Protection of Privacy Right in the Digital Age

- How to Protect Privacy Right by the technology of Information Security-

Atsuko Miyaji, Dr of Sci.
Associate Professor

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

MIYAJI LAB

Outline

1. Discuss the privacy leakage from our usual life.

Our life has been digitalized.

→Show 4 common scenarios.

1. through the Internet
2. at a shop
3. In a library
4. In a hospital

Our privacy may be leaked out.

How and Why? – give the reason in the detail.

2. Is there any technological solution to protect privacy?

anonymity (pseudonym), unlink-ability

group identification, probabilistic encryption

MIYAJI LAB

Our life has been digitalized

Shop

SSL/TLS

VISA

Go to a shop.

Smart Card

Internet

Use internet

Alice

Hospital

Go to Hospital for eye checkup.

RFID

12AXX-horror

Borrow a book with RFID
(Radio Frequency Identification)

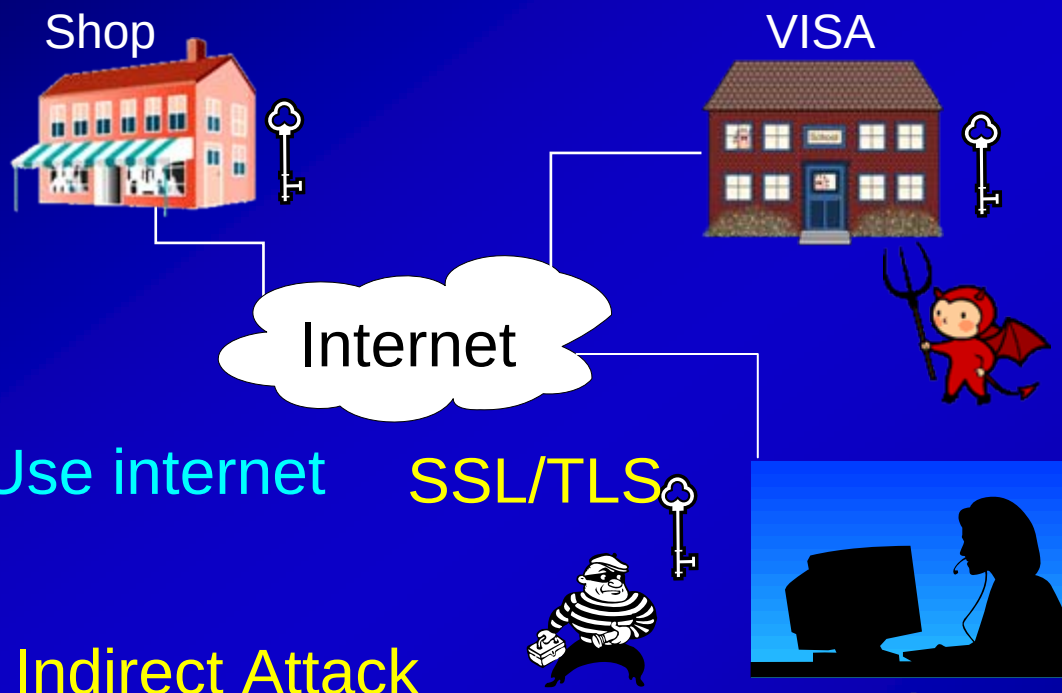
MIYAJI LAB

Our privacy is leaked out 1

It seems secure by encryption.

➡ Keep security analysis against algorithm.

Need a fault tolerance system that stands if a key is stolen.



Direct Attack

The algorithm has been already broken or exposed under a new attack such as SHA1.

SHA1: International Standard Hash function

Our privacy may be leaked out without awareness!!

Indirect Attack

Her key has been stolen.

Alice ➡

Because we share a desktop with others.

MIYAJI LAB

Our privacy is leaked out 2

It seems secure: face-to-face communication without Internet, a smart card, assured theoretically, and a card never stolen.

➡ Pay attention to realistic analysis as well as theoretical analysis.

Indirect Attack
Side-channel attack

Use the leaked device information like power consumption during process and guess a key easily than a direct (theoretical) attack.

Our privacy may be leaked out without awareness!!

Our privacy is leaked out 3

It seems secure by end to end encryption based on SSL/TLS.

➡ Encryption is not enough.

Anonymity (or pseudonym) is necessary.

Our independent privacy may be gathered to reveal serious privacy even if each is secure during transaction.

Our privacy may be leaked out without awareness!!

MIYAJI LAB

Our privacy may be leaked out 4

What is privacy? – name, address and income are all?

➡ Our simple & various privacy such as location, opinion, idea, etc have been digitalized.

Anonymity is not enough.

Unlink-ability between information is necessar

Back to home

A person who loves horror lives here.

Go to a shop.

A person who loves horror stopped here.

linkable

Borrow a book with RFID

Go to a hospital.

A person who loves horror is here.

Relation of privacy protect & information security

Why our privacy may be leaked out? Because

- Weak algorithm or implementation
- We've lost a key (human fault)
- Independent information are combined
- Linkage among information

What technology protects our privacy?

- Analyze a secure algorithm & implementation.
- Key evolving algorithm: minimize damage of a lost key
- Group Identification: authenticate without revealing private inf.
- Probabilistic Encryption: randomize information

MIYAJI LAB

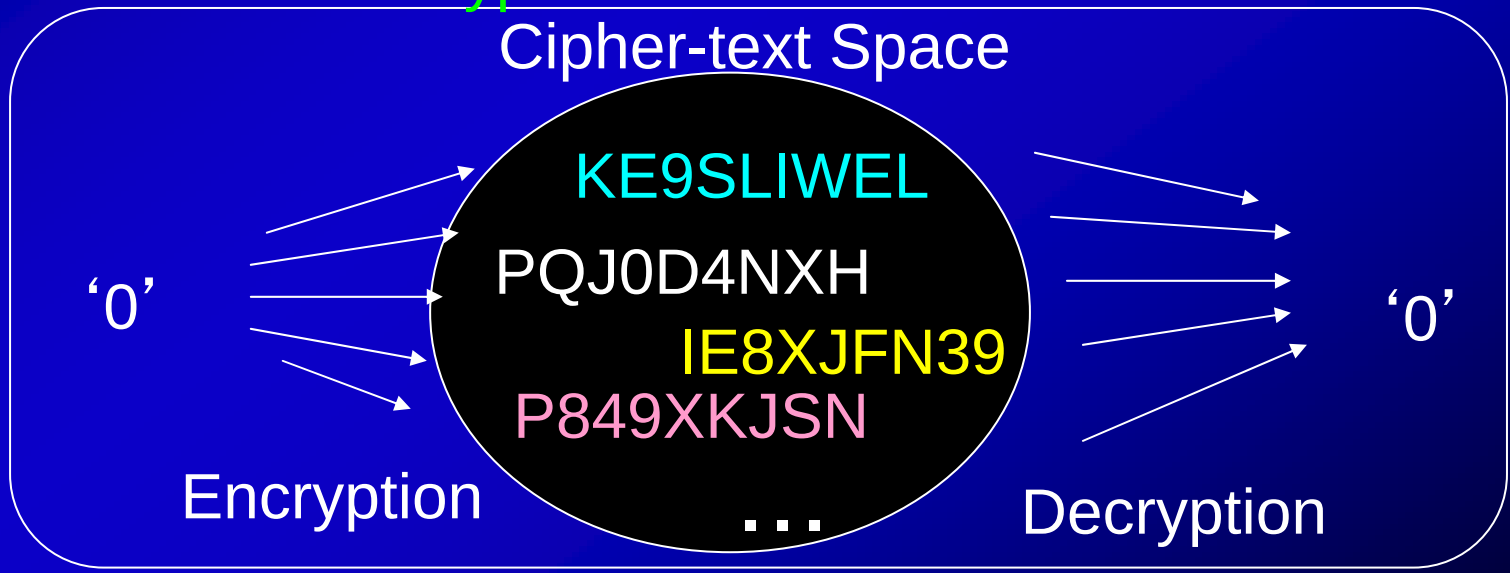
Probabilistic Encryption

Deterministic Enc: A plaintext is encrypted to one cipher-text.
Probabilistic Enc: A plaintext is encrypted to two and more different cipher-texts.

Deterministic Encryption

‘0’ → SJAJIWE54S → ‘0’
encryption decryption

Probabilistic Encryption

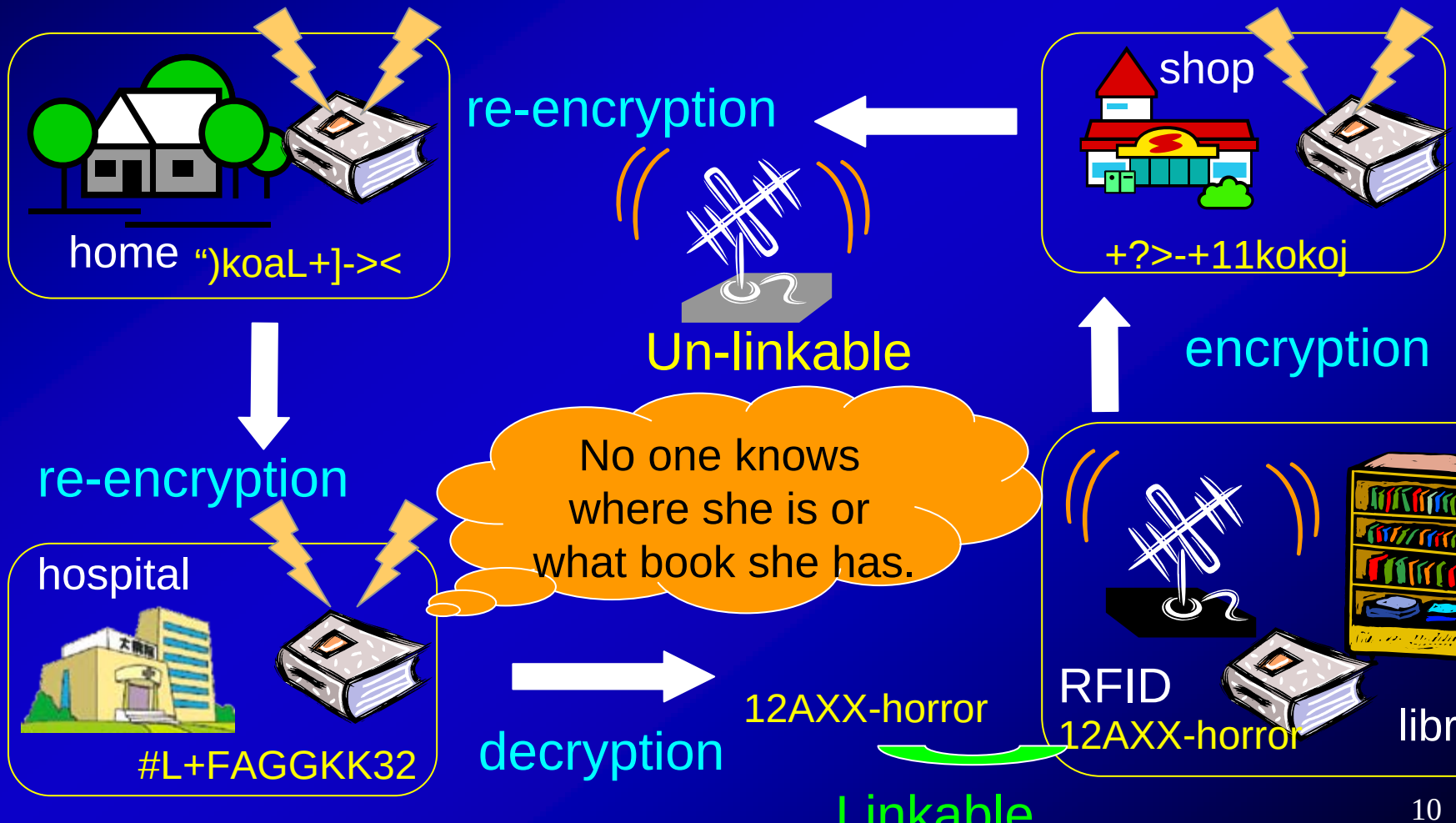


Privacy Protection by Probabilistic Enc

MIYAJI LAB

Encrypt ID information by a probabilistic enc.

Realize unlink-ability among privacies.



Protect Privacy by Security Integration

MIYAJI LAB

Shop

VISA

Secure against SCA

Smart Card

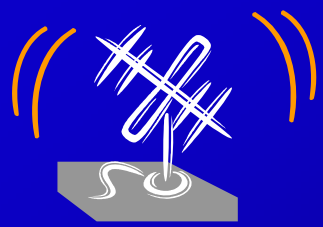
+*?/
Ski

Internet

Group identification

Anonymity
Never combined

- Update secure algorithm according to recent works.
- Key evolving algorithm



Hospital

234LK +>/?

X+**>
Tumor

Unlink-ability

Randomization of information

12AXX horror

RFID

MIYAJI LAB

Concluding Remarks

We have shown how information security protects our privacy.

- Analyze a secure algorithm & implementation.
- Key evolving algorithm ensures the security of a lost key.
- Group identification realizes anonymous authentication.
- Probabilistic encryption randomizes information.

Is there another key technology?

- Public verification realizes the transparency even if it is executed anonymously.

In future work, more flexible security integration will be required.

- Give a way that a user can control the privacy level.
  - Security requirement depends on people or case.
- Provide the minimum integration to various privacy level.
  - Each work is done independently and simple combination makes system huge and inconvenient.

Question or Comment?

Thank you for your attention