a projective line on the figure 2.

The red line is the projective line which is generated by the intersection between each vectors lines of the vector space and in this case the line $y = 1$.

— **Slide 6** : Over the vector space $\mathbb{R}^3$ we can see the projective line as the line that generates the affine plane. As we can see in the following figure 3.

Here the red plane is the projective line which is generated by the intersection between every vectors of the vector space and the plane of equation $z = 1$.

— **Slide 7** : So to resume what I've said since the beginning, the projective plane is a sphere where we cut a slice, in general at $z = 1$ and the plane we get is our affine slice which is a circle. Therefore thanks to the equivalence relation and limits, we have that the infinity point $\mathcal{O}$ is the intersection of every vertical line of the affine slice and the y-intercept. Henceforth $\mathcal{O}$ is the neutral element of the group.

— **Slide 8** : Here is the definition of elliptic curves.

The condition 2 guaranty us that our curve is smooth which simply means that there is only one tangent per point.

On the figure 5 we can see a representation of an elliptic curve on the affine slice where the discriminant is negative hence there is only one roots.

— **Slide 9** : The Weierstrass normal equation give use elliptic curves that are symmetric around the x-intercept.

By definition rationals points of an elliptic curves are the projective points that are solutions of the Weierstrass normal equation.

Here is the coordinates of the infinity point $\mathcal{O}$.

— **Slide 10** : To build our abelian binary operation, which we'll call addition henceforth.

First thing first we need to look what will happen when you take the chords between to points of the curve or the tangent of a point ? While asking ourselves are these lines always give us a third point on the curve. The answer is yes thanks to the projective plane and the infinity point.

Therefore thanks to this non associative binary operation we have the foundation to build the addition that we're looking for.

— **Slide 11** : Here is the addition that we obtain thanks to a smart symmetry. Indeed if we take the opposite of the point we've obtained through our non associative binary operation. We obtain the result of the addition between two points of the group.

— **Slide 12** : Modern cryptography's foundation are build upon a tested hypothesis and others assumptions which are still holding today.

In our case their is the following assumptions that are important :

- One-way functions exist and the addition, we've built, is one of them.
- The discrete logarithm problem is unsolvable in a polynomial time.
- There is no other way to solve Diffie-Hellman's problem without solving the discrete logarithm problem.

— **Slide 13** : Here is the Diffie-Hellman protocol which is the basis of today's online transaction.

Two person Alice and Bob would like to share a secret key publicly. Hence they proceed as followed :

- They choose a finite field K, an elliptic curve E and a base point P and publish this triplet.
- Then they both chose a secret integer and compute this integer times the base point. Then they respectively send their result to the other.
- Lastly they compute again their secret integer times what they've received. Which give them their secret key.

Hence the Diffie-Hellman protocol is a secure way to share a key publicly.

— **Slide 14** : The group of rationals point of an elliptic curve have many benefits compared to the multiplicative group of the invertible of a finite field K. Among them there is :

- The structure is more abstract.
- The keys' length is way shorter for equivalent security.
- It can be use on low resources systems.
- It can be implemented in an hybrid cryptosystem which is the combination between a symmetric cryptosystem to encrypt data and an asymmetric cryptosystem to share secret key.

However, as anything else there is restriction. For example :

- There is already a lot of patent rights own by companies.
- There is always hazard and in our case if the triplet we use is not properly, efficiently and randomly selected there is the risk or back door as the alleged claim of NSA using such a method.

Which let's me conclude with the following statement ...

Thank you everyone for your attention. My presentation is done and now is question time.

Table 1 – Assessment grid

voc-graph	
voc-your-field-of-research	
Gram-com/sup	
Gram-questions	
Gram-passive	
Gram-quantity	
Syntax-link-words	
Syntax-condition and complex-sentences	
Word **stress**	