Towards Fine-Grained Secure Communications

Tatsuaki Okamoto
(NTT)

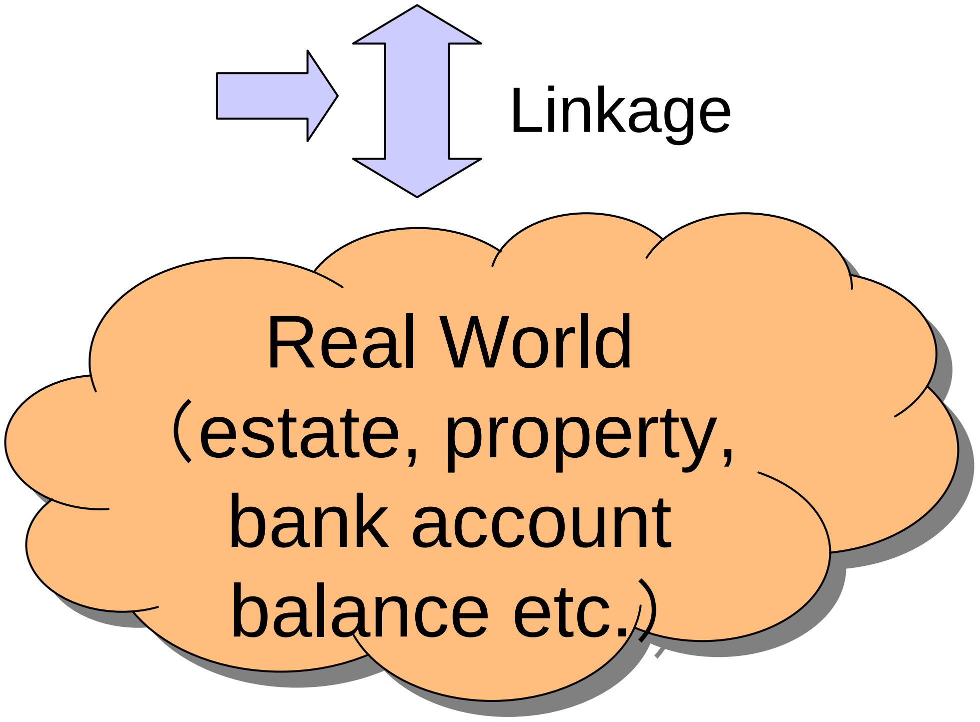
The Role of Cryptography and Information Security

ICT systems ・・・ Virtual World

（Every information is communicated and recorded by digital data）

Cryptography and

Information Security



Basic Properties of Cryptography

- Confidentiality: Data flow control

  (a data item is only accessed by qualified persons) … encryption
- Authentication: Correctness of data and users/parties … signatures, identification
- Privacy: Anonymity of users/parties

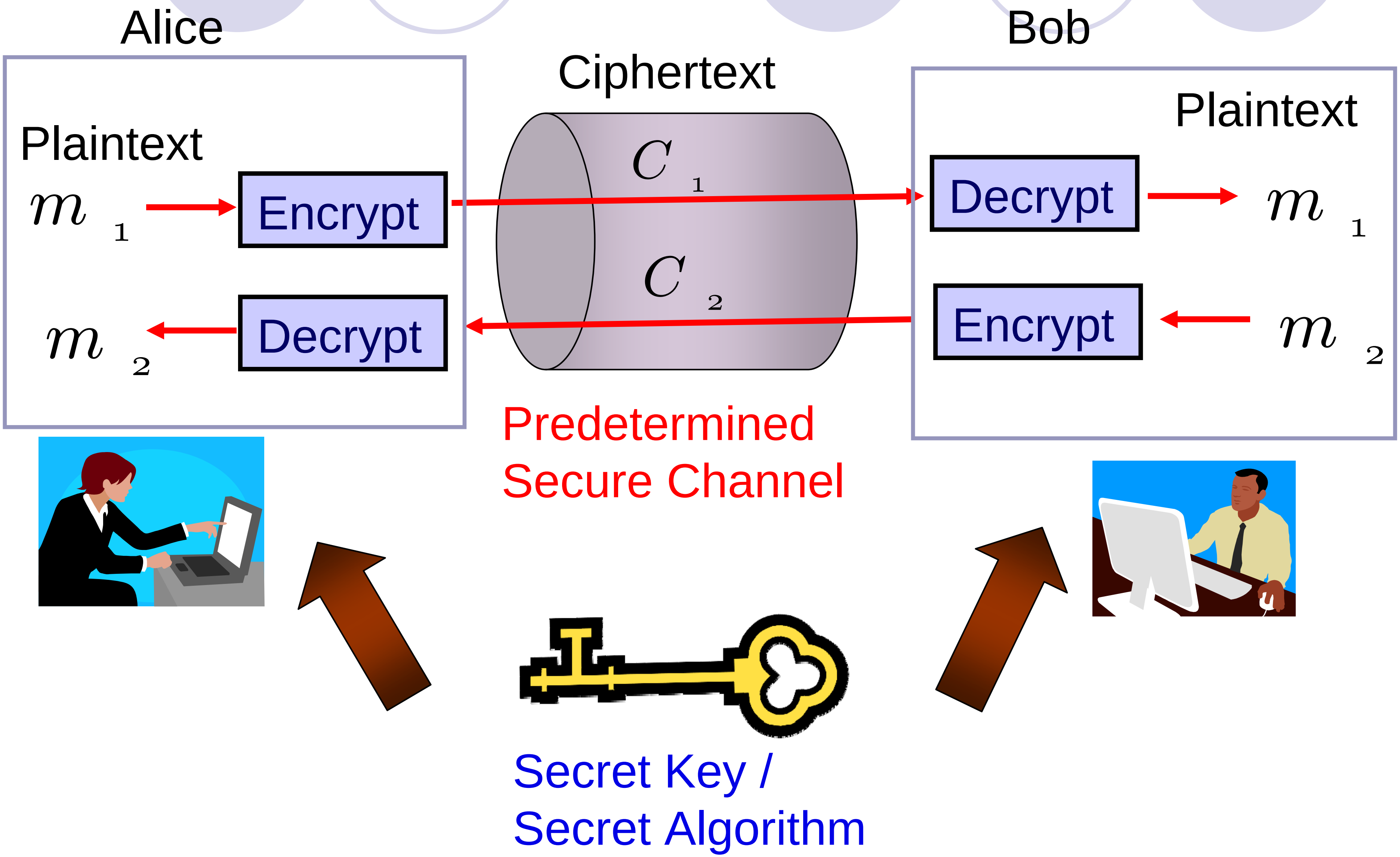
  … privacy-enhanced primitives

Confidentiality

The Most Traditional Way to Realize Confidentiality

- Symmetric Encryption: realized by sharing a secret algorithm or a secret key between a pair of sender and receiver.
- Long history for several thousand years (similar to that of civilizations of human beings).

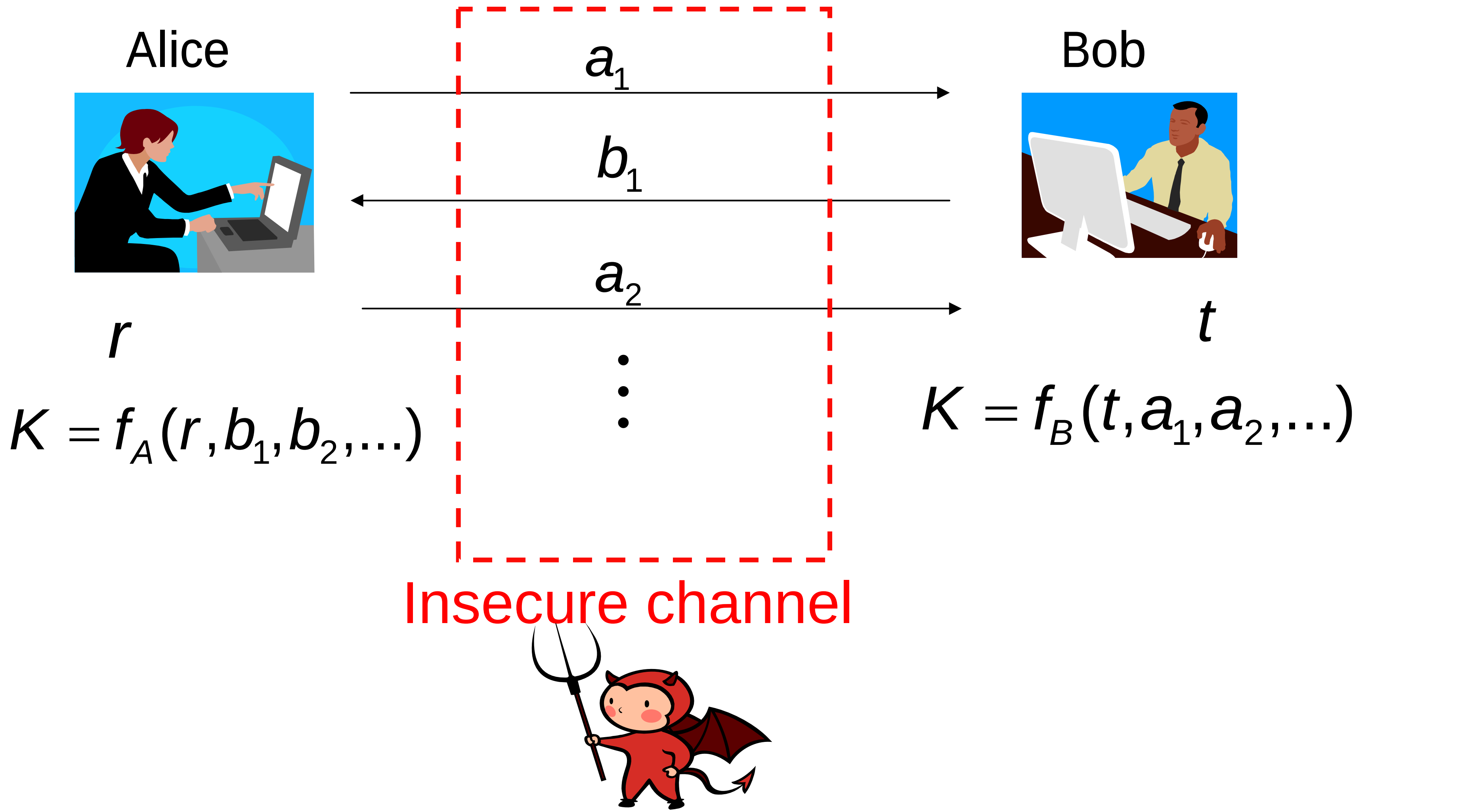
Symmetric Encryption



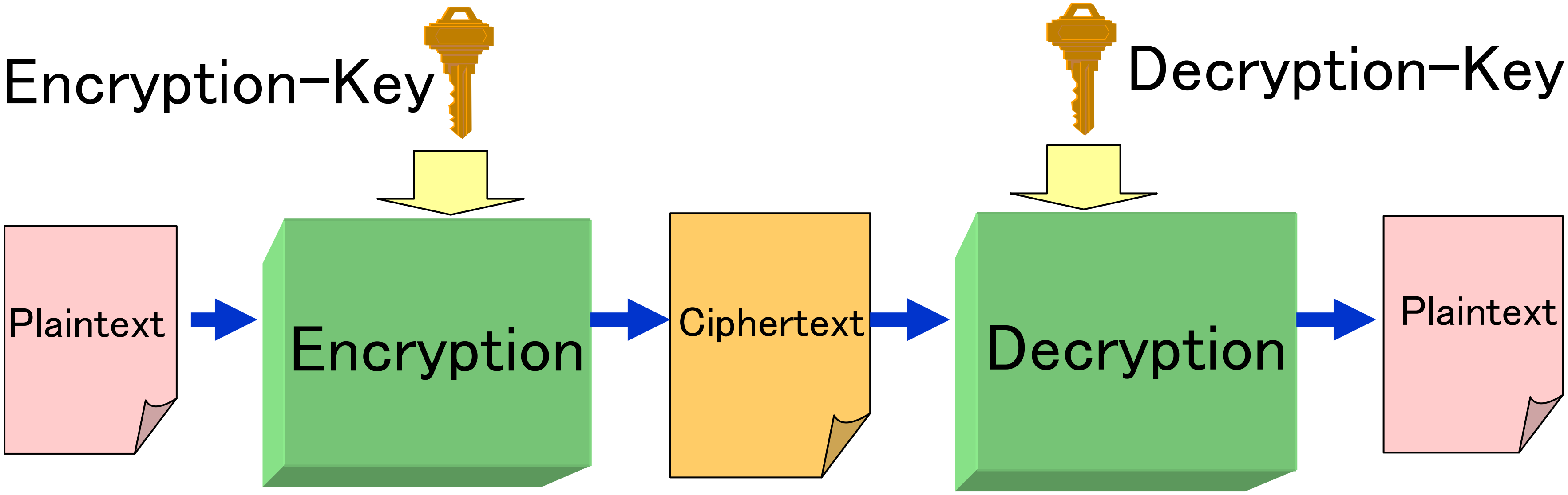
A problem raised in the early 1970's

- The early 1970's： ARPANET (the origin of the Internet）started growing.
- Problem: Is it possible for two parties to share a secret key securely through an insecure channel, where all messages exchanged by the two parties are wiretapped by the adversary?

Secret Key Sharing over Insecure Channels

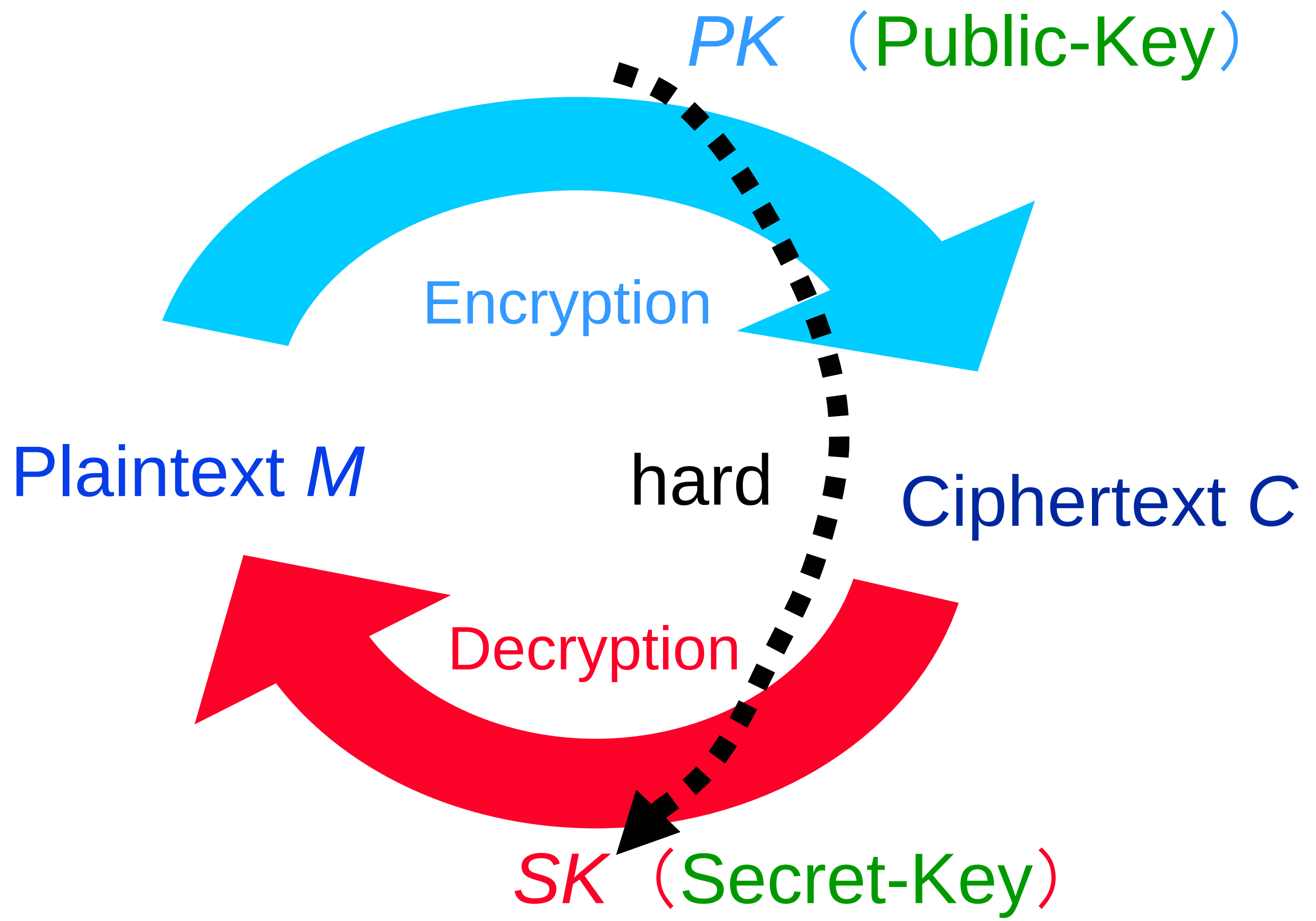


Public-key Encryption（1976 ）

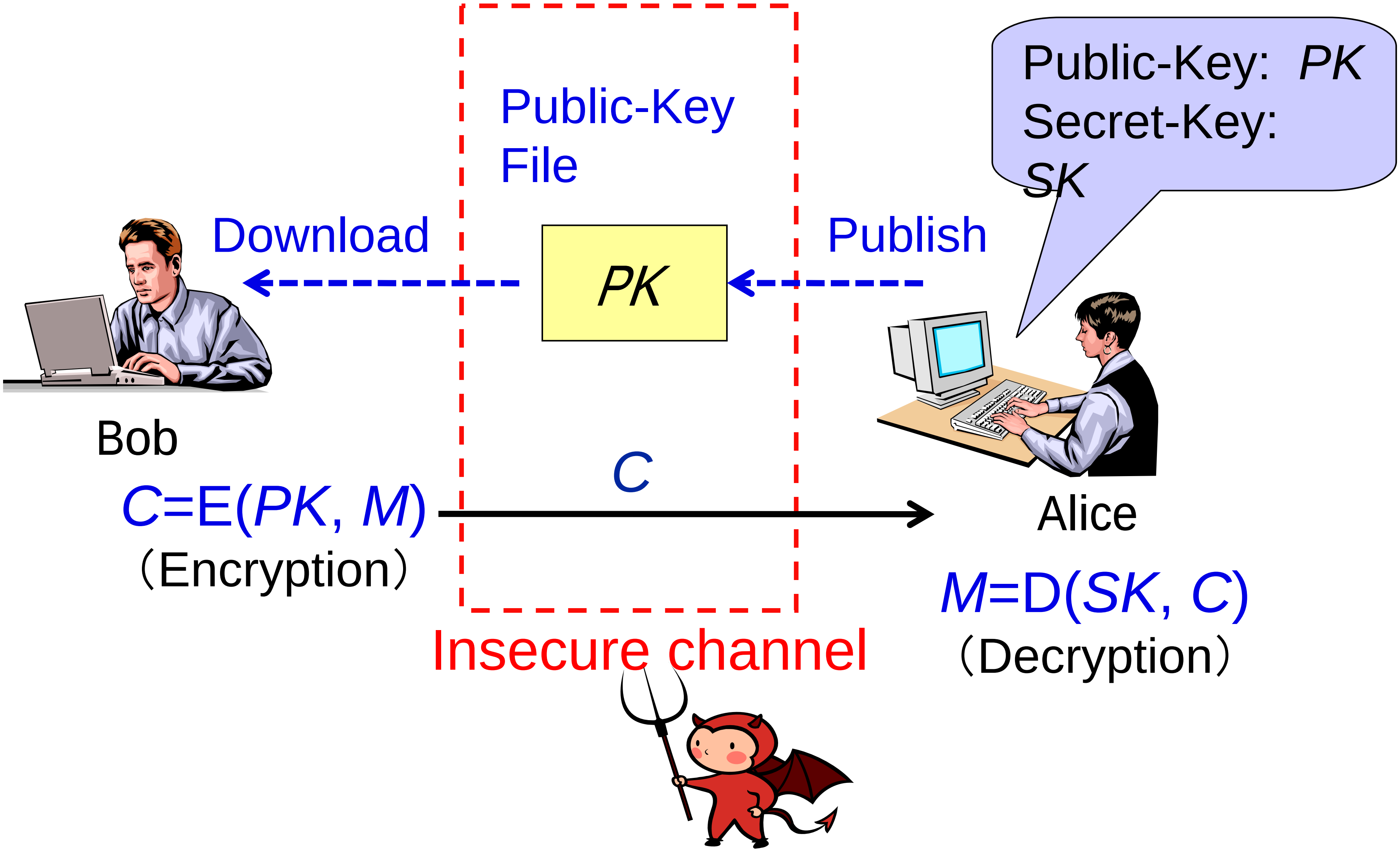


Symmetric Encryption	Encryption−Key ＝ Decryption−Key
Public−key Encryption	Encryption−Key ≠ Decryption−Key

Principle of Public-key Encryption



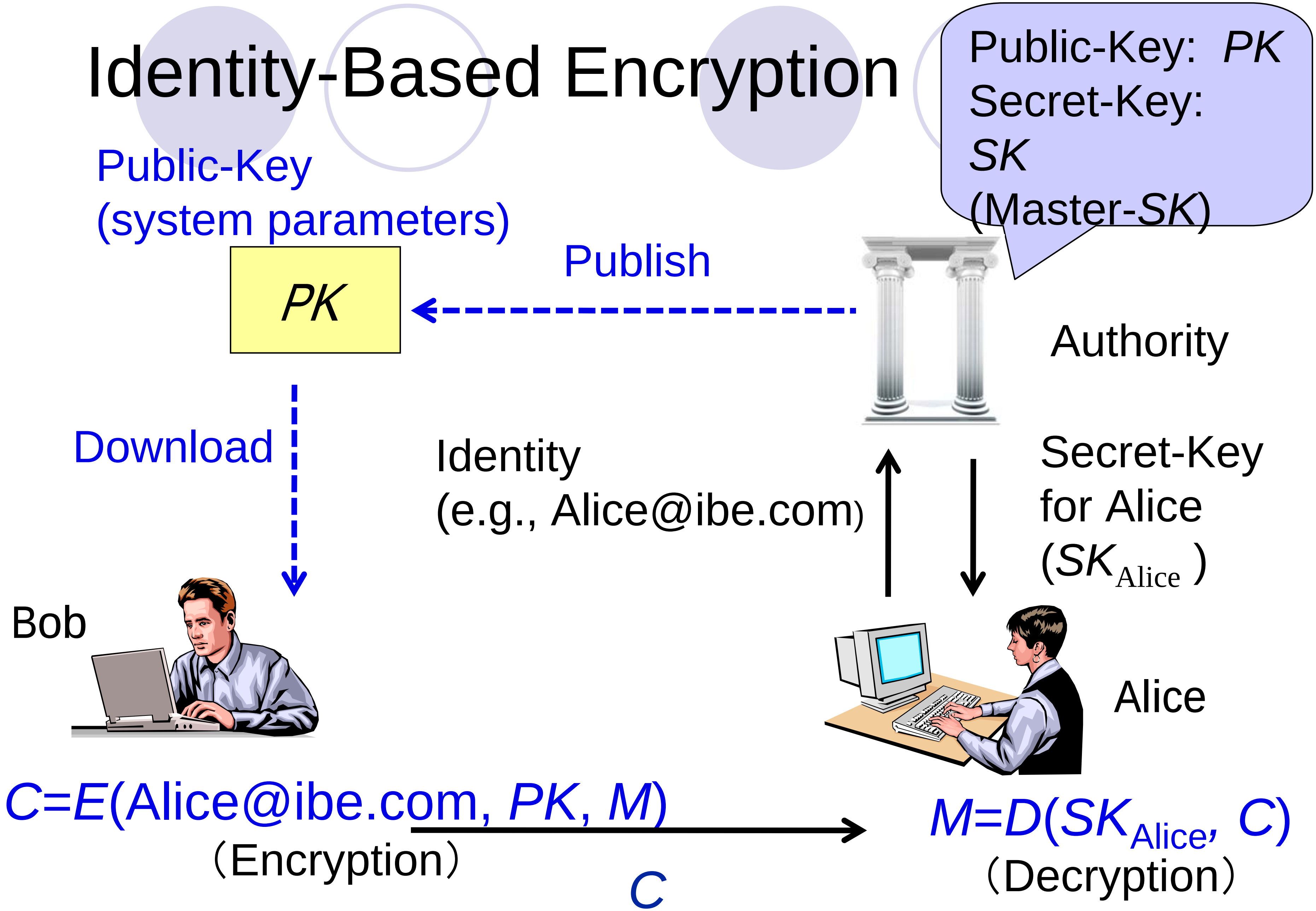
Public-key Encryption



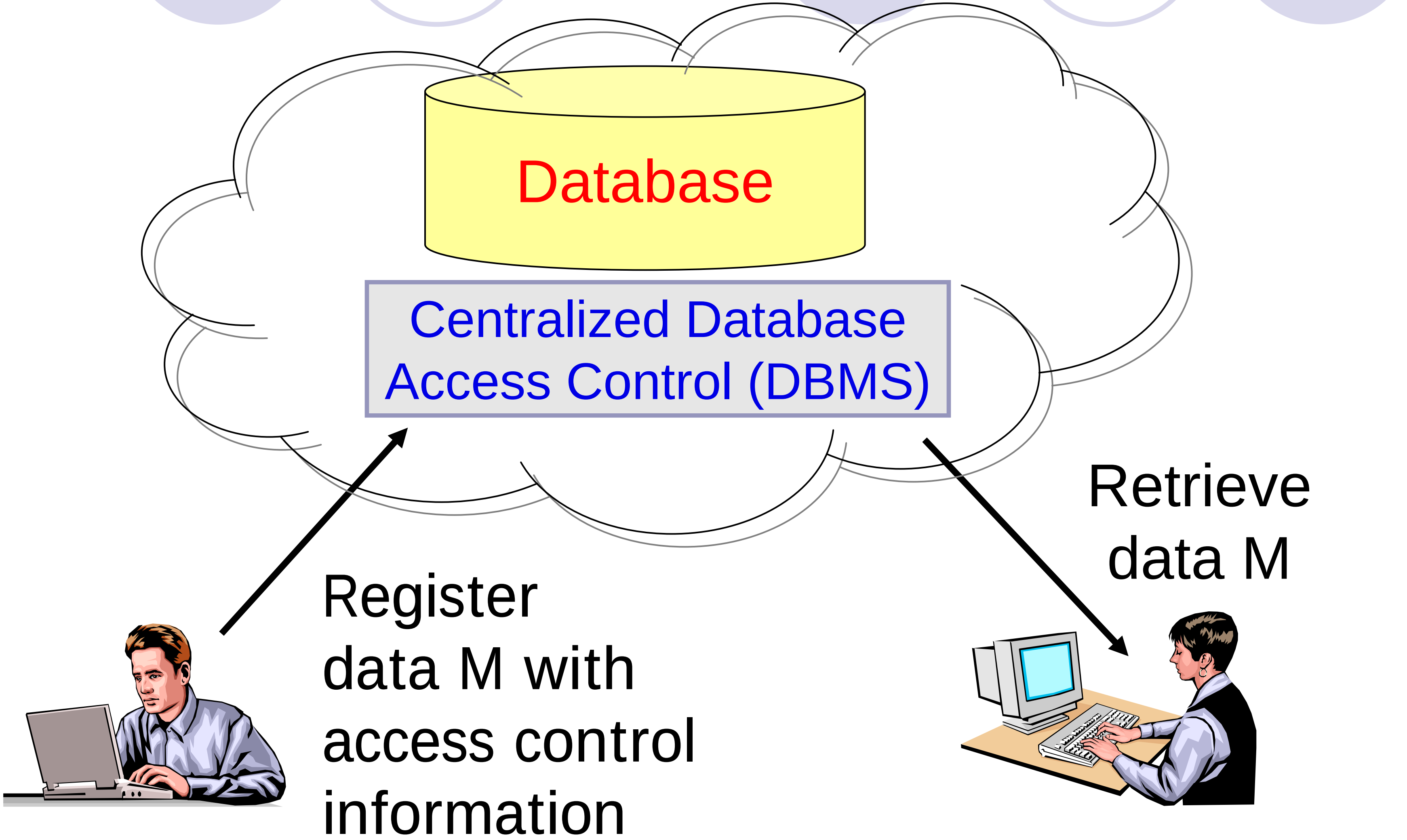
A New Concept of Encryption

- Public-key encryption as well as symmetric encryption are now widely used in many applications, especially in the internet.
- To get a public-key of each receiver may be a problem in some applications.
- Can we use an identity (e.g., email address) of a receiver in place of the public-key?
- No, it is impossible, in the concept of public-key encryption.
- It may be possible in a new concept of encryption.

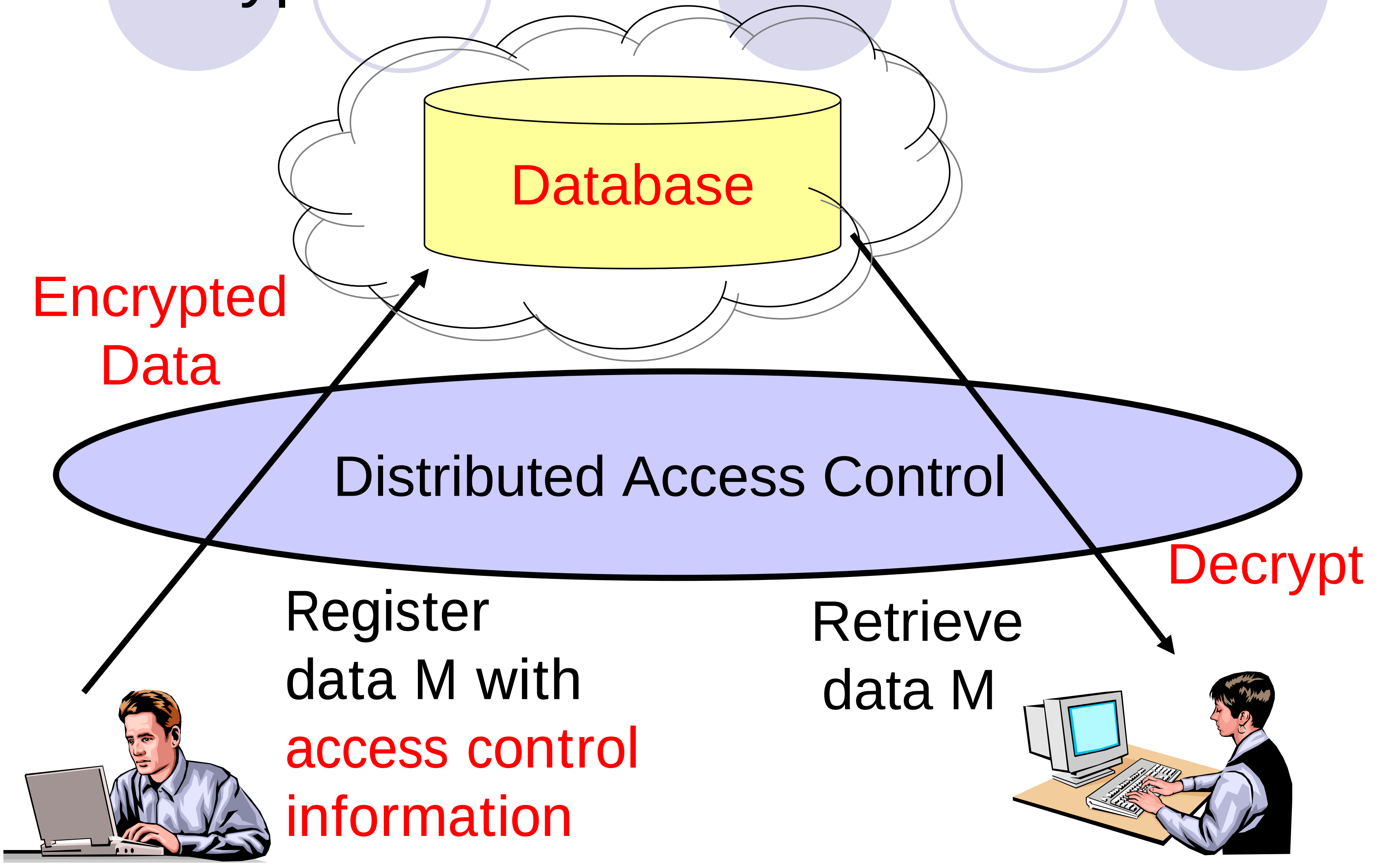
Identity-Based Encryption



Centralized Access Control of Database Services



Distributed Access Control with Encryption for Database Services



Fine-Grained Encryption (Predicate Encryption)

Public-Key: *PK*
Secret-Key: *SK*
(Master-*SK*)

Public-Key
(system parameters)

PK

Publish

Authority

Download

Predicate *f*

Secret-Key for *f*
(SK_f)

Bob

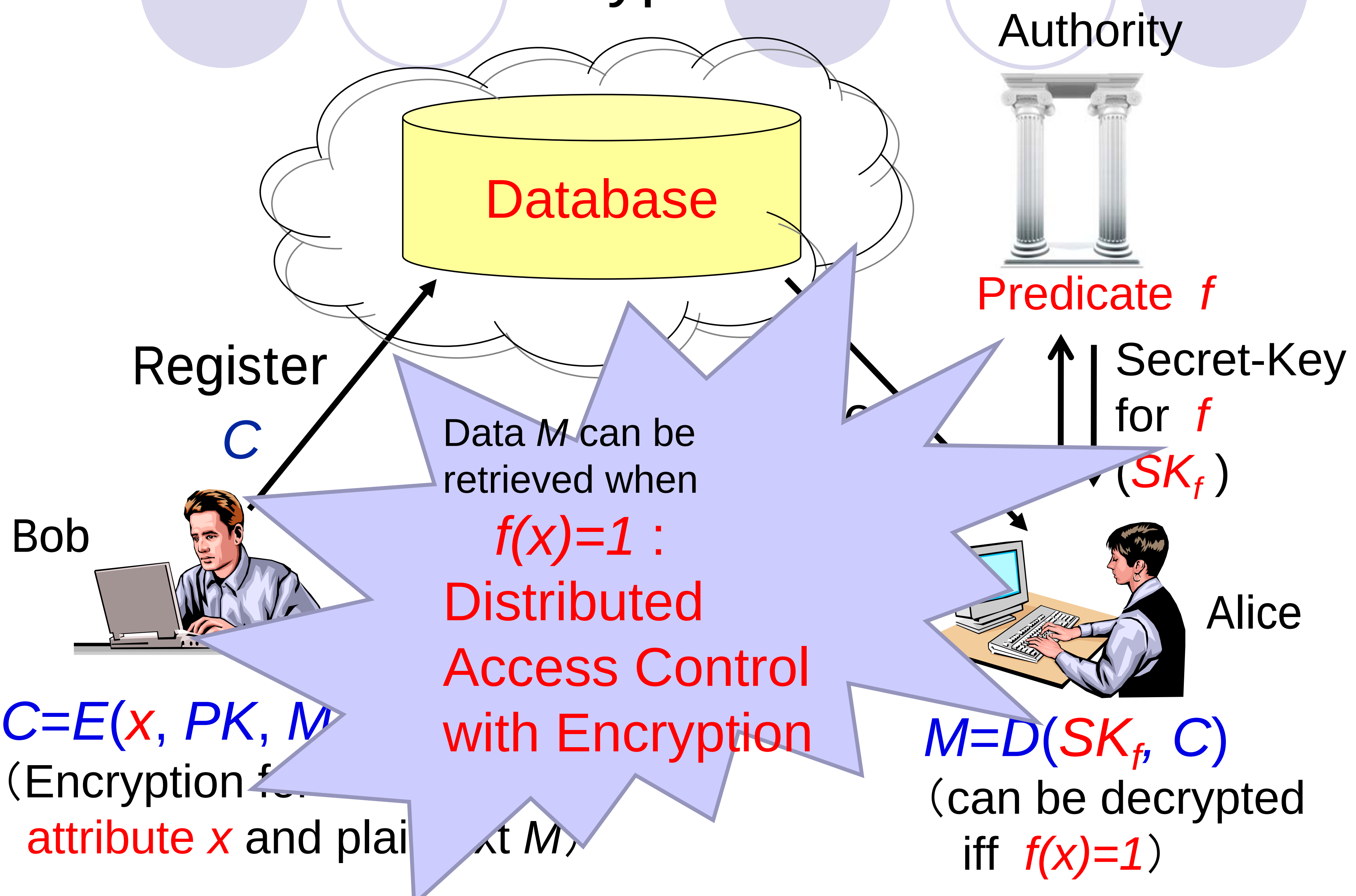
Alice

$C=E(x, PK, M)$
（Encryption for attribute *x* and plaintext *M*）

C

$M=D(SK_f, C)$
（can be decrypted iff $f(x)=1$）

Distributed Access Control by Fine-Grained Encryption



Example 1 of Predicates and Attributes

- Predicate f with parameters a :

  $$f(X) \equiv (X=a)$$

- Acceptable attribute x is a,
- Application: Identity-based encryption

a = Alice@ibe.com

$SK_{Alice} = SK_{a}$

Alice

$C=E(a, PK, M)$
(Encryption)

C

$M=D(SK_{a}, C)$
(Decryption)

Example 2 of Predicates and Attributes

- Predicate *f* with parameters *a, b* and *c* :

  $f(X,Y,Z) \equiv (X=a) \wedge ((Y=b) \vee (Z=c))$

- Acceptable attributes: *x = (a,b,d), (a,e,c)*
- Application Example:

  a $\equiv$ [Type: Animation],

  b $\equiv$ [Price: Zone 2],

  c $\equiv$ [Restriction: Class 1],

- Secret-key SK_f is given to a person (receiver) who purchases the secret key.
- A ciphertext of a content with attribute (Animation, Price Zone 2, Class 2) or (Animation, Price Zone 1, Class 1) can be decrypted by SK_f .

Fine-Grained Encryption (Predicate Encryption)

Public-Key: *PK*
Secret-Key: *SK*
(Master-*SK*)

Public-Key
(system parameters)

PK

Publish

Authority

Download

Predicate *f* =
(X=Animation) ∧
(Y=Price Zone 2 ∨ Z=Class 1)

Secret-Key
for *f*
(SK_f)

Bob

Alice

$C=E(x, PK, M)$
(Encryption for
attribute $x = (X,Y,Z)$ =
(Animation, Price Zone 2, Class 2))

C

$M=D(SK_f, C)$
(can be decrypted
iff $f(x)=1$)

Example 3 of Predicates and Attributes

- Predicate f with parameters a, b and c :

  $f(X,Y,Z) \equiv (X \neq a) \wedge ((Y < b) \vee (Z = c))$
- Acceptable attributes: $x = (c,d,e)$ (s.t. $c \neq a$ and $d < b$), (c,e,c) (s.t. $c \neq a$ and $e > b$), …
- Application Example:

  a $\equiv$ [Type: Animation],

  b $\equiv$ [Price: $100],

  c $\equiv$ [Restriction: Class 1],
- Secret-key SK_f is given to a person (receiver) who purchases the secret key.
- A ciphertext of a content with attribute (Drama, $70, Class 2) or (News, $200, Class 1) can be decrypted by SK_f .

Fine-Grained Encryption (Predicate Encryption)

Public-Key: *PK*
Secret-Key: *SK*
(Master-*SK*)

Public-Key
(system parameters)

PK

Publish

Authority

Download

Predicate f =
($X \neq Animation$) ∧
(Y< \$100 ∨ Z=Class 1)

Secret-Key for f (SK_f)

Bob

Alice

$C=E(x, PK, M)$
(Encryption for attribute $x = (X,Y,Z)$ =
(Drama, \$70 , Class 2))

C

$M=D(SK_f, C)$
(can be decrypted iff $f(x)=1$)

Example 4 of Predicates and Attributes

- Predicate f with parameters a, b, c and d :

  $f(X,Y,Z,W) \equiv$ TH2 [$(X = a)$, $((Y < b) \vee (Z = c))$, $(W \neq d)$]

  (TH2: threshold function that accepts if at least 2 terms are true.)

- Acceptable attributes: $x = (a,e,g,d)$ (s.t. $e < b$), (d,e,c,g) (s.t. $d \neq a$, $e > b$, $g \neq d$), …

- Application Example:

  a $\equiv$ [Type: Animation], b $\equiv$ [Price: $100],

  c $\equiv$ [Membership: Gold], d $\equiv$ [Restriction: Class 1]

- Secret-key SK_f is given to a person (receiver) who purchases the secret key.

- A ciphertext of a content with attribute (Animation, $70, Silver, Class 1) or (News, $200, Gold, Class 2) can be decrypted by SK_f .

Fine-Grained Encryption (Predicate Encryption 2)

Public-Key: *PK*
Secret-Key: *SK*
(Master-*SK*)

Public-Key
(system parameters)

PK

Publish

Authority

Download

attribute *x*

Secret-Key for *x*
(SK_x)

Bob

Alice

$C=E(f, PK, M)$
（Encryption for predicate *f* and plaintext *M*）

C

$M=D(SK_x, C)$
（can be decrypted iff $f(x)=1$）

Fine-Grained Encryption (Predicate Encryption 2)

Public-Key: *PK*
Secret-Key: *SK*
(Master-*SK*)

Public-Key
(system parameters)

PK

Publish

Authority

Download

Attribute x = (*X*,*Y*,*Z*) =
(NTT, Age:30, Female)

Secret-Key
for *x*
(SK_x)

Bob

Alice

$C=E(f, PK, M)$
（Encryption for
predicate *f* =
X=NTT ∧ (*Y*< 35 ∨ *Z*=Male) ）

C

$M=D(SK_x, C)$
（can be decrypted
iff $f(x)=1$）

From Coarse-Grained to Fine-Grained Encryption

- Symmetric Encryption (ancient ～)

  - sender and receiver should be fixed/restricted.

- Public-Key Encryption (1976 ～) DH

  - receiver should be restricted by the public-key (registered string), but sender is not restricted.

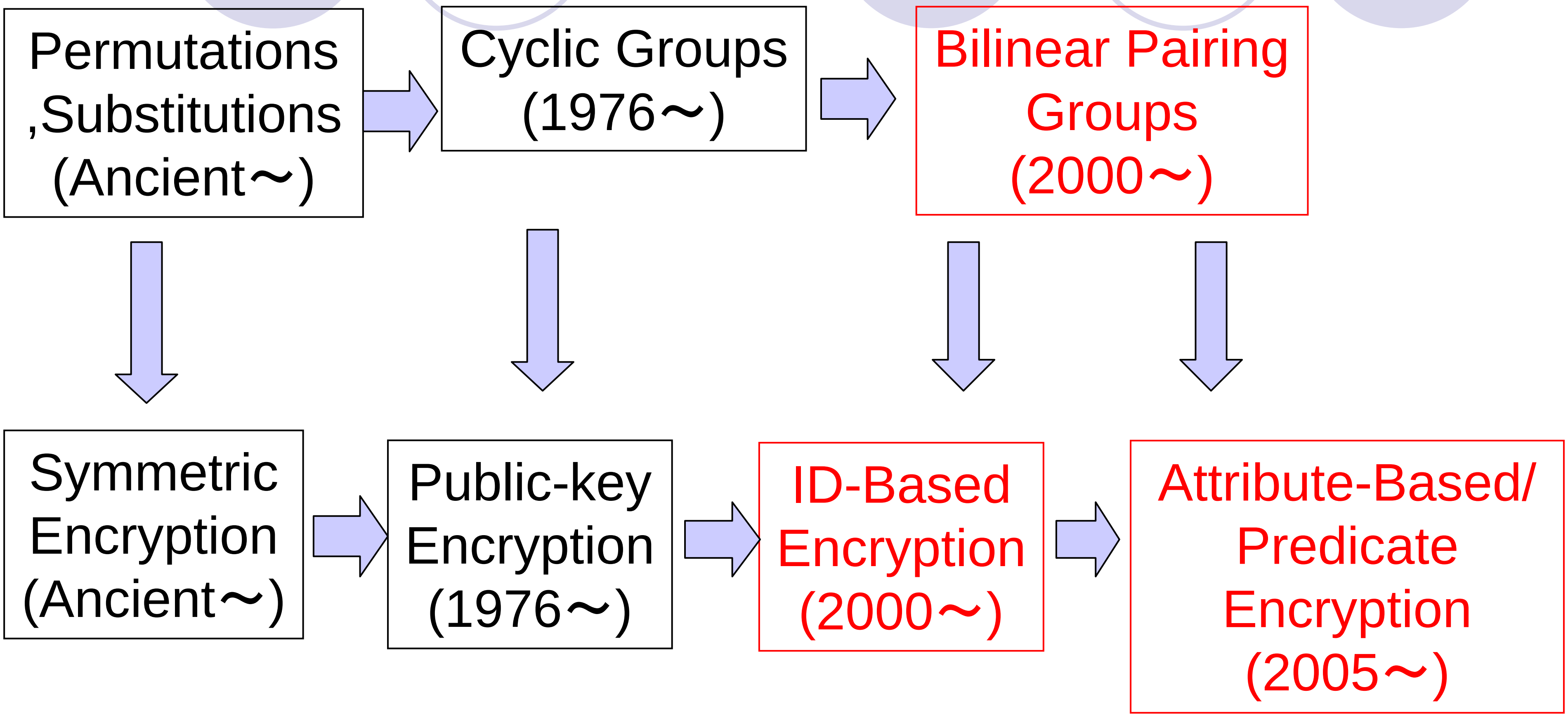
- Identity-Based Encryption (1984/2000～) S,SK/BF,..

  - senders and receivers are related by an arbitrary string (e.g., identity), and sender is not restricted.

- Predicate/Attribute-Based Encryption (2005～) SW,..

  - senders and receivers are only related by logical conditions (predicate-attribute relations）, and sender is not restricted.

Mathematics to Realize Cryptosystems



Cryptography and the Internet

Public-key cryptosystem

RSA scheme

IPSEC, SSL
PKI

Identity-Based Encryption

Attribute-Based / Predicate Encryption

1969 1976 1983 1988 1991 1993 2000 Present

Arpanet (the origin of the Internet) started

TCP/IP protocol (changed from original NCP)

Commercial usage started

World Wide Web by CERN

Browser (Mosaic)

Web 2.0

Cloud computing

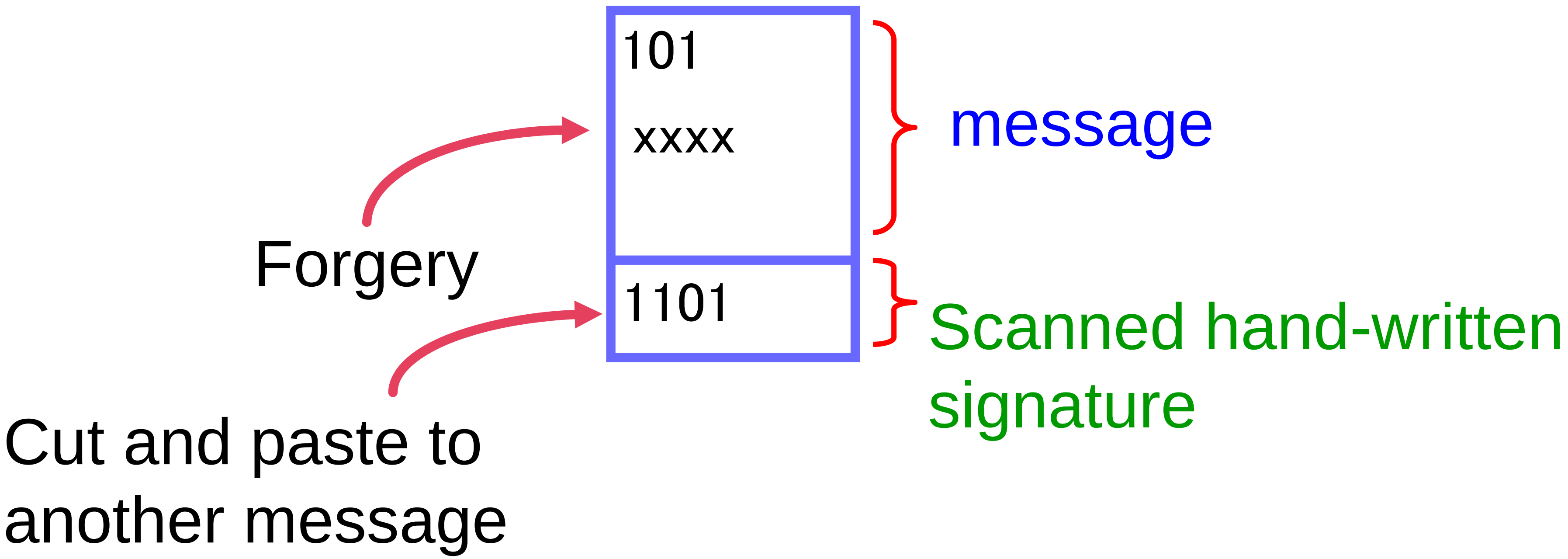
Authentication

Another problem raised in the early 1970's

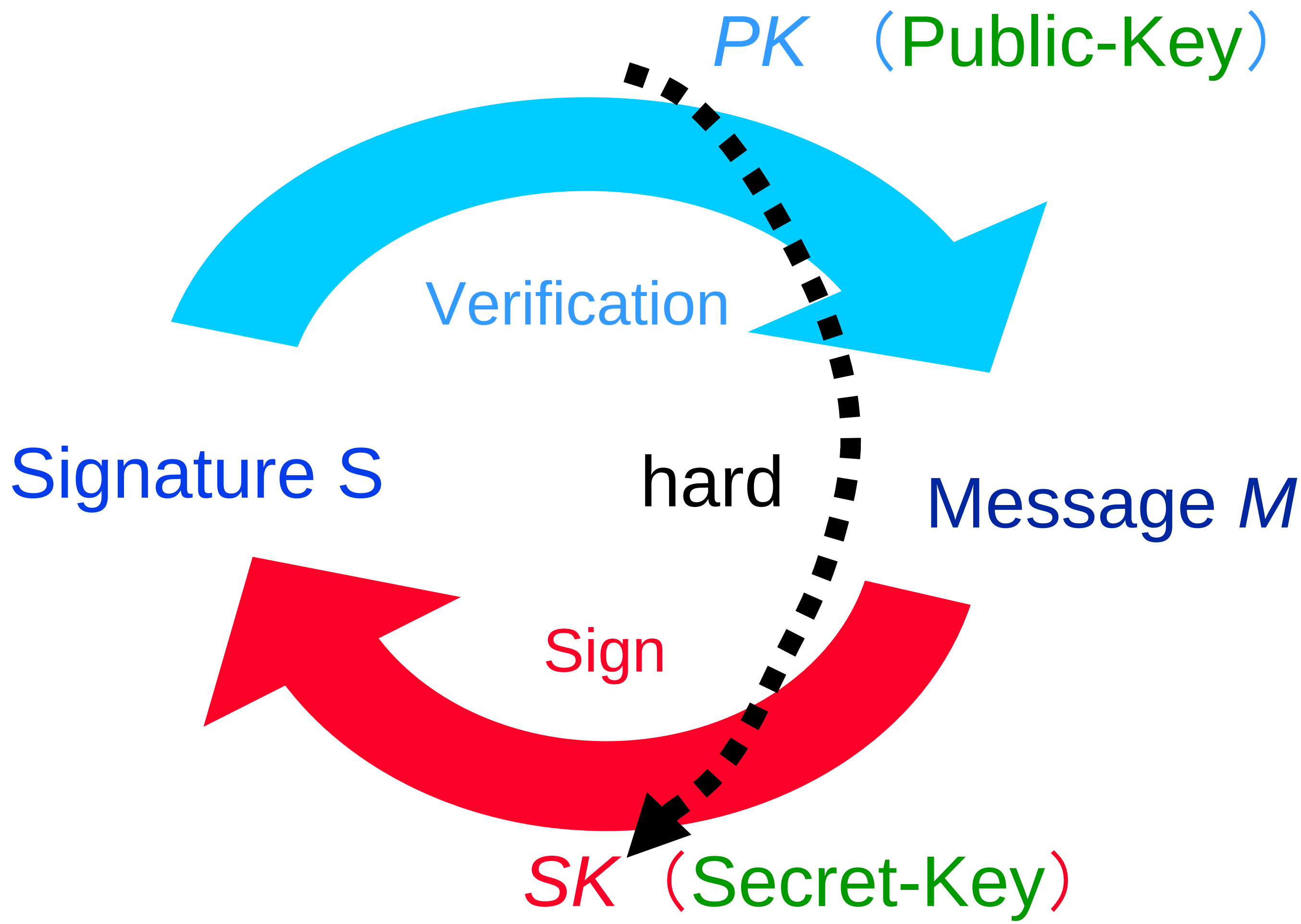
- Problem: Is it possible to sign on an electronic (digital) message?

Difficulty of Realizing Electronic Sigantures

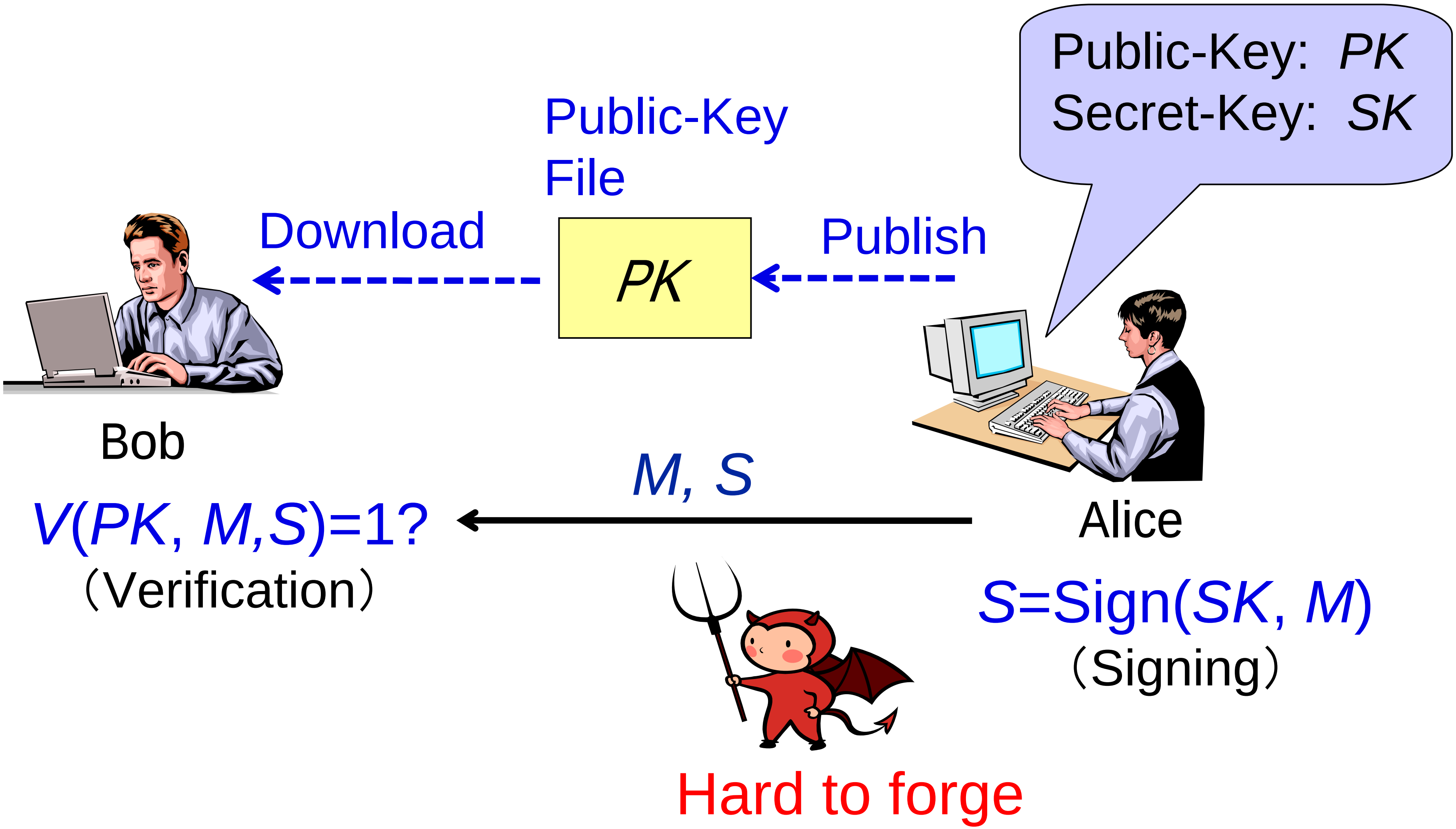
Easy to forge a digital message with no mark



Principle of Digital Signatures

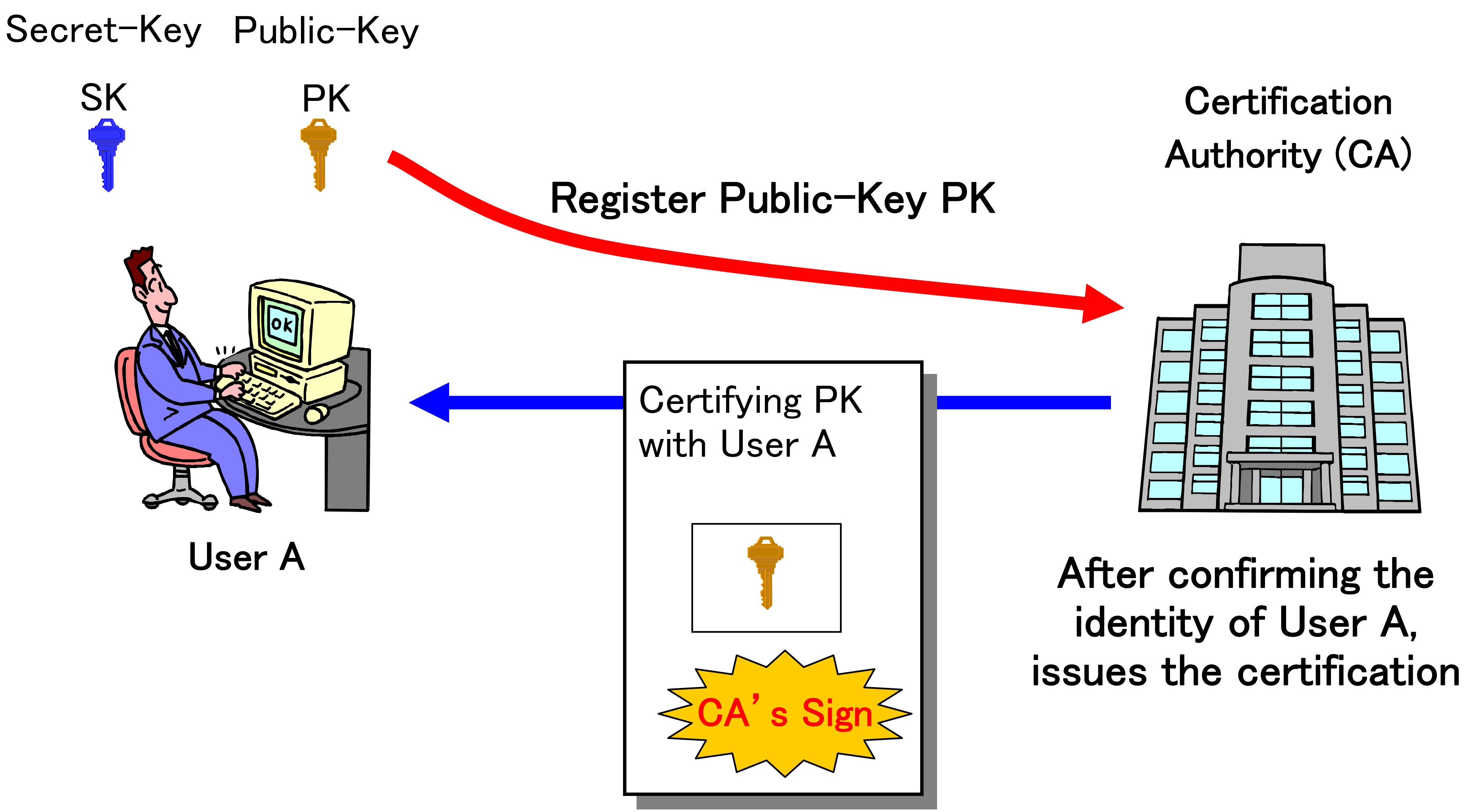


Digital Signatures



Public-Key Infrastructures (PKI) Certification Authority（CA）

Organization to certify a public-key

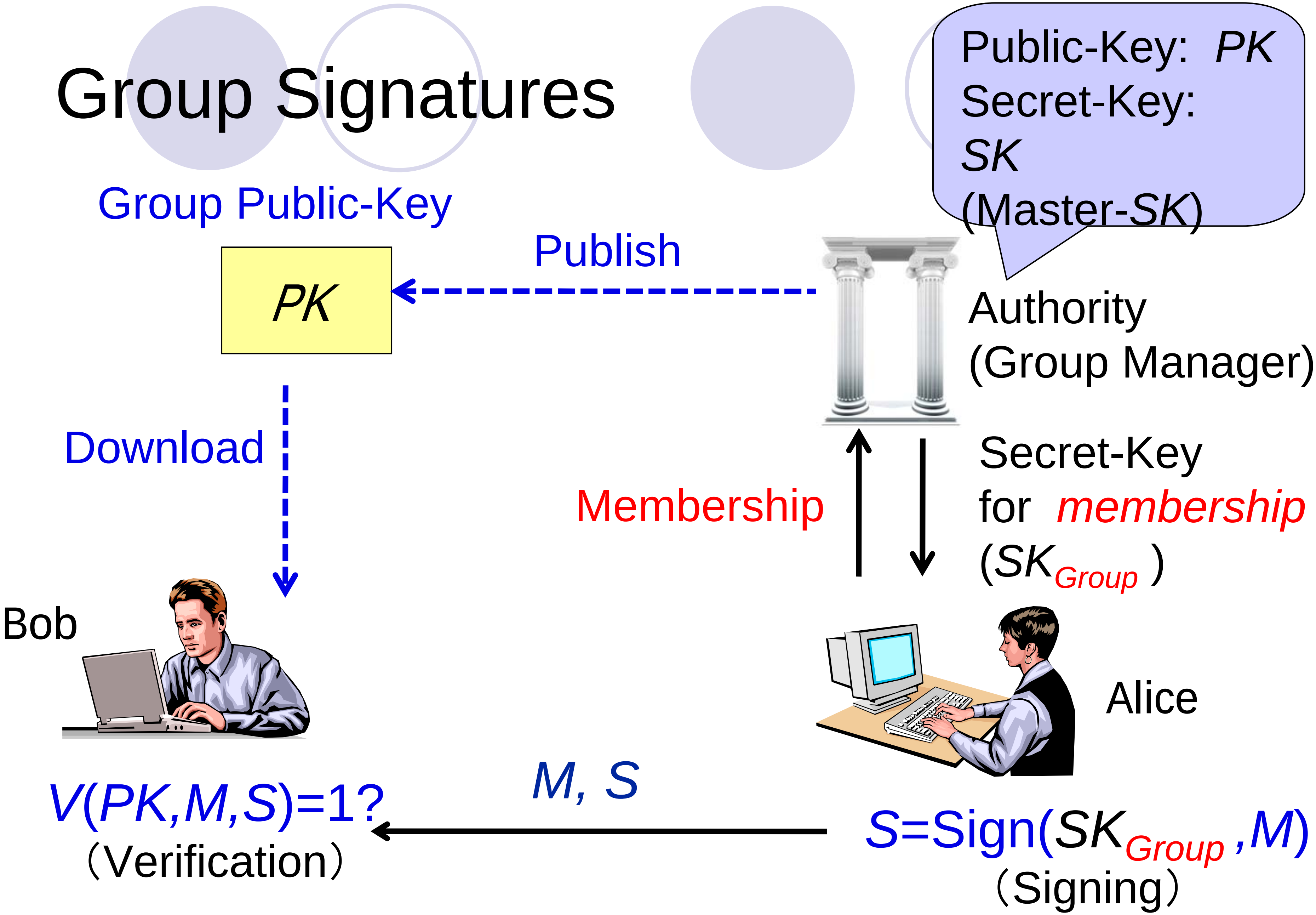


Privacy-Enhanced Authetication

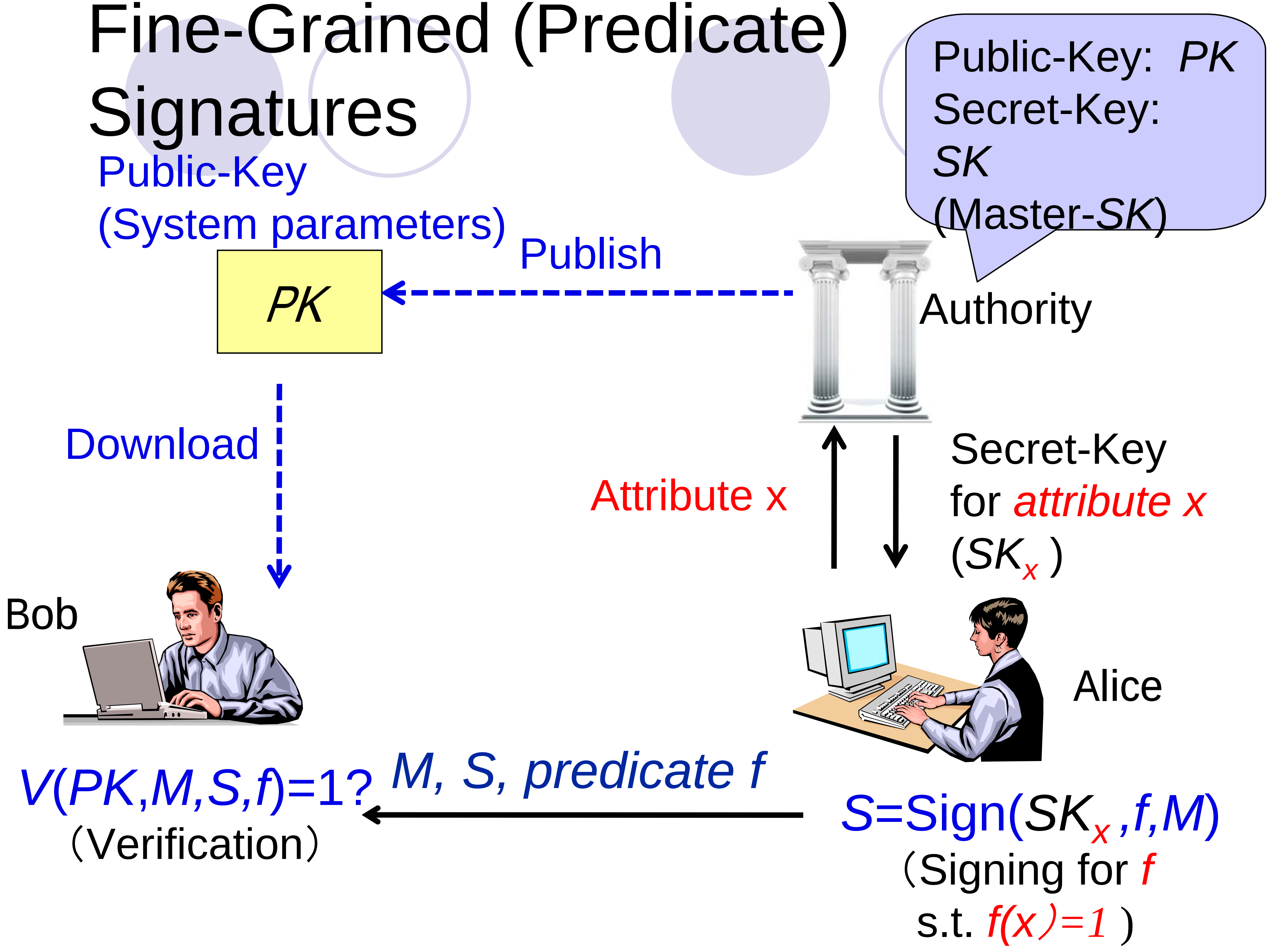
Privacy-Enhanced Signatures

- PKI-based digital signatures:

  The signer's identity of signatures is rigorously confirmed. It is good for the standard usage of applications of signatures.
- In some applications, it is not good, where the signer should be anonymous, and some qualification (e.g., a member of a group) of the signer should be authenticated.


Group Signatures
Public-Key: PK
Secret-Key: SK (Master-SK)
Group Public-Key
PK
Publish
Authority (Group Manager)
Download
Membership
Secret-Key for membership (SK_{Group})
Bob
Alice
M, S
V(PK,M,S)=1?
(Verification)
S=Sign(SK_{Group}, M)
(Signing)

Fine-Grained (Predicate) Signatures



Example of Predicates and Attributes

- Attribute x = (X,Y,Z)
  = ([Group: Group 2], [Age: 30], [Gender: Female])
- Secret-key SK_x is given to a person who has the attributes.
- Predicate *f* with parameters *a, b* and *c*:

  $f(X,Y,Z) \equiv (X = a) \wedge ((Y < b) \vee (Z = c))$, where

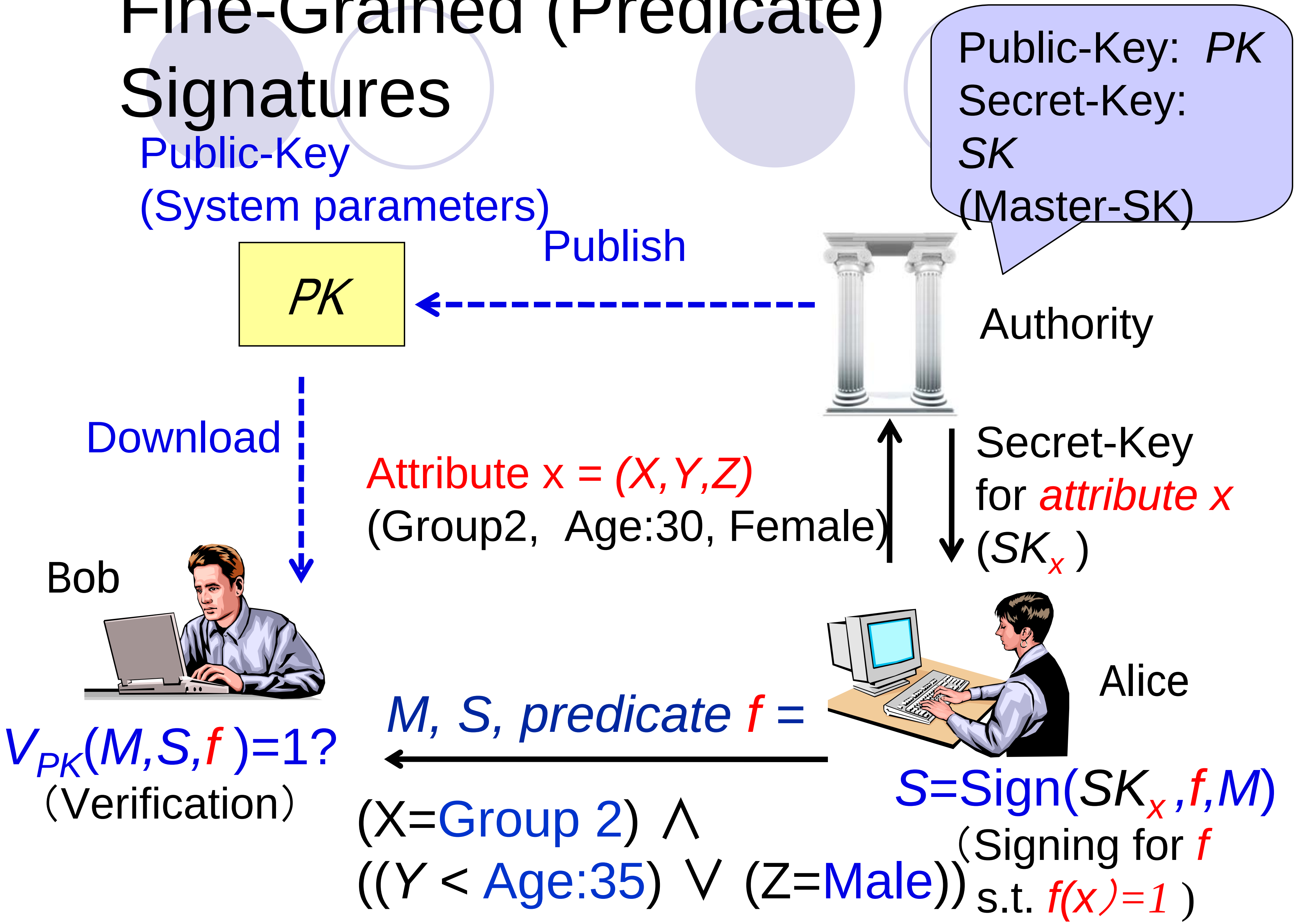
  a $\equiv$ [Group: Group 2],

  b $\equiv$ [Age: 35],

  c $\equiv$ [Gender: Male]
- A signature with predicate *f* implies that the attributes of the signer satisfies the predicate *f*,

  i.e., $(X=\mathit{Group\ 2}) \wedge ((Y < 35) \vee (Z=\mathit{Male})) = 1$ (True)

Fine-Grained (Predicate) Signatures



Example of Predicates and Attributes

- Attribute x = (X,Y,Z,W) = ([Group:Group 1], [Age: 20], [Gender:Male], [Member:Silver])
- Secret-key SK_x is given to a person who has the attributes.
- Predicate *f* with parameters *a, b, c* and *d*:

  $f(X,Y,Z,W) \equiv$ TH2 [(X = a), ((Y < b) $\vee$ (Z = c)), (W $\neq$ d)]

  (TH2: threshold function that accepts if at least 2 terms are true.)
- Application Example:

  a $\equiv$ [Group: Group 2], b $\equiv$ [Age: 30],

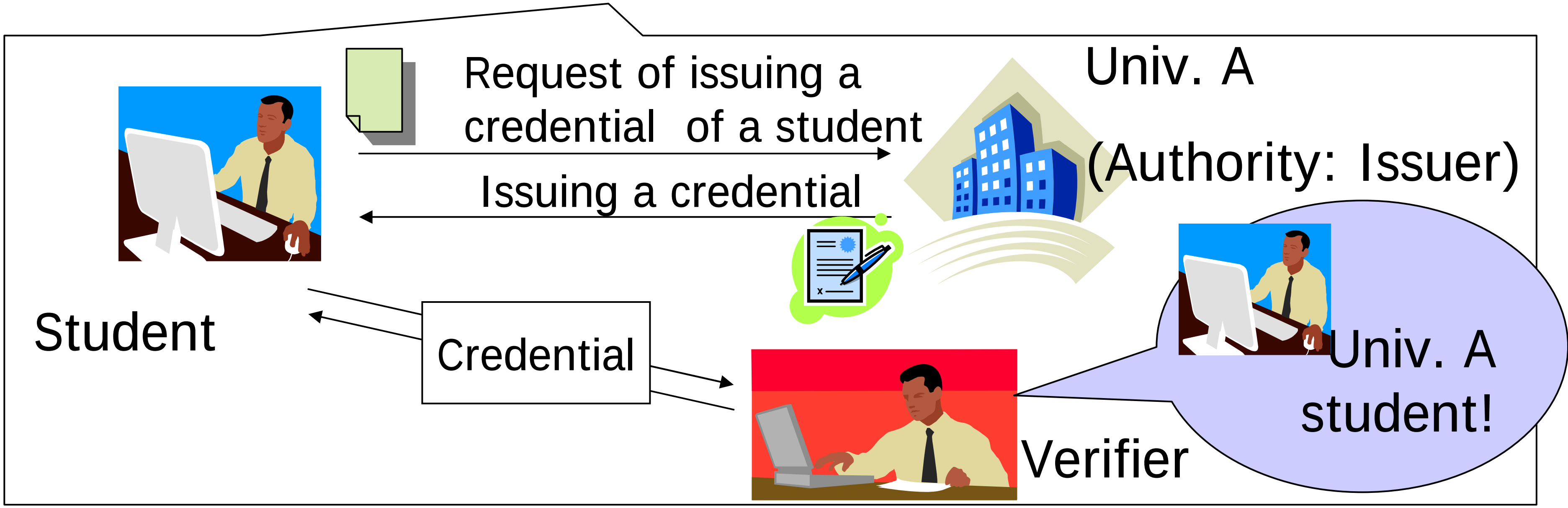
  c $\equiv$ [Gender: Female], d $\equiv$ [Member: Gold],
- A signature with predicate *f* implies that the attributes of the signer satisfies the predicate *f*, i.e.,

  TH2 [(X=*Group 2*), ((*Y* < *30*) $\vee$ (Z=Female)), (W $\neq$ Gold)] =1.

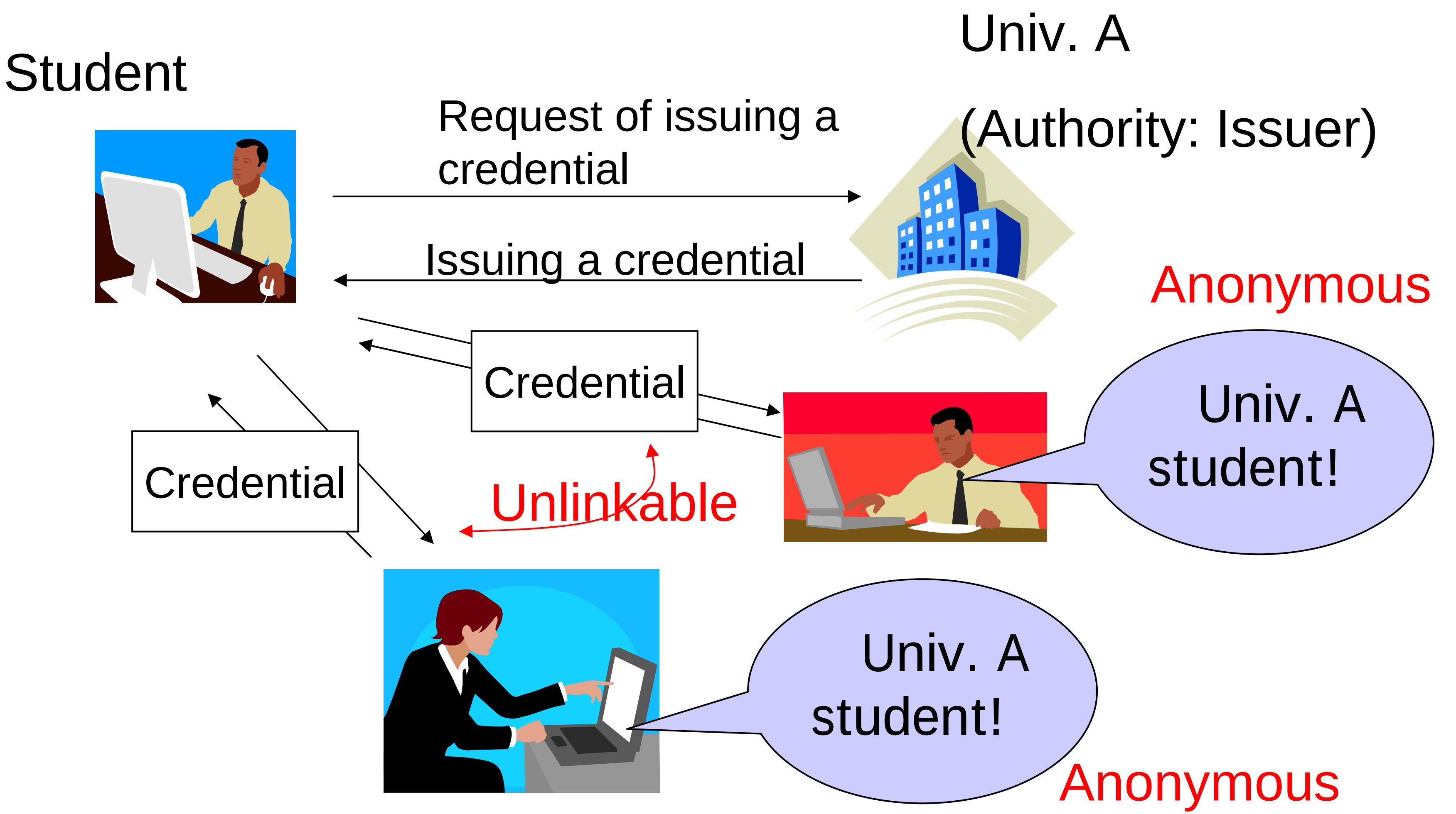
Credential

Certificate for person's qualification/attribut

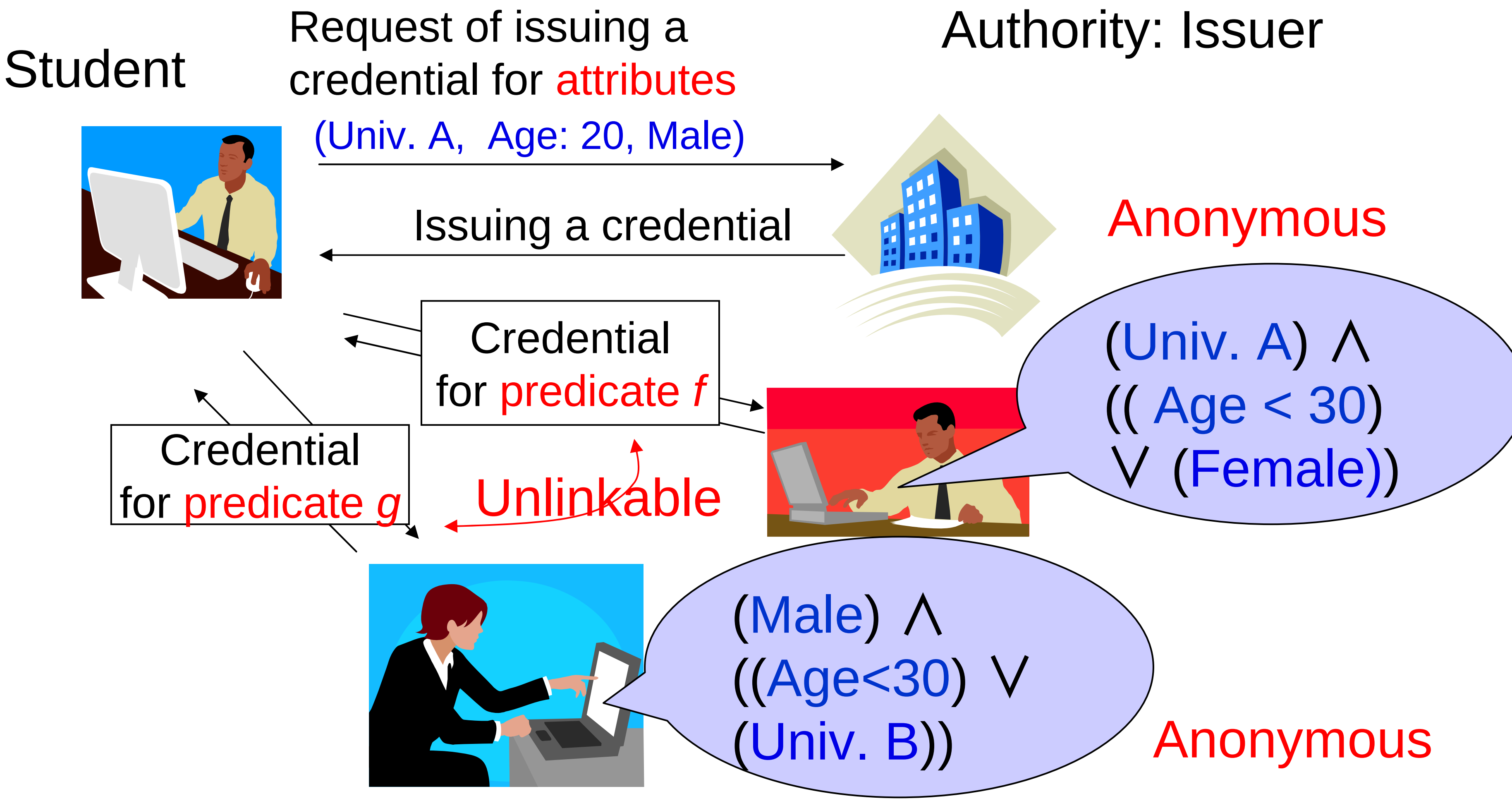
Eg.) "Student of University A", "Right to enter a room"



Anonymous Credential



Fine-Grained Anonymous Credential



For Applications of Fine-Grained Crypto to Practice

- Some standard frameworks (classifications and formats) defining attributes and predicates
- Management and usage rules and tools: New infrastructures (like PKI)
- It took around 20 years to establish PKI after the concept of public-key cryptosystem was proposed. It will take a certain period for the fine-grained cryptosystems to be widely used in practice.

For Your Further Study

- IACR (International Association for Cryptologic Research) ePrint Archive

  http://www.iacr.org/

- Key Words:

  - Predicate Encryption

  - Attribute-Based Encryption (ABE)

  - Attribute-Based Signatures (ABS)

Thank you !!