Discrete Logarithmic Problem- ELLIPTIC CURVE CRYPTOSYSTEMS

Vaishali Gupta
B.Tech NIT Sikkim

Content

- Introduction
- Trapdoor One Way Function
- Discrete Logarithmic Problem and General DLP
- Attacks against the DLP
- Diffie Hellman Key Exchange and its Security Aspects
- Elliptic Curve Cryptosystem
- Definition of elliptic curves
- Elliptic Curve Discrete Logarithmic Problem(ECDLP)
- Elliptic Curve Diffie Hellman Key Exchange(ECDH)
- Security Aspects of ECC
- References

Introduction

- Rapidly increasing needs for flexible and secure transmission of information require to use new cryptographic methods.
- Public key cryptography makes use of two keys:

  public key: which may be known to anybody and can be used to encrypt messages and verify signatures.

  private key: known only to the recipient, used to decrypt the messages and sign(or create) signatures.
- Unlike, symmetric key cryptography, public key cryptosystems do not require to send the key through a secure channel to the two nodes in communication.

- The use of two keys has profound consequences in the areas of confidentiality, key distribution, and authentication.

- It solves the problem of distributing the key for encryption. Everyone publishes their public keys and private keys are kept secret.

- One of the main advantages is that it provides non-repudiation. Digitally signing a message is akin to physically signing a document. It is an acknowledgement of the message and thus, the sender cannot deny it.

- The biggest drawback in this public key cryptography is the authenticity of public keys.

In his 1874 book *The Principles of Science*, William Stanley Jevons wrote:

Can the reader say what two numbers multiplied together will produce the number 86164607998657234?
I think it is unlikely that anyone but myself will ever know.

The above problem is factorization problem which is quite similar, hard but much more simpler than Discrete Logarithmic Problem.

Trapdoor One Way Function

- The main idea behind asymmetric key cryptography is the concept of trapdoor one way function.
- A one way function is such that:
  - Given x, Y=f(x) is easy to compute.
  - Given Y, it is computationally infeasible to calculate x= $f^{-1}(x)$.
- A function ***f* :*X* -> *Y*** is trapdoor one-way function with a third property
  - Given Y, and some **trapdoor(secret)** , x can be computed.

DLP is one such one-way function in which exponentiation is easy but logarithmic is difficult.

Discrete Logarithmic Problem(DLP)

Types of cyclic groups used in public key cryptosystems:

Z_p^* , $GF(2^n)$, Elliptic Curves

Discrete Logarithm Problem (DLP) in $Zp*$

- Given is the finite cyclic group $Zp*$ of order $p-1$ and a primitive element $\alpha \in Zp*$ and another element $\beta \in Zp*$.
- The DLP is the problem of determining the integer $1 \leq x \leq p-1$ such that $\alpha^x \equiv \beta \bmod p$ *or* $x = log_\alpha \beta$

Above computation is called the **discrete logarithmic problem.**

The Generalized Discrete Logarithmic Problem

- Given is a finite cyclic group *G* with the group operation ◦ and cardinality *n*.
- We consider a primitive element $\alpha \in G$ and another element $\beta \in G$.
- The discrete logarithm problem is finding the integer *x*, where $1 \leq x \leq n$, such that:

$$\beta = \underbrace{\alpha \circ \alpha \circ \alpha \circ . . . \circ \alpha}_{\text{x times}} = \alpha^{x}$$

Attacks against the Discrete Logarithmic Problem

The following algorithms for the computing discrete logarithms exists:

Generic algorithms: Work in any cyclic group

- Brute-Force Search
- Shanks‘ Baby-Step-Giant-Step Method
- Pollard‘s Rho Method(best for Elliptic curves)
- Pohlig-Hellman Method

Non-generic Algorithms: Work only in specific groups, in particular in Z*p*

- The Index Calculus Method

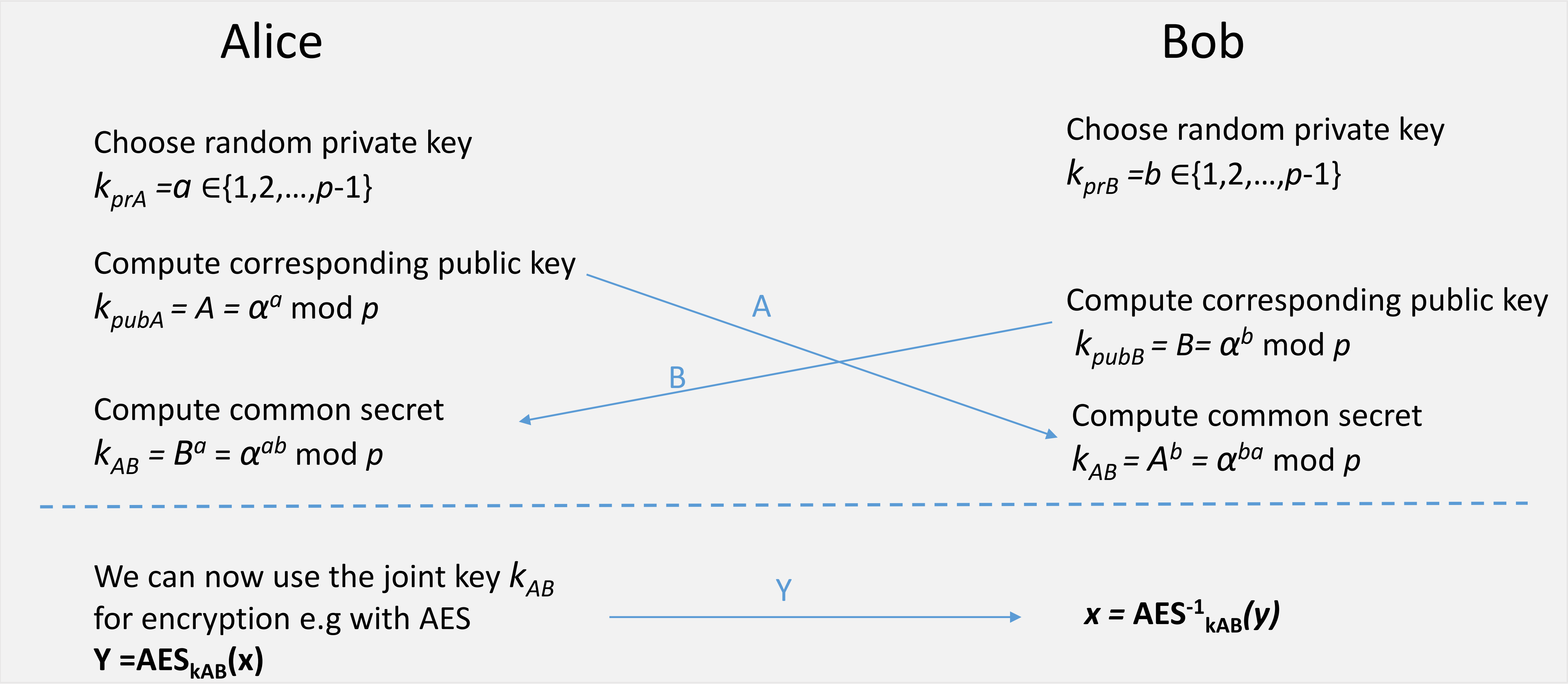
Diffie Hellman Key Exchange: Overview

- Proposed in 1976 by Whitfield Diffie and Martin Hellman and hence the name.
- Widely used in SSH, TLS and IPSec.
- The Diffie Hellman Key Exchange is a key protocol and not used for encryption.

Diffie Hellman Key Exchange : Set-up

- Choose a large prime p.
- Choose an integer $\alpha \in \{2,3, . . . , p-2\}$.
- Publish *p and* α*.*

Diffie Hellman Key Exchange



Alice

Choose random private key

$k_{prA} = a \in \{1,2,\ldots,p\text{-}1\}$

Compute corresponding public key

$k_{pubA} = A = \alpha^{a} \text{ mod } p$

Compute common secret

$k_{AB} = B^{a} = \alpha^{ab} \text{ mod } p$

Bob

Choose random private key

$k_{prB} = b \in \{1,2,\ldots,p\text{-}1\}$

Compute corresponding public key

$k_{pubB} = B = \alpha^{b} \text{ mod } p$

Compute common secret

$k_{AB} = A^{b} = \alpha^{ba} \text{ mod } p$

We can now use the joint key k_{AB} for encryption e.g with AES

$Y = \text{AES}_{kAB}(x)$

$x = \text{AES}^{-1}_{kAB}(y)$

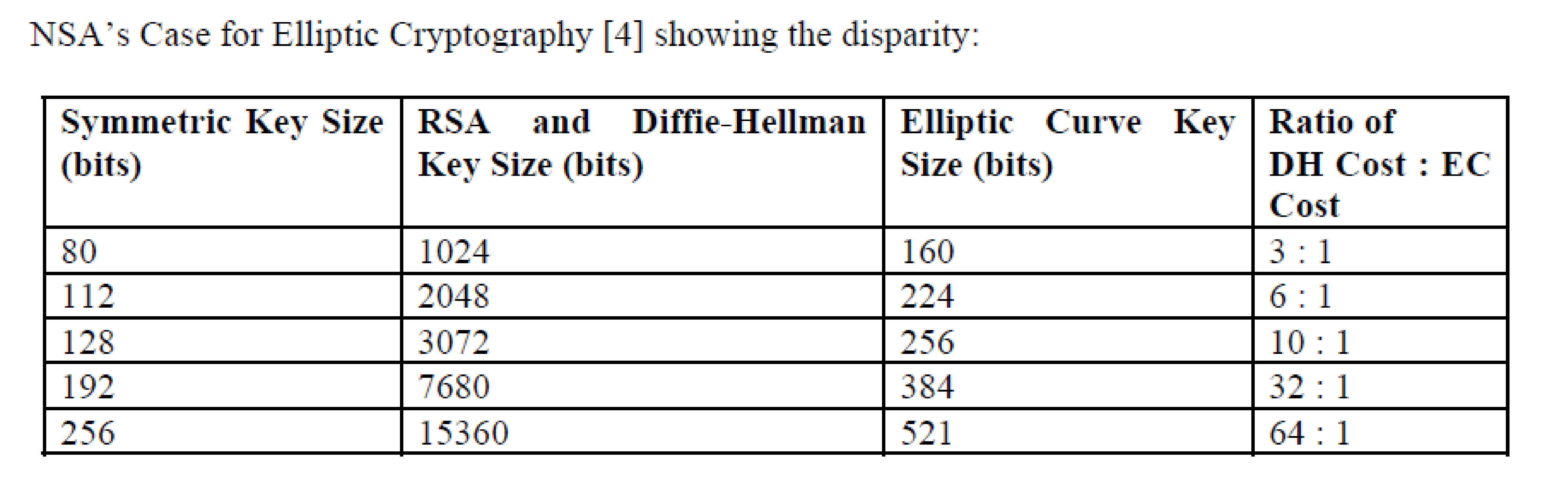
Security of the classical Diffie Hellman Key Exchange

- Eve only has the following information:
  - α, p
  - k_{pubA} = A = α^{a} mod p
  - k_{pubB} = B = α^{b} mod p
- The only way to find DHP is to solve the DLP i.e. by
  - Computing $a = log_{\alpha}\ A\ mod\ p$ | | $b = log_{a}B\ mod\ p$
  - And $k_{AB} = B^{a} = A^{b} = \alpha^{ab}$ mod p
- To prevent DLP from getting solved , it is required to choose the prime p > 2^{1024}

Elliptic Curve Cryptosystems

- Introduced in 1980s , ECC provides the same level of security as RSA or discrete logarithm systems with considerably shorter operands (approximately 160–256 bit vs. 1024–3072 bit in RSA).

- ECC is based on the generalized discrete logarithm problem, and ergo DL-protocols such as the Diffie–Hellman key exchange can also be realized using elliptic curves.



NSA's Case for Elliptic Cryptography [4] showing the disparity:

Symmetric Key Size (bits)	RSA and Diffie-Hellman Key Size (bits)	Elliptic Curve Key Size (bits)	Ratio of DH Cost : EC Cost
80	1024	160	3 : 1
112	2048	224	6 : 1
128	3072	256	10 : 1
192	7680	384	32 : 1
256	15360	521	64 : 1

Elliptic Curves

- An *elliptic curve* is a special type of polynomial equation that define points on the (simplified) *Weierstras Equation*.

- For cryptographic use, we need to consider the curve not over the real numbers but over a finite field.

- The most popular choice is prime fields *GF*(*p*), where all arithmetic is performed modulo a prime *p*.

Definition of Elliptic Curves

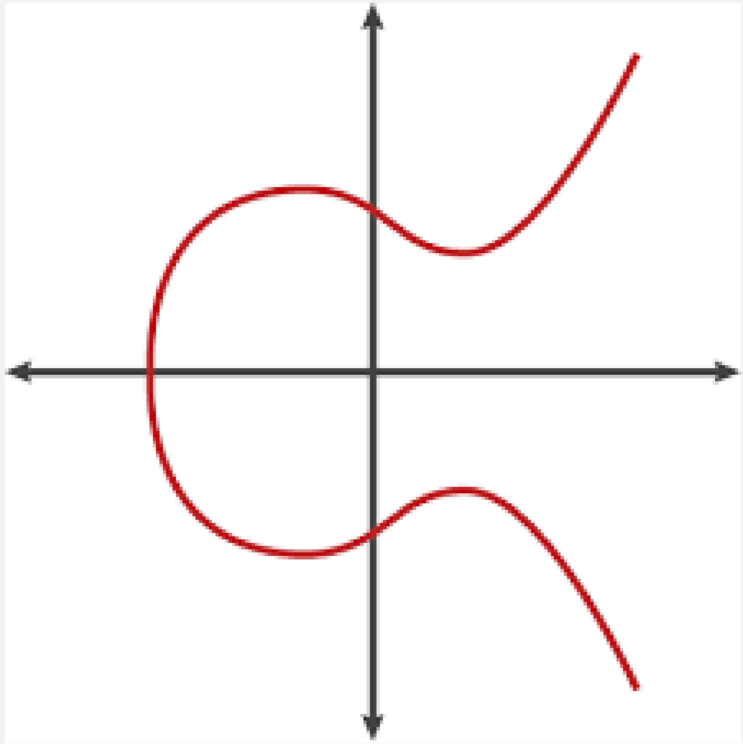
The elliptic curve *over* Zp, *p* > 3, *is the set of all pairs* (*x*,*y*) ∈ Zp *which fulfill the equation defined by :*

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

together with an imaginary point of infinity *O, where a,b* ∈ Zp *and the condition:*

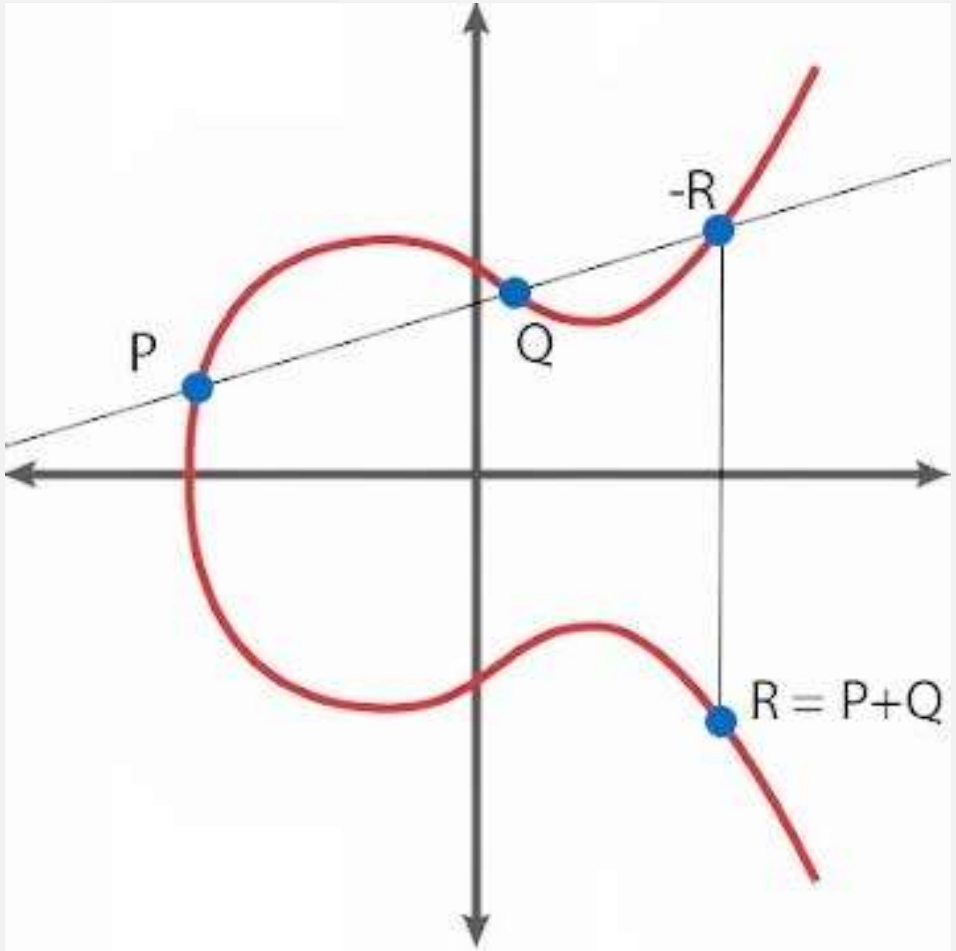
$$4.a^3+27.b^2 \neq 0 \bmod p.$$

The below figure represents the elliptic curve $y^2 = x^3 -3x+2$ shown over real numbers R:



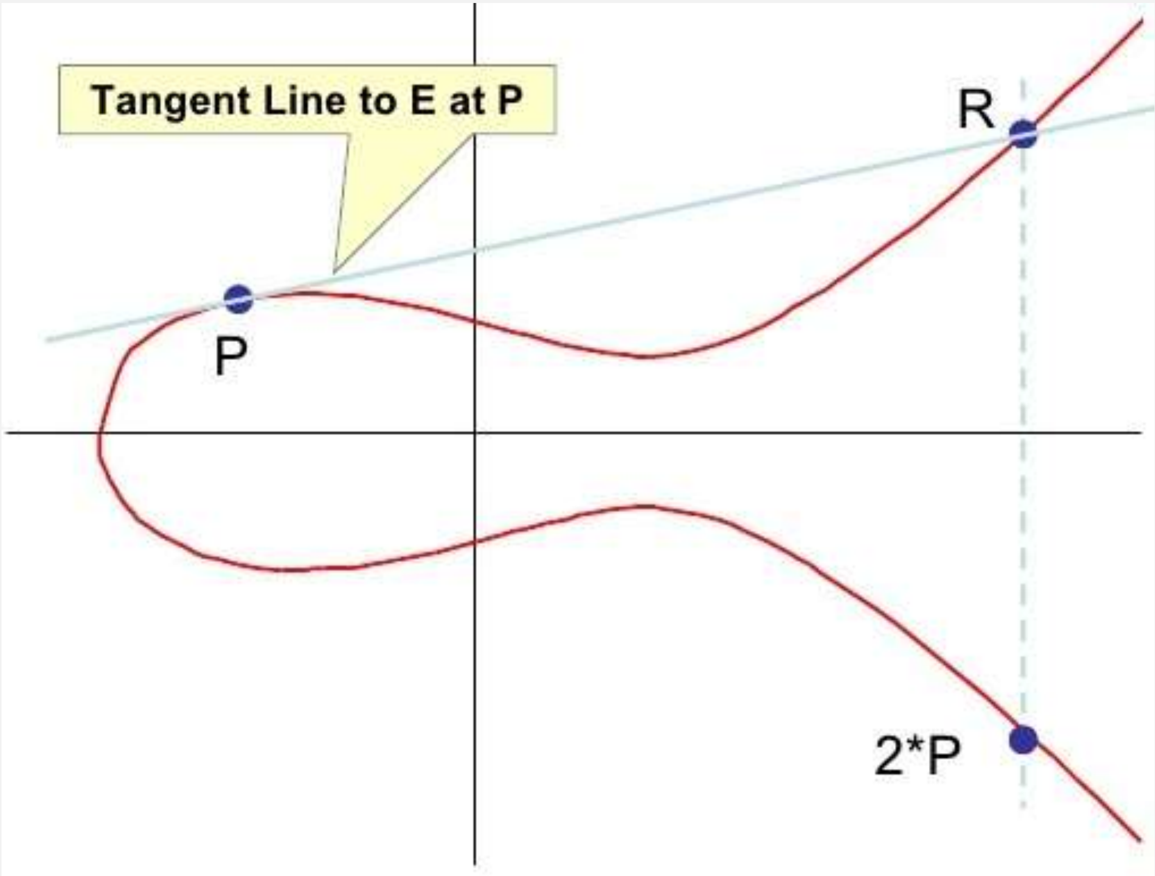
Group Operations on Elliptic Curves

- <u>Case 1</u> :: When P ≠Q



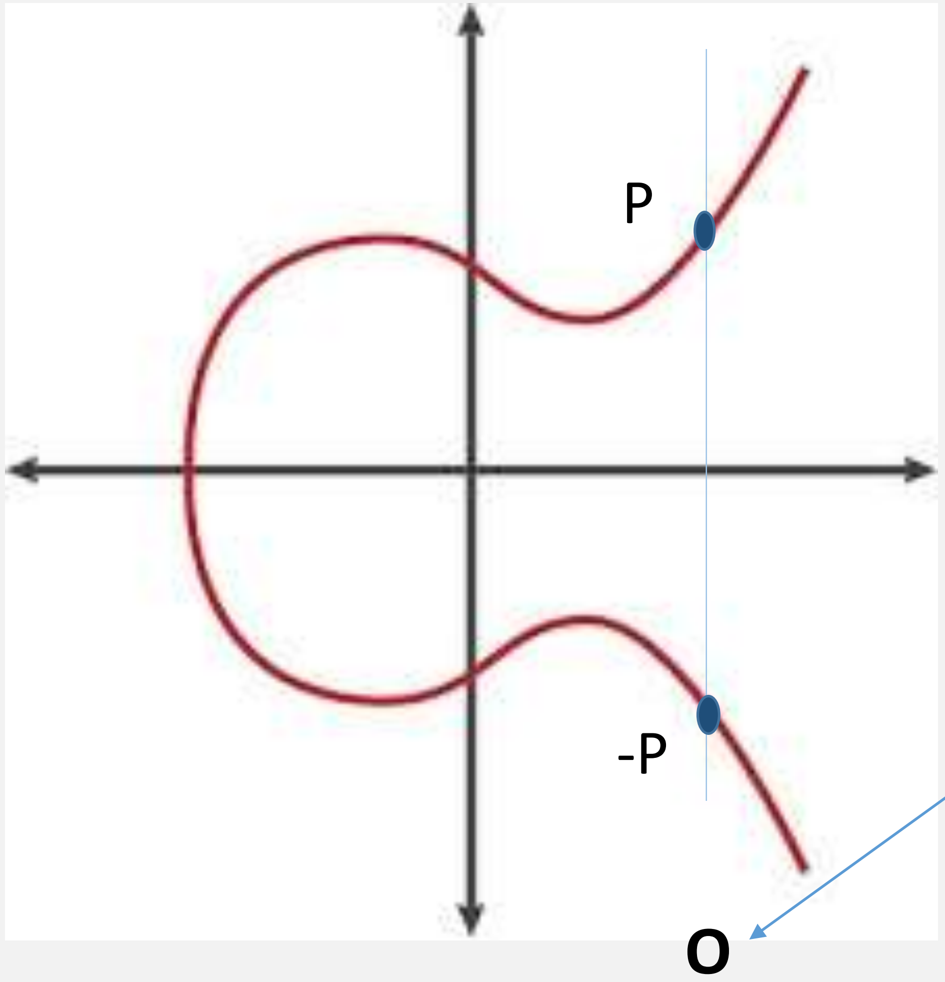
Point Addition

- Case 2 :: When P = Q



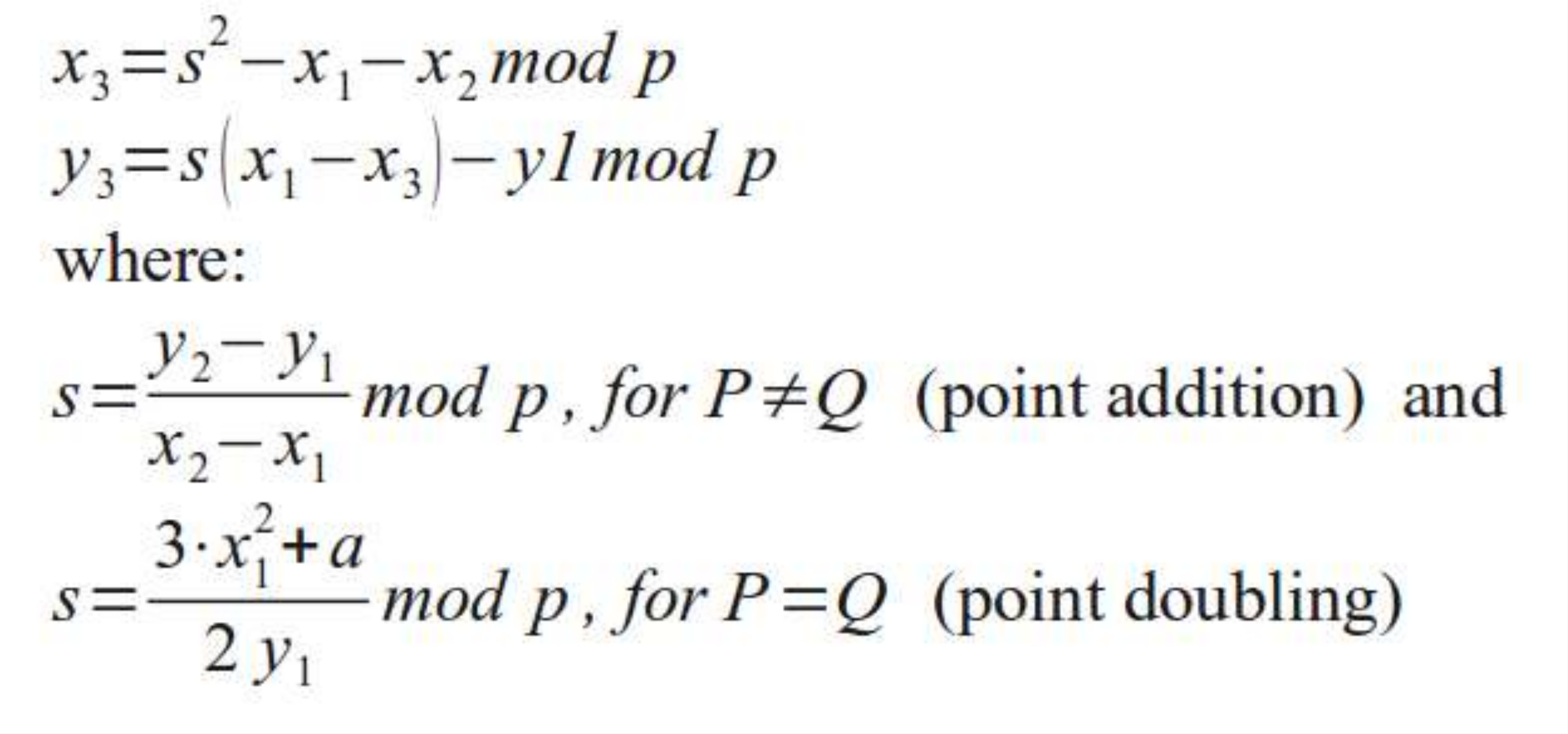
Point Doubling

- Case 3:: When Q = ∞



Point at Infinity

Formulae of addition in different cases in elliptic curves



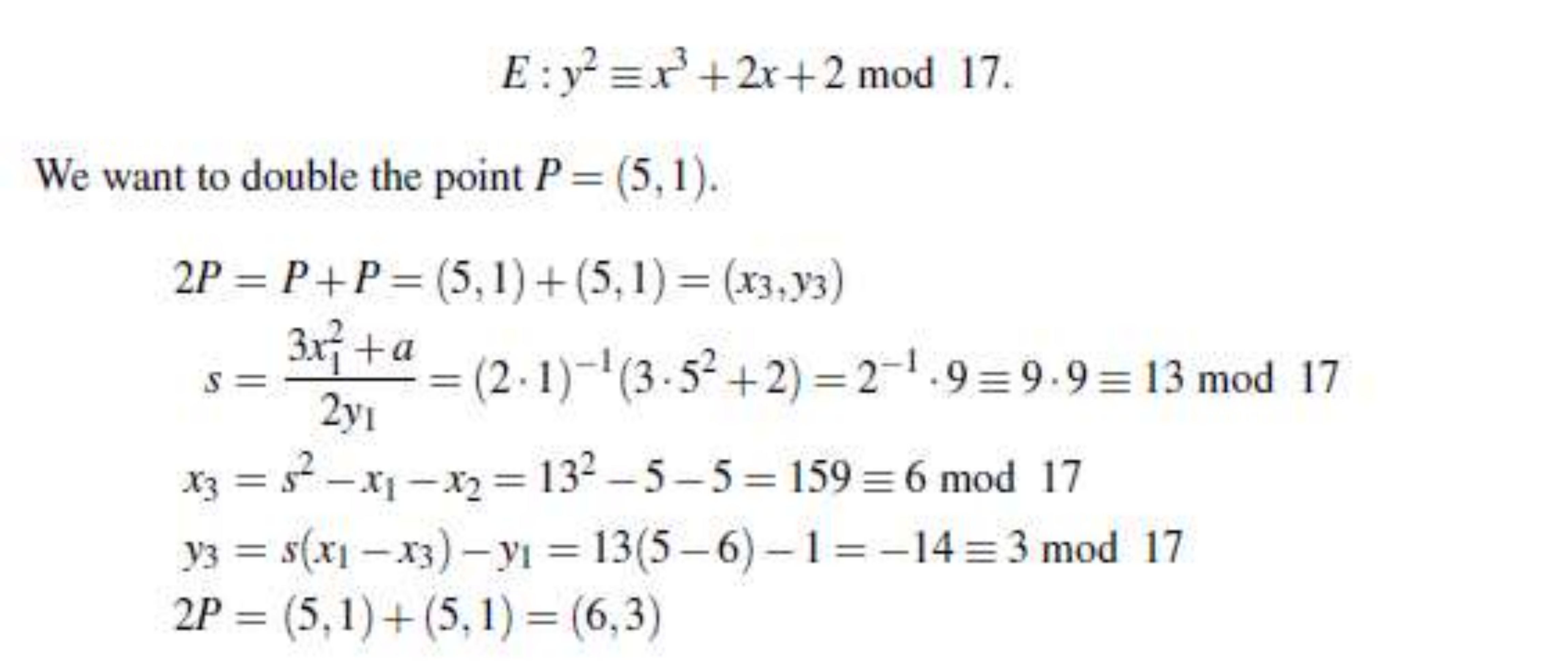
$$x_3 = s^2 - x_1 - x_2 \, mod \ p$$

$$y_3 = s\left(x_1 - x_3\right) - y1 \, mod \ p$$

where:

$$s = \frac{y_2 - y_1}{x_2 - x_1} \, mod \ p \, , \, for \ P \neq Q \quad \text{(point addition)} \quad \text{and}$$

$$s = \frac{3 \cdot x_1^2 + a}{2 \, y_1} \, mod \ p \, , \, for \ P = Q \quad \text{(point doubling)}$$



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

We want to double the point $P = (5,1)$.

$$2P = P + P = (5,1) + (5,1) = (x_3, y_3)$$

$$s = \frac{3x_1^2 + a}{2y_1} = (2 \cdot 1)^{-1}(3 \cdot 5^2 + 2) = 2^{-1} \cdot 9 \equiv 9 \cdot 9 \equiv 13 \bmod 17$$

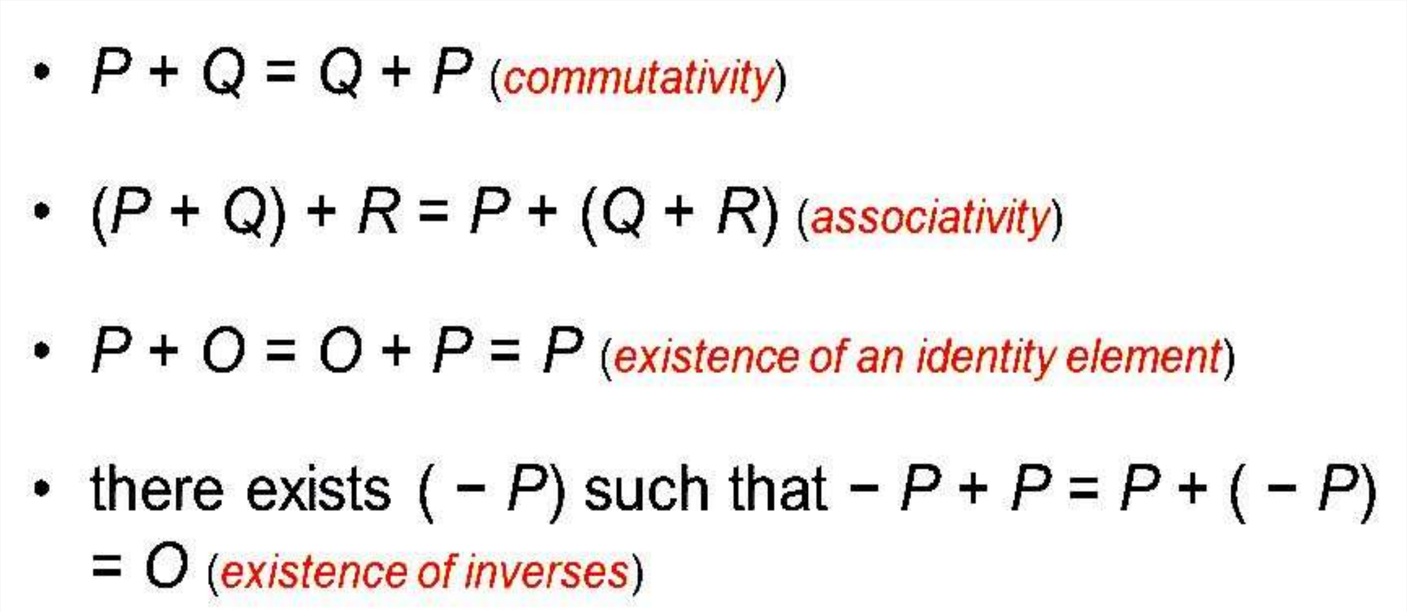
$$x_3 = s^2 - x_1 - x_2 = 13^2 - 5 - 5 = 159 \equiv 6 \bmod 17$$

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

$$2P = (5,1) + (5,1) = (6,3)$$

The Abelian Group

Given two points P,Q in E(Fp) , there is a third point, denoted by P+Q on E(Fp) , and the following relations hold for all P,Q,R in E(Fp)



- $P + Q = Q + P$ (*commutativity*)
- $(P + Q) + R = P + (Q + R)$ (*associativity*)
- $P + O = O + P = P$ (*existence of an identity element*)
- there exists $(- P)$ such that $- P + P = P + (- P) = O$ (*existence of inverses*)

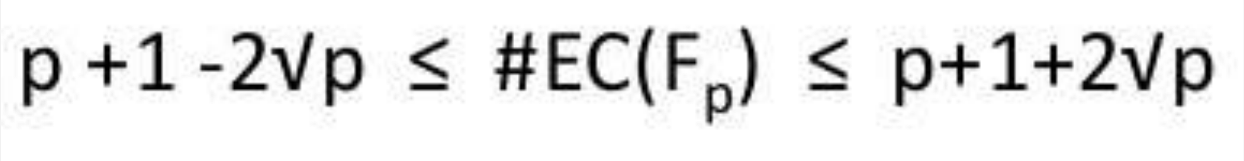
Elliptic curves follow all the conditions of an abelian group.

Order of an Elliptic Curve

The number of discrete points that can be on an elliptic curve defines its order.

In general, determining point count on the curve is quite hard.

But **Hasse's theorem** gives a bound on the number of points with his formulae as:



$$p + 1 - 2\sqrt{p} \leq \#EC(F_p) \leq p+1+2\sqrt{p}$$

It is proved that for large values of prime p, #E is equivalent to p.

Elliptic Curve Discrete Logarithmic Problem(ECDLP)

Cryptosystems rely on the hardness of the Elliptic Curve Discrete Logarithmic Problem.

Definition: Elliptic Curve Discerte Logarithmic Problem(ECDLP)

Given a primitive element P and another element T on an elliptic curve .
The ECDLP problem is to found the integer d, where 1<d<#E such that:

$$\underset{d\text{ times}}{\underleftrightarrow{P + P + P\ldots\ldots P}} = dP = T$$

Diffie Hellman Key Exchange with Elliptic Curves

ECDH Domain Parameters

- Choosing a prime p and the values of a and b for elliptic curve.

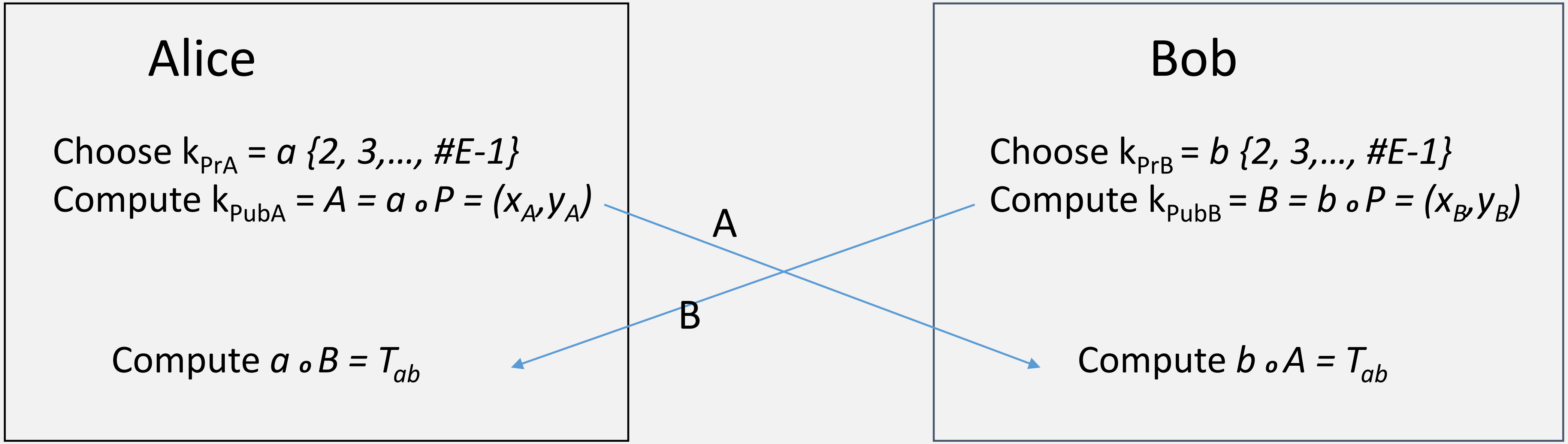
$$E: y^2 = x^3 + a.x + b \bmod p$$

- Choosing a primitive element P = (xp, yp)

(a, b, P, p) ---> domain parameters

The actual key exchange is done the same way as it was done for the conventional Diffie Hellman Protocol.

Elliptic Curve Diffie Hellman Key Exchange(ECDH)



Alice

Choose $k_{PrA} = a \; \{2, 3, \ldots, \#E\text{-}1\}$

Compute $k_{PubA} = A = a \circ P = (x_A, y_A)$

Compute $a \circ B = T_{ab}$

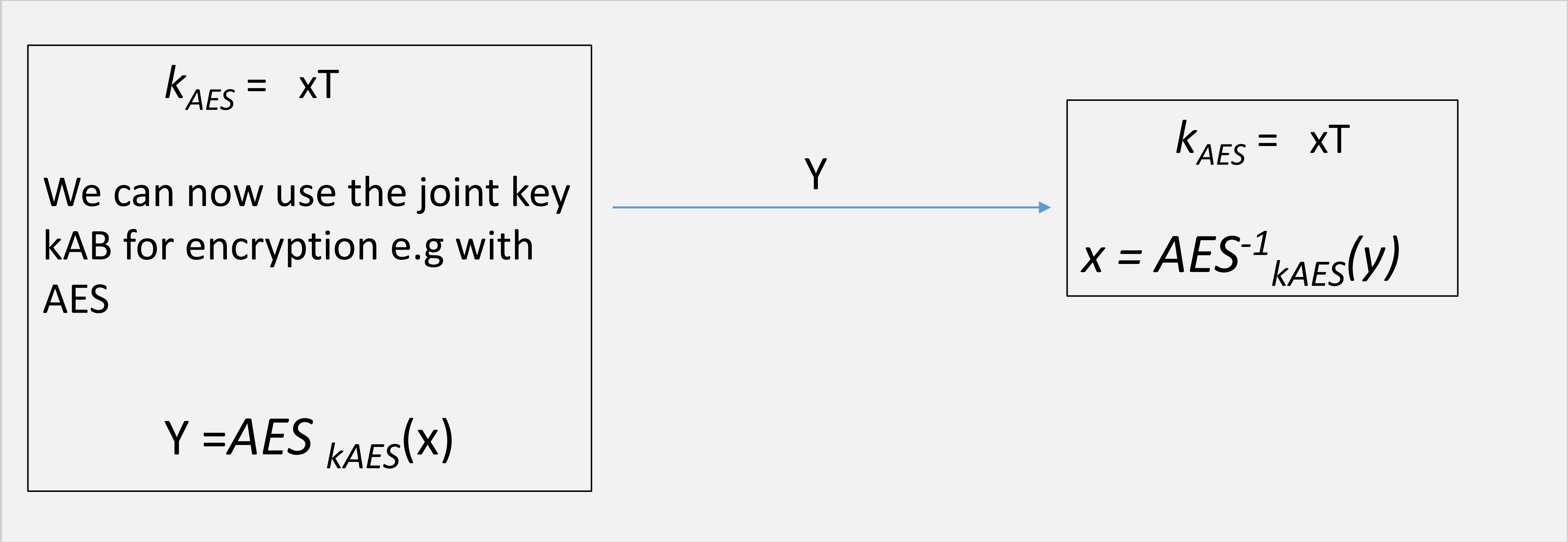
Bob

Choose $k_{PrB} = b \; \{2, 3, \ldots, \#E\text{-}1\}$

Compute $k_{PubB} = B = b \circ P = (x_B, y_B)$

Compute $b \circ A = T_{ab}$

The T_{ab} key received by both of them can be used to encrypt any message.



k_{AES} = xT

We can now use the joint key kAB for encryption e.g with AES

Y =AES_{kAES}(x)

Y

k_{AES} = xT

$x = AES^{-1}_{kAES}(y)$

Security Aspects

Why are parameters significantly smaller for elliptic curves (160-256 bit) than for RSA(1024-3076 bit)?

- Attacks on groups of elliptic curves are weaker than available factoring algorithms or integer DL attacks
- Best known attacks on elliptic curves (chosen according to cryptographic criterions) are the Baby-Step Giant-Step and Pollard-Rho method
- Complexity of these methods: on average, roughly $\sqrt{p}$ steps are required before the ECDLP can be successfully solved.

Implications to practical parameter sizes for elliptic curves:

- An elliptic curve using a prime p with 160 bit (and roughly 2^{160} points) provides a security of 2^{80} steps that required by an attacker (on average).
- An elliptic curve using a prime p with 256 bit (roughly 2^{256} points) provides a security of 2^{128} steps on average.

References

- Understanding Cryptography by Prof. Christof Paar and Jan Pelzl (Springer) pdf
- http://itchyfish.com/advantages-and-disadvantages-of-symmetric-and-asymmetric-key-encryption-methods/
- https://www.youtube.com/watch?v=2aHkqB2-46k&list=PL6N5qY2nvvJE8X75VkXglSrVhLv1tVcfy
- www.crypto-textbook.com
- http://security.stackexchange.com/questions/5402/what-are-private-key-cryptography-and-public-key-cryptography-and-where-are-the

THANK YOU