

# Elliptic curves cryptography

Yann-Arby Bebba

Université Picardie Jules Verne

*yann-arby.bebba@etud.u-picardie.fr*

June 22, 2022

# Introduction

- What do we need to construct the group ?
- How to construct the group ?
- What are its application in cryptography ?
- Why it works ?
- What are the cons and pros ?

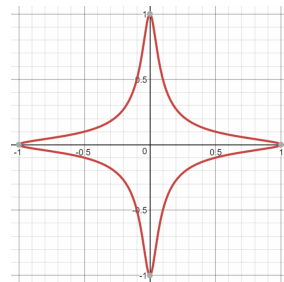


Figure 1: Edwards' Curve :  
 $x^2 + y^2 = 1 + 300x^2y^2$

- 1 Introduction
  - Research papers
  - Tools
- 2 Projective Geometry
  - Projective plane
  - Projective plane and infinity point
- 3 Elliptic curves
  - Elliptic curves' definition
  - Rationals points
- 4  $(E,+)$  group
  - Non associative binary operation
  - $(E,+)$  abelian binary operation
- 5 Application
  - The discrete logarithm problem
  - Public key-sharing protocol
  - Elliptic curves' pros and cons
- 6 References

- Neal Koblitz, *Elliptic curve cryptosystems*, 1985 [4]
- Victor S. Miller, *Use of elliptic curve in cryptography*, 1985 [6]



Neal Koblitz



Victor Saul Miller

# The tools to build $(E, +)$

- Projective plane
- Projective lines
- Straight and tangent lines
- Rationals points

# Projective plane

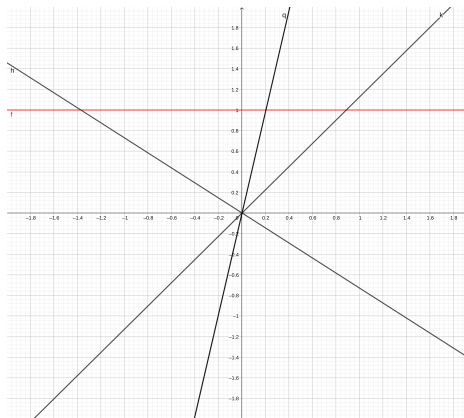


Figure 2: Projective line in red

# Affine slice of the projective plan and the infinity point

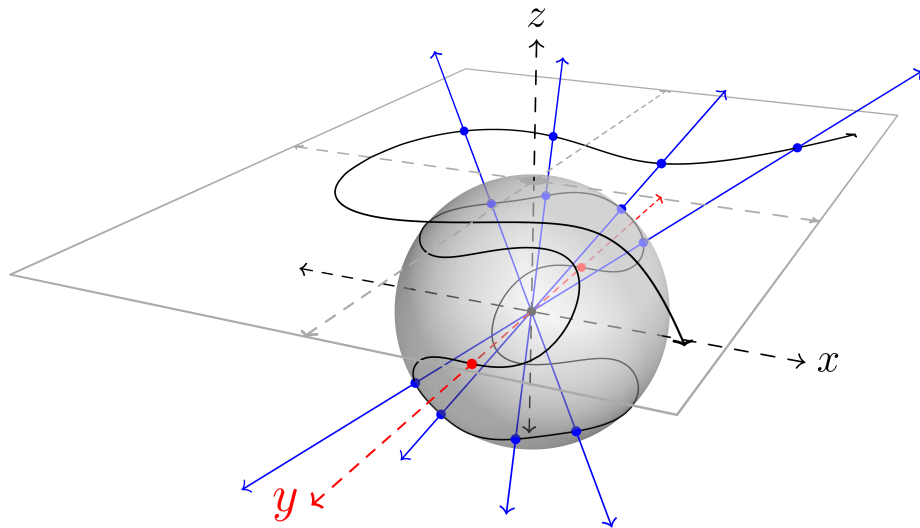


Figure 3: Elliptic curve of equation  $y^2 = x^3 - x + 1$  on the projective plane

## Definition

An elliptic curve define over a field  $K$  is a projective plane curve where its homogeneous equation is

$$y^2z = x^3 + axz^2 + bz^3, \quad (1)$$

where  $a$  and  $b$  are elements of  $K$  which verify the following condition

$$\Delta = -(4a^3 + 27b^2) \neq 0. \quad (2)$$

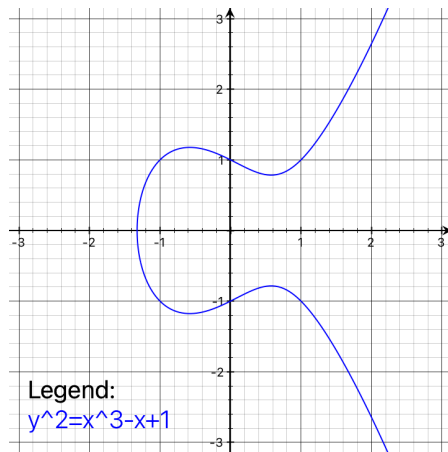


Figure 4: canonical curves with  $\Delta < 0$



# Weierstrass normal equation and rational points

- Weierstrass normal equation

$$y^2 = x^3 + ax + b,$$

- Rational points set

$$E(K) = \{P \in \mathbb{P}_2 \mid y^2 = x^3 + ax + b\} \cup \{\mathcal{O}\}$$

- Infinity point

$$\mathcal{O} = [0, 1, 0].$$

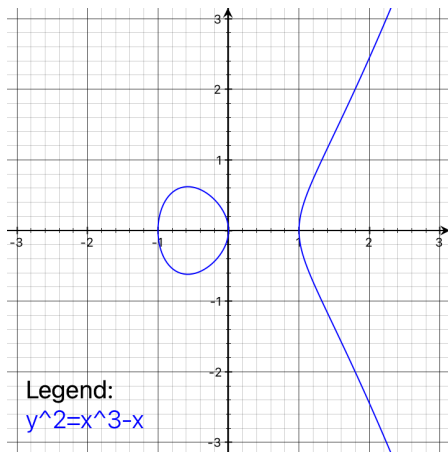


Figure 5: canonical curves with  $\Delta > 0$

# Non associative binary operation

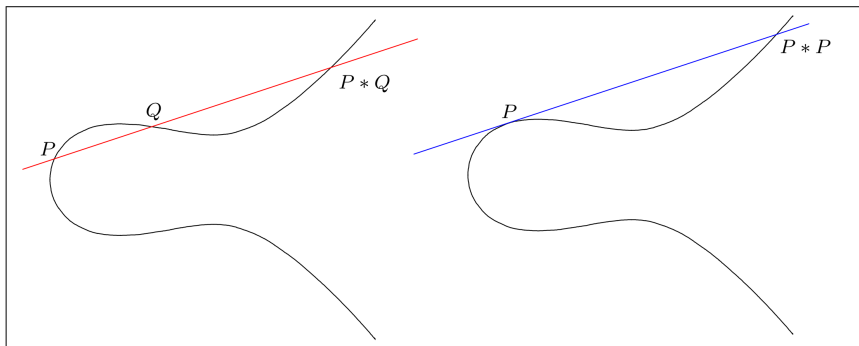


Figure 6: binary operation of chords and tangent of the curve

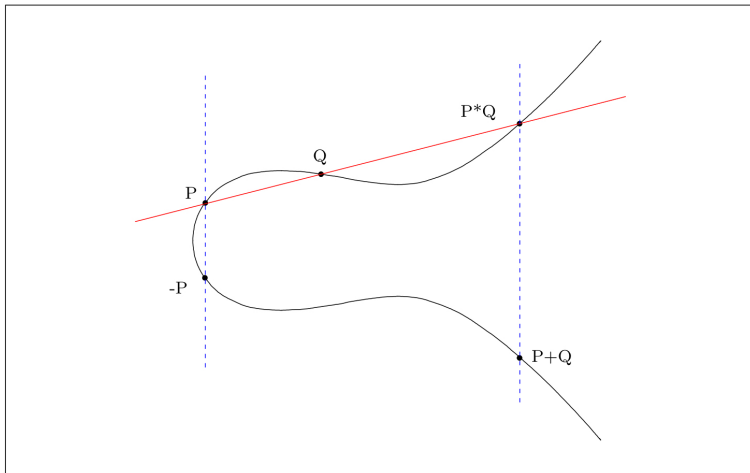


Figure 7: Geometric representation of rational points' addition

## The problem of discrete logarithm

Let  $E$  be an elliptic curve define over a field  $K$ .

Let  $Q \in E(K)$  be a rational point.

Given a rational point  $P \in E(K)$ , the discrete logarithm problem is to find  $n \in \mathbb{N}$ , if its exists, such as  $P = nQ$ .

Why it works:

- One-way functions exist.
- Unsolvability of the logarithm problem.
- No other way to solve the Diffie-Hellman's problem.

## Diffie-Hellman protocol

Alice and Bob would like to share a secret key (i.e. know only by them) over a non-secure channel.

To do this they proceed the following way:

- 1) They choose and publish the triplet  $(K, E, P)$ .
- 2) Alice choose  $a > 0$  and compute  $P_a = aP$ , which she sends to Bob.
- 3) Bob  $b > 0$  and compute  $P_b = bP$ , which she sends to Bob.
- 4) Alice and Bob compute  $aP_b$  and  $bP_a$  which give  $P_{ab}$ .

## Pros

- Abstract structure.
- Shorter secret key length.
- Low ressources usage.
- Hybrid cryptosystem compatibility.

## Cons

- Many are patented
- Build-in trap doors? [3] [2]

The following is a statement of Serge Lang in his book

*Elliptic curve: Diophantine analysis*, 1978 [5]:

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

Pictures sources:

- Trustica.cz [7].
- Stackexchange forum [9].
- allaboutcircuits.com [1]
- Alchetron.com [8]

- [1] Dr. Neal Koblitz: *Independent Co-creator of Elliptic Curve Cryptography* - News. URL: <https://www.allaboutcircuits.com/news/dr.-neal-koblitz-independent-co-creator-of-elliptic-curve-cryptography/> (visited on 06/20/2022).
- [2] Dan Goodin. *We don't enable backdoors in our crypto products, RSA tells customers*. Ars Technica. Sept. 20, 2013. URL: <https://arstechnica.com/information-technology/2013/09/we-dont-enable-backdoors-in-our-crypto-products-rsa-tells-customers/> (visited on 06/21/2022).
- [3] *How the NSA (may have) put a backdoor in RSA's cryptography: A technical primer*. The Cloudflare Blog. Jan. 6, 2014. URL: <http://blog.cloudflare.com/how-the-nsa-may-have-put-a-backdoor-in-rsas-cryptography-a-technical-primer/> (visited on 06/21/2022).
- [4] Neal Koblitz. *Elliptic curve cryptosystems*. 1985. URL: <https://www.ams.org/journals/mcom/1987-48-177/S0025-5718-1987-0866109-5/S0025-5718-1987-0866109-5.pdf>.
- [5] Serge Lang (auth.) *Elliptic Curves: Diophantine Analysis*. 1st ed. Grundlehren der mathematischen Wissenschaften 231. Springer-Verlag Berlin Heidelberg, 1978. ISBN: 978-3-642-05717-5. (Visited on 06/20/2022).



- [6] Victor S. Miller. *Use of elliptic curves in cryptography*. Lecture Notes in Computer Science. Vol. 218. Springer, 1985. URL: <https://web.archive.org/web/20090206165338/http://dsns.csie.nctu.edu.tw/research/crypto/HTML/PDF/C85/417.PDF> (visited on 06/16/2022).
- [7] Trustica » *Elliptic curves: point at infinity revisited*. URL: <https://trustica.cz/en/2018/04/05/elliptic-curves-point-at-infinity-revisited/> (visited on 06/16/2022).
- [8] Name Victor Miller Role Mathematician Education Harvard University and Columbia University. *Victor S Miller - Alchetron, The Free Social Encyclopedia*. Alchetron.com. Aug. 18, 2017. URL: <https://alchetron.com/Victor-S-Miller> (visited on 06/20/2022).
- [9] Iñaki Viggers. *In Elliptic Curve, what does the point at infinity look like?* Cryptography Stack Exchange. May 13, 2019. URL: <https://crypto.stackexchange.com/q/70507> (visited on 06/20/2022).