NORTHERN ARIZONA UNIVERSITY®

INF 638
Cryptography & Cryptosystems

Section 9 ECC Key Distribution

Dr. Bertrand Cambou
Professor of Practice NAU, Cybersecurity
School of Informatics, Computing, and Cyber-Systems
Bertrand.cambou@nau.edu

NORTHERN ARIZONA UNIVERSITY

INF 638: Cryptography & Cryptosystems

- 1- Motivation & Definitions
- 2- Elements of Number theory
- 3- Early Cryptographic methods
- 4- Symmetrical Cryptography: DES
- 5- Symmetrical Cryptography: AES
- 6- Quantum Cryptography: Key distribution
- 7- Elements of Asymmetrical Cryptography
- 8- Asymmetrical Cryptography: RSA
- 9- ECC Key Distribution
- 10- PKI & Digital Signatures
- 11- Hash Functions
- 12- Smartcards

Elliptic Curves (ECC): Motivation

Symmetric Key Size (bits)	RSA and Diffie-Hellman Key Size (bits)	Elliptic Curve Key Size (bits)
80	1024	160
112	2048	224
128	3072	256
192	7680	384
256	15360	521

Table 1: NIST Recommended Key Sizes

- **RSA** needs long keys compared with symmetrical cryptography for the same protection

  For example the equivalent of 128 long key in AES require 3,072 long key in RSA

- **ECC** is an asymmetrical cryptography acting with a "square root" efficiency

  For example the equivalent of 128 long key in AES require only 256 long key in ECC

Note: the number of computing cycles needed to break a 128 bit long AES is 2^{128} = 3.4 10^{38}

The equivalent efficiency of ECC is "only" $\sqrt{2^{256}} = 2^{256/2} = 2^{128}$

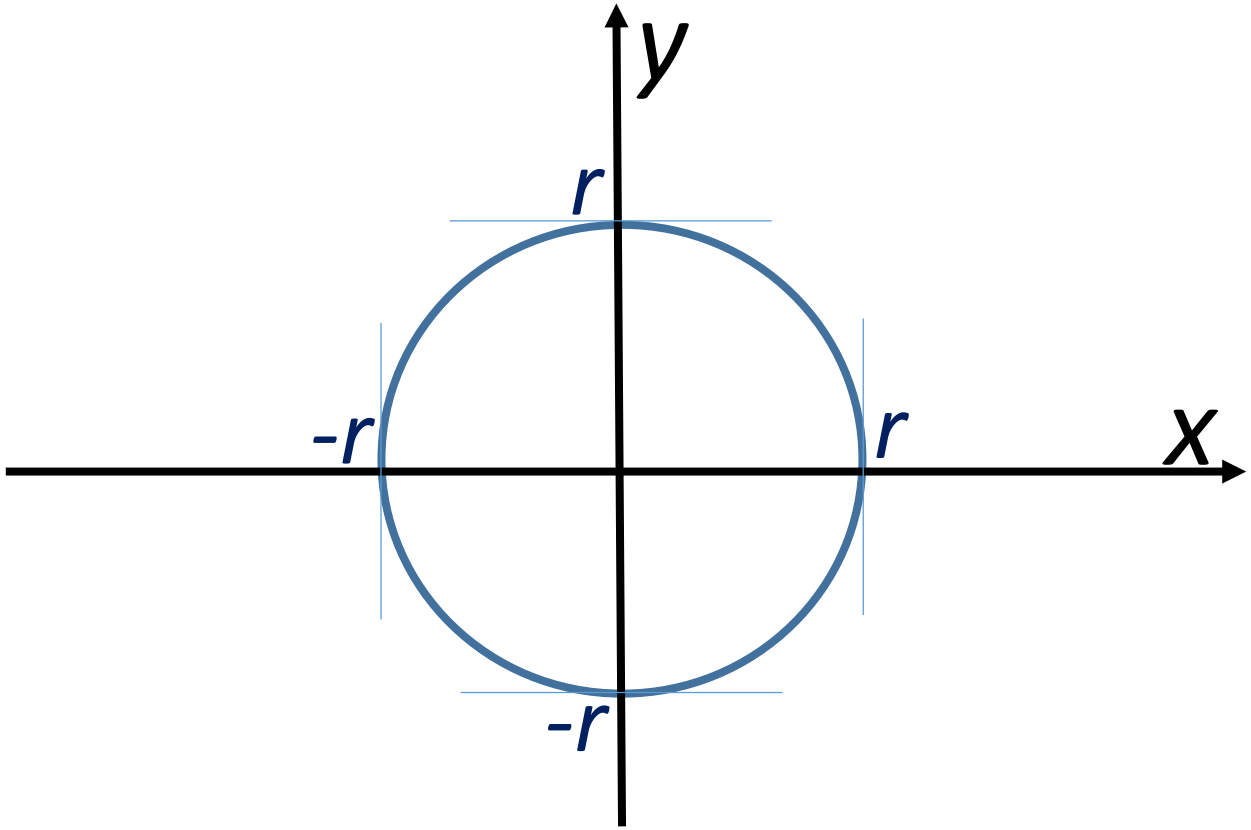
NORTHERN ARIZONA UNIVERSITY

9- Elliptic Curve Cryptography (ECC)

- 9-1 Elliptic curve: number theory
  - Elliptic curves
  - circular finite groups
  - Arithmetic of finite group
- 9-2 Key distribution with ECC
- 9-3 ECC with extended Galois field

Example of Elliptic Curves (EC): the circle

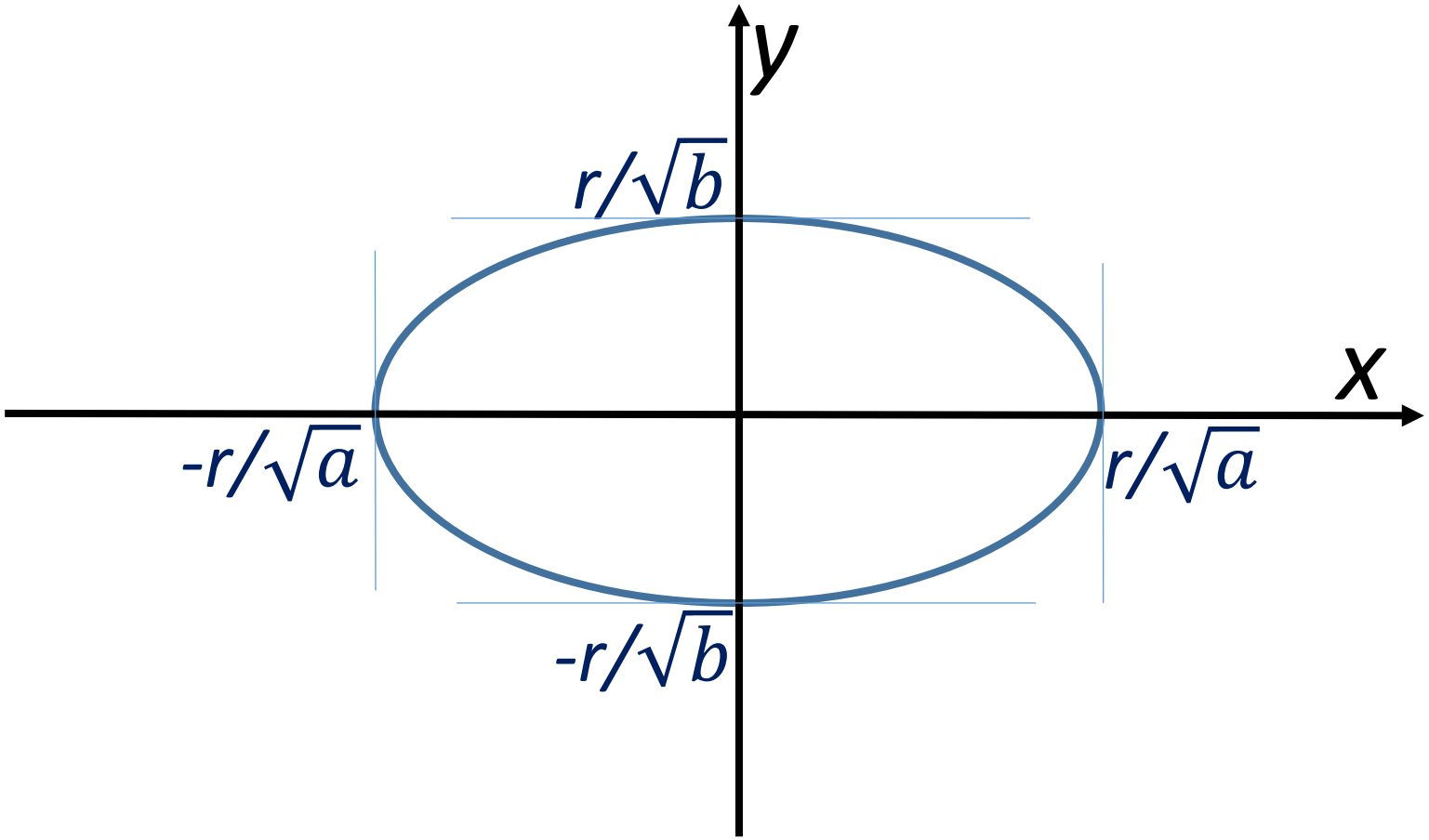
All pairs (x, y) ϵ $\mathbb{R}$ verifying: $x^2 + y^2 = r^2$



Example of Elliptic Curves (EC): the ellipse

All pairs (x, y) ϵ $\mathbb{R}$; a and b >0

verifying: $ax^2 + by^2 = r^2$

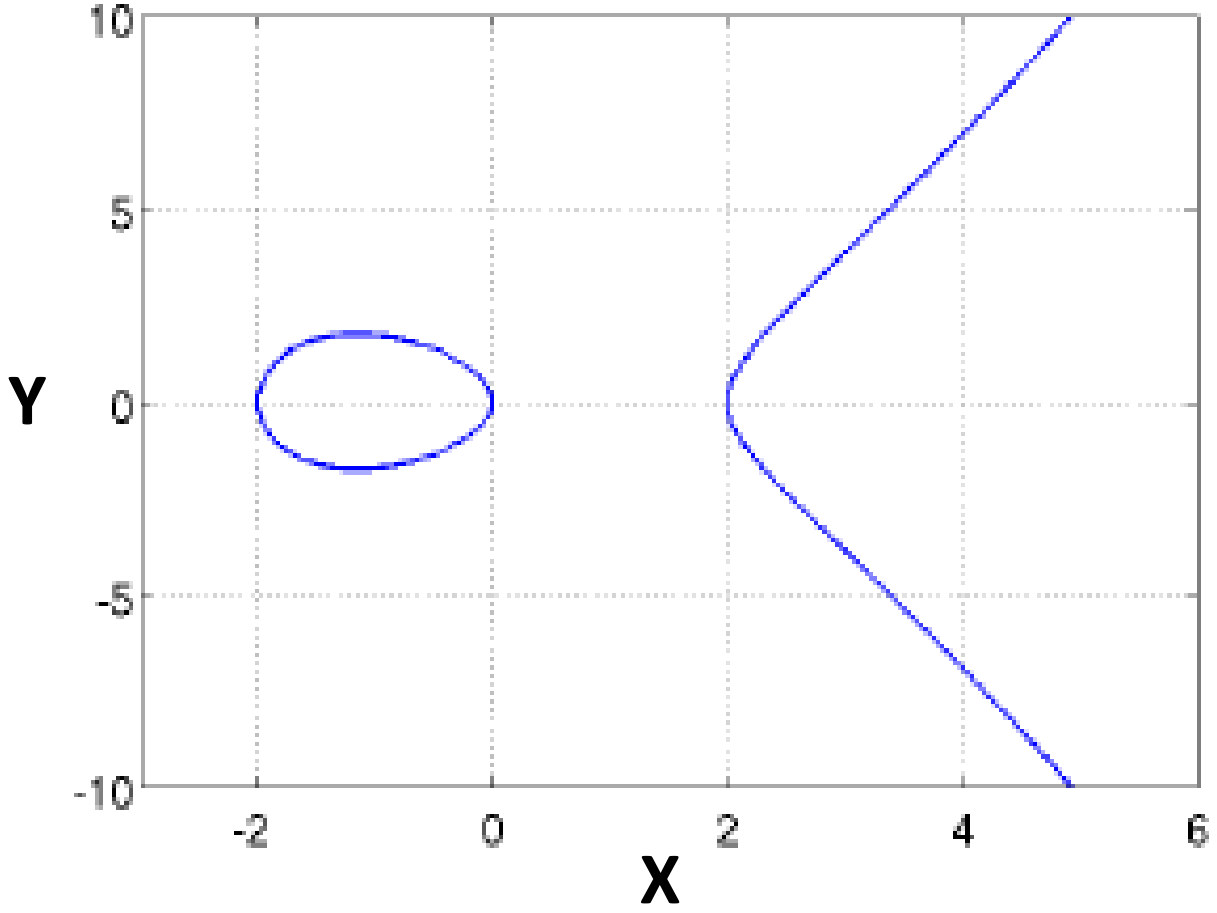


Elliptic Curves (EC) for cryptography

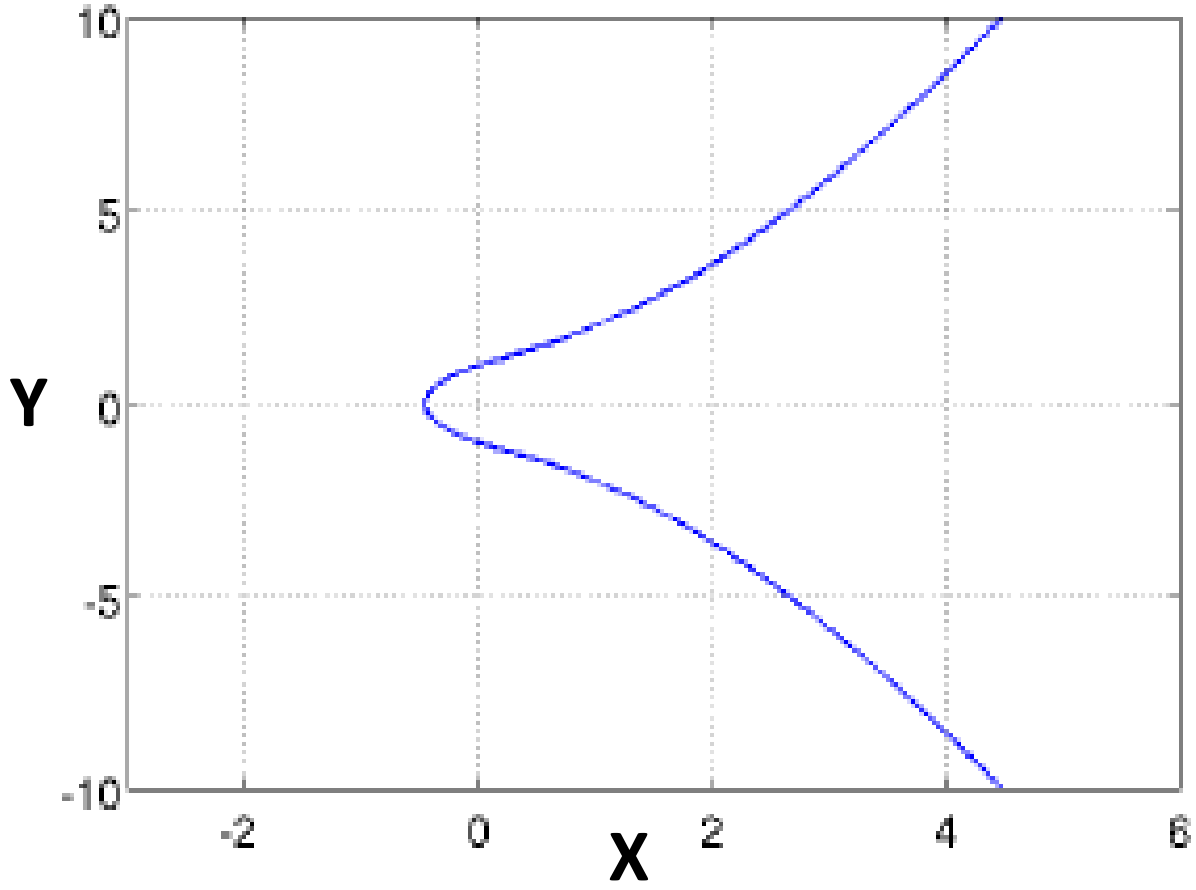
The set of all integer pairs (x, y, a, b) ϵ $\mathbb{Z}$ verifying: $y^2 = x^3 + a \cdot x + b$

(These elliptic curves are symmetric with the x axes: y_i and -y_i have the same x_i)

$y^2 = x^3 - 4 \cdot x + 0$



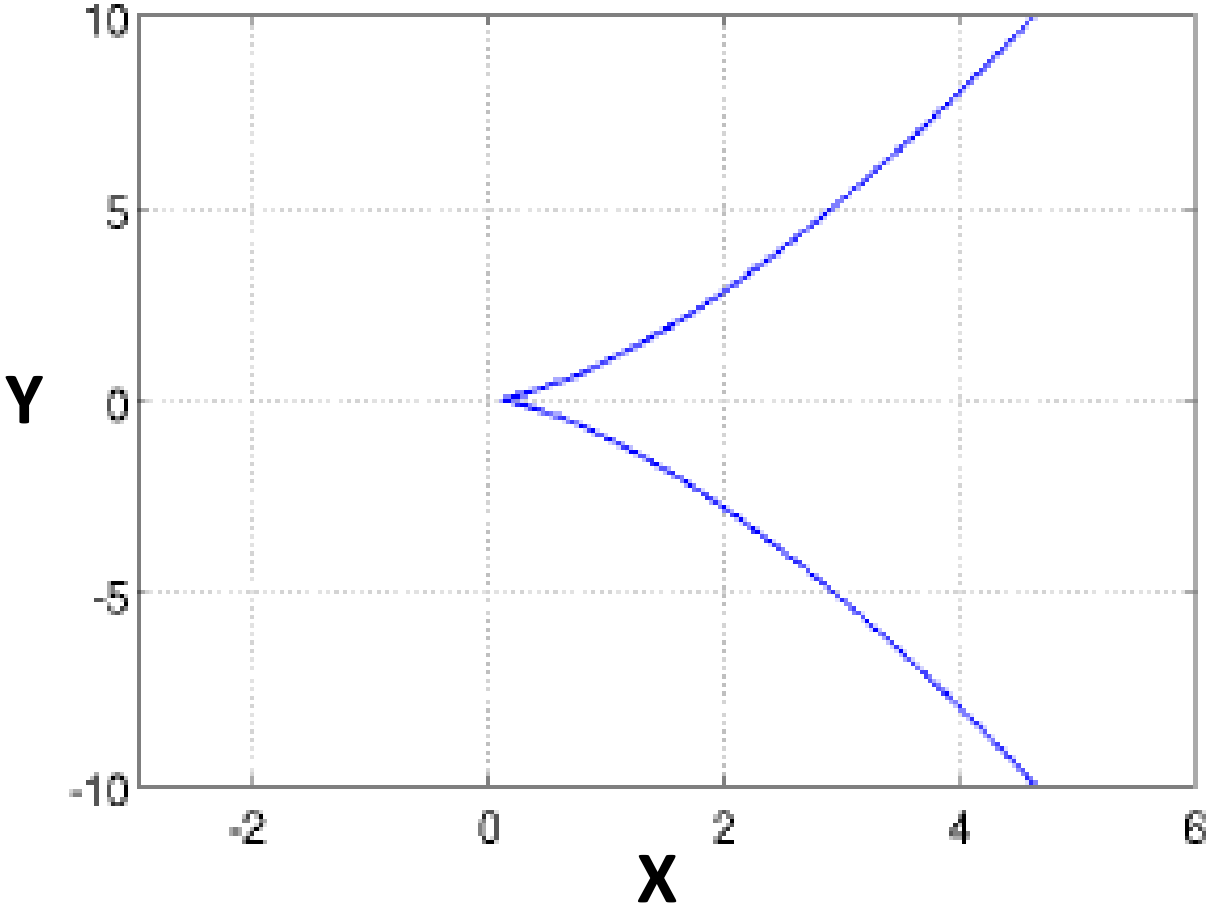
$y^2 = x^3 + 2 \cdot x + 1$



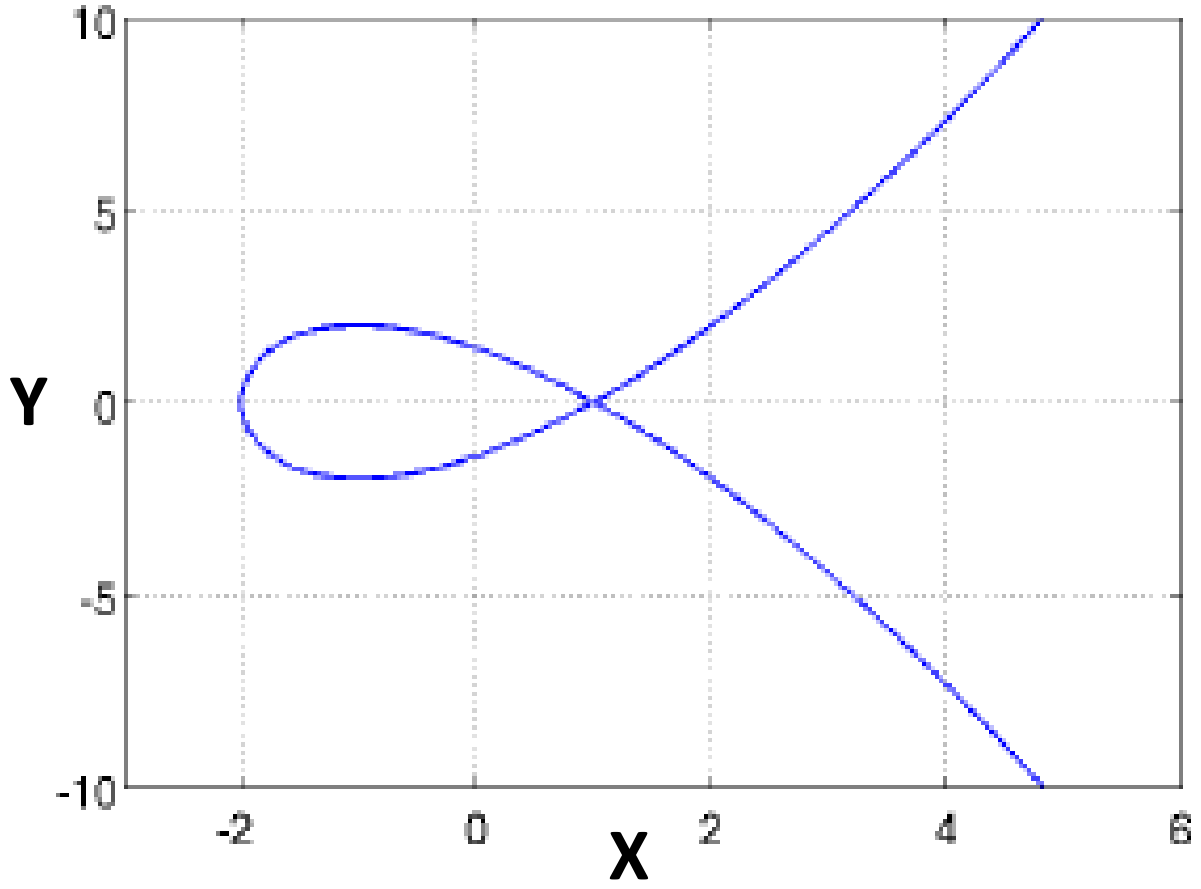
Elliptic Curves (EC) for cryptography

Other examples:

$y^2 = x^3 + 0 \cdot x + 0$



$y^2 = x^3 - 3 \cdot x + 2$



NORTHERN ARIZONA UNIVERSITY

Elliptic Curve Cryptography (ECC)

- 1- Elliptic curve: number theory
  - Elliptic curves
  - circular finite groups
  - Arithmetic of finite group
- 2- Key distribution with ECC
- 3- ECC with extended Galois field

Definition of a circular finite ECC group G

The ECC group G is based on the modular group $\mathbb{Z}_m$

(m>3) is the set of all integer pairs (x, y) ∈ $\mathbb{Z}_m$ verifying:

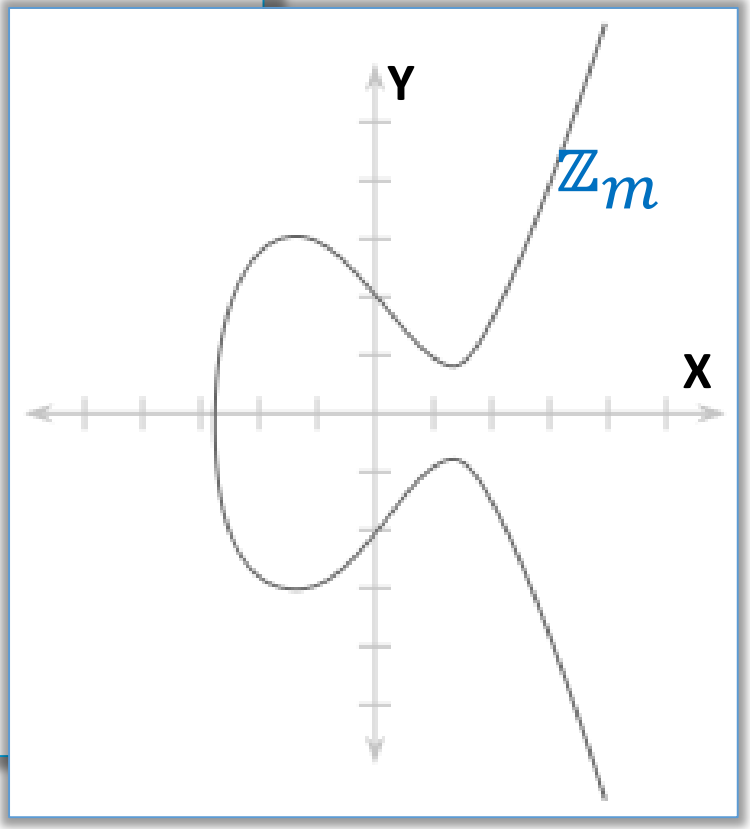
$$y^2 \equiv x^3 + a \,.\, x + b \bmod m$$

a, b ∈ $\mathbb{Z}_m$

$$4 \,.\, a^3 + 27 \,.\, b^2 \neq 0 \bmod m$$

Ex: $y^2 \equiv x^3 - 3 \,.\, x + 3 \bmod m$

The neutral is the point of infinity Θ



General definition the operation •

Group element: a point on the curve (a_x, a_y)

1- Closed:	$a \bullet b = c \in G$	For all $a, b \in G$;
2- Associative:	$a \bullet (b \bullet c) = (a \bullet b) \bullet c$	For all $a, b, c \in G$
3- Commutative:	$a \bullet b = b \bullet a$	For all $a, b \in G$
4-Neutral element Θ ϵ G:	$a \bullet \Theta = \Theta \bullet a = a$	For all $a \in G$
5-Inverse "$-a$" ϵ G:	$a \bullet (-a) = (-a) \bullet a = \Theta$	For all $a \in G$

Arithmetic in the group operation (•) = "+" on ECC

Two elements:

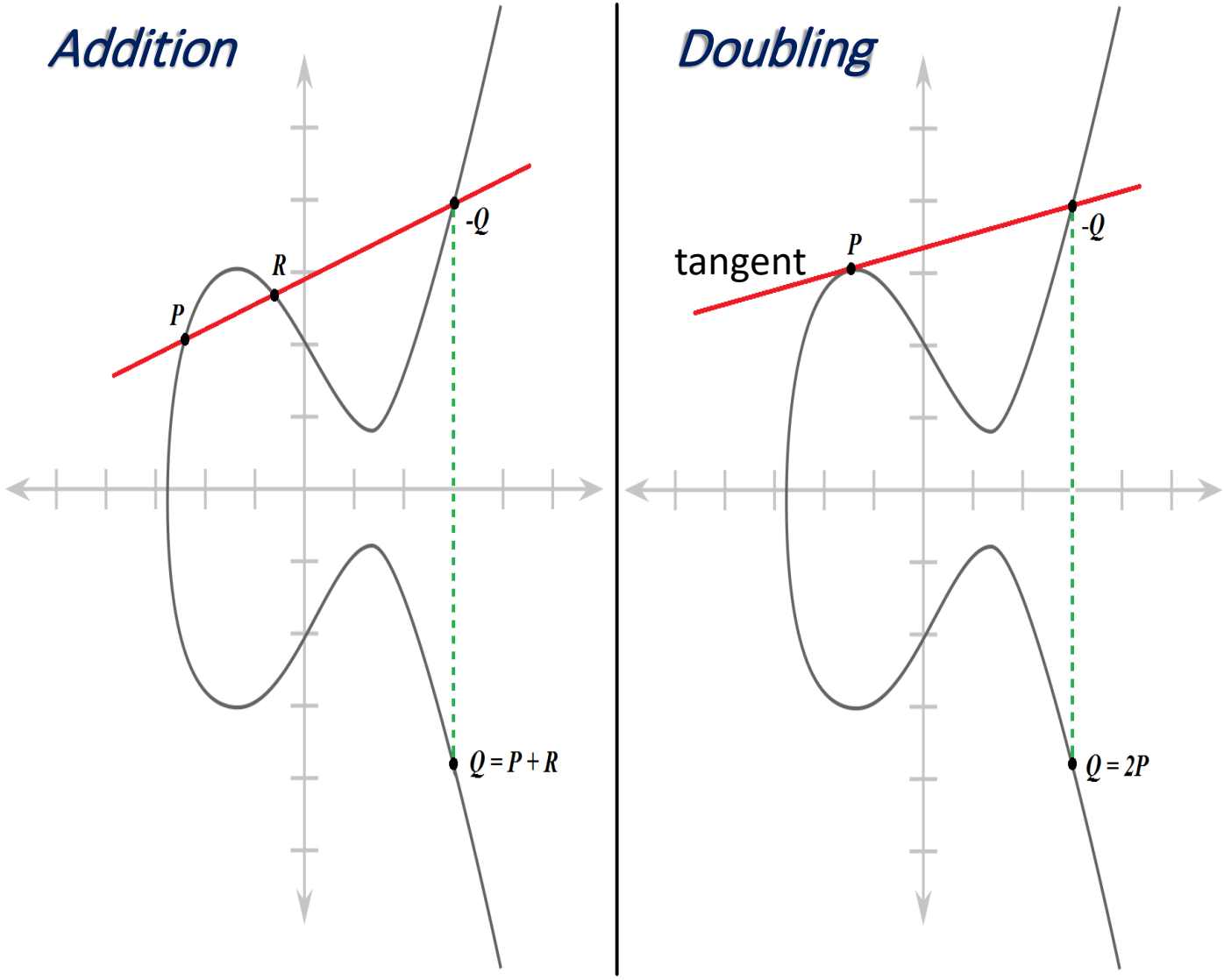
$P(x_1, y_1)$; $R(x_2, y_2) \in G$

Addition:

$P + R = Q$ $\quad Q(x_3, y_3)$

Point doubling:

$P + P = 2P = Q$



Formula: Point addition & doubling

$P = (x_1, y_1)$; $Q = (x_2, y_2)$; $R = (x_3, y_3)$

Point addition & doubling :

$$x_3 \equiv s^2 - x_1 - x_2 \bmod m$$

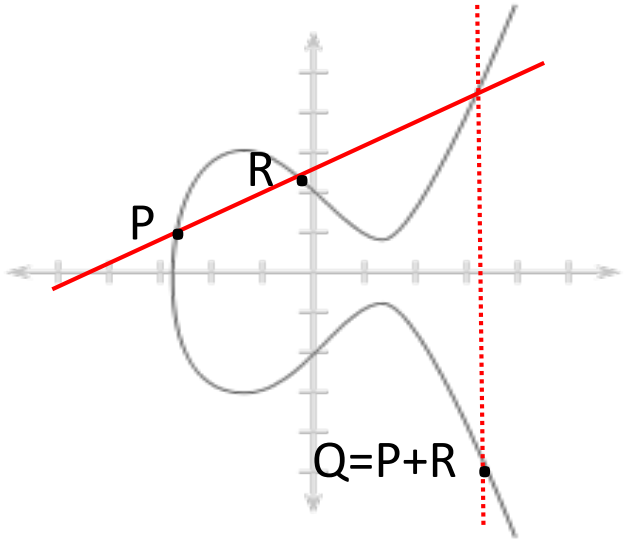
$$y_3 \equiv s\,(x_1 - x_3) - y_1 \bmod m$$

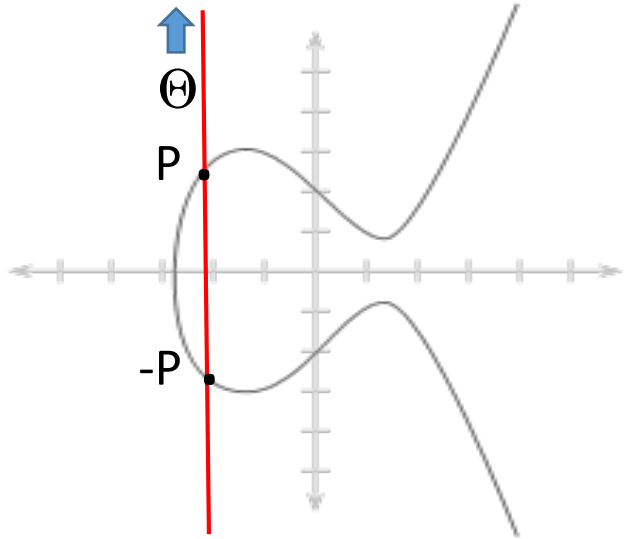
Where:

if $P \neq Q$ addition ➔ $s = (y_2 - y_1)\,(x_2 - x_1)^{-1} \bmod m$

if $P = Q$ doubling ➔ $s = (3x_1^2 + a)\,(2\,y_1)^{-1} \bmod m$

s is the slope of the EC





Neutral: $P + \Theta = P$

Inverse: $P + (-P) = \Theta$

$P = (x_1, y_1)$ => $(-P) = (x_1, -y_1)$

Mathematics behind ECC arithmetic: monic polynomial

Monic polynomials have the upper term at 1:

$$P(x) = x^n + a_{n-1}\, x^{n-1} + \ldots + a_1\, x + a_0$$

Polynomials have up to n roots $r_n\,; r_{n-1}; \ldots; r_1$

$$P(x) = (x - r_n)(x - r_{n-1}) \ldots (x - r_1)$$

$$a_{n-1} = -(r_n + r_{n-1} + \cdots + r_1)$$

Example of polynomial with n=3:

$$P(x) = x^3 + a_2\, x^2 + a_1\, x + a_0$$

Mathematics behind point addition

The points are part of the strait line:

$y = \alpha x + \beta$ $\alpha = s = (y_2 - y_1)/(x_2 - x_1)$

$s = (-y_3 - y_1)/(x_3 - x_1)$

Extract y_3:

$y_3 + y_1 = s\,(x_1 - x_3)$ ➔ $y_3 = s(x_1 - x_3) - y_1$

Construction of the monic polynomial:

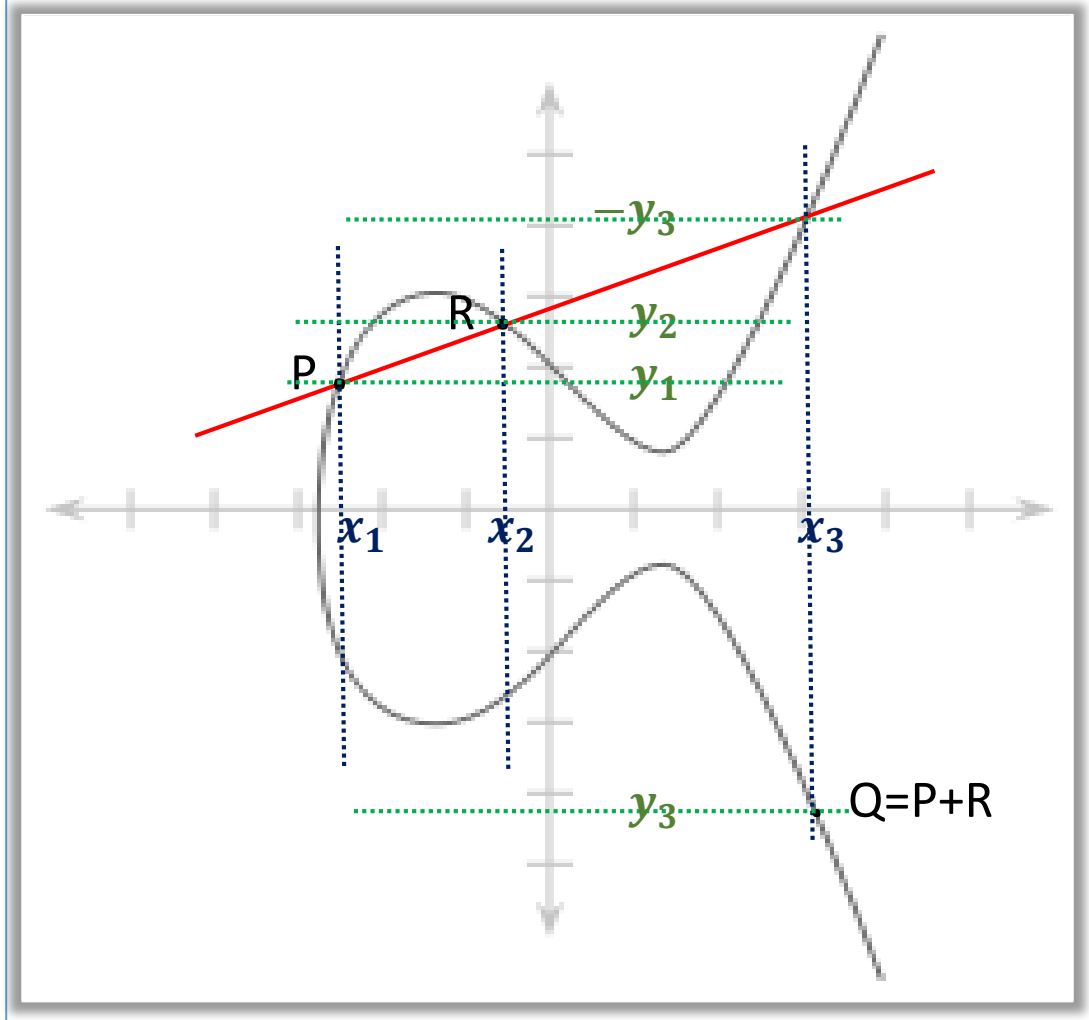
Elliptic curve: $y^2 = x^3 + a\,x + b$

$(sx + \beta)^2 = x^3 + a\,x + b$

$0 = x^3 - s^2\,x^2 + (a - 2s\beta)\,x + (b - \beta^2)$

x_1, x_2, x_3 are roots of the monic polynomial:

$s^2 = x_1 + x_2 + x_3$ ➔ $x_3 = s^2 - x_1 - x_2$



Mathematics behind point doubling

The points are part of the elliptic curve:

$$y^2 = x^3 + a\,x + b$$

Differential: $2y\,dy = 3x^2 dx + a\,dx$

$$s = dy/dx = (3x_1^2 + a)(2\,y_1)^{-1}$$

Extract y_3:

$$S = (-y_3 - y_1)/(x_3 - x_1)$$

$$y_3 + y_1 = s\,(x_1 - x_3) \rightarrow \boxed{y_3 = s(x_1 - x_3) - y_1}$$

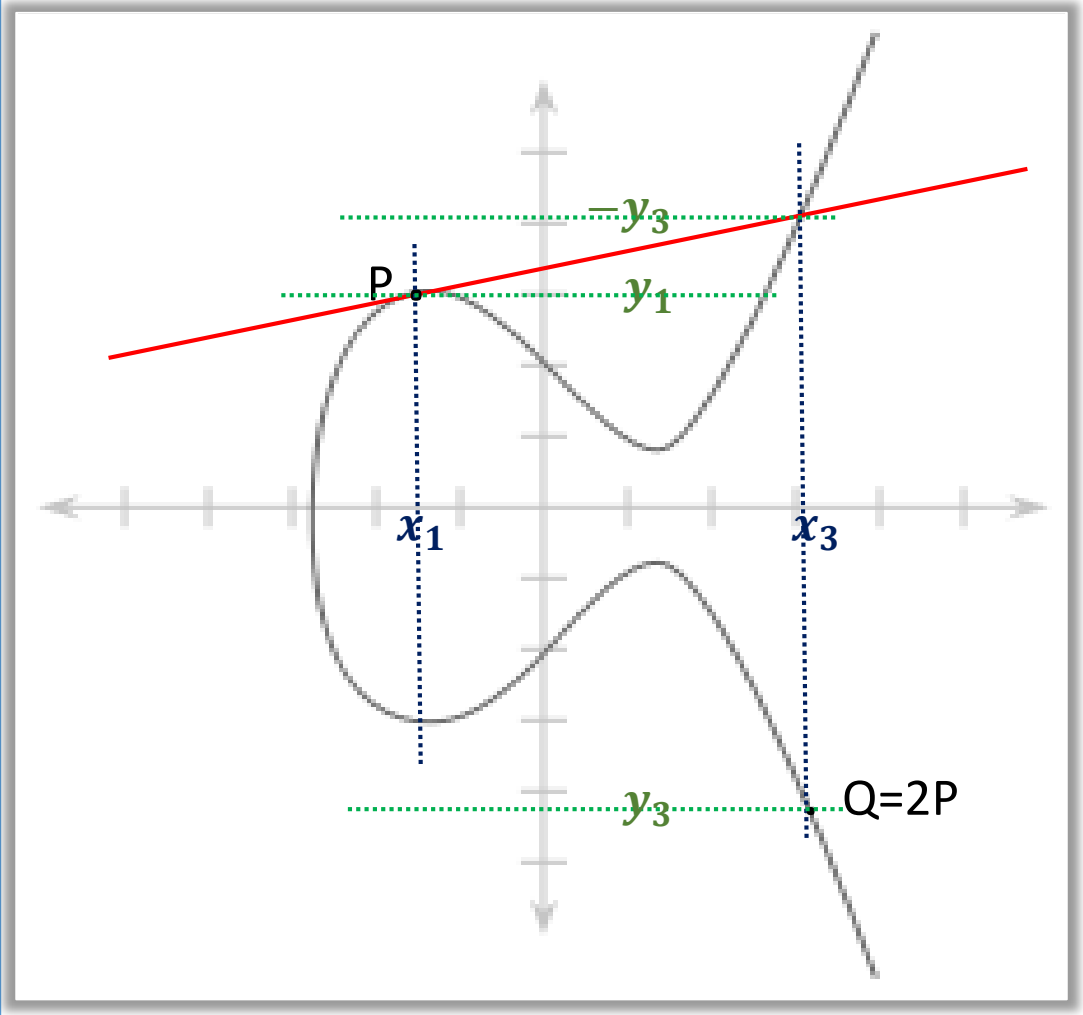
Construction of the monic polynomial:

$$(sx + \beta)^2 = x^3 + a\,x + b$$

$$0 = x^3 - s^2\,x^2 + (a - 2s\beta)\,x + (b - \beta^2)$$

x_1, x_1, x_3 are roots of the monic polynomial

$$s^2 = x_1 + x_1 + x_3 \rightarrow \boxed{x_3 = s^2 - 2x_1}$$



Example: Point doubling

We consider the small group $\mathbb{Z}_{17}$ => E: $y^2 \equiv x^3 + 2x + 2 \bmod 17$

We want to double the point **P = (5, 1)** => 2 P = (5, 1) + (5, 1)

$$s = (3x_1^2 + a)(2\ y_1)^{-1} = (75 + 2)(2)^{-1} \equiv 9 \cdot 9 \bmod 17 \equiv 13 \bmod 17$$

$$x_3 \equiv s^2 - x_1 - x_2 = 159 \equiv 6 \bmod 17$$

$$y_3 \equiv s(x_1 - x_3) - y_1 = 13(5 - 6) - 1 = -14 \equiv 3 \bmod 17$$

2 P = (6, 3)

This point is actually on the EC curve:

$$y^2 \equiv x^3 + 2x + 2 \bmod 17$$

$$3^2 \equiv 6^3 + 2 \cdot 6 + 2 \bmod 17$$

Creation of cyclic subgroup from EC

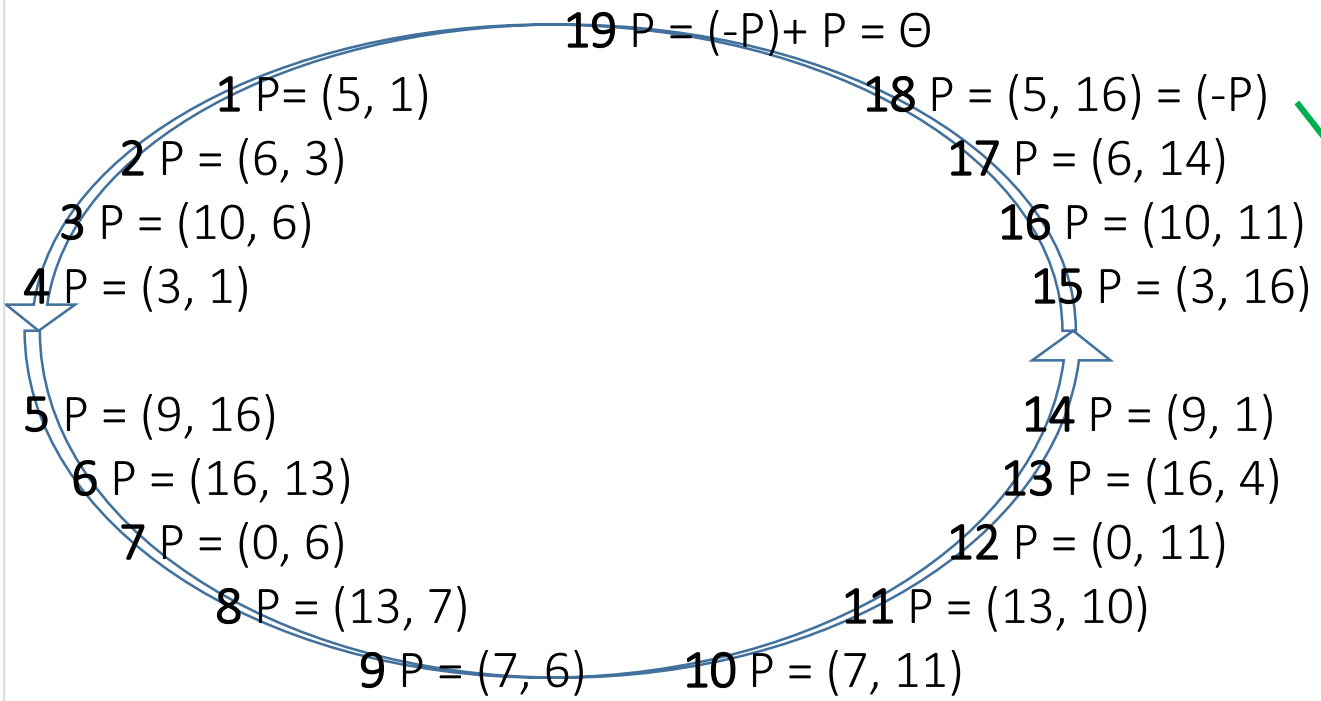
Theorem:

The points on an elliptic curve together with Θ have elliptic subgroups.
Under certain conditions all points on an elliptic curve form a cyclic group.

Example:

E: $y^2 \equiv x^3 + 2x + 2 \bmod 17$

Primitive element: P = (5, 1), the order is $\#E = 19$



Hasse's Theorem:

Given an EC E modulo m, the number of points on the curve denoted by $\#E$ is bounded by:

$$m + 1 - 2\sqrt{m} \leq \#E \leq m + 1 + 2\sqrt{m}$$

Proof:
18 P = (5, 16) = (5, -1) = (-P)
-1 = 16 mod 17

Homework – 8A

Verify several points on the circular group

$$y^2 \equiv x^3 + 2x + 2 \bmod 17$$

Primitive element: **P = (5, 1)**

Ex#1: **(9, 16)** + **(9, 16)**

Ex#2: **(9, 16)** + **(5, 16)**

NORTHERN ARIZONA UNIVERSITY

Elliptic Curve Cryptography (ECC)

- 1- Elliptic curve: number theory
  - Elliptic curves
  - Definition of circular finite groups
  - Arithmetic of the group
- 2- Key distribution with ECC
- 3- ECC with extended Galois field

EC Discrete Logarithm Problem (ECDLP)

Definition:

Given a cycling subgroup E of an elliptic curve we consider a primitive element *P*, and another element *T*.

The problem is finding integer *d*, where: $1 \leq d \leq \#E$

$$\underbrace{P + P + \ldots\ldots + P}_{d \text{ times}} = d \,.\, P = T = (x_T, y_T)$$

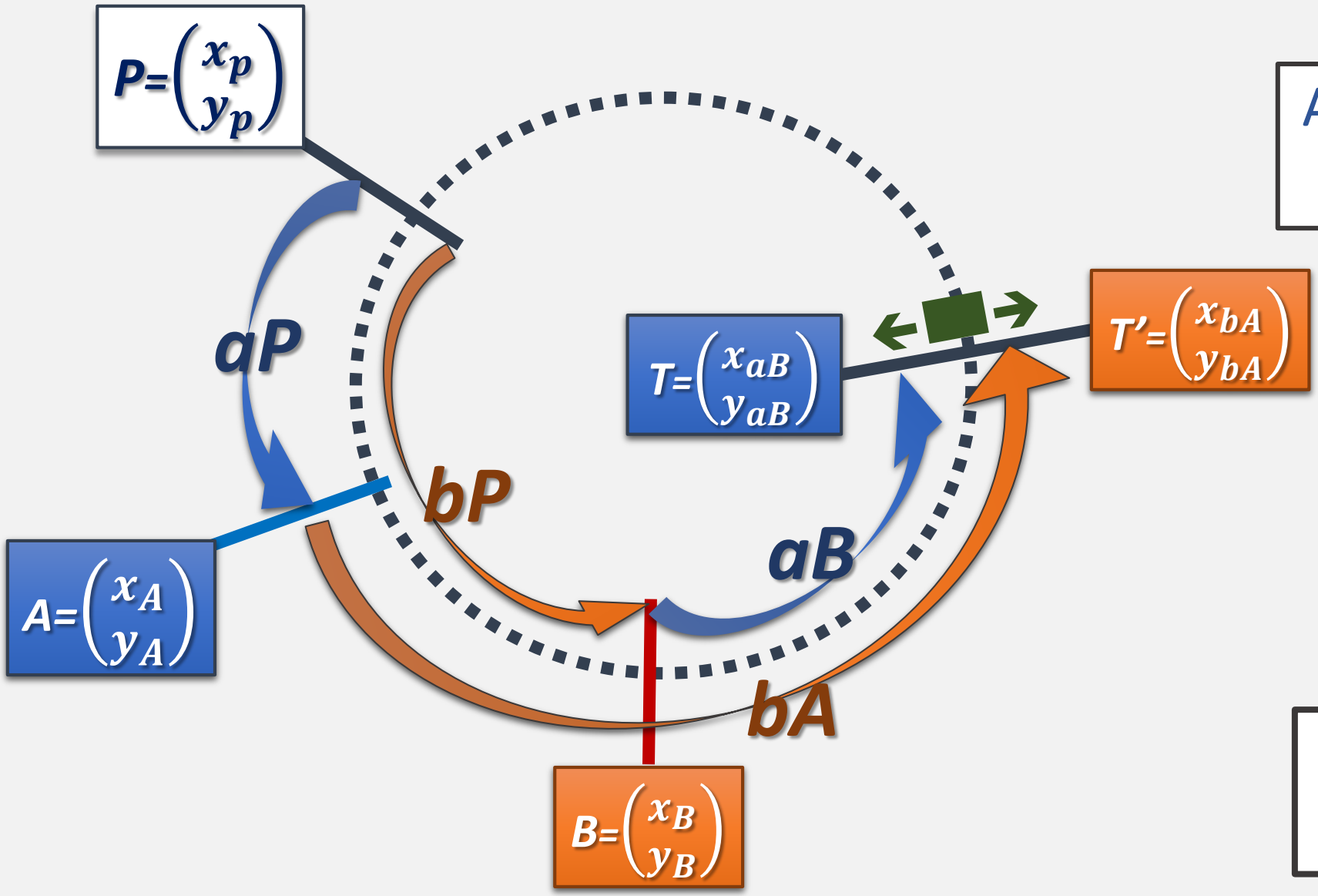
In cryptography systems:

d is the private key, and $T = (x_T, y_T)$ is the public key

$$T = d \,.\, P$$

Ex: P (5,1) T(16, 4) ➔ d=13

EC Diffie-Hellman Key Exchange (ECDHKE)



Alice encrypt with AES using x_{aB} as a key

Bob decrypt with AES using x_{bA} as a key

EC Diffie-Hellman Key Exchange (ECDHKE)

$$x_{aB} = x_{bA}$$

Proof:

a B = a (b P) = (a b) P = b (a P) = b A

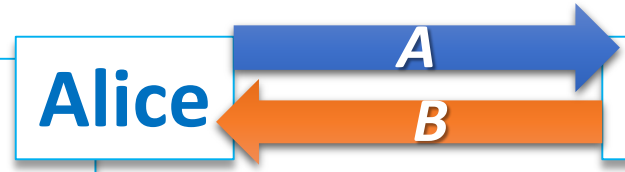
Alice and Bob have now exchanged AES keys that are unique to them offering asymmetrical cryptography type attributes

EC Diffie-Hellman Key Exchange (ECDHKE)

1- Choose a prime m and the elliptic curve E $\quad y^2 \equiv x^3 + \alpha \,.\, x + \beta \bmod m$

2- Chose a primitive element $\quad P = (x_P, y_P)$

This give a domain with $\#E$ integers in the cyclic group having separate pairs



Key Exchange:

Choose a private key

$P_{PrivA} = a \;\; \epsilon \{2, 3, \dots, \#E\text{-}1\}$

Calculate a public key

$P_{PubA} = A = a\,P = (x_A, y_A)$

Key Exchange:

Choose a private key

$P_{PrivB} = b \;\; \epsilon \{2, 3, \dots, \#E\text{-}1\}$

Calculate a public key

$P_{PubB} = B = b\,P = (x_B, y_B)$

Cryptography: Compute aB

$T_{AB} = (x_{AB}, y_{AB})$

Encrypt with AES using the key x_{AB}

Cryptography: Compute Ba

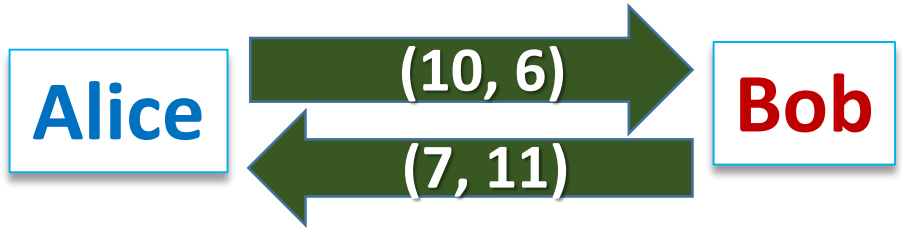
$T_{BA} = (x_{BA}, y_{BA})$

Decrypt with AES using the key x_{BA}

Example of key exchange

Group E defined by the following EC: $y^2 \equiv x^3 + 2x + 2 \bmod 17$

Base P = (5, 1) #E = 19



Private key $P_{PrivA} = a = 3$

Public key $P_{PubA} = A = 3\ P = (10, 6)$

Compute:

$aB = T_{AB} = 3\ (7, 11) = (13, 10)$

Private key $P_{PrivB} = b = 10$

Public key $P_{PubB} = B = 10\ P = (7, 11)$

Compute:

$bA = 10(10, 6) = (13, 10)$

(3 x 10) P = 30 P = 30-19 P = 11P

Encrypt with AES using 13 as a key

Decrypt with AES using 13 as a key

Fast addition for elliptic curve

Find public key A= P x 5321

Reason why ECC is secure

5321 = 1010011001001

Find public key: 17 operations versus 5320

m = 1+ 2^{256}

Find public key: 256 operations versus 2^{255}

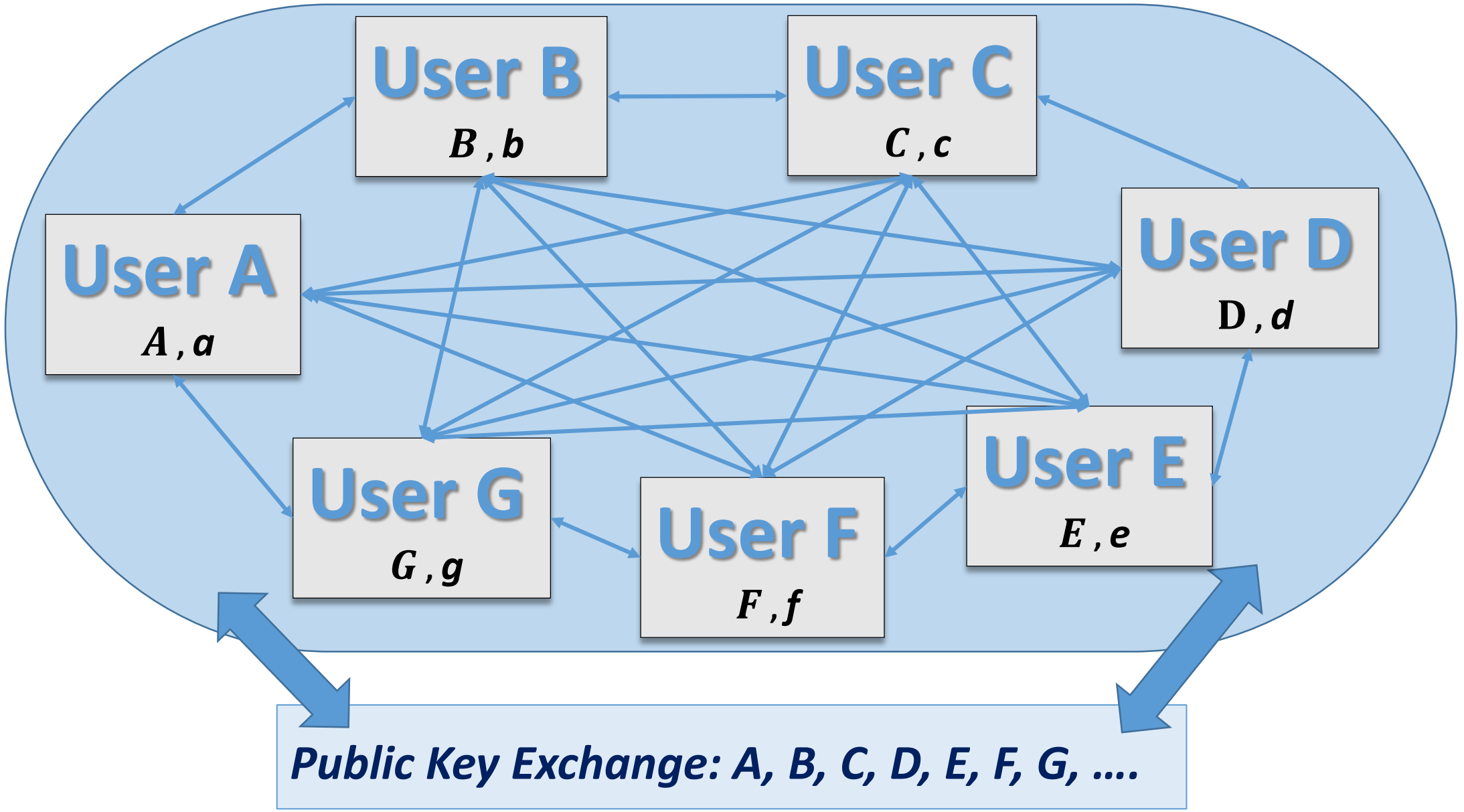
If one operation takes 1 µs:

256 operations take 256 µs

2^{255} operations take 1 10^{62} years

	1	0	1	0	0	1	1	0	0	1	0	0	1	
Dou	1	0												P + P
Dou	1	0	0											2P + 2P
Add	1	0	1											4P + P
Dou	1	0	1	0										5P + 5P
Dou	1	0	1	0	0									10P + 10P
Dou	1	0	1	0	0	0								20P + 20P
Add	1	0	1	0	0	1								P + 40P
Dou	1	0	1	0	0	1	0							41P + 41P
Add	1	0	1	0	0	1	1							P + 82P
Dou	1	0	1	0	0	1	1	0						83P + 83P
Dou	1	0	1	0	0	1	1	0	0					166P + 166P
Dou	1	0	1	0	0	1	1	0	0	0				332P + 332P
Add	1	0	1	0	0	1	1	0	0	1				P + 664P
Dou	1	0	1	0	0	1	1	0	0	1	0			665P + 665P
Dou	1	0	1	0	0	1	1	0	0	1	0	0		1330P + 1330P
Dou	1	0	1	0	0	1	1	0	0	1	0	0	0	2660P + 2660P
Add	1	0	1	0	0	1	1	0	0	1	0	0	1	P + 5320P

PKI with ECC Key exchange



NORTHERN ARIZONA UNIVERSITY

Elliptic Curve Cryptography (ECC)

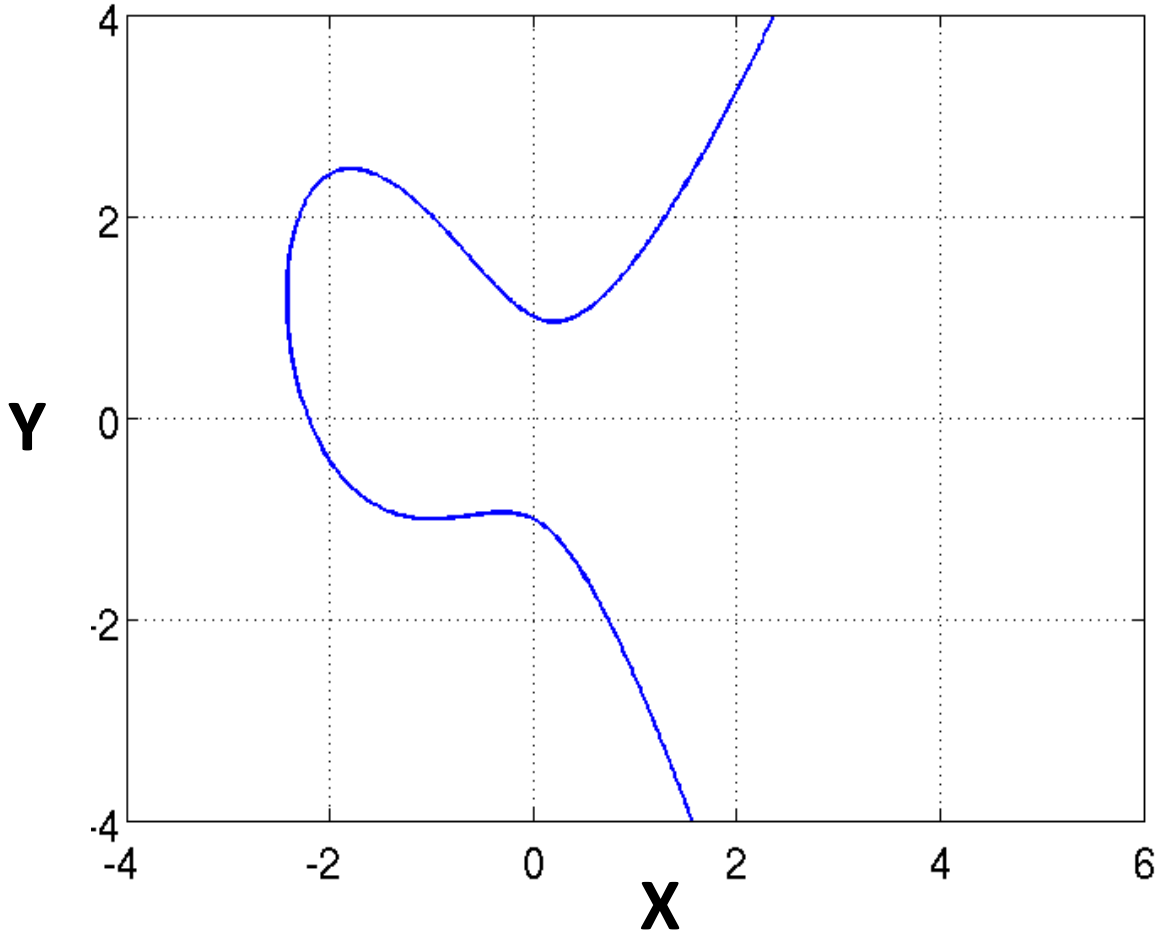
- 1- Elliptic curve: number theory
  - Elliptic curves
  - Definition of circular finite groups
  - Arithmetic of the group
- 2- Key distribution with ECC
- 3- ECC with extended Galois field

Elliptic Curves (EC) with extended Galois Field

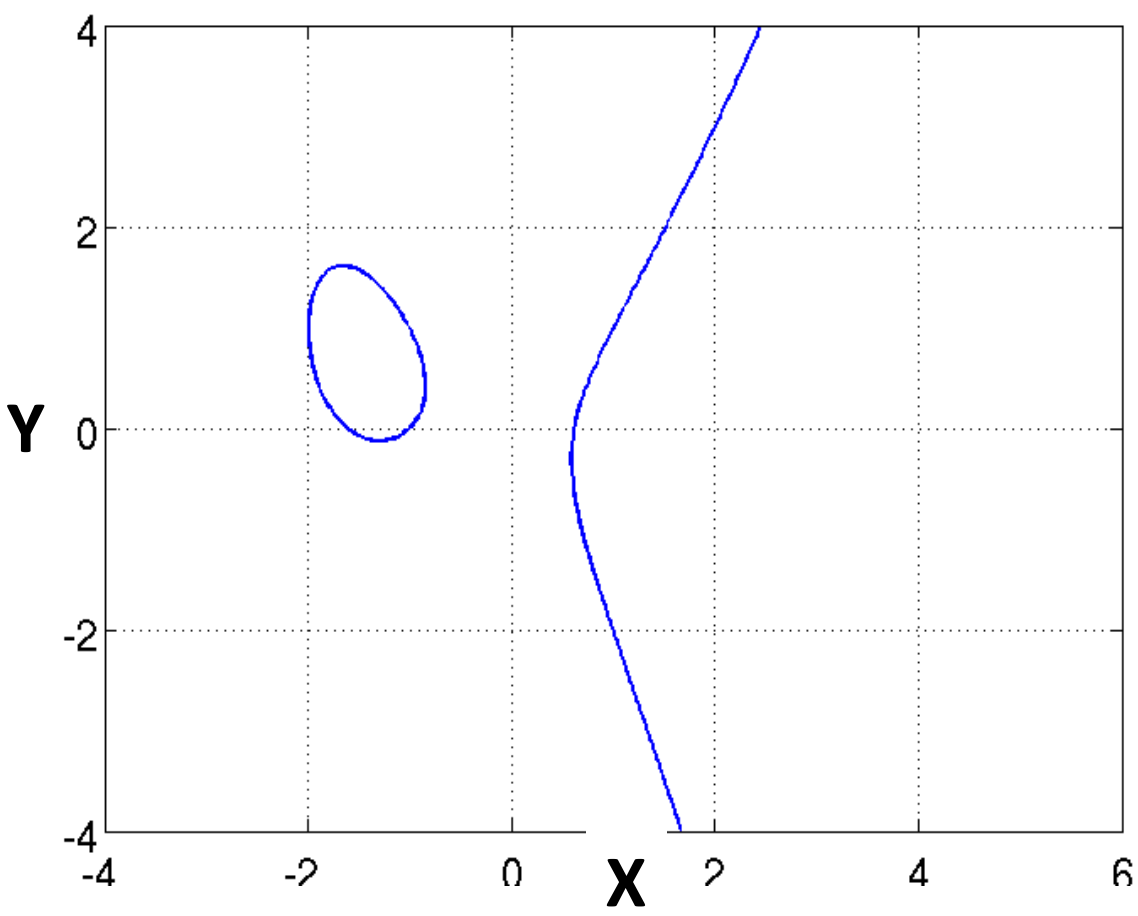
The set of all integer pairs (x, y, a, b) ϵ $\mathbb{Z}$ verifying: $y^2+xy= x^3+ a.x^2+ b$

(These elliptic curves are NOT symmetric with the x axes)

$y^2+xy= x^3+ 2.x^2+ 1$



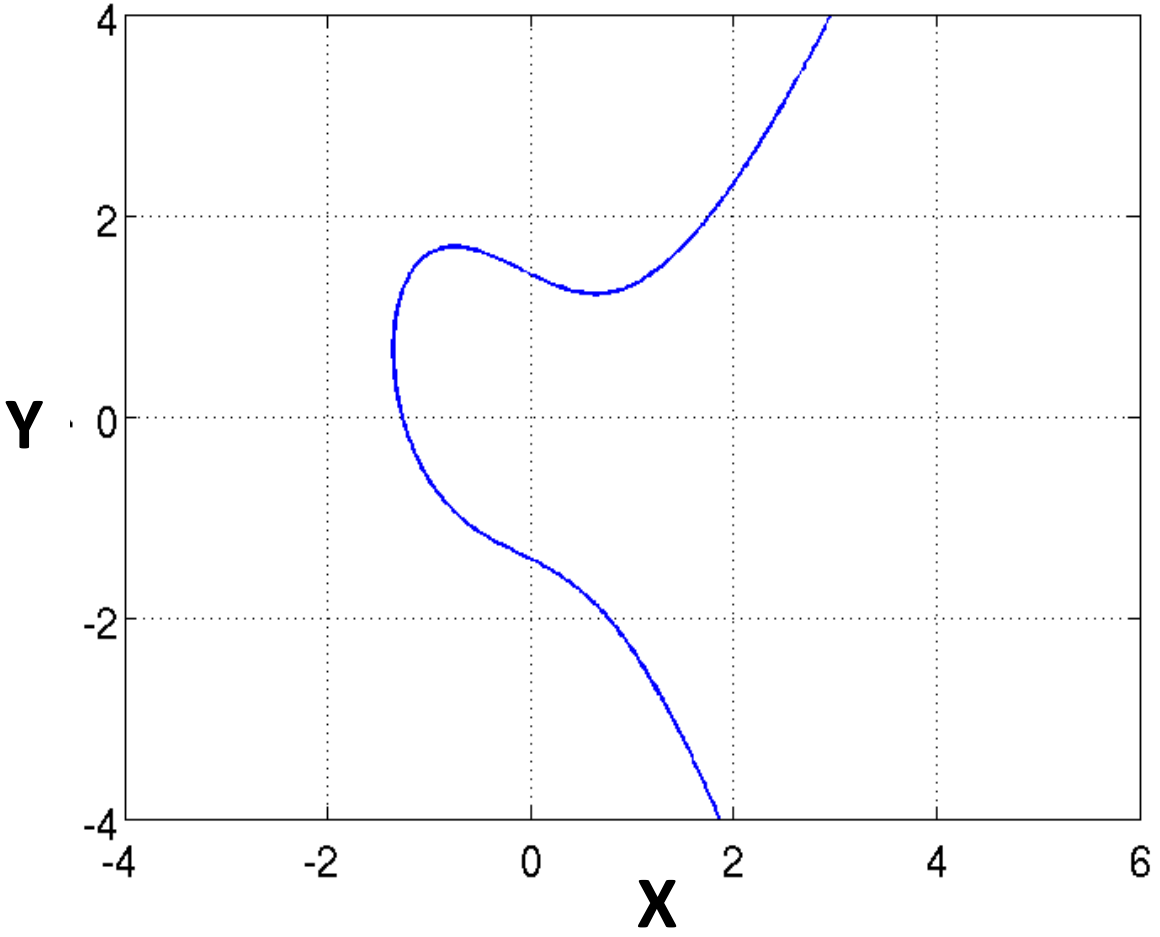
$y^2+xy= x^3+ 2.x^2 - 1$



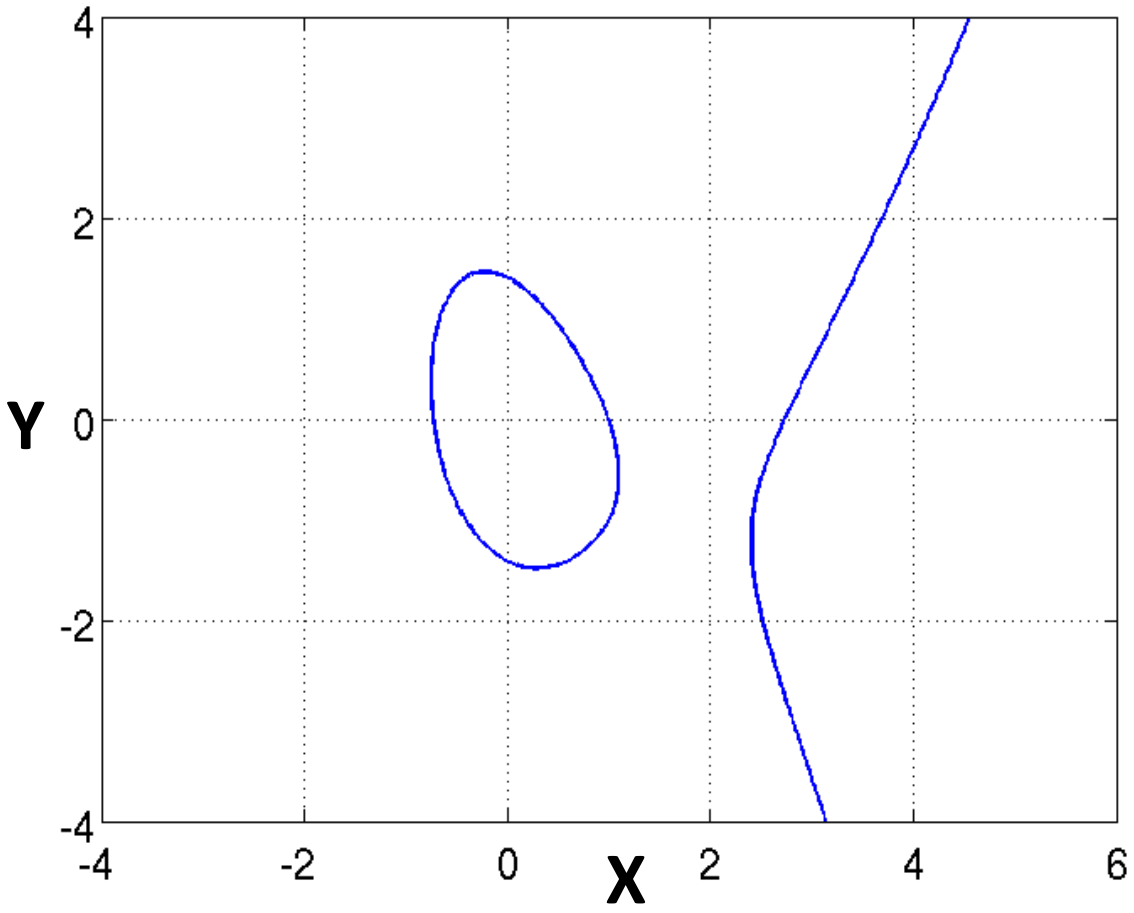
Elliptic Curves (EC) with extended Galois Field

Other examples

$y^2+xy= x^3+ 0.x^2+ 2$



$y^2+xy= x^3 - 3.x^2 + 2$



The circular finite ECC group G is based on $\mathcal{F}2^m$

G is the set of all pairs (X, Y) ϵ $\mathcal{F}2^m$ verifying:

$$Y^2 + XY \equiv X^3 + aX^2 + b \bmod P(x) \; ; \quad b \neq 0$$

Polynomials: $X = a_{m-1}\, x^{m-1} + \ldots + a_i\, x^i + \ldots + a_1\, x^1 + a_0$

$P(x)$ is an irreducible polynomial of $\mathcal{F}2^m$

Ex: for $\mathcal{F}2^4$, $P(x) = x^4 + x + 1$

Formula: Point addition & doubling for $\mathcal{F}2^m$

$P = (x_1, y_1)$; $Q = (x_2, y_2)$; $R = (x_3, y_3)$; $(x_i, y_i) \in \mathcal{F}2^m$;

$$y^2 + xy = x^3 + ax^2 + b \bmod P(x)$$

Point addition, $P+G=R$:

$$x_3 \equiv s^2 + s - x_1 - x_2 - a \bmod P(x)$$

$$y_3 \equiv s(x_1 - x_3) - y_1 - x_3 \bmod P(x)$$

Where: $s = (y_2 - y_1)(x_2 - x_1)^{-1} \bmod P(X)$

Point doubling, $2P=R$:

$$x_3 \equiv s^2 + s - 2x_1 - a \bmod P(x)$$

$$y_3 \equiv -s^2 - s + a - sx_3 - y_1 + (2 + s)x_1 \bmod P(x)$$

Where: $s = (3x_1^2 + 2ax_1 - y_1)(2y_1 + x_1)^{-1} \bmod P(X)$

Simplified formula: Point addition & doubling for $\mathcal{F}2^m$

$P = (x_1, y_1)$; $Q = (x_2, y_2)$; $R = (x_3, y_3)$; $(x_i, y_i) \in \mathcal{F}2^m$;

$y^2 + xy = x^3 + ax^2 + b \bmod P(x)$

Point addition, $P+G=R$:

$x_3 \equiv s^2 + s + x_1 + x_2 + a \bmod P(x)$

$y_3 \equiv s(x_1 + x_3) + y_1 + x_3 \bmod P(x)$

Where: $s = (y_2 + y_1)(x_2 + x_1)^{-1} \bmod P(X)$

Point doubling, $2P=R$:

$x_3 \equiv s^2 + s + a \bmod P(x)$

$y_3 \equiv s(x_1 + x_3) + y_1 + x_3 \bmod P(x)$

Where: $s = x_1 + y_1/x_1 \bmod P(X)$

Mathematics behind point addition for $\mathcal{F}2^m$

The points are part of the strait line:

$y = \alpha x + \beta \qquad \alpha = s = (y_2 - y_1)/(x_2 - x_1)$

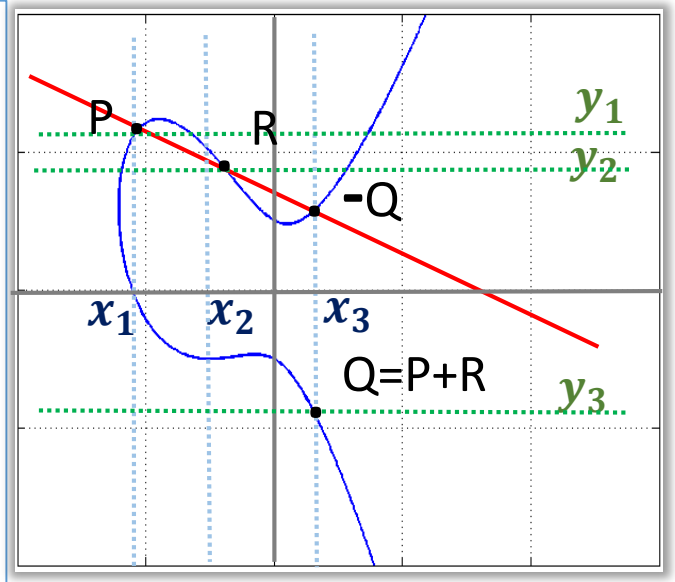
The points are part of the elliptic curve:

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

The inverse of $Q=(x_3, y_3)$ is $-Q=(x_3, -(x_3 + y_3))$

$$(-(x_3+y_3))^2 - (x_3 + y_3)x_3 = x_3^3 + ax_3^2 + b$$
$$x_3^2 + y_3^2 + 2x_3y_3 - x_3^2 - x_3 y_3 = x_3^3 + ax_3^2 + b$$
$$\rightarrow y_3^2 + x_3y_3 = x_3^3 + ax_3^2 + b$$

Note: $T=(x_3, -y_3)$ is NOT in the curve!!!



Mathematics behind point addition for $\mathcal{F}2^m$

The points are part of the strait line:

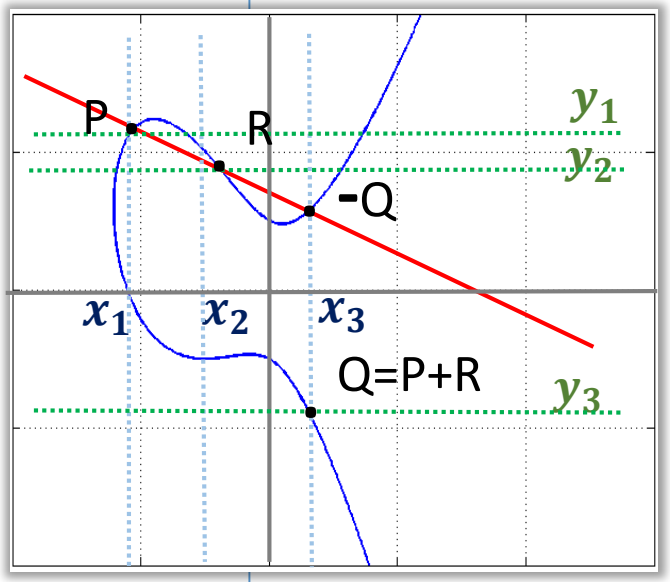
$y = \alpha x+\beta$ $\quad \alpha=s=(y_2 - y_1)/(x_2 - x_1)$

The points are part of the elliptic curve:

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

$$(sx+\beta)^2+(sx + \beta)x = x^3 +ax^2 +b$$

$$0= x^3 - (s^2+s - a)x^2 - (\beta + 2s\beta)x +(b-\beta^2)$$



x_1, x_2, x_3 are roots of the monic polynomial:

$s^2 + s - a=x_1 + x_2 + x_3$ ➔ $x_3 = s^2+s - a - x_1 - x_2$

The coordinates of –Q are (x'_3, y'_3)

$s=(y'_3 - y_1)/(x'_3 - x_1)$ ➔ $y'_3 - y_1= s\,(x'_3 - x_1)$

$$y'_3= s\,(x_3 - x_1) + y_1$$

$$y_3 = -(y'_3 + x'_3)= s\,(x_1 - x_3) - y_1 - x_3$$

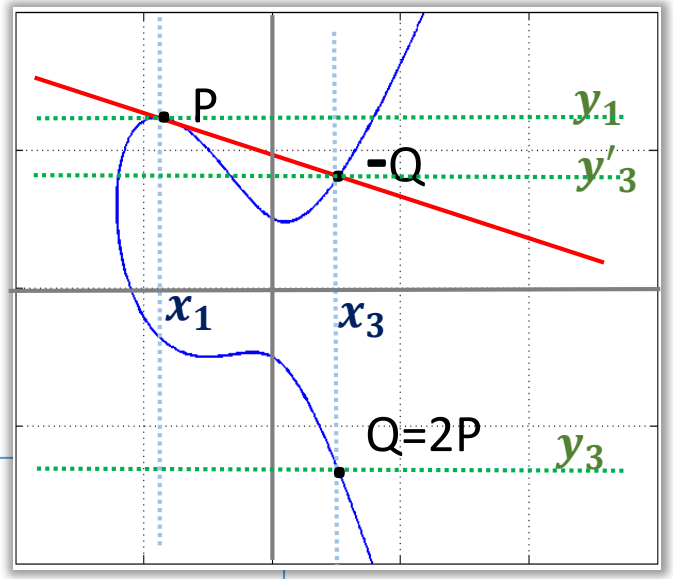
Mathematics behind point doubling for $\mathcal{F}2^m$

The points are part of the elliptic curve:

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

$$2y\,dy + x\,dy + y\,dx = 3x^2\,dx + 2ax\,dx$$

$$s = \frac{dy}{dx} = (3x_1^2 + 2ax_1 - y_1)(2y_1 + x_1)^{-1}$$



The points are part of the elliptic curve:

$$(sx+\beta)^2 + (sx + \beta)x = x^3 + ax^2 + b$$

$$0 = x^3 - (s^2 + s - a)x^2 - (\beta + 2s\beta)x + (b - \beta^2)$$

x_1, x_1, x_3 are roots of the monic polynomial

$$s^2 + s - a = x_1 + x_1 + x_3 \rightarrow x_3 = s^2 + s - a - 2x_1$$

$$s = (y'_3 - y_1)/(x'_3 - x_1) \rightarrow y'_3 = s(x_3 - x_1) + y_1$$

$$y_3 = -(y'_3 + x'_3) = s(x_1 - x_3) - y_1 - x_3$$

Elliptic Curve over $\mathcal{F}2^m$

The element $g = (0...010)$ is a **generator** for the field.

The powers of g are: g^x

g^0=(0...001) g^1=(0...010) g^2=(0...100) g^3=(0..1000) ....

$P = (g^x, g^y)$, is part of an elliptic curve:

$$(g^y)^2 + g^x g^y \equiv (g^x)^3 + a(g^x)^2 + b \bmod P(x)$$

Example of Elliptic Curve over $\mathcal{F}2^4$

The element ***g = (0010)*** is a generator for the field. $P(x) = x^4 + x + 1$

The powers of g are:

g^0 = (0001) g^1 = (0010) g^2 = (0100) g^3 = (1000)

g^4 = (0011) g^5 = (0110) g^6 = (1100) g^7 = (1011)

g^8 = (0101) g^9 = (1010) g^{10}= (0111) g^{11}= (1110) $g^{-x} = g^{15-x}$

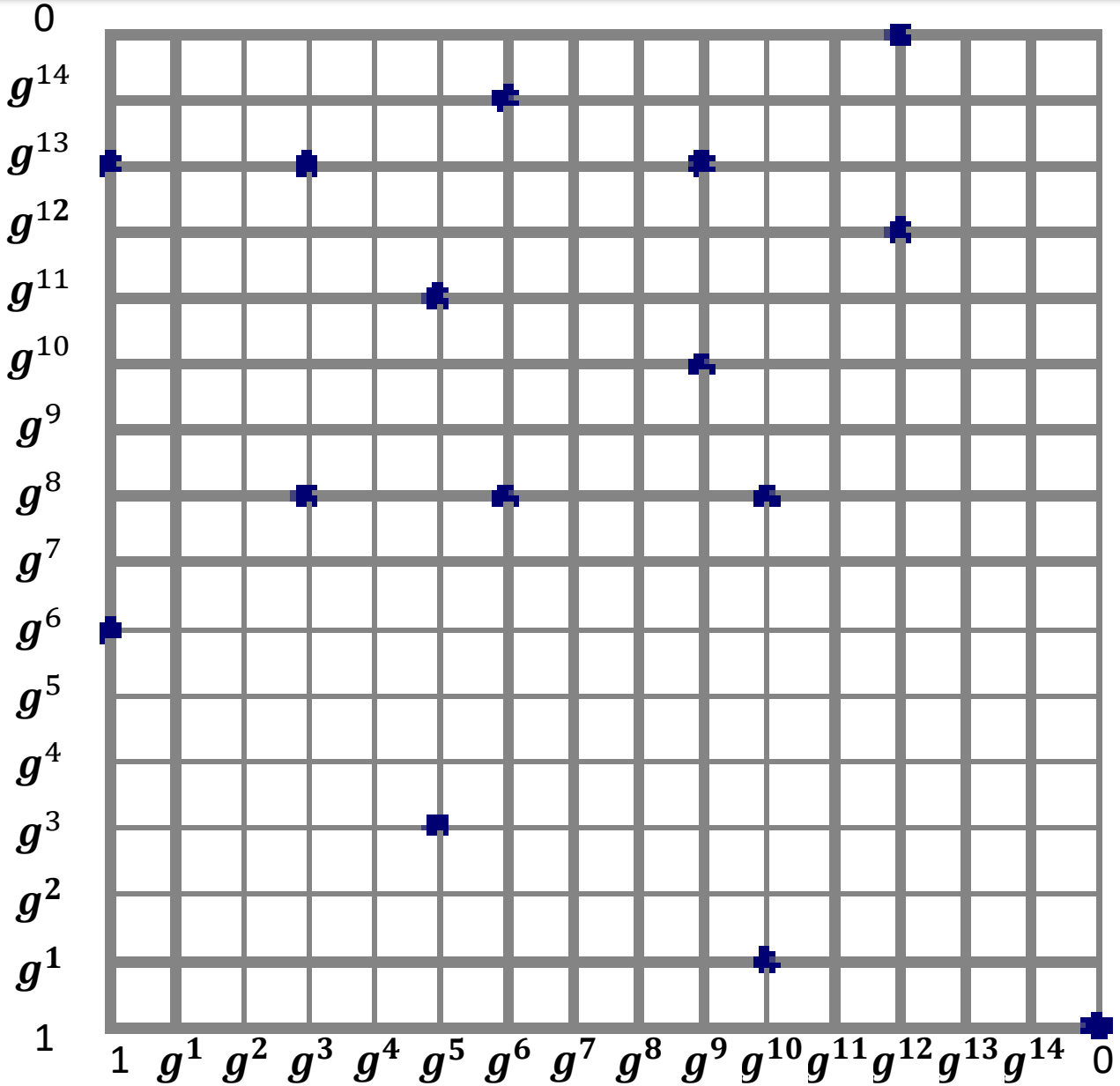
g^{12}= (1111) g^{13}= (1101) g^{14}= (1001) g^{15}= (0001) =1 = g^0

Consider the elliptic curve: $y^2 + xy \equiv x^3 + g^4 x^2 + 1 \bmod P(x)$

The points on *E* are:

(g^5, g^3)(1, g^{13})(g^{10}, g)(0, 1)(g^{10}, g^8)(1, g^6)(g^5, g^{11}) 0 (g^3, g^{13}) (g^6, g^{14})
(g^9, g^{13}) (g^3, g^8) (g^6, g^8) (g^9, g^{10}) (g^{12}, 0) (g^{12}, g^{12})

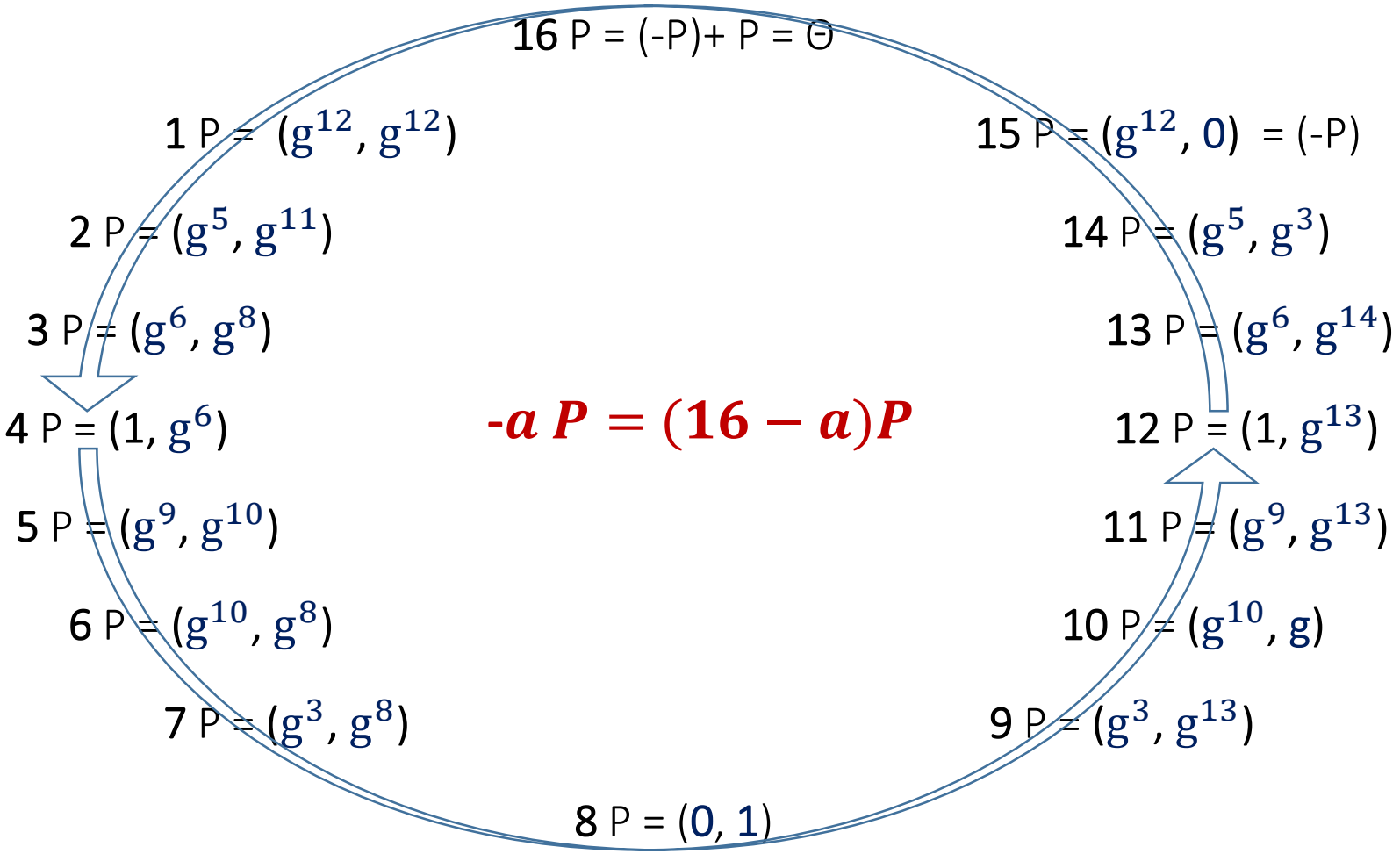
Elliptic Curve over $\mathcal{F}2^4$: Graphical representation



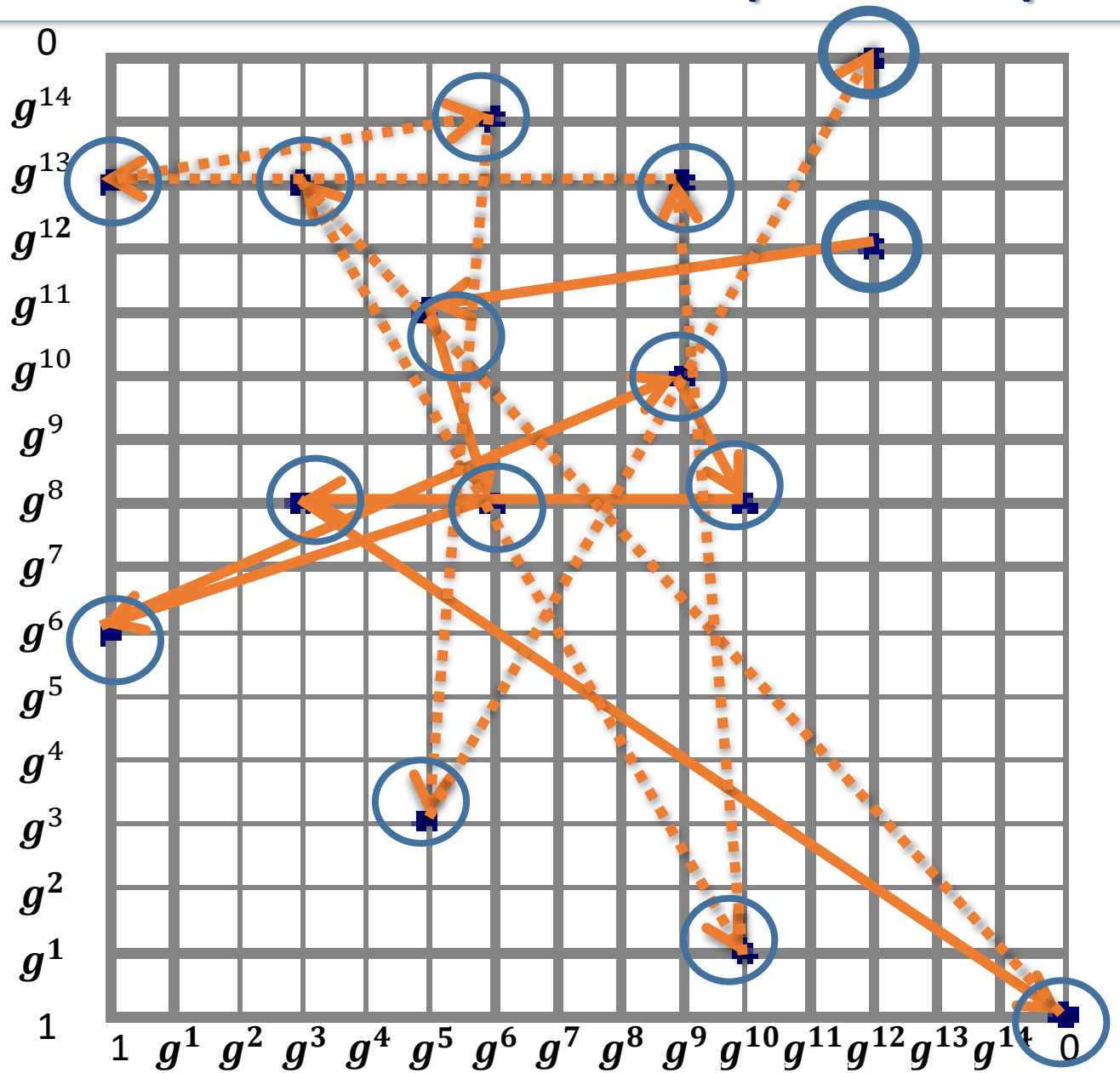
Consider the elliptic curve:

$$y^2 + xy \equiv x^3 + g^4 x^2 + 1 \bmod P(x)$$

Primitive element: P =(g^{12}, g^{12})



Elliptic Curve over $\mathcal{F}2^4$: Graphical representation



Example of Point addition

$A = (g5, g3)$; $B = (g9, g13)$; $R = (gX, gY)$

Point addition, R=A+B:

$$s = (y_2 + y_1)\,(x_2 + x_1)^{-1} = (g3+g13)/(g5+g9) = g8/g6 = g2$$

g3 = 1000

g13 = 1101

g3 + g13 = 0101 = g8

g5 = 0110

g9 = 1010

g5 + g9 = 1100 = g6

g-6=g15-6=g9

g8/g6=g8 g9 = g17 = g2

Example of Point addition

$A = (g5, g3)$; $B = (g9, g13)$; $R = (gX, gY)$

Point addition, R=A+B:

$$s = g2$$

$$x_3 \equiv s^2 + s + x_1 + x_2 + a = (g2)^2 + g2 + g5 + g9 + g4 = g3$$

g2 = 0100

g5 = 0110

g9 = 1010

g2 + g5 + g9 = 1000 = g3

Example of Point addition

$A = (g5, g3)$; $B = (g9, g13)$; $R = (gX, gY)$

Point addition, R=A+B:

$s = g2$

$x_3 = g3$

$y_3 \equiv s\,(x_1 + x_3) + x_3 + y_1 = g2(g5+g3)+g3+g3 = g13$

g5 = 0110

g3 = 1000

g5 + g3 = 1110 = g11

g2 g11 = g13

P+Q = R = (g3, g13)

Verification

$A = (g5, g3)$; $B = (g9, g13)$ ➔ $R = A + B = (g3, g13)$

$A = 14\ P$

$B = 11P$

$A+B = 25\ P = (25-16)\ P = 9\ P = (g3, g13)$

Example of Point doubling

$A = (g5, g3); \quad R = (gX, gY)$

Point doubling, R=2A

$$s = x_1 + y_1(x_1)^{-1} = g5 + g3/g5 = g7$$

g-5 = g10

g3 x g10 = g13

g5 = 0110

g13 = 1101

g3 + g11 = 1011 = g7

Example of Point doubling

$A = (g5, g3); \quad R = (gX, gY)$

Point doubling, $R=2A$

$$s = g7$$

$$x_3 \equiv s^2+s+a = (g7)^2+g7+g4 = g14+g7+g4 = 1$$

g14 = 1001

g7 = 1011

g4 = 0011

g8+ g7 + g4 = 0001 = 1

Example of Point doubling

$A = (g5, g3);\quad R = (gX, gY)$

Point doubling, R=2A

$$s = g7$$

$$x_3 = 1$$

$$y_3 \equiv s\,(x_1 + x_3) + x_3 + y_1 = g7(g5+1)+1+g3 = \mathbf{g13}$$

g5 = 0110
1 = 0001
g5 + 1 = 0111 = g10

g2 = 0100
1 = 0001
g3 =1000

g2+1+g3 = 1101= g13

$2A = R = (1, g13)$

Verification

$$A = (g5, g3) \rightarrow R = 2A = (1, g13)$$

$$A = 14\ P$$

$$2A = 28\ P = (28\text{-}16)\ P = 12\ P = (1, g13)$$

Homework – 8B

Verify several points on the circular group based on $\mathcal{F}_{2^m}$

$$y^2 + xy \equiv x^3 + g^4 x^2 + 1 \bmod P(x)$$

$$P(x) = x^4 + x + 1$$

The element ***g = (0010)*** is a generator

Primitive element: P = (g^{12}, g^{12})

Ex#1: $(g^{12}, 0) + (g^{12}, 0)$

Ex#2: $(g^{12}, 0) + (0, 1)$

Elliptic Curve over $\mathcal{F}2^m$

The element ***g = (00…10)*** is a generator for the field with ***P(x)***

The powers of **g** are:

g^0 = (00…01) g^1 = (00…10) g^2 = (0…100) …

… g^n = $(a_{n-1}\ a_{n-1} \ldots a_1\ a_0)$ … g^{2^m-1} = (0…001) =1 = g^0

How to calculate the inverse of g^n when ***n*** is unknown?

When a ϵ $\mathcal{F}2^m$ → $a^{2^m-1} = 1$

$$a^{-1} = a^{-1}\ a^{2^m-1} = a^{2^m-2}$$

$$(g^n)^{-1} = (g^n)^{-1}((g^n)^{-1})^{2^m-1} = ((g^n)^{-1})^{2^m-2}$$

Patent war around ECC

- The general idea of ECC was not patented, but there are a number of patents regarding the efficient implementation from the underlying layer (finite field arithmetic) to the highest layer (protocols)

- The patent issue for elliptic curve cryptosystems is the opposite of that for RSA and Diffie-Hellman, where the cryptosystems themselves have patents, but efficient implementation techniques often do not

- ***Certicom*** holds more than 130 patents related to ECC. It has sold 26 patents to NSA and NISA in the value of 26 million US$, which covers the prime field curves with primes of 256 bits, 384 bits and 521 bits.

- ***Certicom*** was taken over by the ***RIM*** (Research in Motion) with the offer of 130 million C$ in 2009.

NORTHERN ARIZONA UNIVERSITY®

QUESTIONS ?

Dr. Bertrand Cambou
Professor of Practice NAU, Cybersecurity
School of Informatics, Computing, and Cyber-Systems
Bertrand.cambou@nau.edu