Inventing the Future of Network Society by Information Security

Tatsuaki Okamoto
(NTT)

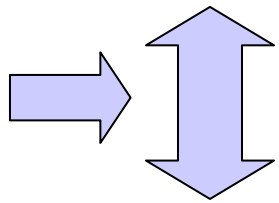
Information Security

The Role of Cryptography and Information Security

ICT systems ・・・ Virtual World

（Every information is communicated and recorded by digital data）

Cryptography and Information Security



Linkage

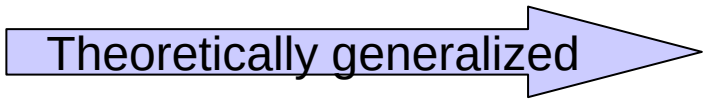
Real World
（estate, property, bank account balance etc.）

Cryptography and Information Security

- Protecting Systems
  - Protect systems and databases from hackers to intrude and attack
- Promoting Business over Networks
  - Payment via networks (correctness)
  - Signing and contracting via networks
- Promoting Social Activities over Networks
  - Voting and auction via networks (privacy)
- Promoting Entertainment over Networks
  - Coin flipping and lottery over networks (fairness)

Cryptography: Key Technology in Information Security

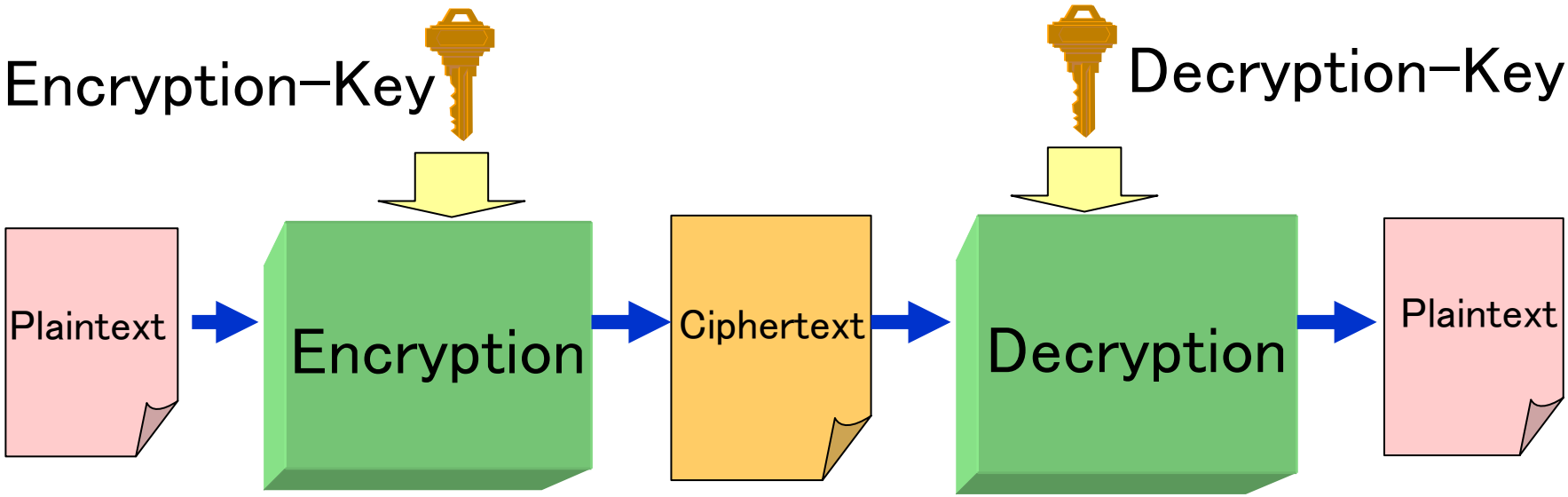
- Basic primitives
  - Confidentiality (Encryption, Key distribution)
  - Authentication (Signatures)
- Cryptographic Protocols
  - Privacy-enhanced basic-primitives
  - Electronic voting
  - Electronic payment/money
  - Electronic contracting
  - Electronic gaming



Multi-party protocols

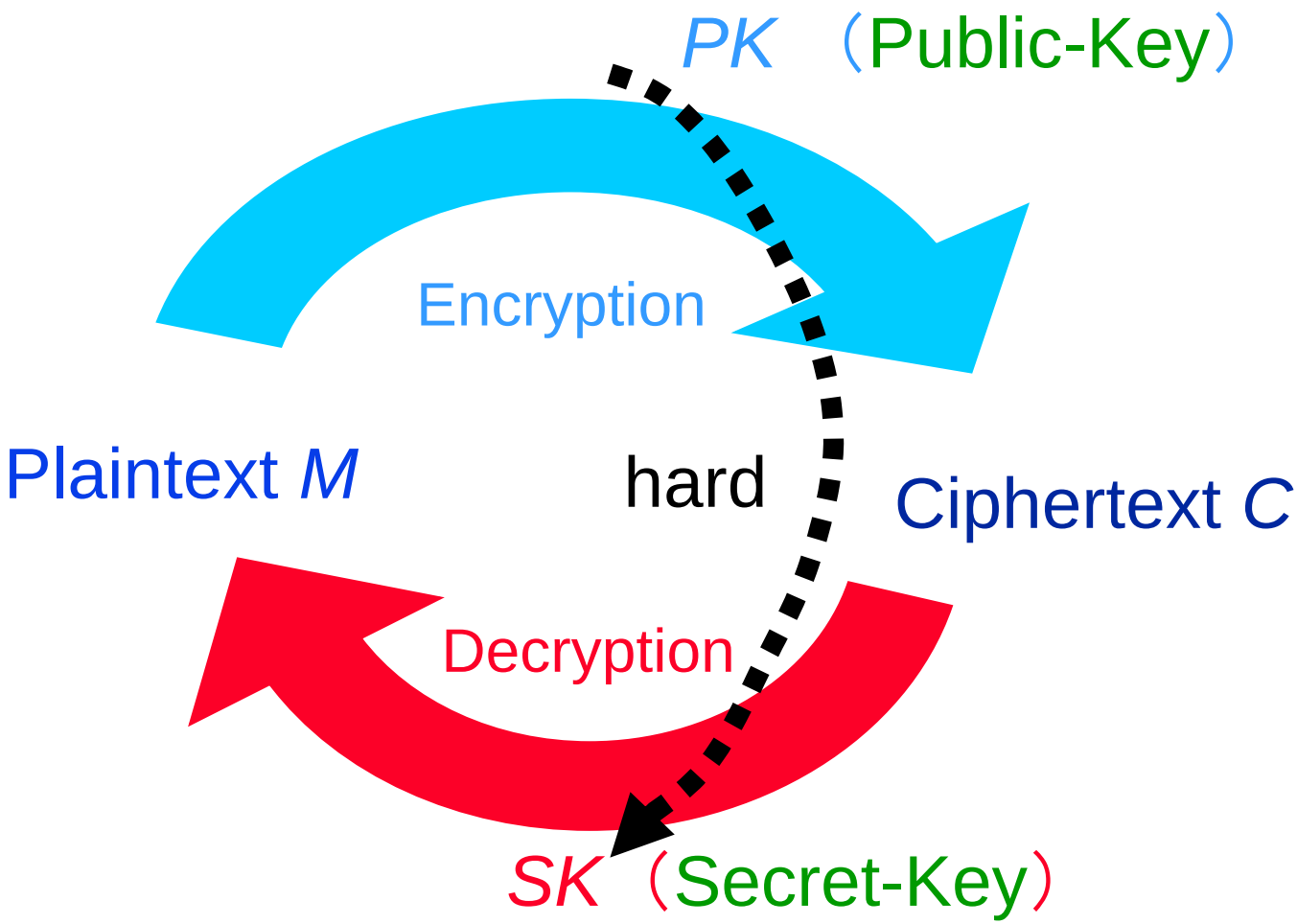
Current Technology

Symmetric and Public-key Encryption

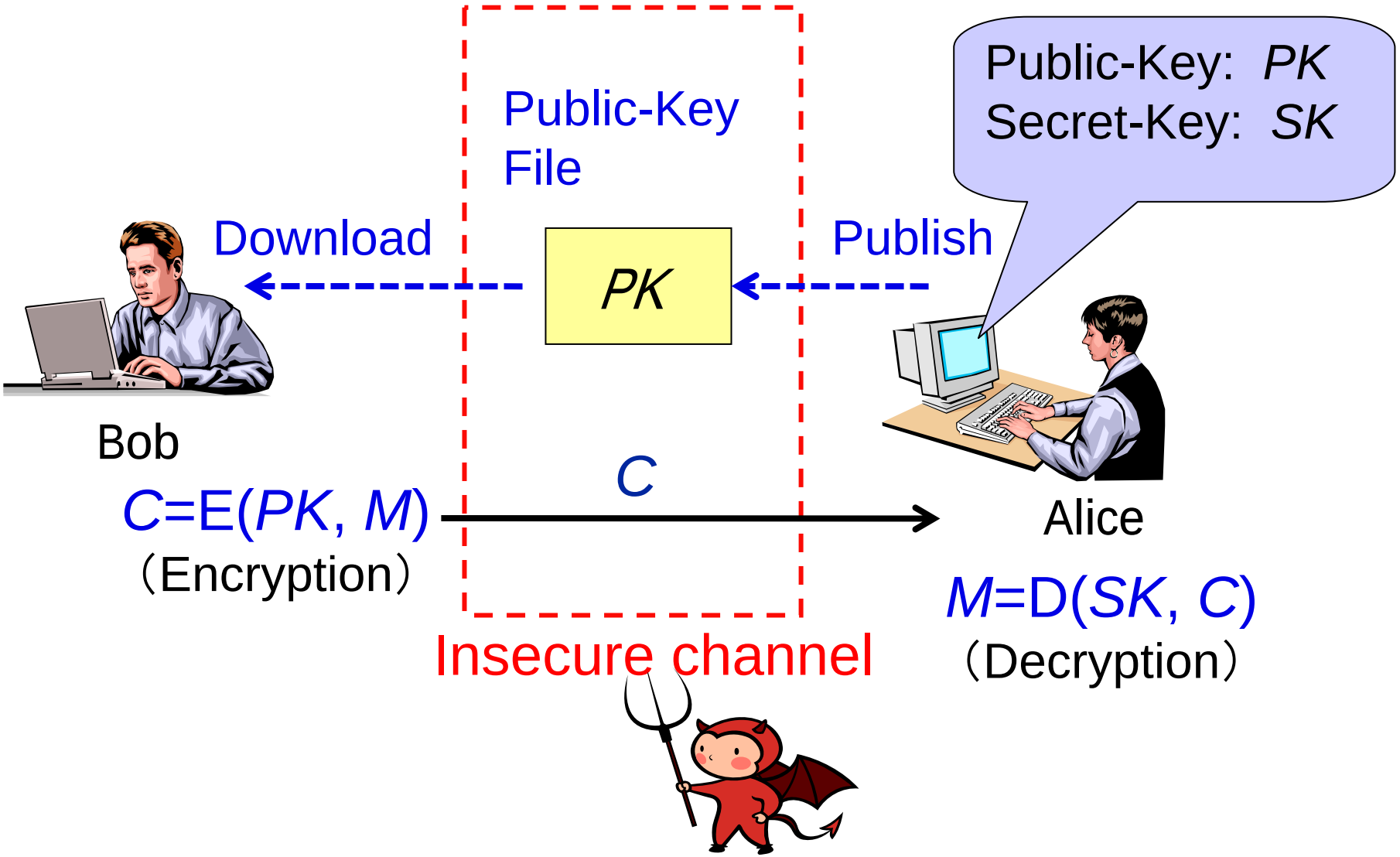


Symmetric Encryption	Encryption-Key ＝ Decryption-Key
Public-key Encryption	Encryption-Key ≠ Decryption-Key

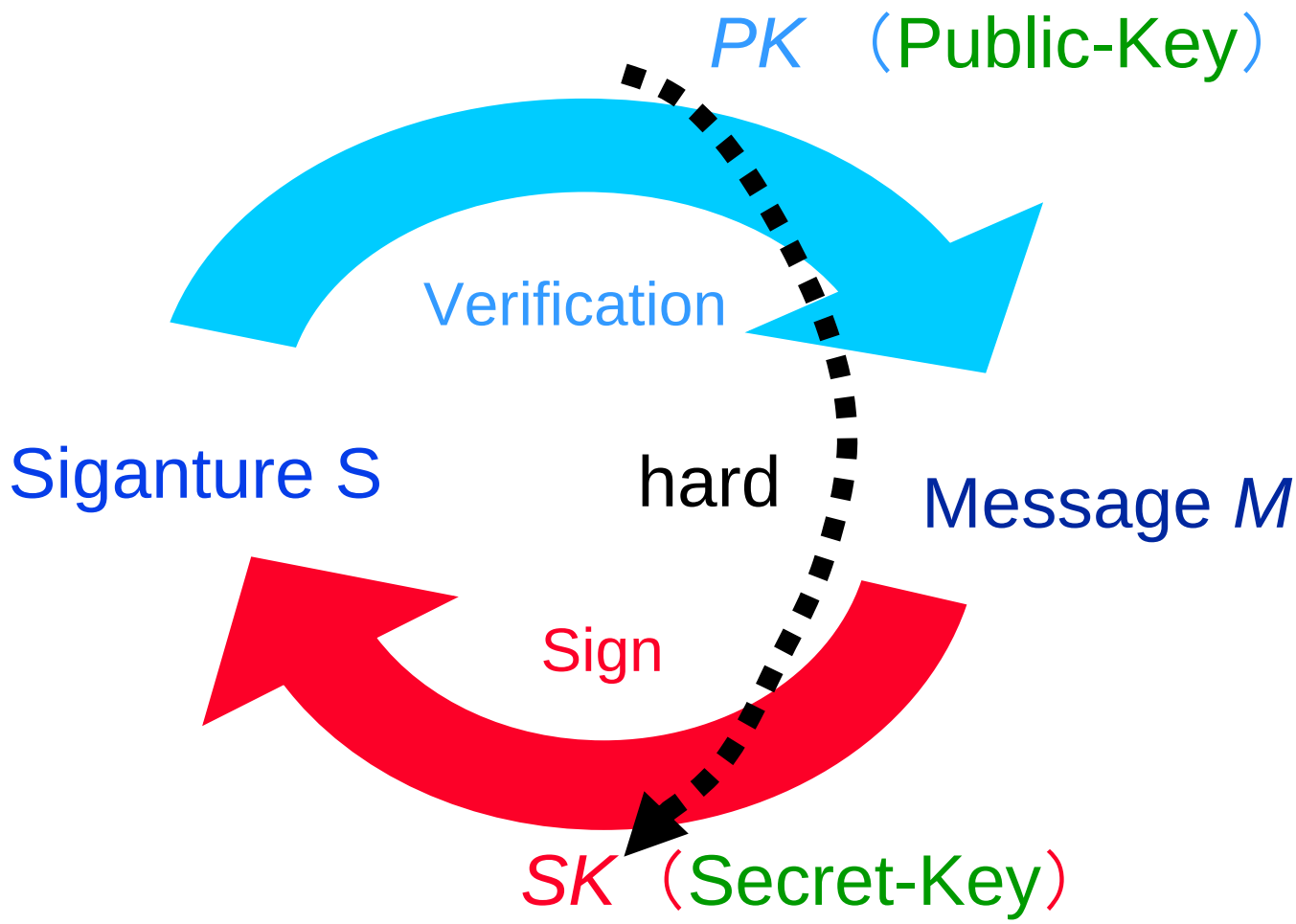
Principle of Public-key Encryption



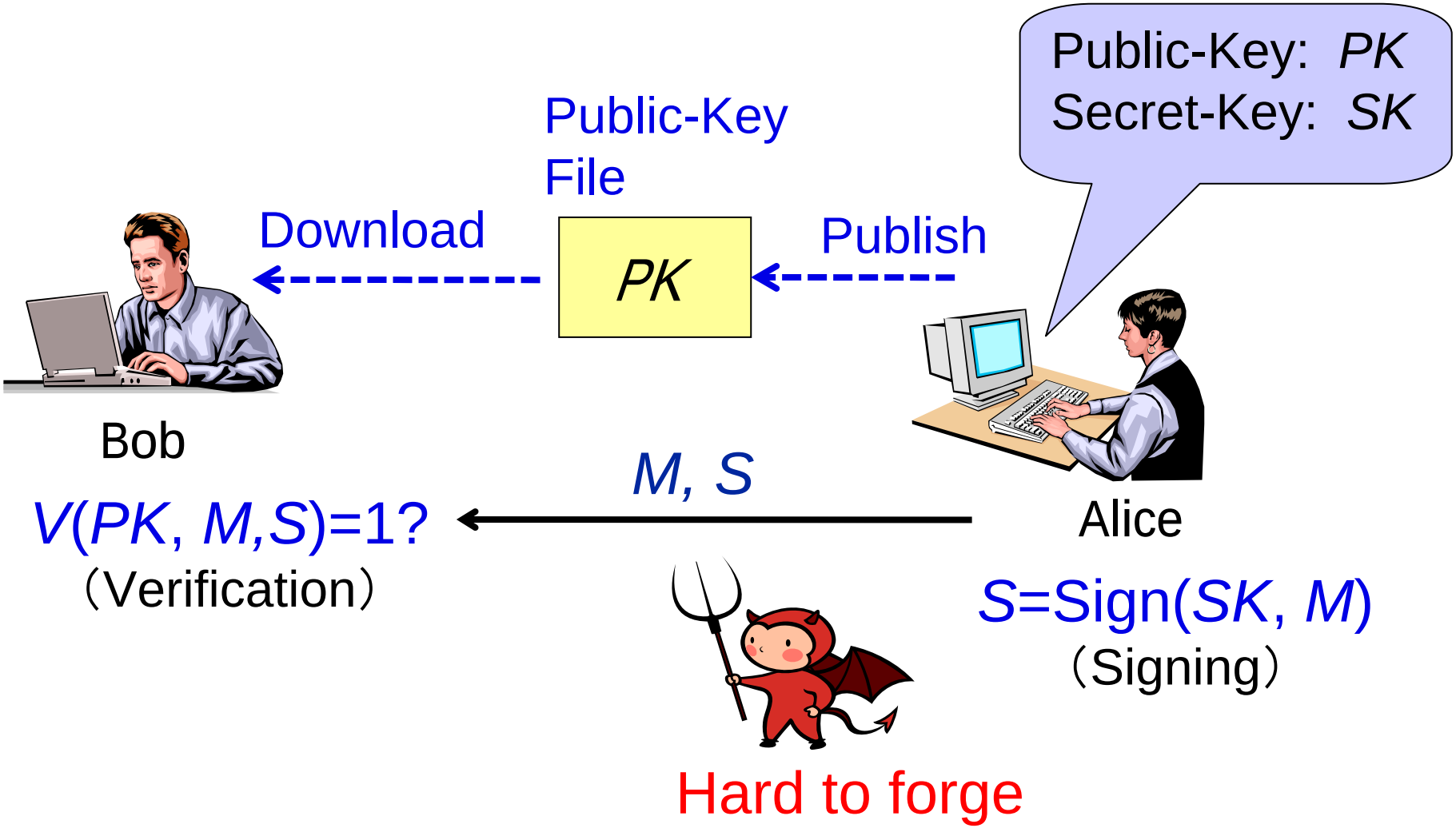
Public-key Encryption



Principle of Digital Signatures

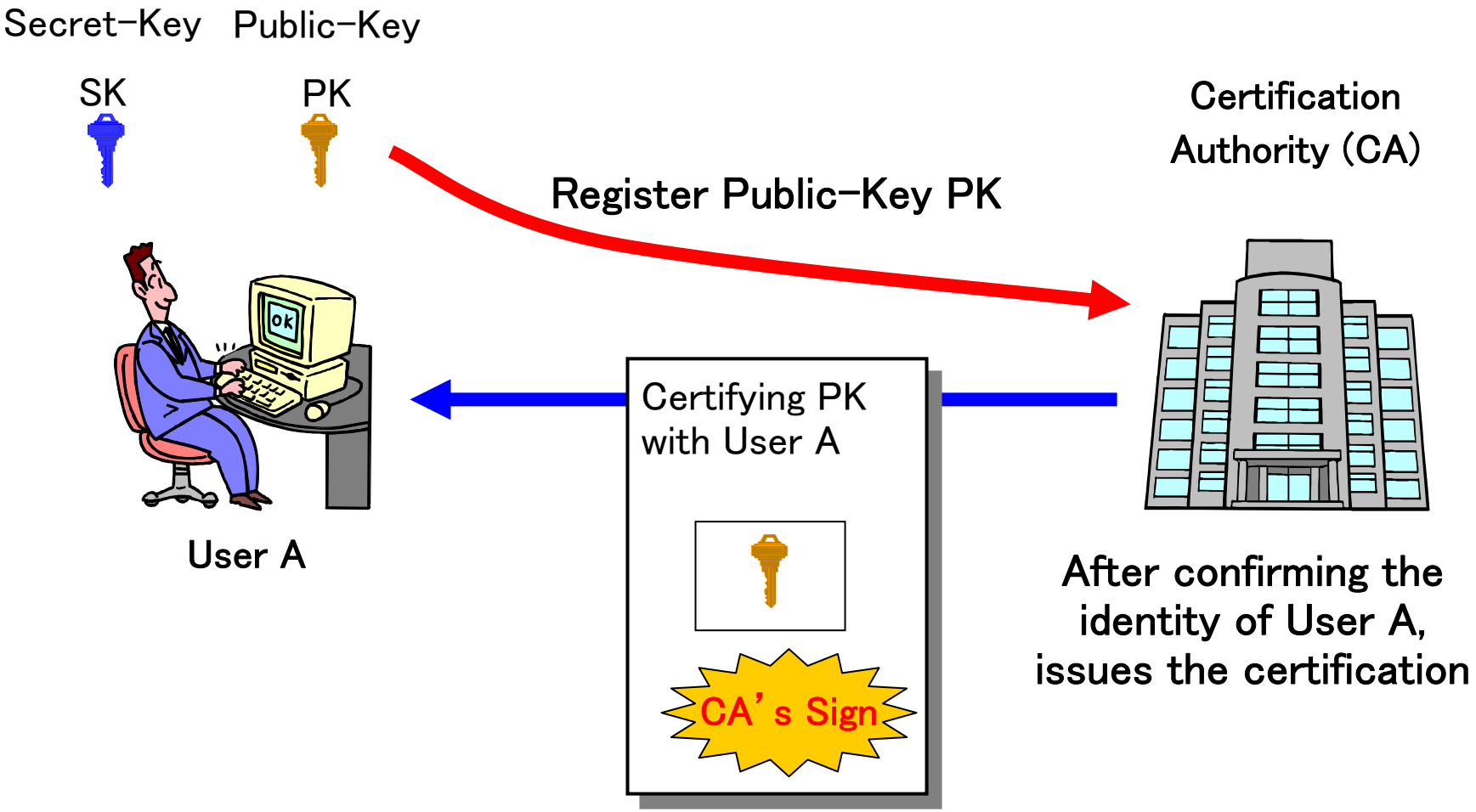


Digital Signatures



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

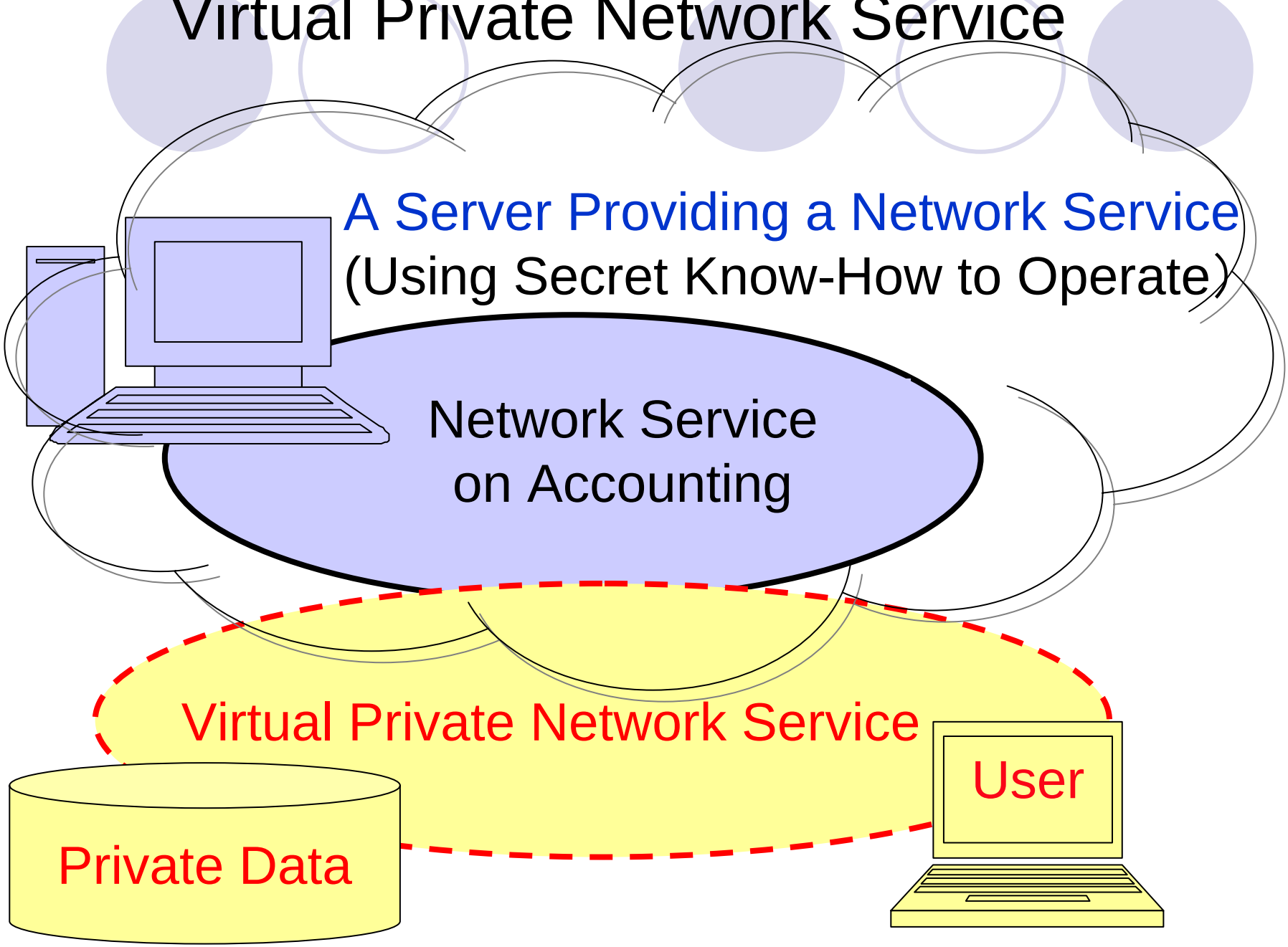
Organization to certify a public-key



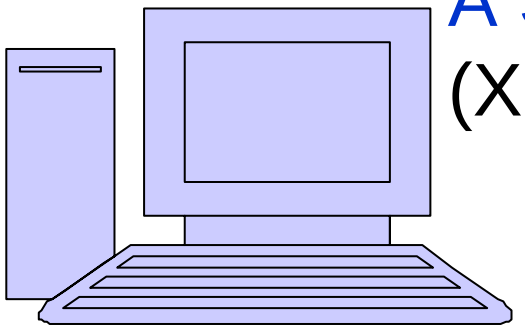
New Technology

(for New Network Services like Cloud Computing)

Virtual Private Network Service



Virtual Private Network Service



A Server Providing a Network Service
(X: Secret Know-How to Operate)

X

by Multi-Party Protocols

F: Computation of the Service

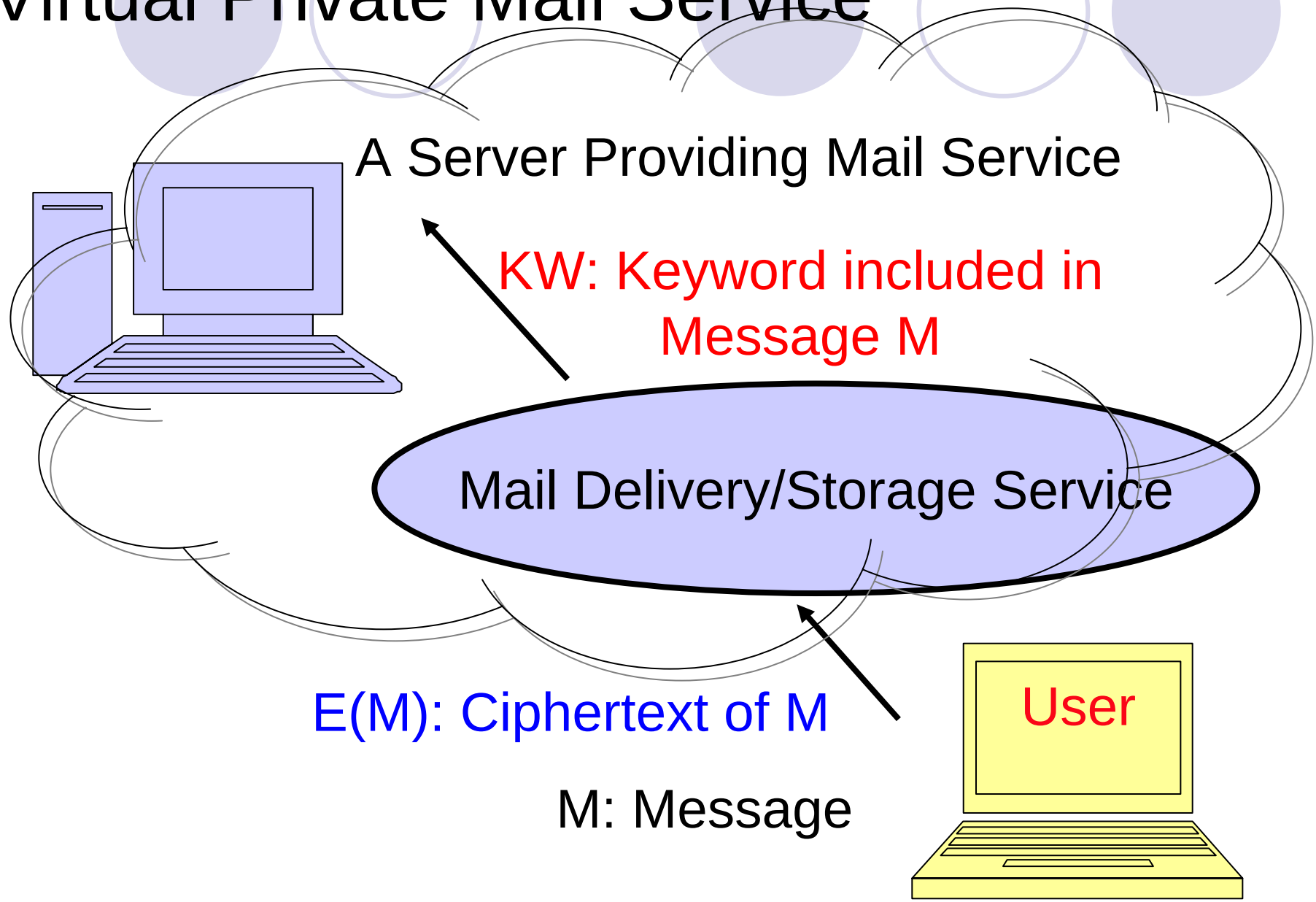
Y

F(X,Y)

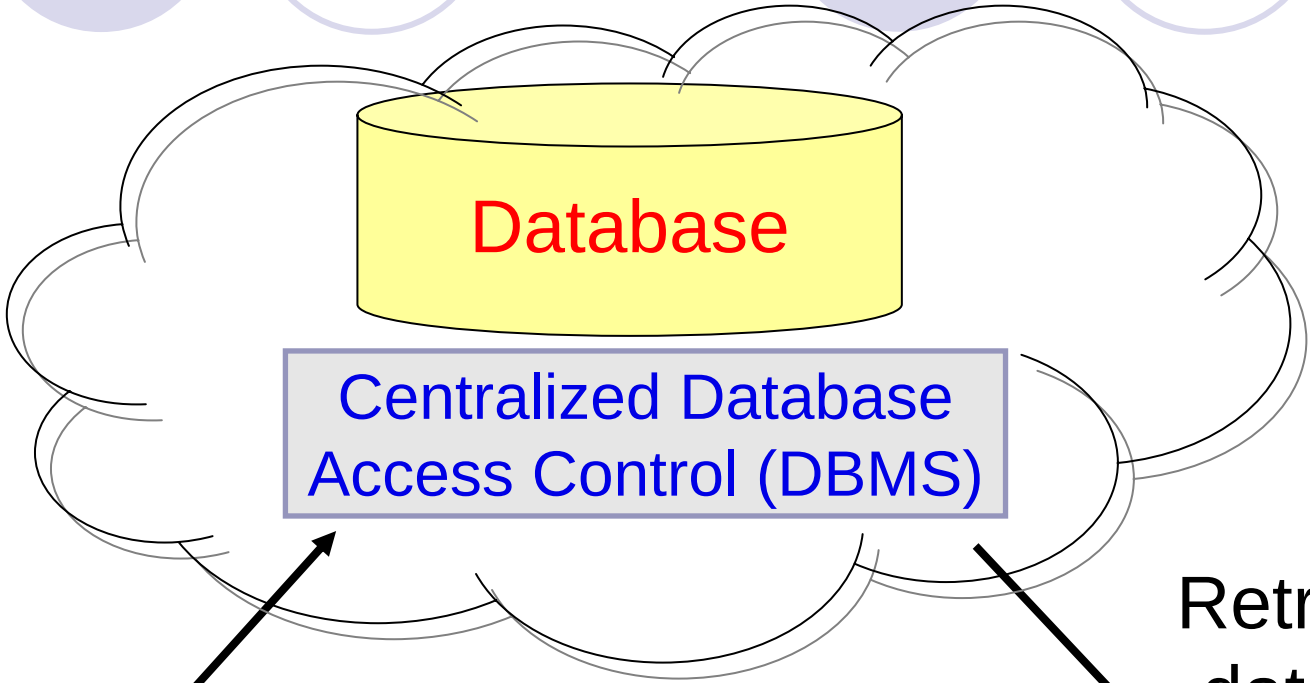
Y: Private Data

User

Virtual Private Mail Service



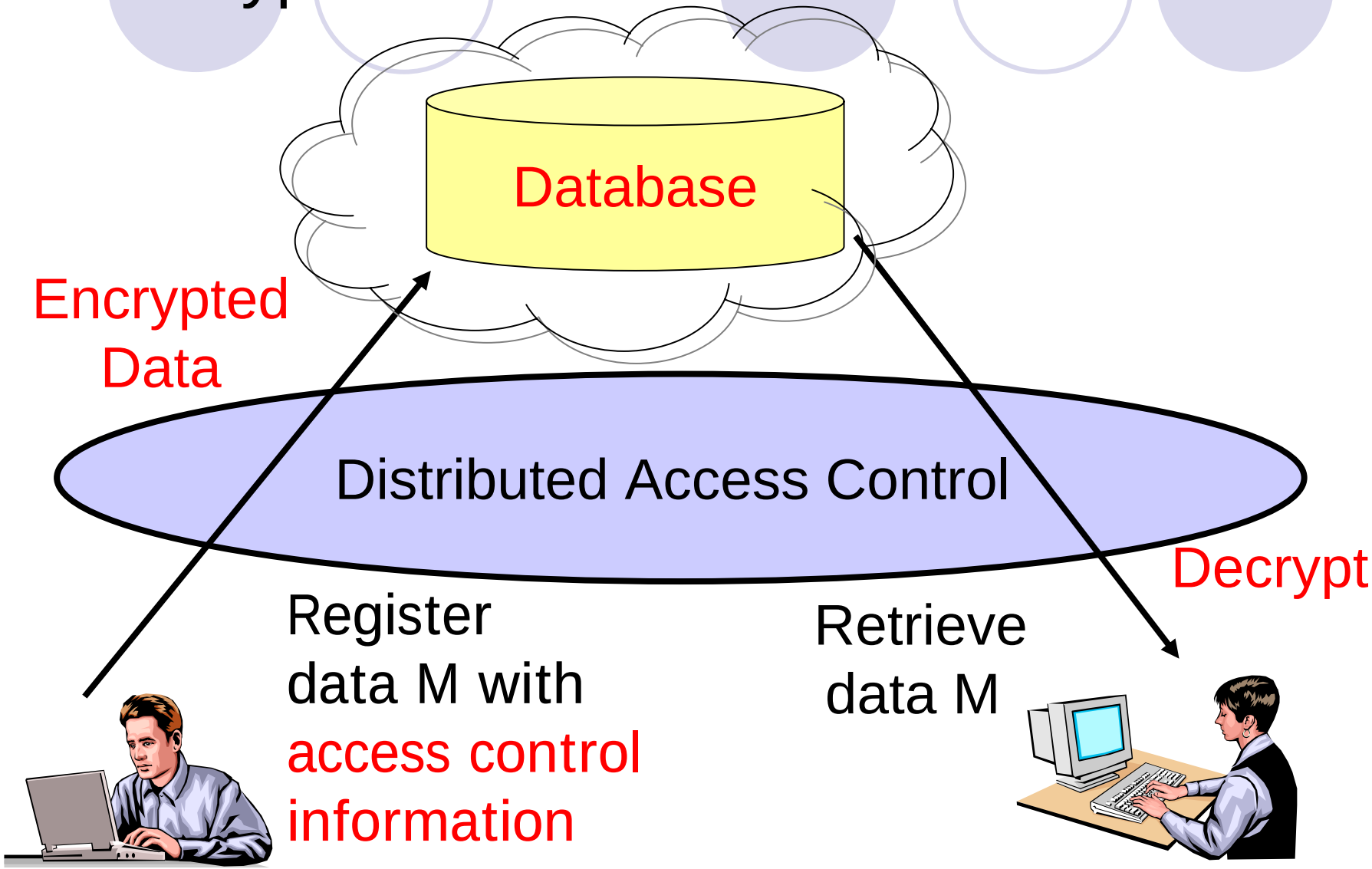
Centralized Access Control of Database Services



Register data M with access control information

Retrieve data M

Distributed Access Control with Encryption for Database Services



Advanced 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

$C=E(x, PK, M)$

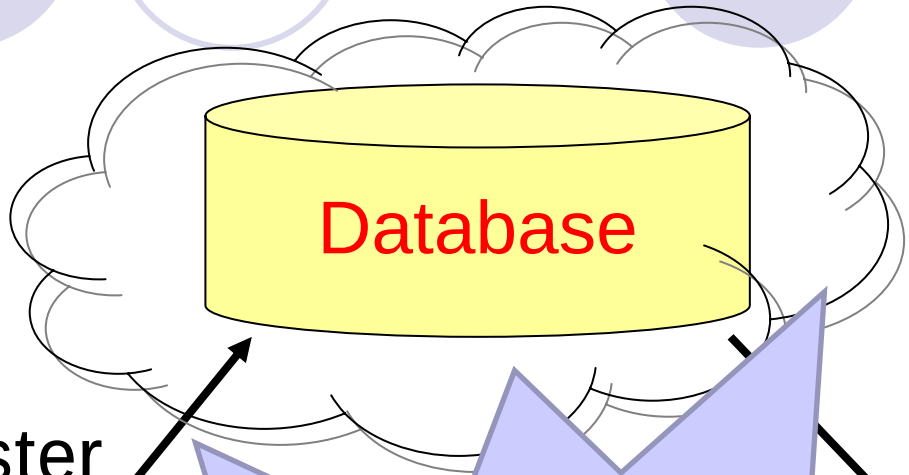
（Encryption for attribute *x* and plaintext *M*）

C

$M=D(SK_f, C)$

（can be decrypted iff $f(x)=1$）

Distributed Access Control by Advanced Encryption



Authority

Predicate f

Secret-Key for f (SK_f)

Register C

Data M can be retrieved when $f(x)=1$: Distributed Access Control with Encryption

Bob

Alice

$C=E(x, PK, M$

(Encryption f

attribute x and plai xt M)

$M=D(SK_f, C)$

(can be decrypted iff $f(x)=1$)

Advanced Encryption 1 (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）

Advanced Encryption 2 (Predicate Encryption)

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）

Summary

- How to guarantee the security in new network services like cloud computing is a key issue in promoting the services.
- New cryptographic (information security) technology guarantees and promotes secure networks services.
  - Multiparty protocols
  - Advanced encryption