HA NOI UNIVERSITY OF SCIENCE AND TECHNOLOGY
SCHOOL OF INFORMATION AND COMMUNICATION TECHNOLOGY

Introduction to Cryptography and Security

Elliptic Curve Cryptosystems

Outline

Motivation:

Find public key family with shorter operands

Symmetric key size (bits)	Keysize for Elliptic Curve based scheme	Keysize for RSA or Diffie-Hellman
80	160	1024
112	224	2048
128	256	3072
192	384	7680
256	521	**15360**

Table: Bit lengths of public-key algorithms for different security levels

Definition

The **elliptic curve over** K is the set of all pairs $(x, y) \in K$ which fulfill

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

together with an imaginary point of infinity $\mathcal{O}$, where

$$a, b \in K$$

and the condition

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

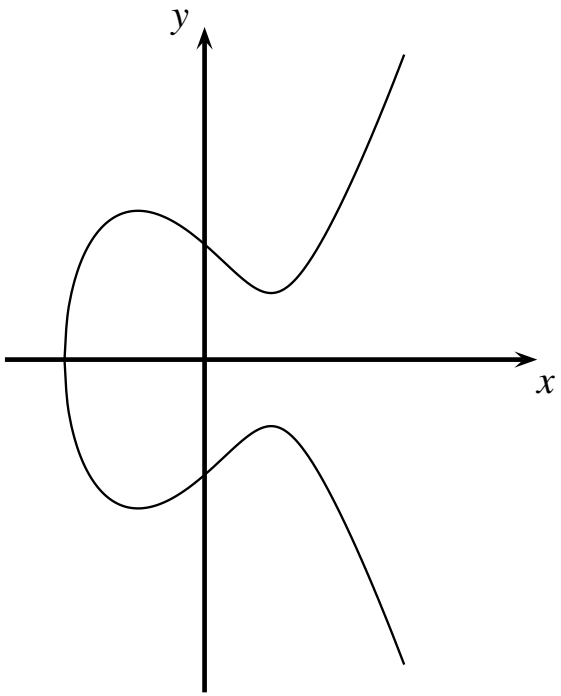
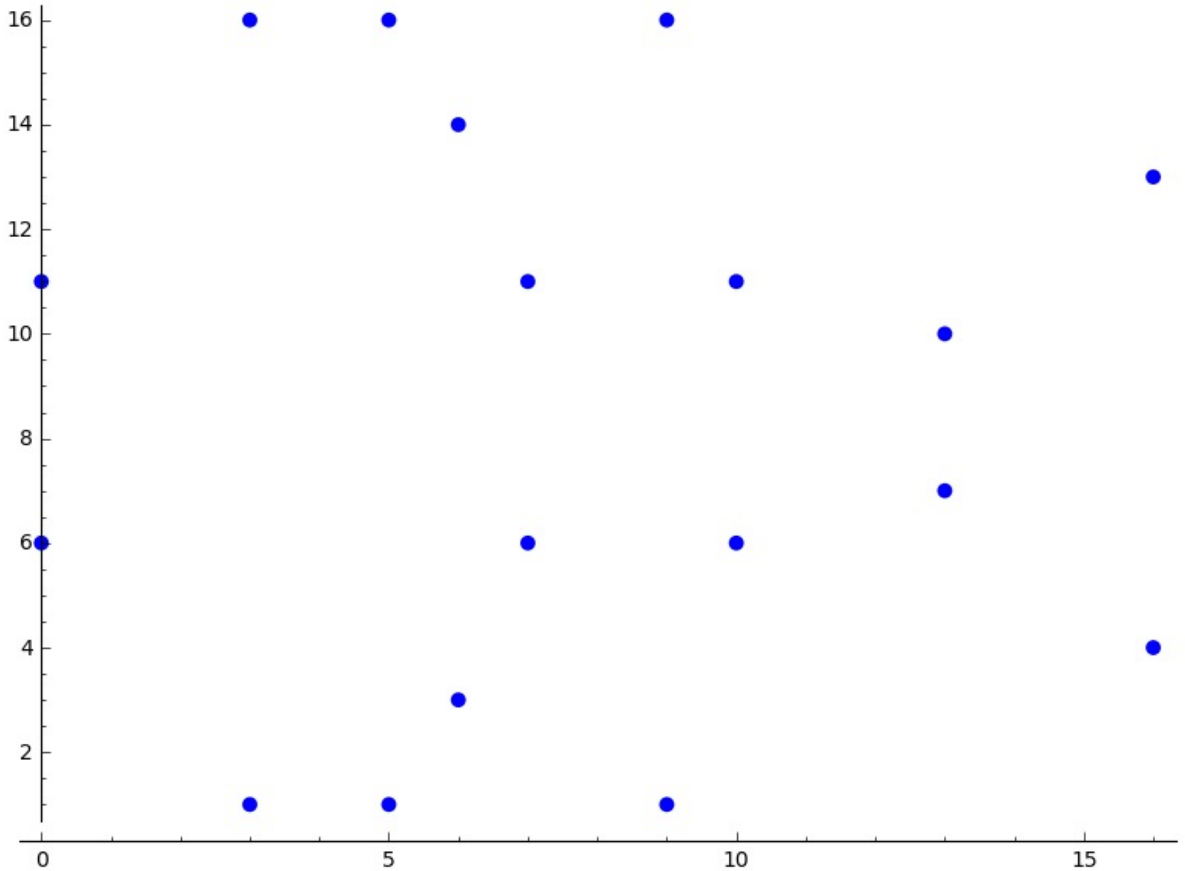


Figure: Elliptic curve $y^2 = x^3 - 3x + 3$ over $\mathbb{R}$

Elliptic curve $y^2 = x^3 + 2x + 2$ over $\mathbb{Z}_{17}$



$$\mathcal{O},$$
$$(0,6),\ (0,11),$$
$$(3,1),\ (3,16),$$
$$(5,1),\ (5,16),$$
$$(6,3),\ (6,14),$$
$$(7,6),\ (7,11),$$
$$(9,1),\ (9,16),$$
$$(10,6),\ (10,11),$$
$$(13,7),\ (13,10),$$
$$(16,4),\ (16,13)$$

Group Operations on EC

- Denote the group operation with addition symbol "$+$".
- Given two points and their coordinates

$$P = (x_1, y_1) \text{ and } Q = (x_2, y_2)$$

we have to compute coordinates of a third point R such that:

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

- **Point Addition** $P + Q$: This is the case where we compute

$$R = P + Q \text{ and } P \neq Q.$$

- **Point Doubling** $P + P$: This is the case where we compute

$$P + Q \quad \text{but} \quad P = Q.$$

Group operations

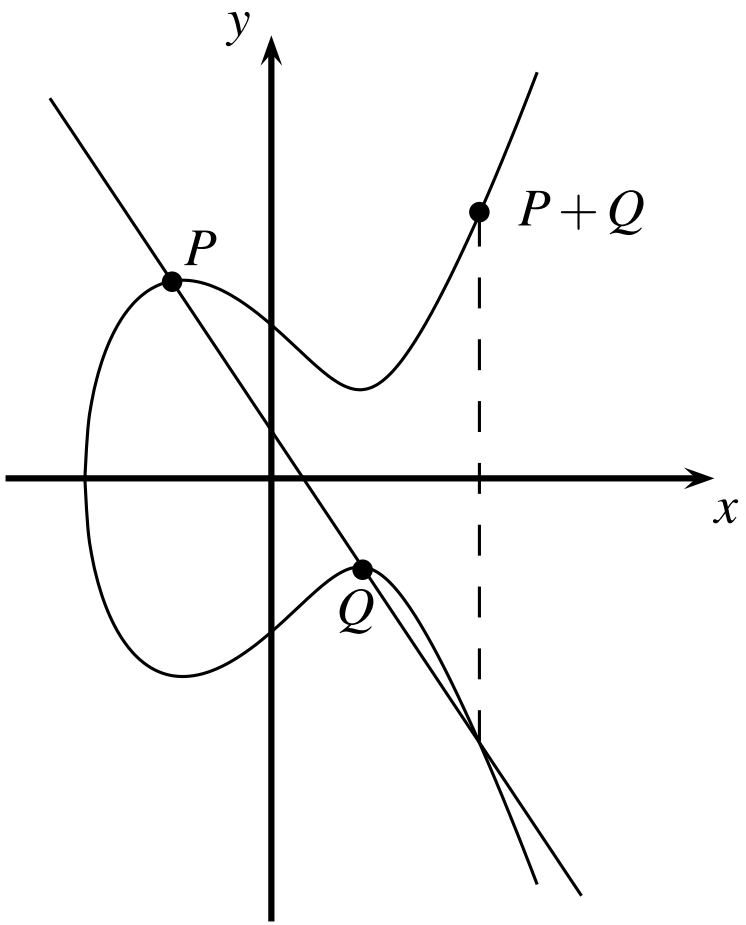


Figure: Point Addition

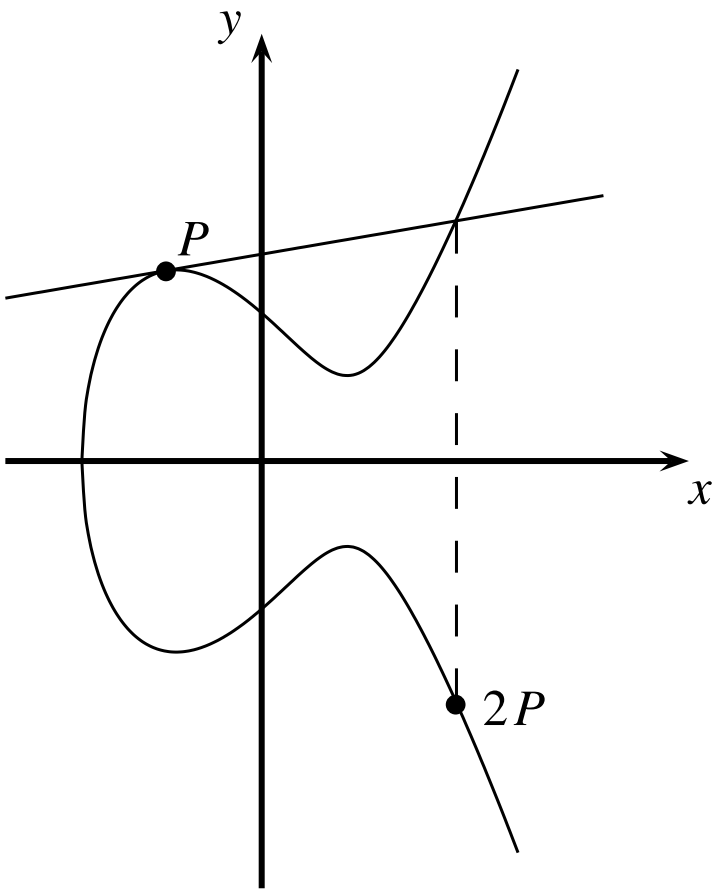


Figure: Point Doubling

Point Addition and Point Doubling

$$x^3 = s^2 - x_1 - x_2 \mod p$$
$$y^3 = s(x_1 - x_3) - y_1 \mod p$$

where

$$s = \begin{cases} (y_2 - y_1)/(x_2 - x_1) \mod p & \text{if } P \neq Q \\ (3{x_1}^2 + a)/(2y_1) \mod p & \text{if } P = Q. \end{cases}$$

Example

Consider the curve

$$E: \qquad y^2 = x^3 + 2x + 2 \mod 17$$

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

$$2P = P + P = (5,1) + (5,1) = (x_3, y_3)$$
$$s = (3{x_1}^2 + a)/(2y_1) = (3 \cdot 5^2 + 2) \cdot (2 \cdot 1)^{-1} = 9 \cdot 2^{-1} = 13 \mod 17$$
$$x_3 = s^2 - x_1 - x_2 = 13^2 - 5 - 5 = 6 \mod 17$$
$$y_3 = s(x_1 - x_3) - y_1 = 13 \cdot (5 - 6) - 1 = -14 = 3 \mod 17$$
$$2P = (5,1) + (5,1) = (6,3)$$

Play with Sagemath

```
sage: E = EllipticCurve(GF(17),[2,2])
sage: E
Elliptic Curve defined by y^2 = x^3 + 2*x + 2 over
    Finite Field of size 17
sage: P = E(5,1)
sage: Q = P + P
sage: print Q
(6 : 3 : 1)
sage: E.is_on_curve(6,3)
True
```

Complete addition laws for elliptic curves

1. $\mathcal{O} + \mathcal{O} = \mathcal{O}$
2. $\mathcal{O} + (x_2, y_2) = (x_2, y_2)$
3. $(x_1, y_1) + \mathcal{O} = (x_1, y_1)$
4. $(x_1, y_1) + (x_1, -y_1) = \mathcal{O}$
5. for $y_1 \neq 0$,

$$(x_1, y_1) + (x_1, y_1) = (s^2 - 2x_1, s(x_1 - x_3) - y_1)$$

where $s = (3{x_1}^2 + a)/(2y_1)$

6. for $x_1 \neq x_2$,

$$(x_1, y_1) + (x_1, y_1) = (s^2 - x_1 - x_2, s(x_1 - x_3) - y_1)$$

where $s = (y_2 - y_1)/(x_2 - x_1)$

Properties

1. $\mathcal{O} + \mathcal{O} = \mathcal{O}$
2. $\mathcal{O} + (x_2, y_2) = (x_2, y_2)$
3. $(x_1, y_1) + \mathcal{O} = (x_1, y_1)$
4. $\underbrace{(x_1, y_1)}_{P} + \underbrace{(x_1, -y_1)}_{-P} = \mathcal{O}$

$\mathcal{O}$ is the identity element of the group.

```
sage: O = P + -P
sage: O
(0 : 1 : 0)
sage: O + O == O
True
sage: P + O
(5 : 1 : 1)
sage: P + O == P
True
sage: O + P == P
True
```

Projective coordinates

- The project point

$$(X : Y : Z),\ Z \neq 0$$

  corresponds to the affine point $(X/Z, Y/Z)$.
- The project equation of elliptic curve is

$$Y^2Z = X^3 + aXZ^2 + bZ^3$$

- The point at infinite $\mathcal{O}$ corresponds to$(0 : 1 : 0)$, while the negative of$(X : Y : Z)$ is $(X : -Y : Z)$.

Benefit of projective cordinates

- The explicit formulas for computing $+$ become much faster, by avoiding field inversions
- Thus the fundamental ECC operation kP becomes much faster

$$(x', y') = 2(x, y)$$

$$s = \frac{3x^2 + a}{2y}$$
$$x' = s^2 - 2x$$
$$y' = s(x - x') - y$$

$$(X' : Y' : Z') = 2(X : Y : Z)$$

$$X' = 2XY\left(3X^2 + aZ^2\right)^2 - 8Y^2XZ$$
$$Y' = (3X^2 + aZ^2)(12Y^2XZ - (3X^2 + aZ^2)^2) - 8Y^4Z^2$$
$$Z' = 8Y^3Z^3$$

Play with Sagemath

```
sage: E = EllipticCurve(GF(17),[2,2])
sage: E
Elliptic Curve defined by y^2 = x^3 + 2*x + 2 over
    Finite Field of size 17
sage: for P in E:
....:     print P
....:
```

```
(0 : 1 : 0)
(0 : 6 : 1)
(0 : 11 : 1)
(3 : 1 : 1)
(3 : 16 : 1)
(5 : 1 : 1)
(5 : 16 : 1)
(6 : 3 : 1)
(6 : 14 : 1)
(7 : 6 : 1)
(7 : 11 : 1)
(9 : 1 : 1)
(9 : 16 : 1)
(10 : 6 : 1)
(10 : 11 : 1)
(13 : 7 : 1)
(13 : 10 : 1)
(16 : 4 : 1)
(16 : 13 : 1)
```

Outline

Cyclic subgroups

Theorem

The points on an Elliptic curve together with $\mathcal{O}$ have a cyclic subgroups. Under certain conditions all points on an elliptic curve form a cyclic group.

Example

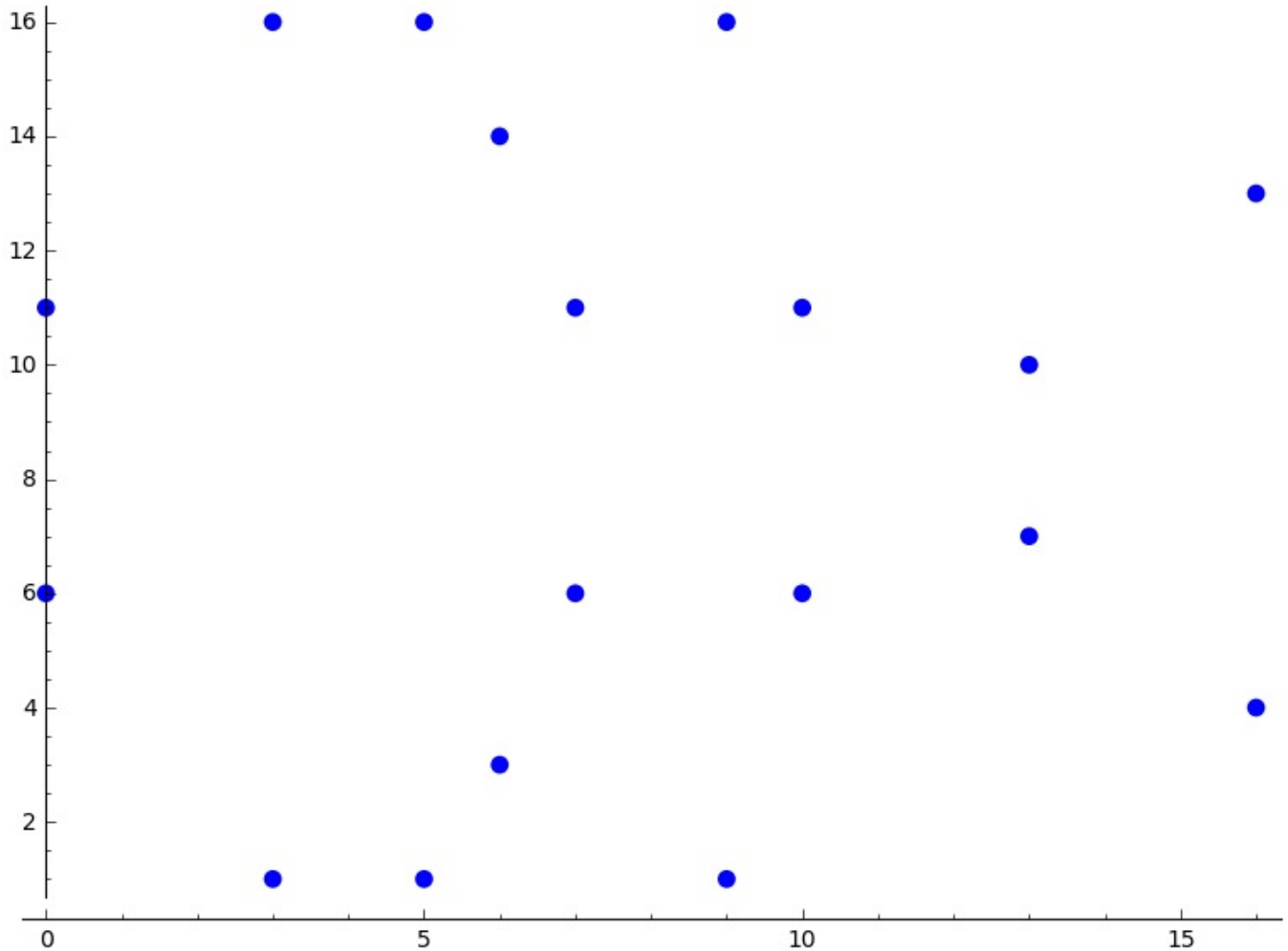
The points on EC $y^2 = x^3 + 2x + 2 \mod 17$ are

```
P  = (5,1)    6P = (16,13)  11P = (13,10) 16P = (10,11)
2P = (6,3)    7P = (0,6)    12P = (0,11)  17P = (6,14)
3P = (10,6)   8P = (13,7)   13P = (16,4)  18P = (5,16)
4P = (3,1)    9P = (7,6)    14P = (9,1)   19P = O
5P = (9,16)   10P = (7,11)  15P = (3,16)
```

Example

$y^2 = x^3 + 2x + 2 \mod 17$

```
P  = (5,1)
2P = (6,3)
3P = (10,6)
4P = (3,1)
5P = (9,16)
6P = (16,13)
7P = (0,6)
8P = (13,7)
9P = (7,6)
10P = (7,11)
11P = (13,10)
12P = (0,11)
13P = (16,4)
14P = (9,1)
15P = (3,16)
16P = (10,11)
17P = (6,14)
18P = (5,16)
19P = 0
```



Elliptic Curved Discrete Logarithm Problem (ECDLP)

Definition

Given is an elliptic curve E. We consider an element P and another element T.

The DL problem is finding the integer d such that

$$\underbrace{P + P + \cdots + P}_{d \text{ times}} = dP = T$$

Exercise

Consider the curve

$$E: \quad y^2 = x^3 + 2x + 2 \mod 17$$

We already computed all "powers" of P.

```
P  = (5,1)    6P = (16,13)  11P = (13,10) 16P = (10,11)
2P = (6,3)    7P = (0,6)    12P = (0,11)  17P = (6,14)
3P = (10,6)   8P = (13,7)   13P = (16,4)  18P = (5,16)
4P = (3,1)    9P = (7,6)    14P = (9,1)   19P = O
5P = (9,16)   10P = (7,11)  15P = (3,16)
```

For $P = (5, 1)$ and $T = (16, 4)$, find the integer d such that $dP = T$.

Group cardinality

Theorem (Hass)

Given an elliptic curve E modulo p, the number of points on the curve is denoted by $\#E$ and is bounded by:

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

- $\#E \approx p$
- If we need an elliptic curve with 2^{256} points, we have to use a prime with 256 bits.

Security

- All EC protocols rely on the hardness of ECDLP
- If EC is chosen carefully, the best algorithm for computing the ECDLP requires $\sqrt{p}$ steps
- Ex: $p \approx 2^{256}$
  Attack requires $\approx \sqrt{2^{256}} = 2^{128}$ steps.

It is believed in general that the best algorithm to solve ECDLP takes time

$$O(\sqrt{L})$$

where L is order of P.

Outline

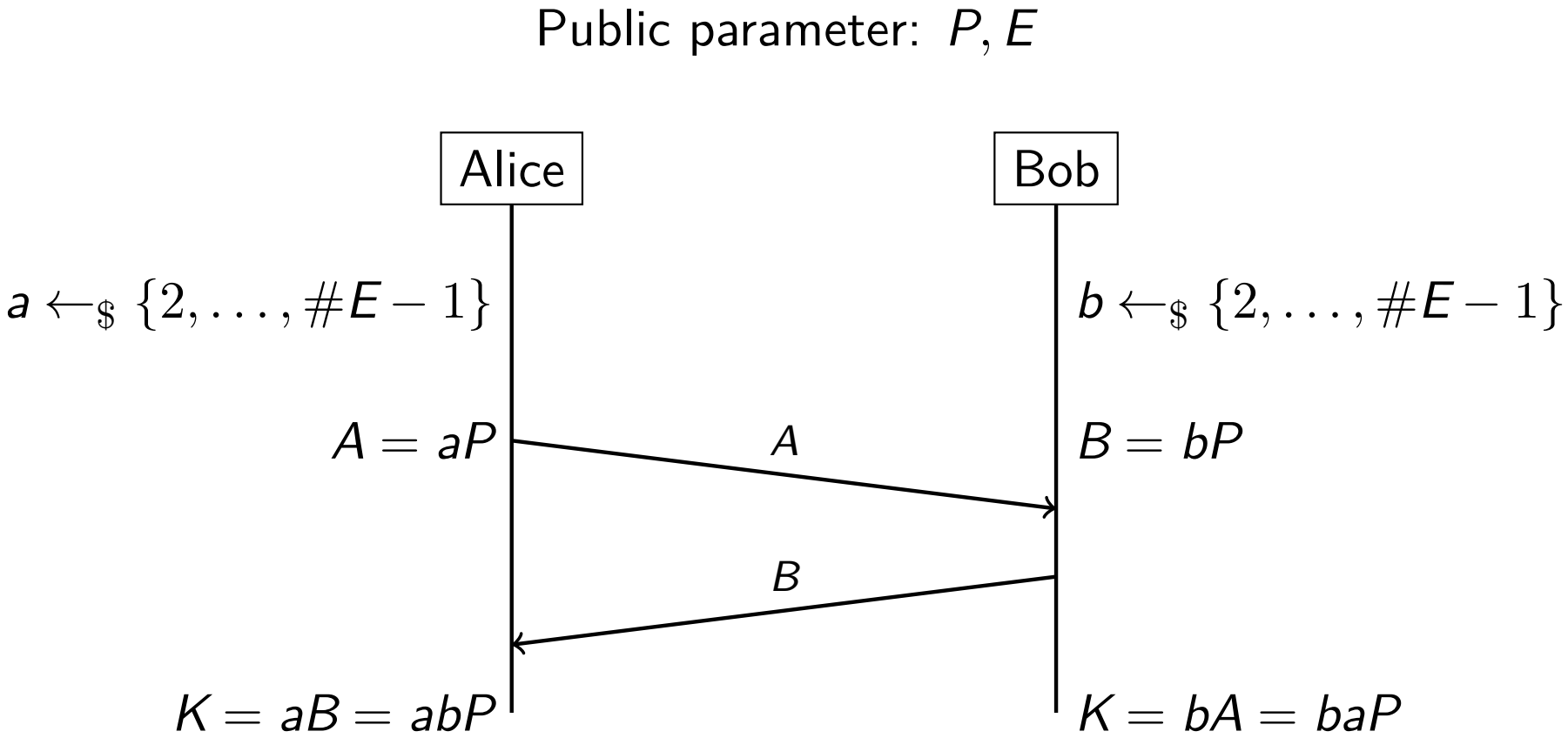
Phase I: ECDH Domain Parameters

1. Choose a prime p and the elliptic curve

$$E: \qquad y^2 = x^3 + ax + b \mod p$$

2. Choose a point $P = (x_P, y_P)$

Phase II: Key Exchange



Single-scalar multiplication

```
1 def scalarmult(n,P):
2     if n == 0: return 0
3     if n == 1: return P
4     R = scalarmult(n//2,P)
5     R=R+R
6     if n % 2: R = R + P
7     return R
```

- CPU time is dominated by time to compute $\log_2(n)$ point doublings
- Example of worst case: 4 doublings; 4 more additions.

$$31P = 2(2(2(2P + P) + P) + P) + P.$$

- Average case is better: 5 doublings; 2 additions.

$$35P = 2(2(2(2(2P))) + P) + P.$$

The security of the DH key exchange

- An eavesdropper sees the values aP and bP
- It has to compute the value $K_{ab} = abP$
- The hardness of the computation is expressed via two problems believed to be difficult

Decision Diffie Hellman (DDH)

Given(P, aP, bP, cP), to decide if $ab = c$.

Computational Diffie Hellman (CDH)

Given(P, aP, bP), to compute abP.

Computational Diffie-Hellman Assumption

Computation DH assumption holds in E if: $P, aP, bP \not\Rightarrow abP$.

for all efficient algorithm A:

$$\Pr[A(P, aP, bP) = abP] < \text{ negligible}$$

where $P \leftarrow_{\$} \{$ generators of $E \}$, $a, b \leftarrow_{\$} \mathbb{Z}_n$

The curve P256

The curve has the form

$$y^2 = x^3 - 3x + b \mod p$$

where

- the prime $p = 2^{256} - 2^{224} + 2^{192} + 2^{96} - 1$
- and b in hexadecimal is:

  `5ac635d8 aa3a93e7 b3ebbd55 769886bc 651d06b0 cc53b0f6 3bce3c3e`

The curve P256

- The prime p is close to 2^{256}, the number of points is also close to 2^{256}.
- Then, computing discrete log take approximately 2^{128}.
- How was the odd looking parameter b in P256 selected? We don't know!
- P256 is widely used in practice.

Quiz 1

Consider the curve

$$E: \quad y^2 = x^3 + 2x + 2 \mod 17$$

and two points $P = (5, 1)$ and $Q = (10, 6)$ on E.

What is $R = P + Q$?

1. $R = (15, 7)$
2. $R = (15, 7)$
3. $R = \mathcal{O}$

Quiz 2

Consider the curve

$$E: \quad y^2 = x^3 + 2x + 2 \mod 17$$

and two points $P = (5, 1)$ and $Q = (10, 6)$ on E.

What is the integer d where $1 \leq d \leq \#E$, such that: $dQ = P$?

1. $d = 1$
2. $d = 13$
3. $d = 17$
4. There is no d.

ĐẠI HỌC BÁCH KHOA

25 YEARS ANNIVERSARY SOICT

VIỆN CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG

SCHOOL OF INFORMATION AND COMMUNICATION TECHNOLOGY

Thank you!

soict.hust.edu.vn/ fb.com/groups/soict