Application of Number Theory to Cryptology

Atsuko Miyaji, Dr of Sci.
Professor

Japan Advanced Institute Science & Technology
miyaji@jaist.ac.jp

Outline

There are many application with using cryptology.

- Examples of products with using cryptology
- SSL through Internet
- SSL uses public key cryptosystems

What is the public key cryptosystem?

- principle of the public key cryptosystem
- how to achieve a public key cryptosystem
  - number theory
- Example of public key cryptosystems
  - ElGamal encrypion

What are elliptic curve cryptosystems?

- why Elliptic curve encryption is the most efficient?

A new tool from mathematics achieves a new function

- how to apply a bilinear map to a cryptosystem

Products which use cryptology

There are many application using cryptology around us.

- DVD copyright protection
- ETC (Electronic Toll Collection System)
- SSL (Secure Sockets Layer)
- Electronic money Edy
- Electronic train ticket- SUICA, ICOCA
- Wireless LAN

→Cryptology is a key technology of e-commerce.

What is a basic field of cryptology?

Mathematics such as number theory
Computational theory
Information theory
Code theory

SSL (Secure Socket Layer)

Encryption/signature protocol

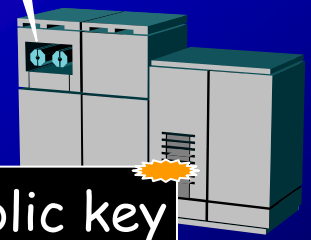
For applications of shopping through internet, achieve secure communication.

SSL-Web site

1. Handshake protocol
   i. server authentication: user gets the public key of a server.
   ii. key agreement: user and server share a secret key.

user

Server



Public key

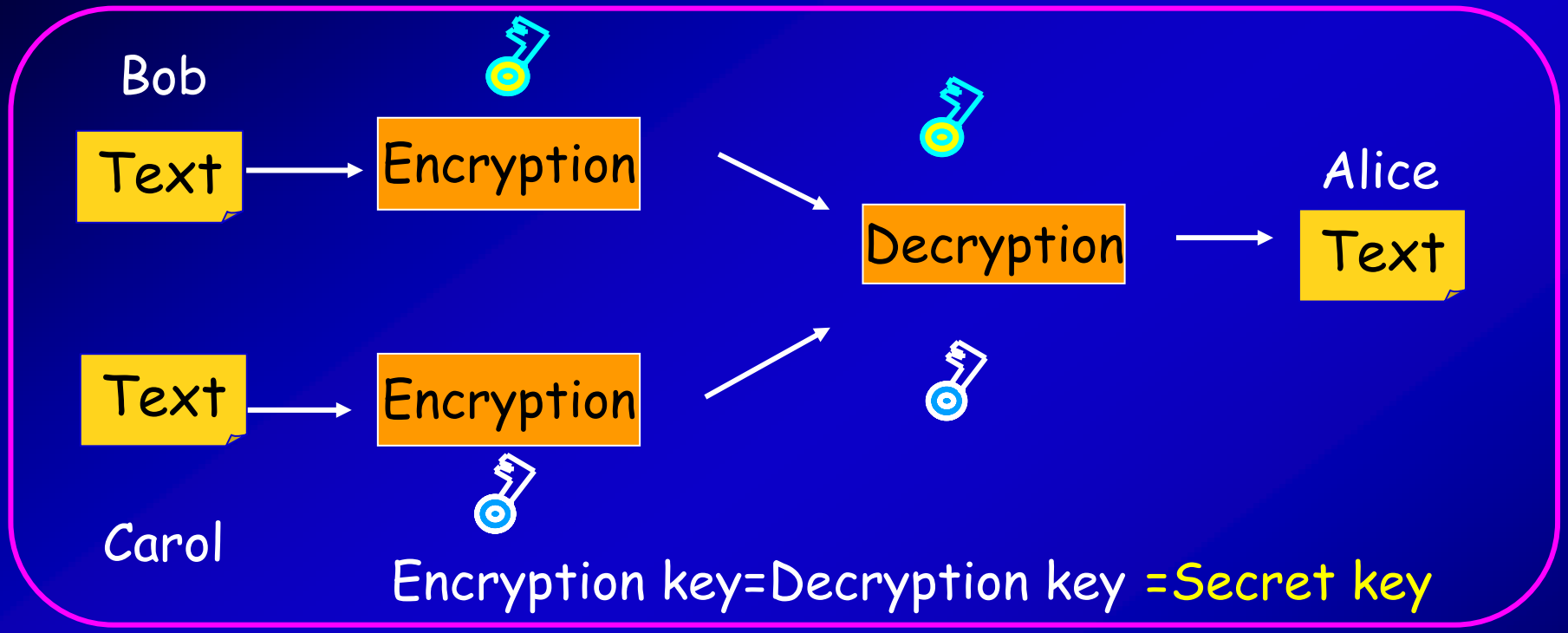
2. Secure communication by encryption

WWW, mail, ftp, etc..

?

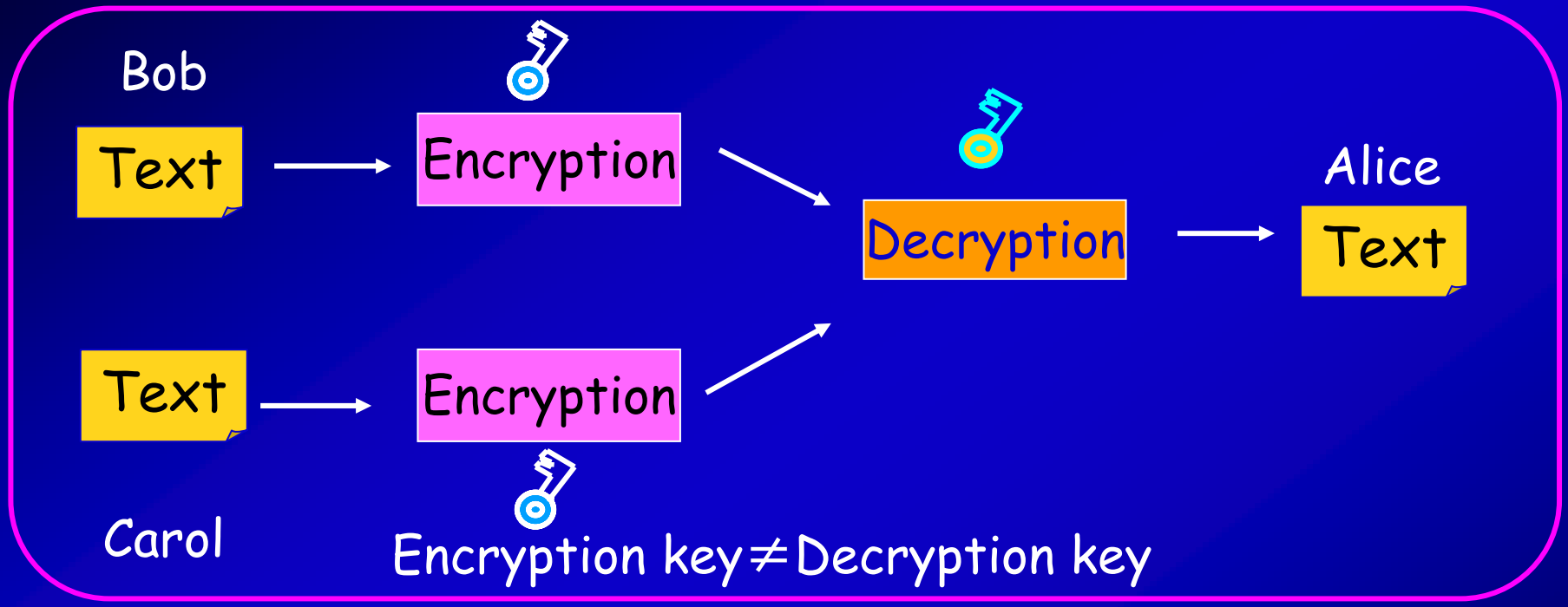
How we shared a key?

Secret key cryptosystems



・Encryption key is the same as decryption key.
→encryption (decryption) key is kept secretly as a secret key.
・Each sender should use a different key. (messy key management)
→For N senders, N keys are required.
・Beforehand, users need to share a key secretly.
→Need a Secure Network or bring a key on foot.
(messy key agreement)

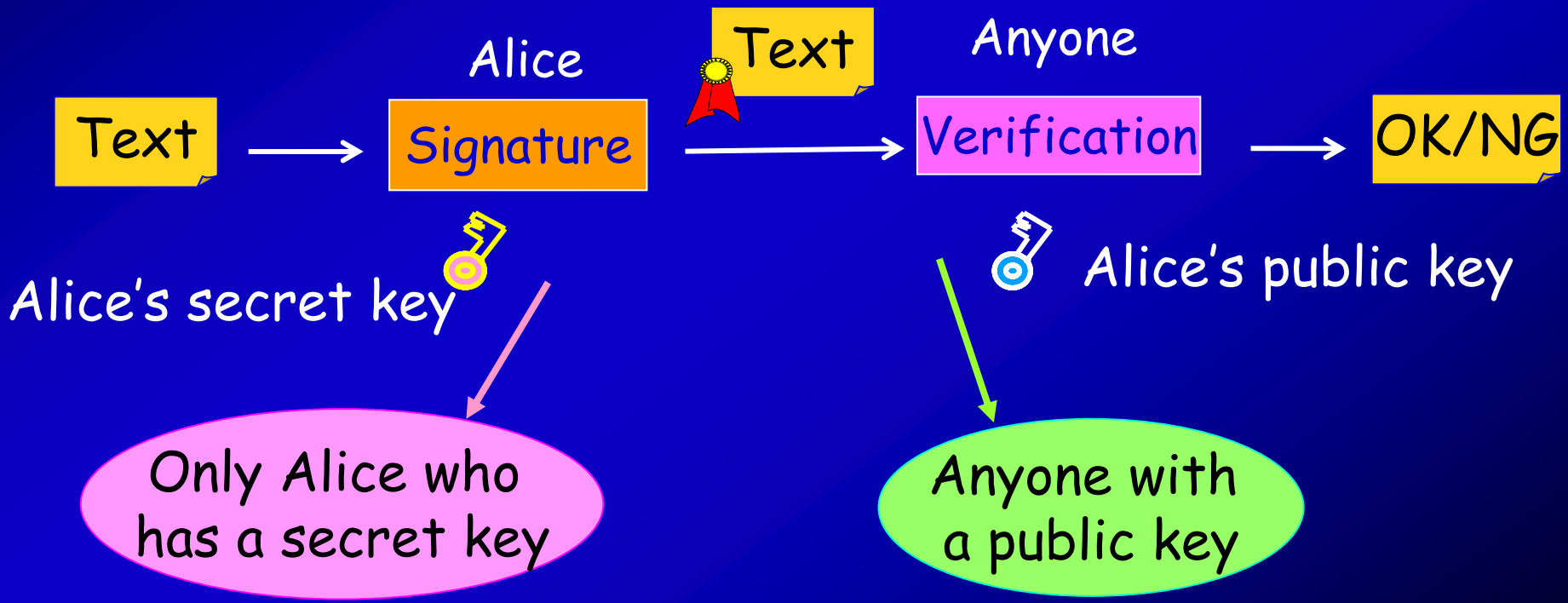
Public key cryptosystems



- Encryption key≠Decryption key
⇒Encryption key is published (public key)
Decryption key is secret (secret key)
- For N senders, 1 key is enough to decrypt.
- Users can communicate with only public data.
- A big advantage in key management and agreement.

Digital Signature

- Signature: Only a user can generate. ⇒by a secret key
- Verification: Anyone can verify. ⇒by a public key



Public key VS Secret key cryptosystem

	Key agreement/ management	signature	Efficiency computation & memory
Public-key cryptosystem	easy	Achieved by anyone	Slow & big
Secret-key cryptosystem	difficult	Not achieved	Fast & small

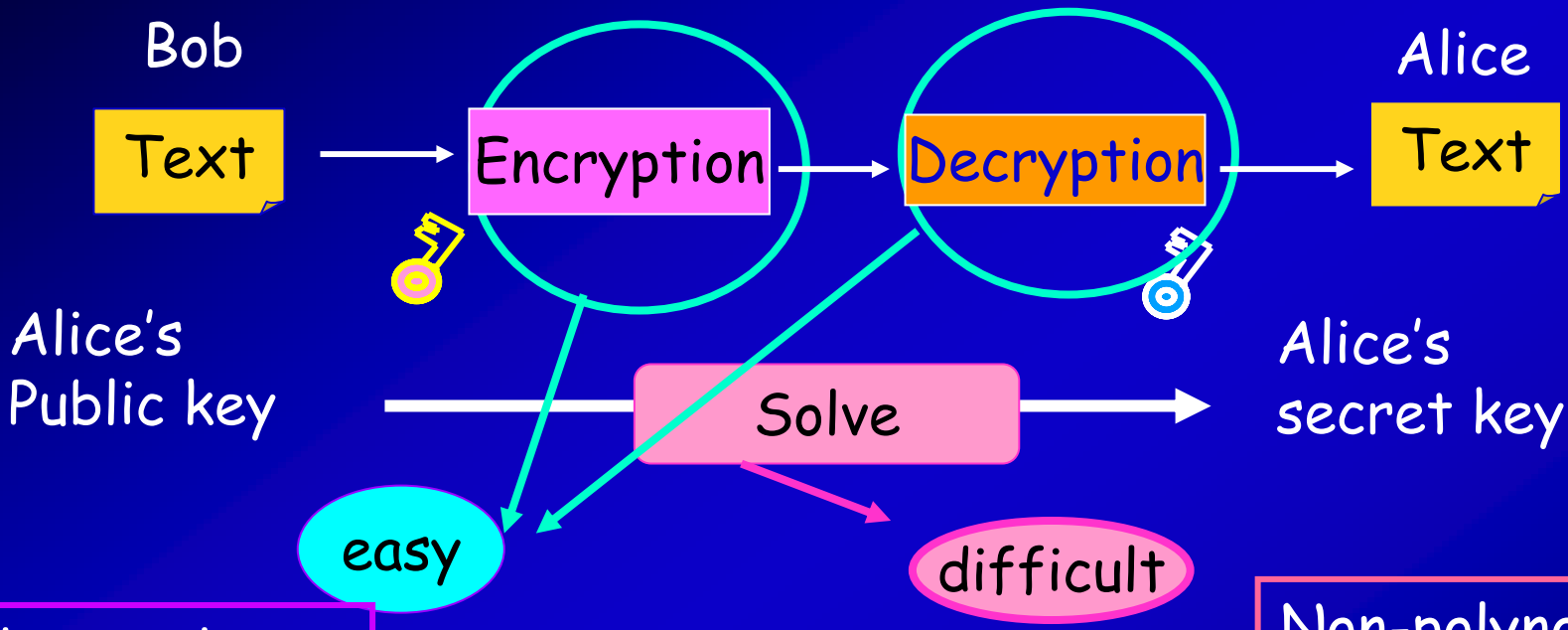
- Use public key cryptosystem for key agreement and signature.
- Use secret key cryptosystem for data encryption.

How to apply public-key cryptosystem to SSL

A public key cryptosystem achieves SSL for any user.

Any user doesn't have to prepare anything.

Principle of public-key cryptosystem



Integer Factorization Problem ('78)
Discrete Logarithm Problem ('85)
Elliptic Curve Discrete Logarithm Problem ('86)
Bilinear Diffie-Hellman Problem ('01)

Preliminary-mathematics-

- Z: Integer Ring
- p: a prime
- $Z/pZ=\{0, 1, \ldots, p-1\}$: a residue ring
  Strictly, $Z/pZ=F_p$: a finite field
- Arithmetic on F_p: arithmetic on Z + residue modulo p
  $F_p \ni a, b$ $\quad a+b = a+b \pmod p$
  $\quad a*b = a*b \pmod p$
- For example: F_5
  $2+3 = 0 \pmod 5$
  $2*3 = 1 \pmod 5$
- $g^k \pmod p$: computed by a polynomial time of k ,
  $O(\log_2(k))$, by using the binary method.

Security Basis

Discrete Logarithm Problem (DLP)

For a finite field F_p and its elements $g, y \in F_p$, DLP is a problem to find $x \in Z_{p-1}$ such that $y=g^x \pmod p$.

Example

$$\text{mod } 17 \begin{cases} 81 = 3^x \text{ (in Z)} \rightarrow x=4 \\ 13 = 3^x \pmod{17} \Rightarrow x \text{ ???} \end{cases}$$

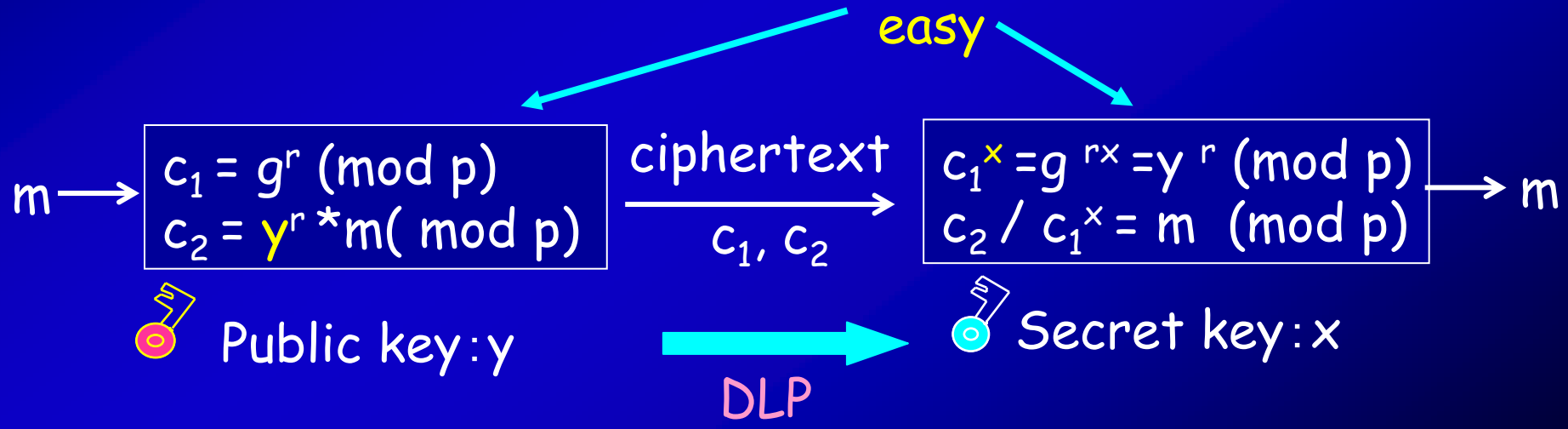
- The best algorithm to DLP works in a sub-exponential-time, which is available to any DLP. Therefore, 1024-bit DLP is believed to be secure.

Example - ElGamal encryption-

Key generation (public key : p, g, y, secret key : x)

1. Choose a finite field F_p and $g \in F_p$ with order q.
2. Generate $1 < x < q-1$.
3. Compute $y = g^x \pmod p$. Public key is a random number

Encryption・Decryption



Generalization of DLP – to ECDLP-

Generalized DLP

G: a finite group with an arithmetic *
For given $G \ni g$ and y,
find an x such that $y=g*g*\cdots*g$ (x-time *).

Condition to achieve a public key cryptosystem

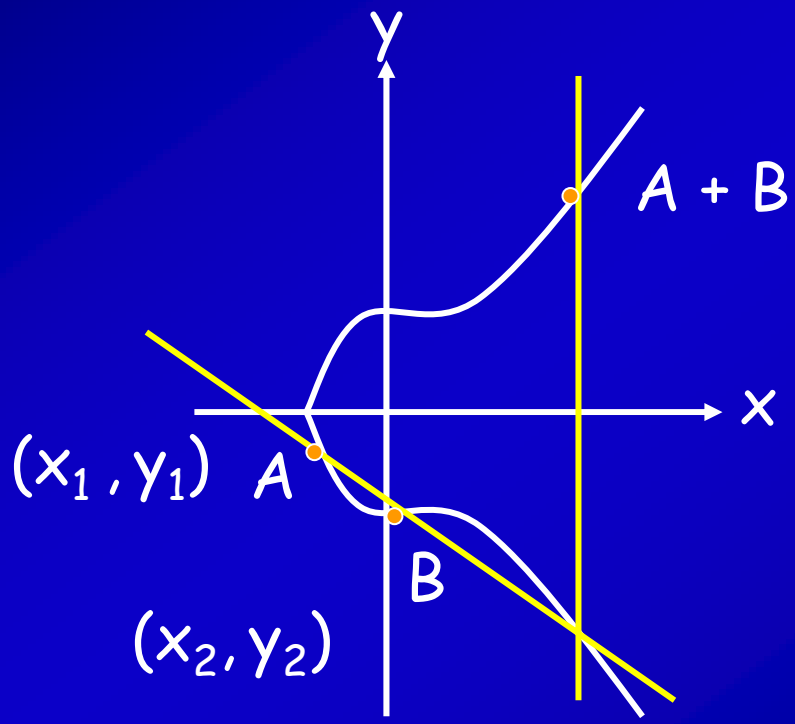
Point1: easy to compute *.
Point2: difficult to compute a generalized DLP.

Practical use

DLP over a finite field
Elliptic curve discrete logarithm problem (ECDLP)

Elliptic Curve

A non-degenerate cubic curve
E: $y^2 = x^3 + ax + b$ ($a, b \in F_p (p>3)$, $4a^3+27b^2 \neq 0$)
Feature
- Addition is defined.→ E is a group.
- Addition is computed easily.



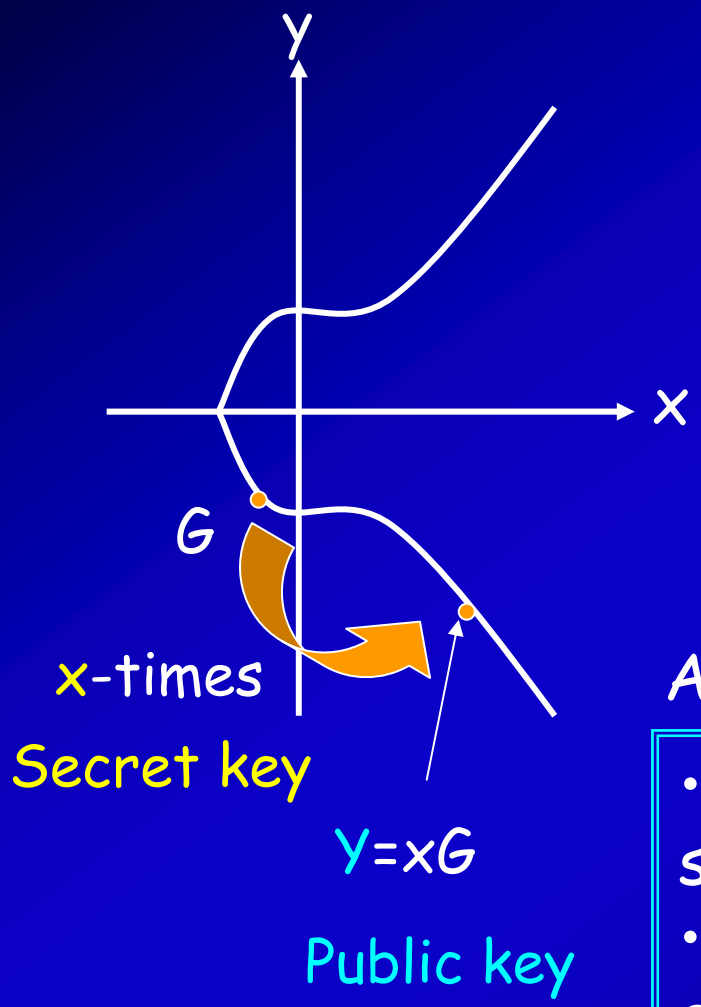
$A + B = (x_3, y_3)$ $(A \neq B)$

$x_3 = ((y_2-y_1)/(x_2-x_1))^2 - x_1-x_2$

$y_3 = (y_2-y_1)(x_2-x_1)(x_1-x_3)-y_1$

computed by a few multiplications.

Elliptic Curve Discrete Logarithm Problem



ECDLP is defined over

$E(F_p)$
$=\{(x,y) \in F_p \times F_p \mid y^2 = x^3 + ax + b\} \cup \{\infty\}$
$E(F_p)$ is a finite abelian group.

ECDLP

For given G, $Y \in E(F_p)$, find x such that $Y = G + \cdots + G = xG$

Advantage over DLP

- No sub-exponential-time algorithm to solve all ECDLP has been proposed.
- Therefore, 160-bit field EC chosen appropriately is believed to be secure.

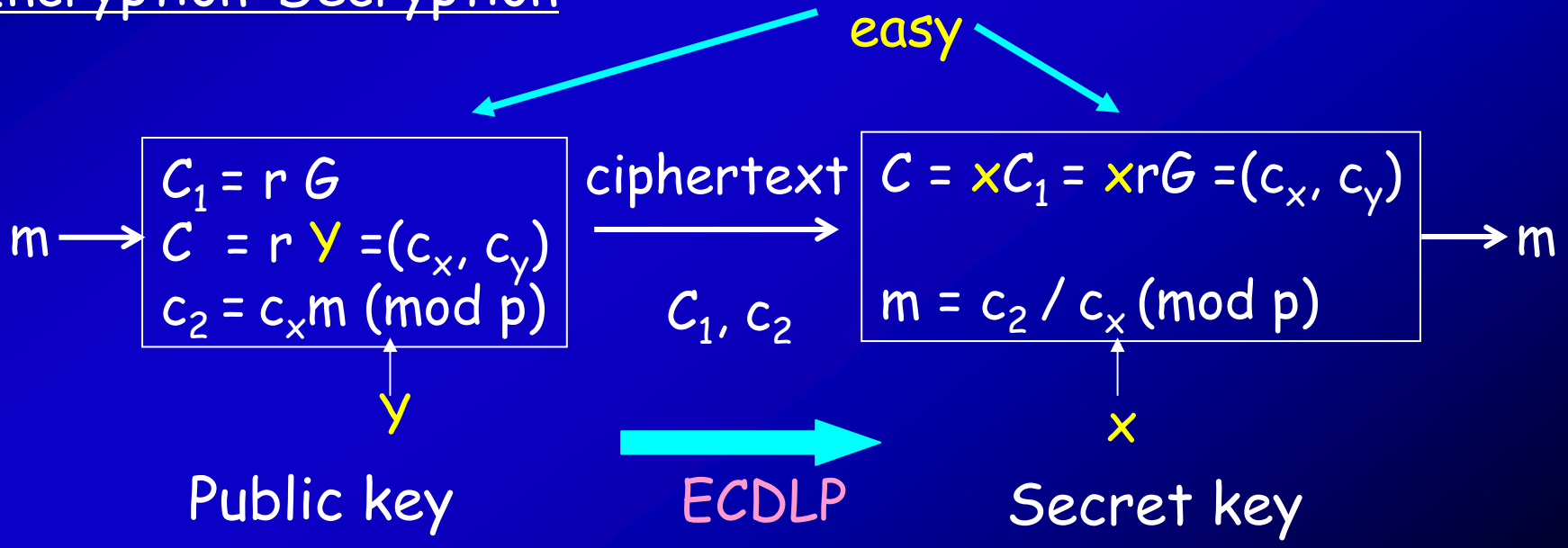
Elliptic curve cryptosystems

Key generation (public key : E/F_p, G, Y, secret key : x)

1. An elliptic curve E/F_p and $G \in E(F_p)$ with order q
2. Generate $1 < \forall x < q$.
3. Compute $Y = xG$.

Public key is a random number

Encryption・Decryption



ECDLP VS DLP

Security

- Any DLP is solved in a sub-exponential-time algorithm.
- Almost ECDLP is not solved in a sub-exponential-time algorithm.
- Therefore, ECDLP is more efficient than DLP with the same security level.

Abundant resources of cryptosystems

- There is one DLP over a finite field F_p.
- There are many secure ECDLP over a finite field F_p.

As a result, elliptic curves, one of important fields of mathematics, has also begun to attract an attention.

We need another mathematical tool.

We have an elliptic curve cryptosystems, which is secure and implemented efficiently.

However, a public key cryptosystem (conventional) is not perfect for a practical use.

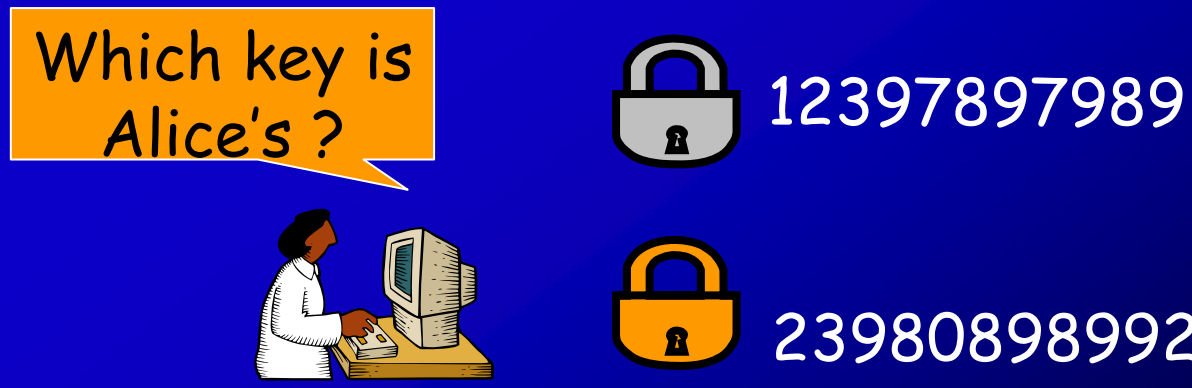
For example, a public key is computed randomly and so it is not clear whether the public key corresponds to a user.

How do we connect a user and a public key?

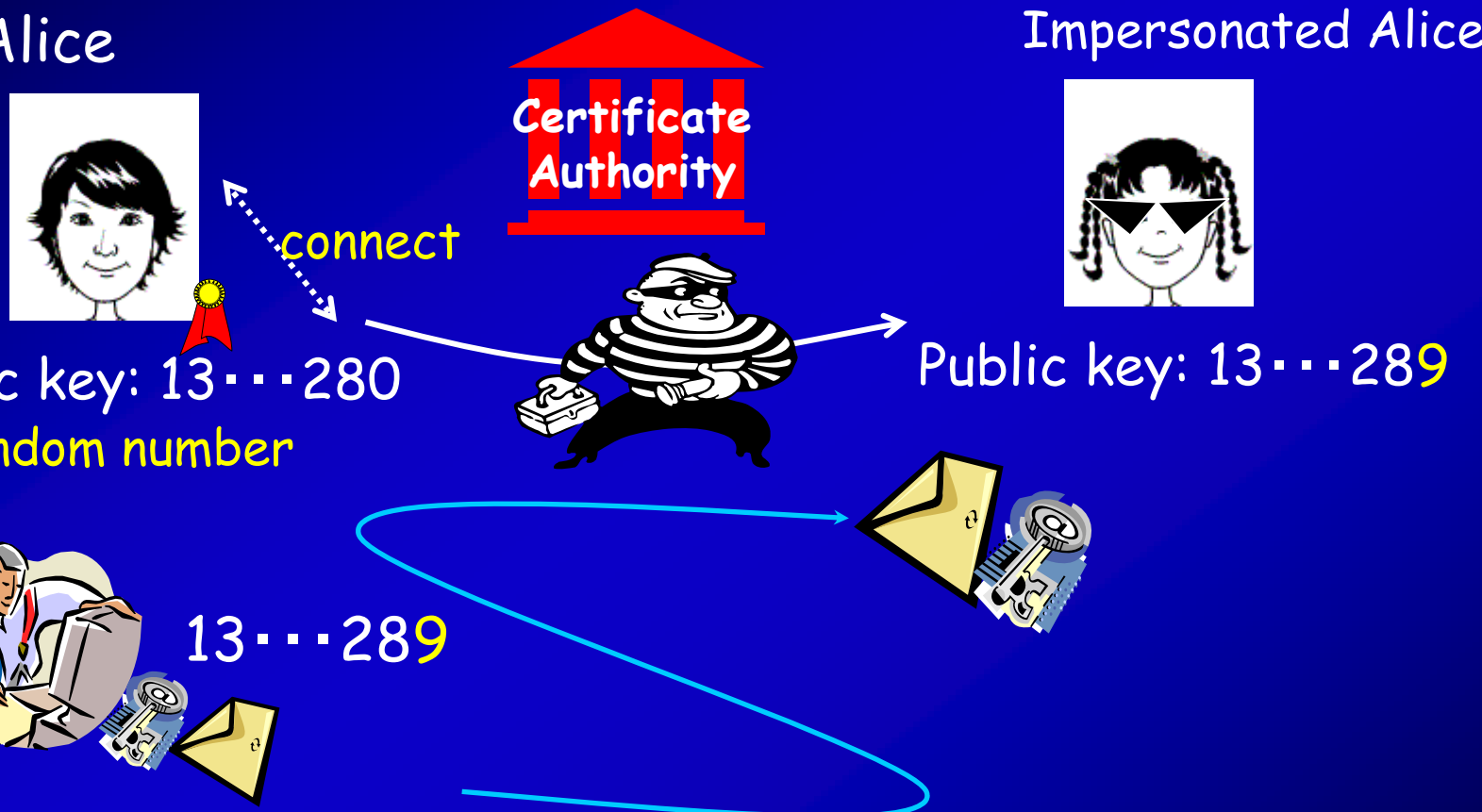
→The solution is ID-based encryption.

But, neither DLP nor ECDLP can achieve ID-based encryption.

So, we have explored another mathematical tool



ID-based Cryptosystems



ID based cryptosystems

A public key is given by ID like a name or an address.
No need for certificate.

ID based encryption

A public key is given by ID.
A secret key is generated by center.

Alice
→123..7800

Public key: Alice

Alice →

← A secret key

To make ID-based encryption on ECDLP

For a user ID Y, need to compute x such that Y = xG
⇔Solve ECDLP on given Y & G
➔ It is impossible to compute x.

Recently, a new mathematical tool of Weil pairing solves this problem.

Application of Weil pairing to cryptology

Weil pairing (non-degenerate pairing)

E/F_p, $G_1, G_2 \in E(F_p)$, $\mathrm{ord}(G_i) = q$, $(\gcd(q, p)=1)$

$E[q] = \{R \in E \mid qR = \mathcal{O}\} = \langle G_1, G_2 \rangle$: q-torsion points

$e: E[q] \times E[q] \rightarrow F_{p^k}^*$: Weil pairing

(1) Bilinear: $e(aG_1, bG_2) = e(G_1, G_2)^{ab} = e(bG_1, aG_2)$

(2) Non-degenerate: $e(G_1, G_2) \neq 1$

Bilinear Diffie-Hellman Problem(BDHP)

For given $\langle aG_1, bG_1, aG_2, cG_2 \rangle$, compute $e(G_1, G_2)^{abc}$.

BDHP achieves ID-based encryption instead of ECDLP.

ID based encryption

An elliptic curve E/F_p and $G_1 \in E(F_p)$ with order q
$e: E[q] \times E[q] \rightarrow F_{p^k}^*$, $H_1: \{ID\} \rightarrow \langle G_1 \rangle$: Hash function
$Y = sG_1$ $(1 < {}^{\forall} s < q)$.
Center's Public key: Y, center's secret key: x

Key generation

Alice

Secret key : sk

Alice ⟶ center

sk ⟵

$sk = sH_1(Alice)$

Encryption/Decryption

m ⟶ $U = rG_1$
$V = e(Y, rH_1(Alice)) + m$

ciphertext (U, V) ⟶

$C = e(U, sk)$
$= e(rG_1, sH_1(Alice))$
$= e(sG_1, rH_1(Alice))$
$= e(Y, rH_1(Alice))$
$m = C - V$

⟶ m

Public key Alice ↑

BDHP ⟶

↑ sk Secret key

Do we need further mathematical improvement?

Bilinear map has achieved ID-based encryption scheme.
Do we need further mathematical improvement?
"Yes, we need."

We need an elliptic curve that is practically used for BDHP.

Condition for a practical BDHP

An elliptic curve E/F_p and $G_1 \in E(F_p)$ with order q
$e: E[q] \times E[q] \rightarrow F_{p^k}^*$
e is computed efficiently
⇔ The range of e, $F_{p^k}^*$, is not large.
⇔ The embedding degree k is not large.
(practical k is around 6 to 15.)
→ However, it is not easy to construct an elliptic curve with such a practical bilinear map

Under research: an elliptic curve with a practical k

There are many elliptic curves over F_p.

$E/F_p : y^2 = x^3 + ax + b$ $(a, b \in F_p)$, $t = p+1-\#E(F_p)$ (t: trace)
Known facts: $|t| \leqq 2\sqrt{p}$ & E/F_p with $|t| \leqq 2\sqrt{p}$

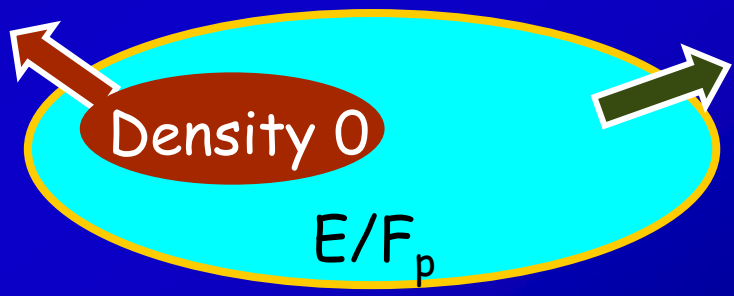
$\#\{t\} = 4\sqrt{p} = 2^{82} \sim 10^{24}$ (F_p:160 bits)
→How many of them has a practical k?

Supersingular

Practical k
$k \leqq 6$

Ordinary

Usually,
$k \gg \log p$ (BK 98)



It is not easy to find an E with a practical k($6 \leqq k \leqq 15$).
→Only 3 algorithms of MNT(Miyaji-Nakabayashi-Takano), BN(Barreto-Naehrig) & Freeman.
→We need more algorithms to find an E with a practical k.

Conclusion

- The cryptology has been widely used as a necessary technology to achieve an electronic market, an electronic government, etc.
- The number theory plays an important role in cryptology, which assures correctness of schemes and their security.
- We believe mathematics will become more important to achieve a new function or strong security of cryptology.