elliptic curves crytography

- **Slide 1** : Hello everyone, let me introduce myself quicky. 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 I'd like to answer the following questions.

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

  In fact, elliptic curves are today's trend in crytography. They are broadly use in signature authentification 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 used key sharing protocol which is known 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.
  - Finaly in section 5, I'll explain why it works, then I'll give an application and conclude by giving a few upsides and downsides of the theory.
- **Slide 3** : So first thing first, the study of the group of rational points of an elliptic curve, aimed towards its application in crytography, was made in parallel between N. Koblitz and Victor S. Miller and was published 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.
  - Then we need to understand projective lines in order to understand the projective plane because they are what generate the projective plane.
  - The next tools we need are straight and tangent lines. They are the two lines that we need to understand in order to treat each case we would stumble upon studying the abelian binary operation of the group.
  - Finaly the last tool is the rational 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 defined over a vector space without its origin, and 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 vector lines of the vector space and in this case the line $y = 1$.
- **Slide 6** : So to resume what I've said since the beginning, the projective plane is a sphere of radius one where we cut a slice of the vector space on top of it, in general at $z = 1$. Therefore the projection of the sphere on this plane gives us the affine slice which is a circle. Moreover thanks to the equivalence relation and limits, we have that the infinity point is the intersection of every vertical line of the affine slice and the y-intercept which is the perimeter of the circle. Henceforth the infinity point is the neutral element of the group.
- **Slide 7** : 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 thus there is only one root.
- **Slide 8** : The Weierstrass normal equation give use elliptic curve that are symmetric around the x-intercept.

  Besides by definition rational points of an elliptic curve are the projective points that are solutions of the Weierstrass normal equation.

  Here are the coordinates of the infinity point.
- **Slide 9** : So to build our abelian binary operation, which we'll call addition henceforth.

  We first need to look what will happen when we take the chord between two points of the curve or the tangent of a point ? Are these lines always giving us a third point on the curve ? The answer is yes thanks to the projective plane and the infinity point.

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

- **Slide 10** : 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 11** : Modern crytography's foundation are built upon a tested hypothesis and other assumptions which are still holding today.

  In our case there 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 12** : 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, a base point P and publish this triplet.
  - Then they both choose 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 shared secret key.

  Hence the Diffie-Hellman protocol is a secure way to share a key publicly.
- **Slide 13** : The group of rational points 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 that is way more abstract.
  - The keys' length is way shorter for equivalent security compared to RSA.
  - It can be use on low resource 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 always downsides. For example :
  - There is already a lot of curves patented by companies.
  - There is always hazard which in our case comes from the triplet which is chosen by Alice and Bob. If the triplet isn't properly, efficiently and randomly selected, there is the risk of a premeditated use of back doors.

Which let's me conclude with the following statement of Serge Lang in his book *Elliptic curve : Diophantine analysis*, which was published in 1978 :

> "It is possible to write endlessly on elliptic curves. (This is not a threat)"

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

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**	