LAURIER
Inspiring Lives.

Chapter 7

ElGamal and Elliptic Curve

Outline

- ElGamal Cryptosystem
- Elliptic Curve Cryptography

Recap: Discrete Logarithm Problem

- Let $(G, \cdot)$ be an abelian group.
- **Discrete Logarithm Problem** Given $g, h \in G$, find an x (if it exists) such that

$$g^x = h.$$

- The difficulty of this problem depends on the group G:
  - Very easy: polynomial time algorithm, e.g. $(\mathbb{Z}_N, +)$
  - Hard: sub-exponential time algorithm, e.g. $(\mathbb{Z}_p, \times)$.
  - Very hard: exponential time algorithm, e.g. elliptic curve groups.

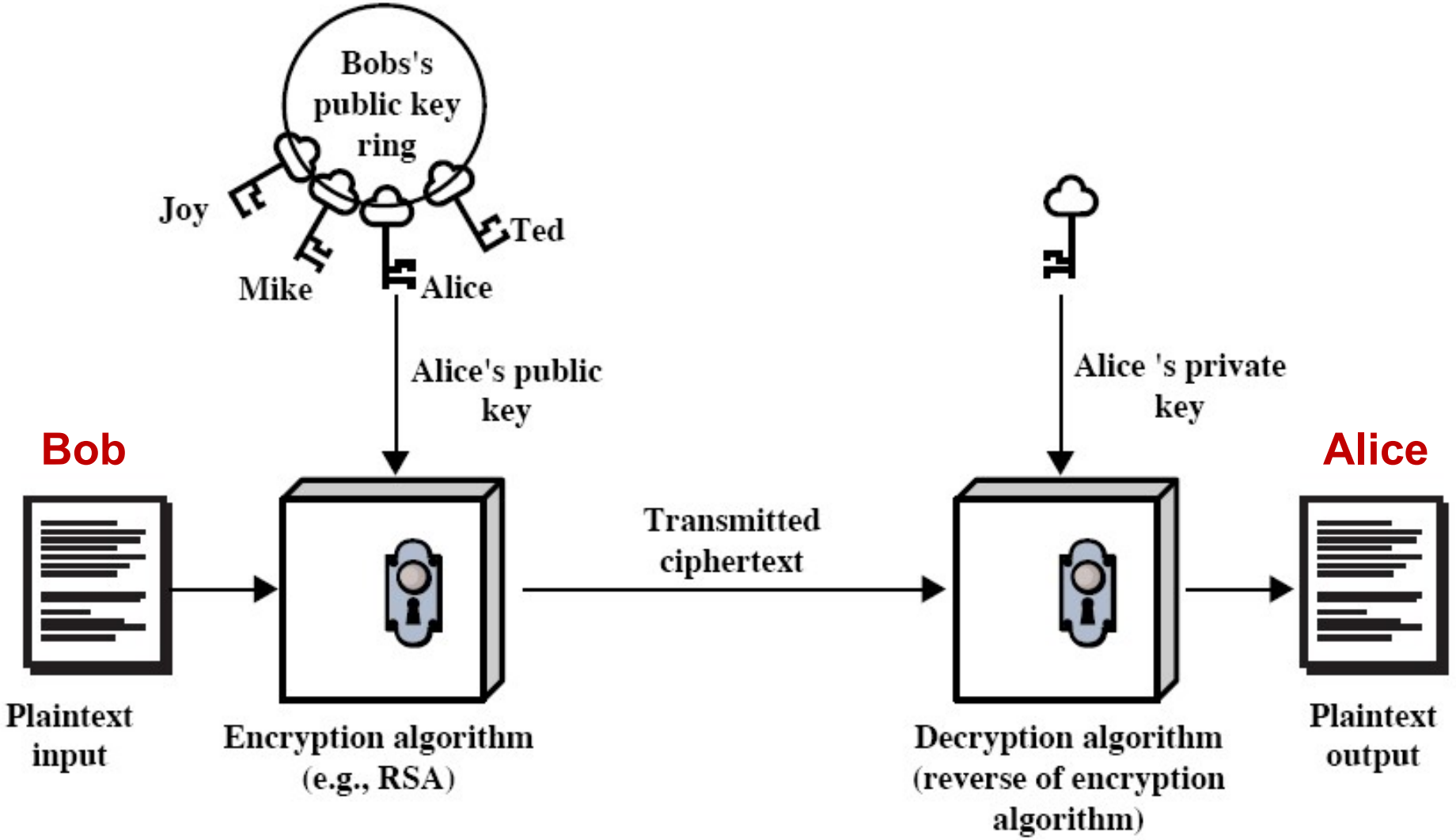
Problems Related DLP

- Given an abelian group $(G, \cdot)$ and $g \in G$ of order n.
- **Discrete Logarithm Problem (DLP)** :
  Given $h \in G$ such that $h = g^x$ find x. $(\mathrm{DLP}(g, h) \rightarrow x)$
- **Computational Diffie-Hellman Problem (CDH)** :
  Given $a = g^x$ and $b = g^y$ find $c = g^{xy}$ $(\mathrm{CDH}(g, a, b) \rightarrow c)$.
- **Decisional Diffie-Hellman Problem (DDH)** :
  Given $a = g^x$, $b = g^y$ and $c = g^z$, determine if

$$g^{xy} = g^z \text{ or equivalently } xy \equiv z \bmod n$$

$(\mathrm{DDH}(g, a, b, c) \rightarrow \text{true/false})$

Recap: Public-Key Cryptography

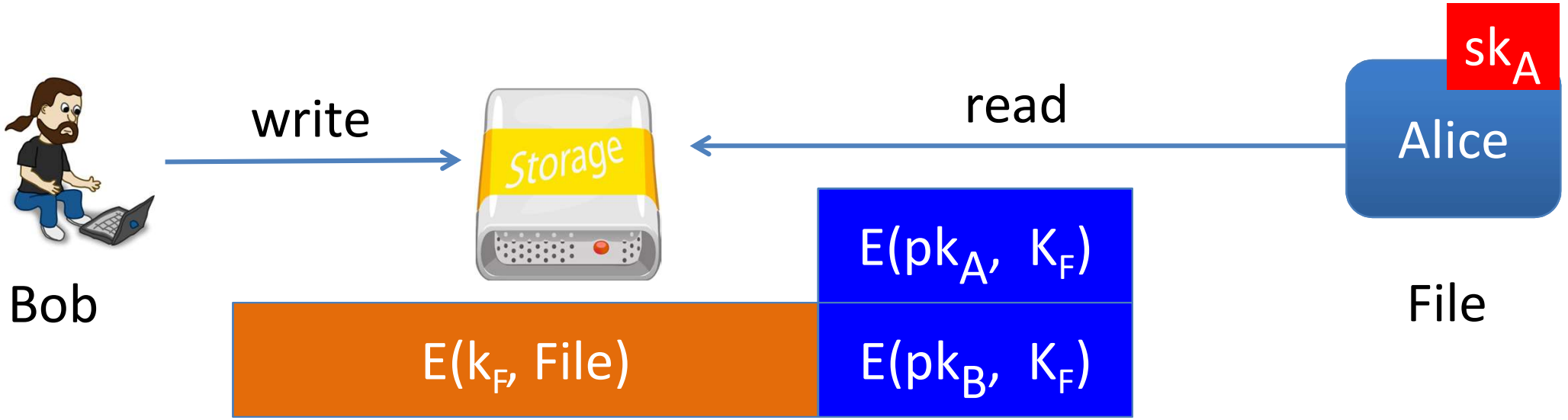


Public-key encryption applications

Key exchange (e.g. in HTTPS)

Encryption in non-interactive settings:

- Secure Email: Bob has Alice's pub-key and sends her an email
- Encrypted File Systems

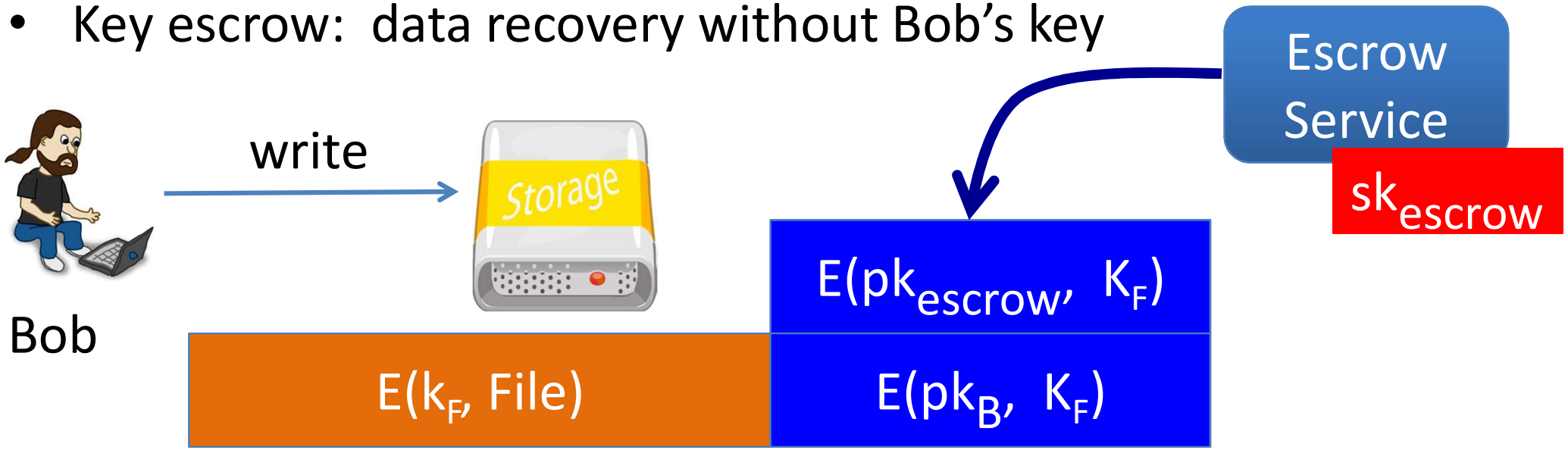


Public-key encryption applications

Key exchange (e.g. in HTTPS)

Encryption in non-interactive settings:

- Secure Email: Bob has Alice's pub-key and sends her an email
- Encrypted File Systems
- Key escrow: data recovery without Bob's key



The Diffie-Hellman protocol (1977)

Fix a finite cyclic group G (e.g $G = (Z_p)^*$) of order n

Fix a generator g in G (i.e. $G = \{1, g, g^2, g^3, \dots, g^{n-1}\}$)

Alice **Bob**

choose random **a** in {1,…,n} choose random **b** in {1,…,n}

$A = g^a$

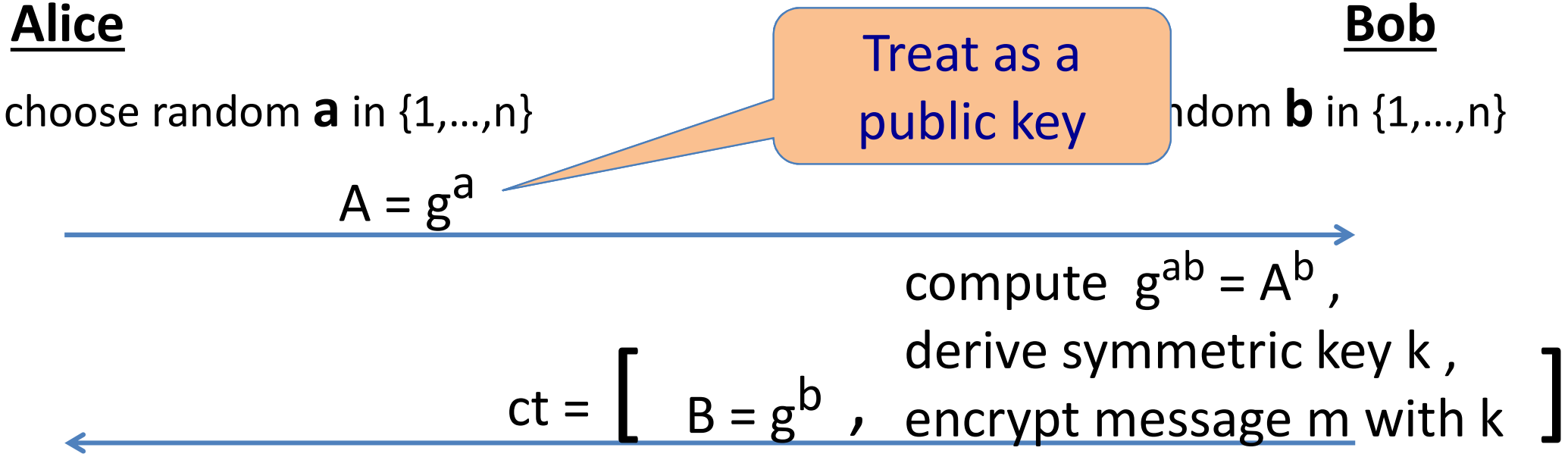
$B = g^b$

$\mathbf{B^a} = (g^b)^a =$ **$k_{AB} = g^{ab}$** $= (g^a)^b = \mathbf{A^b}$

ElGamal: converting to pub-key enc. (1984)

Fix a finite cyclic group G (e.g $G = (Z_p)^*$) of order n

Fix a generator g in G (i.e. $G = \{1, g, g^2, g^3, \ldots, g^{n-1}\}$)



ElGamal: converting to pub-key enc. (1984)

Fix a finite cyclic group G (e.g $G = (Z_p)^*$) of order n

Fix a generator g in G (i.e. $G = \{1, g, g^2, g^3, \ldots, g^{n-1}\}$)

Alice

choose random **a** in {1,…,n}

Treat as a public key

$A = g^a$

Bob

choose random **b** in {1,…,n}

choose symmetric key k ,
compute $C = kg^{ab} = kA^b$,
encrypt message m with k

$ct = [\ B = g^b\ ,$ encrypt message m with k $]$

To decrypt:
compute $g^{ab} = B^a$,
derive k, and decrypt

ElGamal Encryption (1984)

- G: finite cyclic group of order n
- $(sk_A, pk_A)=(a, g^a)$: Alice's secret-public key pair

Bob:

E(pk=(g, pk_A), m) :

$b \xleftarrow{R} Z_n$, $u \leftarrow g^b$,

$v \leftarrow m \cdot pk_A^{\,b}$,

output (u, v)

Alice:

D(sk=a, (u, v)) :

$m \leftarrow v \cdot u^{-a}$

output m

ElGamal Example

1. Setup:

1.Let p = **23,** select a generator g = **11**

2.Choose a private key x = **6**

3.Compute y = 11^{6} (mod **23**) = **9**

Public key is **9** Private key is **6**

2. Encryption:

To encrypt M = 10 using Public key **9**

1 - Generate a random number k = **3**

2 - Compute

$C_1 = 11^3 \bmod 23 = 20$

$C_2 = 10 \times 9^3 \bmod 23$

$= 10 \times 16 = 160 \bmod 23 = 22$

3 - Ciphertext C = (**20** , **22**)

3. Decryption:

To decrypt C = (**20** , **22**)

1 - Compute $20^6 = 16 \bmod 23$

2 - Compute **22** / 16 = 10 mod **23**

3 - Plaintext = 10

ElGamal is CPA Secure

The semantic security of the ElGamal encryption is equivalent to the decision Diffie-Hellman problem [1].

ElGamal is not CCA Secure, Why?

[1] Y. Tsiounis, and M. Yung. "On the security of ElGamal based encryption." In *Proc. of PKC*, pp. 117-134,1998.

The ElGamal system (a modern view)

- G: finite cyclic group of order n
- (E_s, D_s) : symmetric auth. encryption defined over (K,M,C)
- H: $G^2 \longrightarrow K$ a hash function

We construct a pub-key enc. system (Gen, E, D):

- Key generation Gen:
  - choose random generator g in G and random a in Z_n
  - output sk = a , pk = $(g, h=g^a)$

The ElGamal system (a modern view)

- G: finite cyclic group of order n
- (E_s, D_s) : symmetric auth. encryption defined over (K,M,C)
- H: $G^2 \longrightarrow K$ a hash function

E(pk=(g,h), m) :

$b \xleftarrow{R} Z_n$, $u \leftarrow g^b$, $v \leftarrow h^b$

$k \leftarrow H(u,v)$, $c \leftarrow E_s(k, m)$

output (u, c)

D(sk=a, (u,c)) :

$v \leftarrow u^a$

$k \leftarrow H(u,v)$, $m \leftarrow D_s(k, c)$

output m

Performance

E(pk=(g,h), m) :

$b \leftarrow Z_n$, $u \leftarrow g^b$, $v \leftarrow h^b$

D(sk=a, (u,c)) :

$v \leftarrow u^a$

Encryption: 2 exp. (fixed basis)

- Can pre-compute $[\, g^{(2\hat{}i)}$, $h^{(2\hat{}i)}$ for $i=1,\ldots,\log_2 n \,]$
- 3x speed-up (or more)

Decryption: 1 exp. (variable basis)

Outline

- ElGamal Cryptosystem
- Elliptic Curve Cryptography

Elliptic curves over R

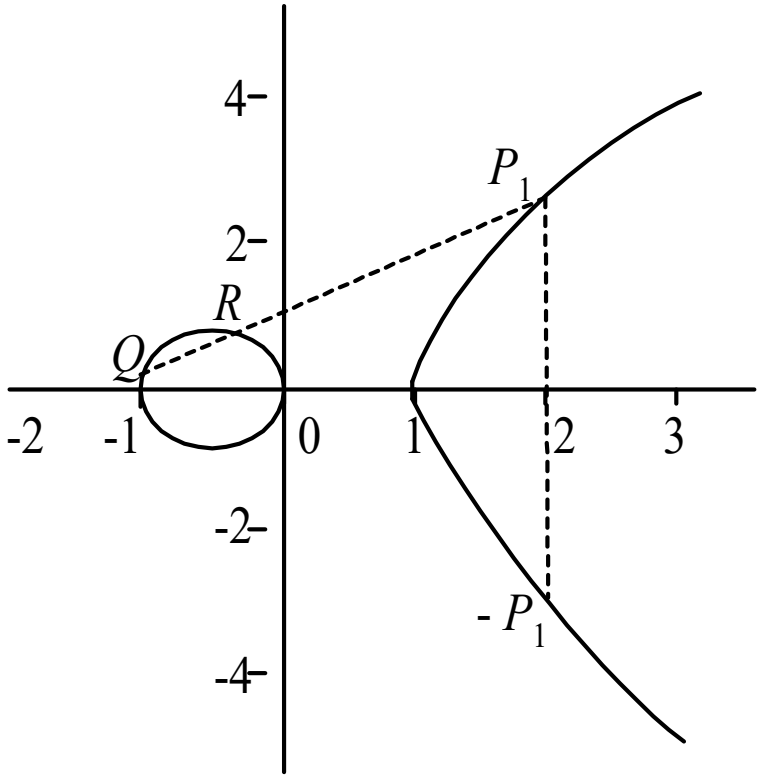
Let *a* and *b* be real numbers. An *elliptic curve* E over the field of real numbers **R** is the set of points (x,y) with *x* and *y* in **R** that satisfy the equation

$$E = \left\{ (x, y) \in \boldsymbol{R} \times \boldsymbol{R} \middle| y^2 = x^3 + ax + b \right\} \cup \left\{ \mathcal{O} \right\}$$

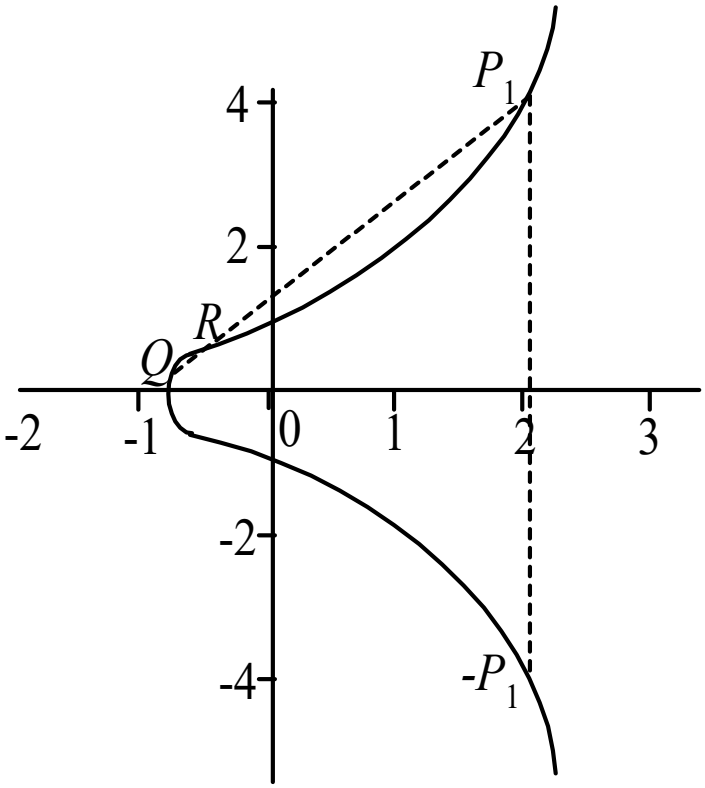
Where $a, b \in \boldsymbol{R}$, $4a^3 + 27b^2 \neq 0$ and $\mathcal{O}$ is called the *point at infinity*.

E is a non-singular elliptic curve

Examples



(a) $y^2=x^3-x$



(b) $y^2=x^3+x+1$

Operation +

Group operation + over E

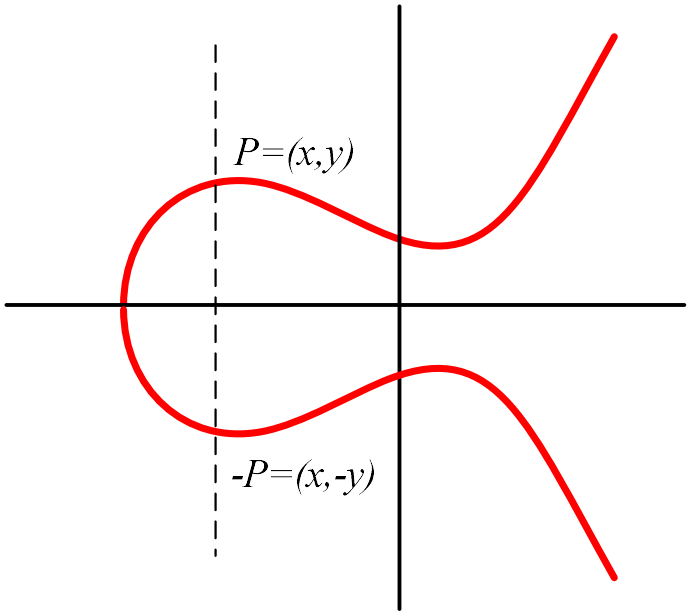
- E is an abelian group
- The point of infinity, $\mathcal{O}$, will be the identity element

Given $P, Q \in E, P = (x_1, y_1), Q = (x_2, y_2)$

$$P + \mathcal{O} = \mathcal{O} + P$$

If $x_1 = x_2$, and $y_1 = -y_2$, then $P + Q = \mathcal{O}$

(i.e. $-P = -(x_1, y_1) = (x_1, -y_1)$)



- Group operation +

  Given $P, Q \in E, P = (x_1, y_1), Q = (x_2, y_2)$

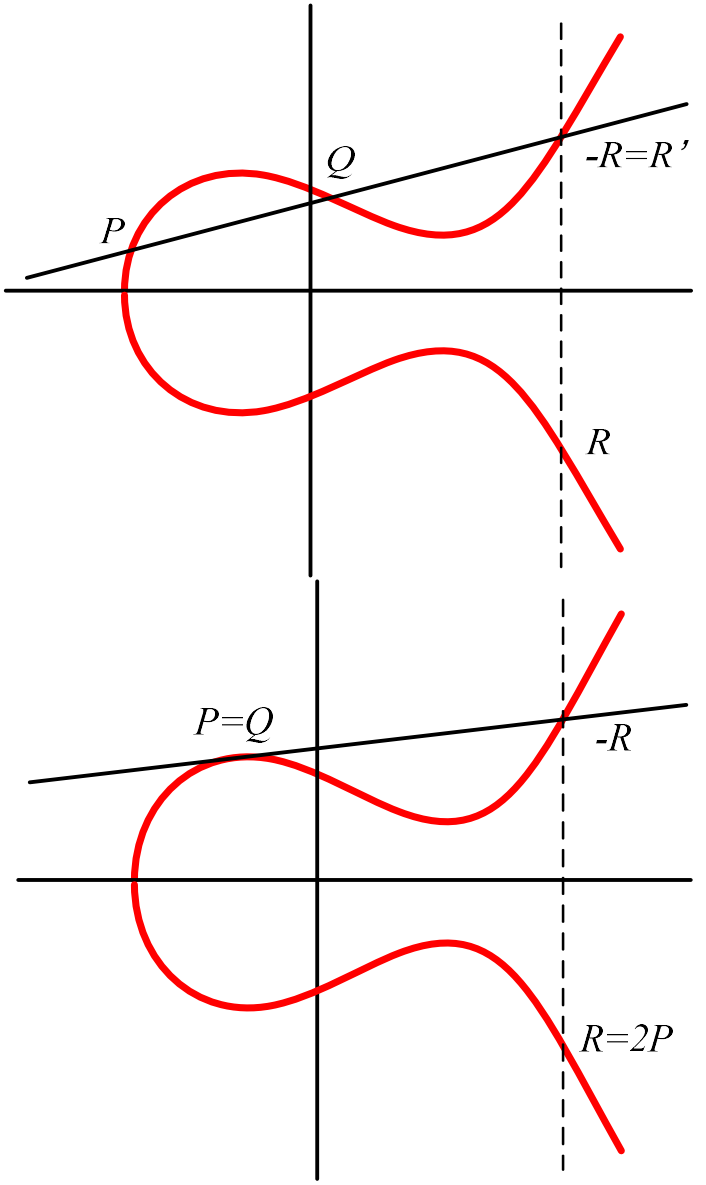
  Compute $R = P + Q = (x_3, y_3)$

  – Addition $(P \neq Q)$

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1}$$
$$x_3 = \lambda^2 - x_1 - x_2$$
$$y_3 = (x_1 - x_3)\lambda - y_1$$

  – Doubling $(P = Q)$

$$\lambda = \frac{3x_1^2 + a}{2y_1}$$
$$x_3 = \lambda^2 - 2x_1$$
$$y_3 = (x_1 - x_3)\lambda - y_1$$



Example: Addition

$$E : y^2 = x^3 - 25x$$

$$P = (x_1, y_1) = (0,0),\ Q = (x_2, y_2) = (-5,0),\ P + Q = (x_3, y_3)$$

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1} = \frac{0 - 0}{-5 - 0} = 0$$

$$x_3 = \lambda^2 - x_1 - x_2 = 0^2 - 0 - (-5) = 5$$

$$y_3 = (x_1 - x_3)\lambda - y_1 = (0 - 5) \times 0 - 0 = 0$$

Example: Doubling

$$E : y^2 = x^3 - 25x$$

$$P = (x_1, y_1) = (-4,6),\ 2P = (x_2, y_2)$$

$$\lambda = \frac{3x_1^{\,2} + a}{2y_1} = \frac{3(-4)^2 - 25}{2 \times 6} = \frac{23}{12}$$

$$x_2 = \lambda^2 - 2x_1 = \left(\frac{23}{12}\right)^2 - 2 \times (-4) = \frac{1681}{144}$$

$$y_2 = (x_1 - x_2)\lambda - y_1 = \left(-4 - \frac{1681}{144}\right) \times \frac{23}{12} - 6 = -\frac{62279}{1728}$$

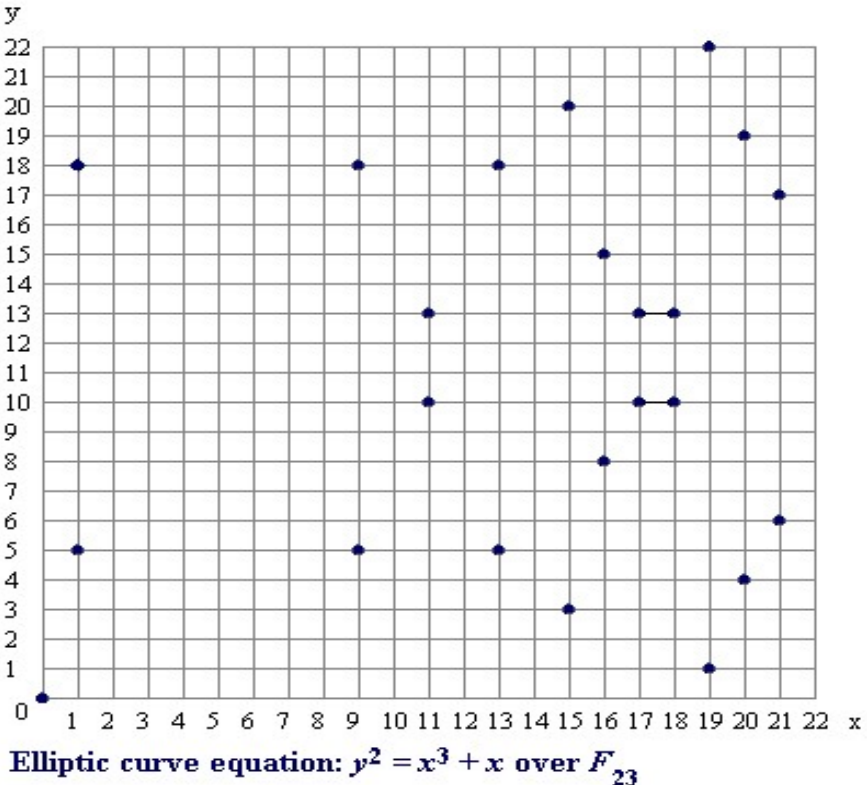
Elliptic curves over Fp

Let $p > 3, a, b \in Z_p,\ 4a^3 + 27b^2 \neq 0 \pmod{p}$

$$E = \left\{ (x, y) \in Z_p \times Z_p \middle| y^2 \equiv x^3 + ax + b \pmod{p} \right\} \cup \{ \mathcal{O} \}$$

Example:

$$E : y^2 = x^3 + x \text{ over } Z_{23}$$



Elliptic curve equation: $y^2 = x^3 + x$ over F_{23}

Example

$E : y^2 = x^3 + x + 6$ over Z_{11}

Find all *(x, y)* and $\mathcal{O}$:

Fix *x* and determine *y*

$\mathcal{O}$ is an artificial point

12 *(x, y)* pairs plus $\mathcal{O}$,

and have *#E=13*

x	$x^3 + x + 6$	quad res?	y
0	6	*no*	
1	8	*no*	
2	5	*yes*	4,7
3	3	*yes*	5,6
4	8	*no*	
5	4	*yes*	2,9
6	8	*no*	
7	4	*yes*	2,9
8	9	*yes*	3,8
9	7	*no*	
10	4	*yes*	2,9

Example (Cont.)

There are 13 points on the group $E(Z_{11})$ and so any non-identity point (i.e. not the point at infinity, noted as $\mathcal{O}$) is a generator of $E(Z_{11})$.

Choose generator

Compute $\alpha = (2,7)$

$$2\alpha = (x_2, y_2)$$

$$\lambda = \frac{3x_1^2 + a}{2y_1} = \frac{3(2)^2 + 1}{2 \times 7} = \frac{13}{14} = 2 \times 3^{-1} = 2 \times 4 = 8 \mod 11$$

$$x_2 = \lambda^2 - 2x_1 = (8)^2 - 2 \times (2) = 5 \mod 11$$

$$y_2 = (x_1 - x_2)\lambda - y_1 = (2 - 5) \times 8 - 7 = 2 \mod 11$$

Example (Cont.)

Compute $3\alpha = (x_3, y_3)$

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1} = \frac{2-7}{5-2} = 2 \mod 11$$

$$x_3 = \lambda^2 - x_1 - x_2 = 2^2 - 2 - 5 = 8 \mod 11$$

$$y_3 = (x_1 - x_3)\lambda - y_1 = (2-8)\times 2 - 7 = 3 \mod 11$$

So, we can compute

$$\alpha = (2,7) \quad 2\alpha = (5,2) \quad 3\alpha = (8,3)$$

$$4\alpha = (10,2) \quad 5\alpha = (3,6) \quad 6\alpha = (7,9)$$

$$7\alpha = (7,2) \quad 8\alpha = (3,5) \quad 9\alpha = (10,9)$$

$$10\alpha = (8,8) \quad 11\alpha = (5,9) \quad 12\alpha = (2,4)$$

Example (Cont.)

Let's modify ElGamal encryption by using the elliptic curve $E(Z_{11})$. Suppose that $\alpha = (2,7)$ and Bob's private key is 7, so

$$\beta = 7\alpha = (7,2)$$

Thus the encryption operation is

$$e_K(x,k) = \big(k(2,7), x + k(7,2)\big),$$

where $x \in E$ and $0 \le k \le 12$, and the decryption operation is

$$d_K(y_1, y_2) = y_2 - 7y_1.$$

Example (Cont.)

Suppose that Alice wishes to encrypt the plaintext x = (10,9) (which is a point on E).
If she chooses the random value k = 3, then

$$y_1 = 3(2,7) = (8,3) \text{ and}$$
$$y_2 = (10,9) + 3(7,2) = (10,9) + (3,5) = (10,2)$$

Hence $y = \big((8,3),(10,2)\big)$. Now, if Bob receives the ciphertext y, he decrypts it as follows: $x = (10,2) - 7(8,3) = (10,2) - (3,5)$

$$= (10,2) + (3,6) = (10,9)$$

Elliptic Curve DLP

Basic computation of ECC

$$Q = kP = \underbrace{P + P + \ldots + P}_{k \text{ times}}$$

where P is a curve point, k is an integer

Elliptic Curve Discrete Logarithm Problem (ECDLP)

- Given curve, the point P, and kP, it is hard to recover k

Security of ECC vs. RSA/ElGamal

- Elliptic curve cryptosystems give the most security per bit of any known public-key schemes.
- The ECDLP problem appears to be much more difficult than the integer factorisation problem and the discrete logarithm problem of Z_p.
- The strength of elliptic curve cryptosystems grows much faster with the key size increases than does the strength of RSA.

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

NIST Recommended Key Sizes

Thank You

Acknowledge

Dan Boneh, **Rong-Jaye Chen,** Guang Gong, and Shaoquan Jiang for PowerPoint Slides and figures

Field

A field is a set F, containing at least two elements, on which two operations + and · are defined so that for each pair of elements a, b in F there are unique elements a + b and a · b in F for which the following conditions hold for all elements a, b, c in F:

- *Associativity* of addition and multiplication: $a + (b + c) = (a + b) + c$ and $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.
- *Commutativity* of addition and multiplication: $a + b = b + a$ and $a \cdot b = b \cdot a$.
- *Additive* and *multiplicative identity*: there exist two different elements 0 and 1 in F such that $a + 0 = a$ and $a \cdot 1 = a$.
- *Additive inverses*: for every a in F, there exists an element in F, denoted $-a$, called *additive inverse* of a, such that $a + (-a) = 0$.
- *Multiplicative inverses*: for every $a \neq 0$ in F, there exists an element in F, denoted by a^{-1}, $1/a$, or $1/a$, called the *multiplicative inverse* of a, such that $a \cdot a^{-1} = 1$.
- Distributivity of multiplication over addition: $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$.

Field examples

- Any field is an abelian group under + and the non-zero elements of a field form an abelian group under $\cdot$.
- Some examples of fields:
  - Real numbers
  - Z_p, the set of *integers modulo* p, where p is a prime number is a *finite* field.
  - For example,

    $Z_7 = \{0, 1, 2, 3, 4, 5, 6\}$ and $Z_{23} = \{0, 1, 2, 3, \ldots, 22\}$.

Finite Field

- Let p be a prime, then $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ is a finite field with p elements.
- Every non-zero element has inverse for multiplication.
- Thus: $\mathbb{F}_p^*, \times$ has $p - 1$ elements.
- Theorem: $\mathbb{F}_p^*, \times$ is cyclic, i.e. there exists a generator α such that $\mathbb{F}_p^* = \{\alpha^0, \alpha^1, \alpha^2, \ldots\}$.
- Extension field $\mathbb{F}_{p^n}$: polynomials over $\mathbb{F}_p$ modulo irreducible polynomial $P(x)$ of degree n, i.e. $\mathbb{F}_p[x]/(P(x))$.