

Minimizing Leak by Cryptographic Protocols

暗号プロトコルを用いた 情報漏洩の最小化

Jun Furukawa and Kazue Sako
NEC Corporation

January, 19th, 2012

4th EU-Japan Symposium on the “New Generation Network” and “Future Internet”

Abstract

■ We discuss two approaches to minimize the leak of secrets from database systems and from authentication procedures by using cryptographic protocols. A database system and authentication are now indispensable to provide a variety of services via the network and are targeted by serious attacks.

- **Encrypted Database**: One approach we discuss here is to encrypt data in a database system and manipulate them without decrypting them

- **Attribute-based Authentication**: The other approach is to authenticate users only by their attributes.

Along these approaches, we pose several problems to be solved and issues to be experimented.

■ データベースからの情報漏洩、認証処理からの情報漏洩を、暗号プロトコルを用いて最小化する二つの方法に関して議論する。今日、データベースや認証は、ネットワークを通じて様々なサービスを提供するために不可欠である。議論する一つ目の方法は、データベースのデータを暗号化し、暗号化したままこれらデータを操作する方法であり、二つ目の方法は利用者をその属性により認証する方法である。これらの方法に関して、解決すべき課題や実験すべき事柄を提示する。

Keywords: database encryption, attribute-based authentication, minimum leak, privacy enhancement, cryptography

Encrypted Database

Leak from Database Systems

- Intrusion, malicious/irresponsible manager, design error/malfunction, physical theft

Database Encryption

- Simplifying strategy, risk confinement,

Benefit Loss

- Computational and communication complexity

Recovering the Benefit of Encrypted Database

- Exact search, range query, fuzzy search, statistics, join, update

Minimum Leak

- Trading with efficiency

Challenges for Primitive Constructions

- Protocol constructions

Summary

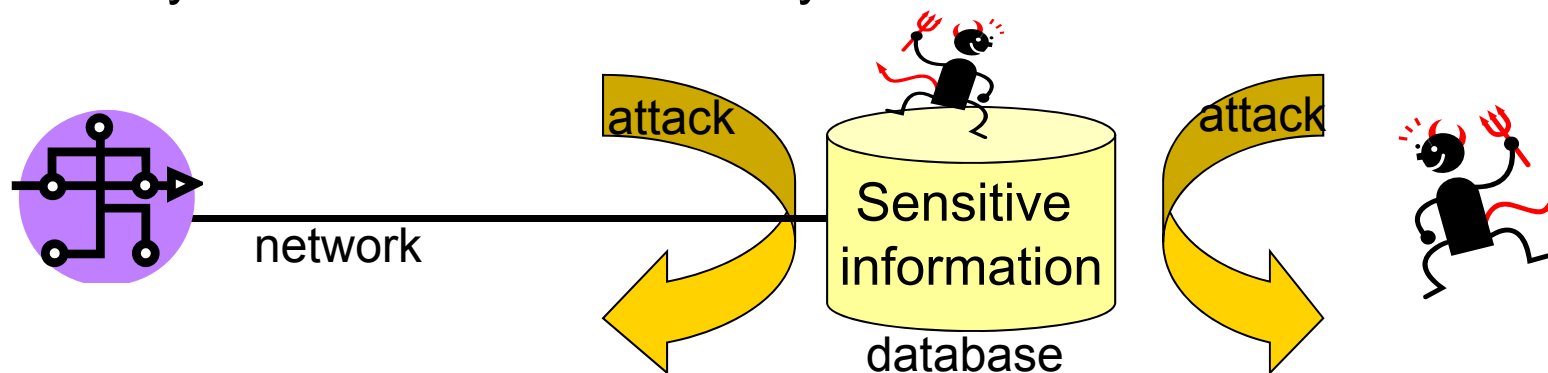
Leak from Database Systems

A database is an indispensable platform for providing variety of services through the network.

Many of databases store **sensitive information** such as customer information, private information, trade secrets, etc.

These information face a threat from leakage by (1) **intrusion via the network**, (2) **abuse by malicious/irresponsible manager**, (3) **design error or malfunction**, (4) **physical theft of storage devices**, etc. Cloud environment makes situation even worse.

Hence, it is crucially important to have a method that unfailingly protect confidentiality of the stored data in many databases.



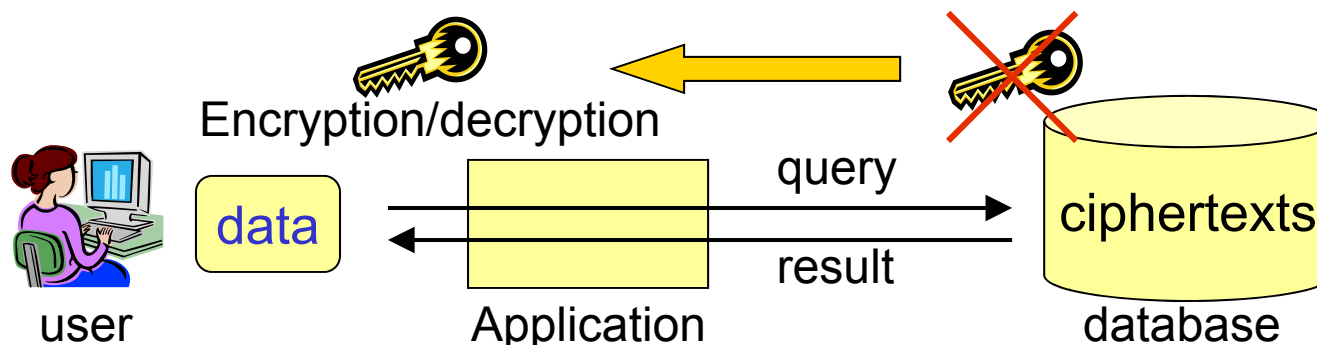
Database Encryption

Access control by authentication, intrusion detection, filtering, etc., is a fairly effective to protect data, but it can no longer be highly reliable if the database itself can potentially be **compromised**.

Hence, **in addition to** access control, it is desirable to enforce the confidentiality of databases by such an encrypting mechanism that **keys for decryption are kept by users**, i.e., data owners, but not by the databases.

Benefits of such encryption are

- Data protection in **different layer** with a **complementing method**
- Risks are confined to only entities other than database system.
- Simple strategy invites less errors
- Effective even against malicious database manager and physical theft

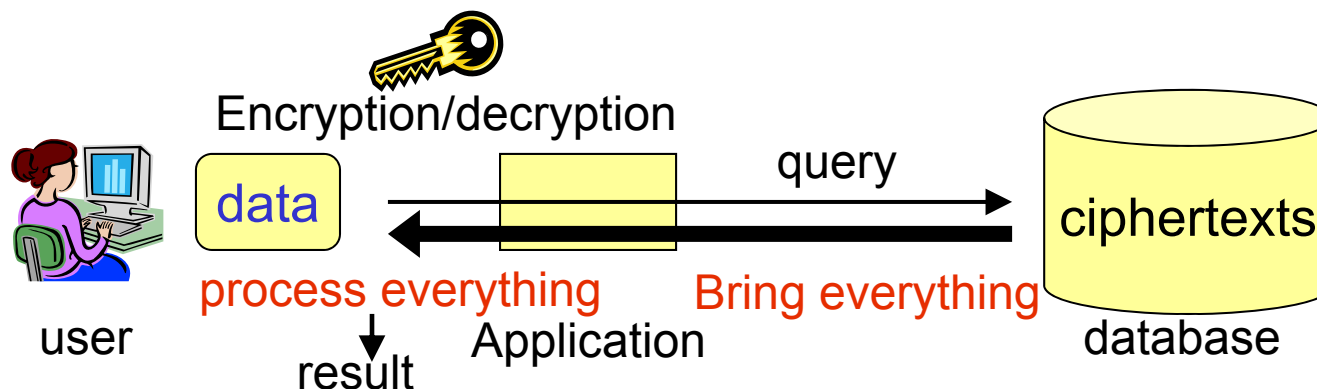


Benefit Loss

While encrypting data is effective in protecting data, it makes database **difficult to process data** so as to answer requests of users.

If a database is unable to process data in variety of ways by itself, a user needs to retrieve all data in the database, decrypt them, find necessary data among them, and process them all by himself when he uses the database.

This imposes a **large amount of computation, communication, and the memory** on the user. Thus the benefit of database is lost.

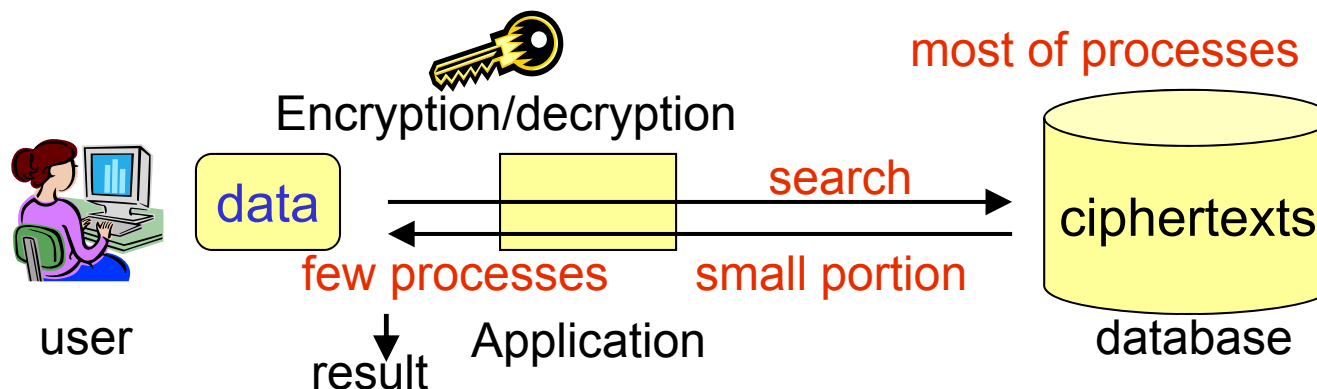


Recovering the Benefit of Encrypted Database (1/2)

A searchable encryption and an order-preserving encryption (OPE) provide a way to recover the benefit of databases in which data are encrypted by users.

- A searchable encryption enables databases to search necessary data without decrypting them
- OPE enables databases to recognize numerical order of data without decrypting them.

Because of these abilities, databases are able to return only ciphertexts of data that are required by users. Hence, their users need few resources for computation, communication, and storage.



Recovering the Benefit of Encrypted Database (2/2)

■ If the amount of data for the query result is **relatively smaller** than the amount of data necessary for processing query, simple data encryption spoils the benefit of database. Hence, designated cryptographic protocols need to be run for most of such cases.

■ Cryptographic protocols for the following procedures are necessary for practically effective encrypted database.

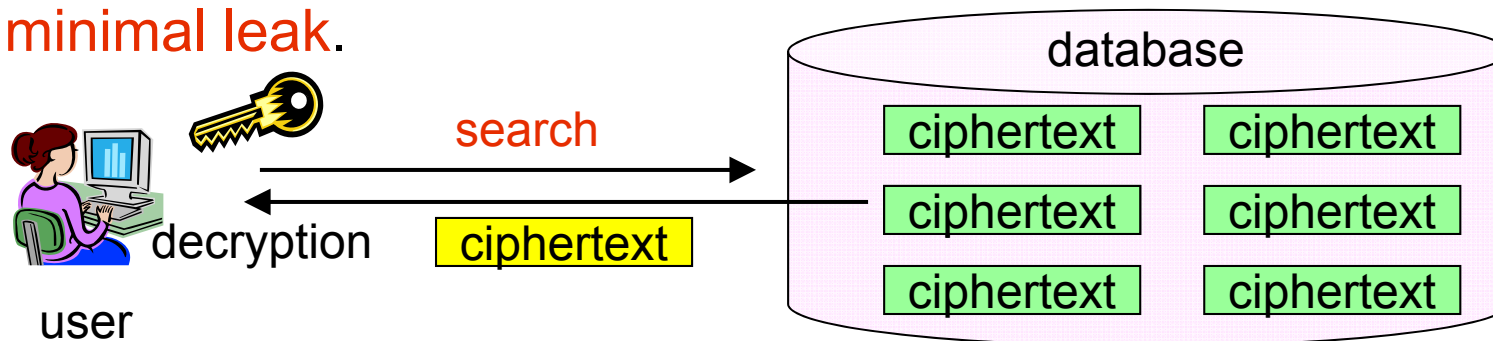
- Exact search: Searchable encryption etc.
- Range query: An order-preserving encryption etc.
- Statistic:
- Fuzzy search:
- Join: Important and frequently required operation if the database is relational.
- (Updates): Updating cryptographic data associated to ordinary updates may not be easy.

Minimal Leak

If user wants to **hide everything** to the database, the database needs to process every data and the response needs to be the maximum possible size data. However, **efficiency** in certain extent (e.g., log time search) is obligatory in current database systems.

We consider it **acceptable trade-off** to reveal database which ciphertexts are handled and which ciphertexts are returned as long as these ciphertexts are not decrypted.

The cryptographic protocols we suppose here are those that allows such a **minimal leak**.



Challenges for Primitive Constructions

Exact search:

- Exact search in encrypted data with minimum leak is easy and efficient in most cases but **updating related data with minimum leak** is not very simple.

Range query:

- Range query can be done by order-preserving encryption (OPE) with minimum leak **only in some cases**. But, in many cases OPE cannot be applied securely and alternative methods are not as efficient as OPE.

Fuzzy search:

- Existing methods are **not very efficient**.

Join:

- Joining tables with both **practical efficiency and minimum leak** is very difficult.

Statistics:

- Using homomorphic encryption, **only simple statistics** such as average, distribution, etc. are easy to be computed.

Update:

- Each cryptographic protocols requires **its own data updating method** with minimum leak

Summary for Encrypted Database

█ Encrypting databases is promising strategy for data protection, which can complements and strengthen protection by access control. However it tends to spoil the benefit of the database if it needs to accept a **variety of queries** such as SQL.

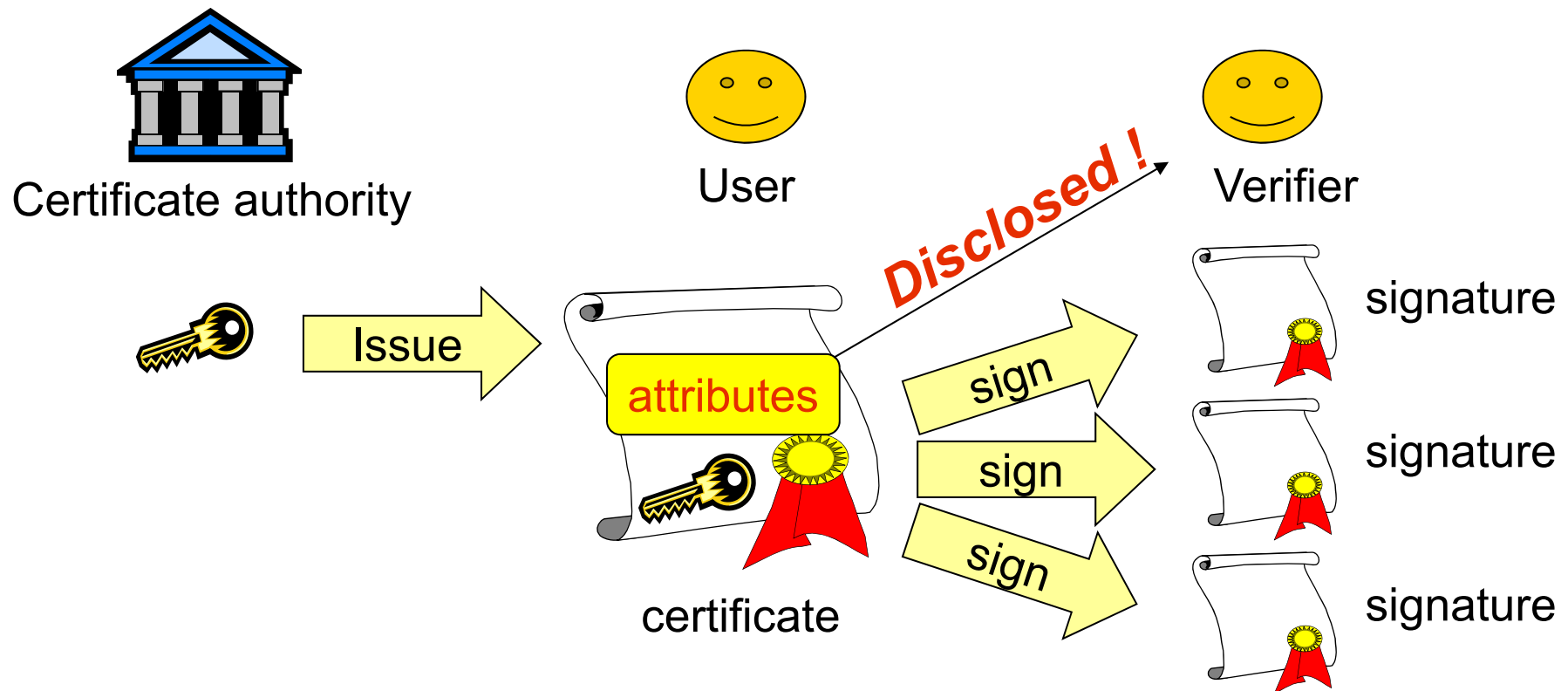
█ To recover those benefits, ingenious cryptographic protocols are necessary. However, current protocols are **not sufficiently efficient** as a total for practical operations. Thus, a lot of research is required for **primitive constructions** such as the discussed examples.

Attribute-Based Authentication

- PKI-based Signature
- Privacy Concerns
- Examples
- Attribute-based authentication
 - Privacy Enhancement via Minimum Leak/disclosure
- Complexities and pilot experiment
 - Variations in revocation, update
 - Experiments in practical applications
- Tools
 - LSI and protocol
- Summary

PKI-based Signature

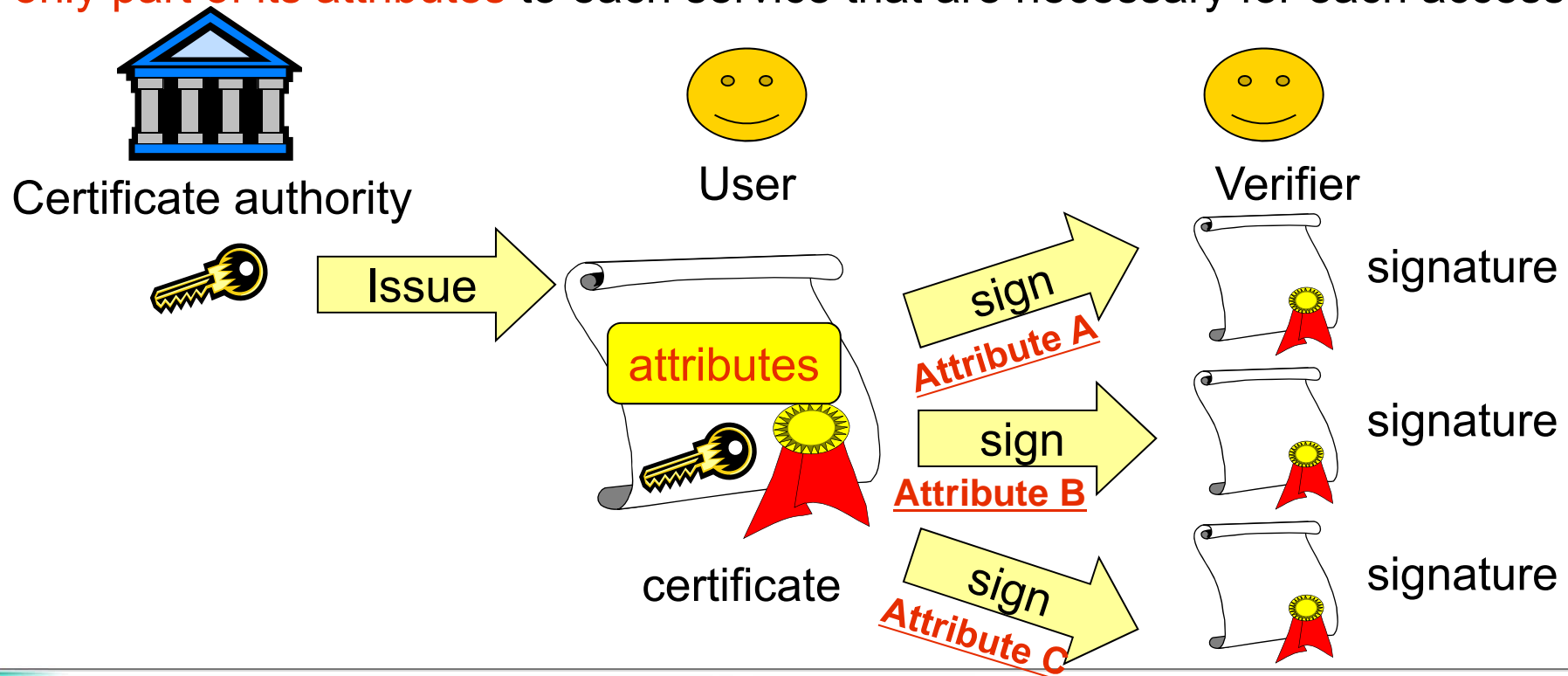
PKI-based signature: A certificate authority issues a certificate to a user. The certificate includes public/private key pairs and attributes of the users. A user generates a signature by using its private key. When a verifier verifies the signature, the certificate of the user with **these attributes are disclosed to the verifier.**



Privacy Concerns

■ If the user is a service provider or an organization, as is in most cases nowadays, disclosing its attributes to those who receive its services causes no problem.

■ If the user is **a person who access to many services**, the user may not want disclose all of its attributes to every service. Such a user wants to disclose **only part of its attributes** to each service that are necessary for each access.



Examples

Identity cards

- Passport, Social security number, Driver license, Health insurance
- Holders may not want to show their identity number. But they need to show that they have a valid number and show a particular set of attributes, and are traceable when necessary.

Electric Payment

- Credit card, debit card, railway/expressway pass
- The card numbers are linked to many attributes of the corresponding card holders. But these attributes are not necessarily disclosed to credit companies.

Social security number

Driver license

Passport

Health insurance

Credit card numbers

Bank accounts

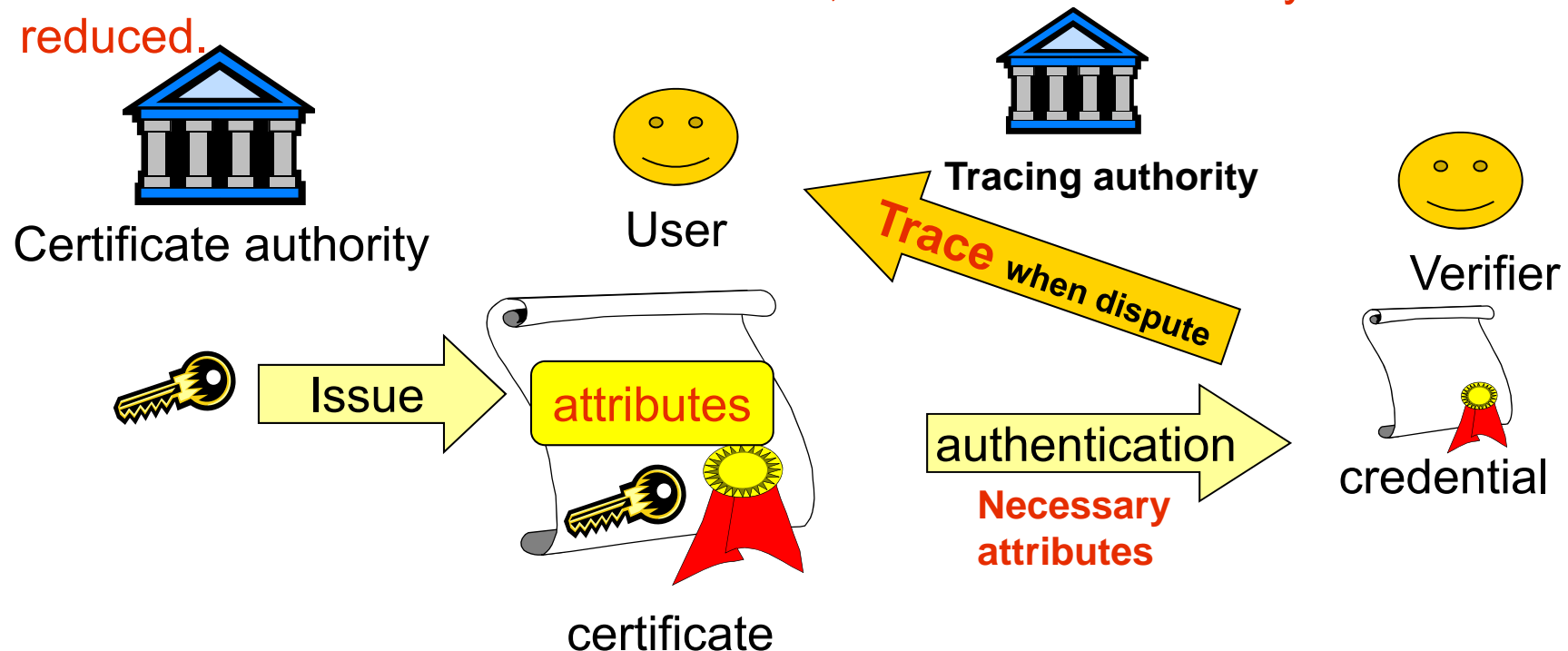
Name, age, address, nationality, phone number,
e-mail, annual income, membership information

Identity card

Attribute-based Authentication

Privacy Enhancement via Minimum Leak/disclosure

- Anonymous credential protocol let a user be authenticated by generating a credential and disclosing **only part of its attributes chosen by the user**.
- Anonymous credential **let an authority trace** the one who generated the credential when dispute while verifier cannot trace it.
- Since the **disclosure is the minimum, what should securely be handled is reduced**.



Complexities and Pilot Experiment

Many type of anonymous credential schemes exist. Most of them have procedures that (1) let certificate authority (CA) **generate its key pair**, (2) let CA **issues certificate** to users, (3) let a certified user be **authenticated** by generating credential that **reveals arbitrary chosen attributes**, (4) let an authority **trace**, from a credential, the user who generated the credential, (5) **revoke** attributes/users, (6) **update** attributes

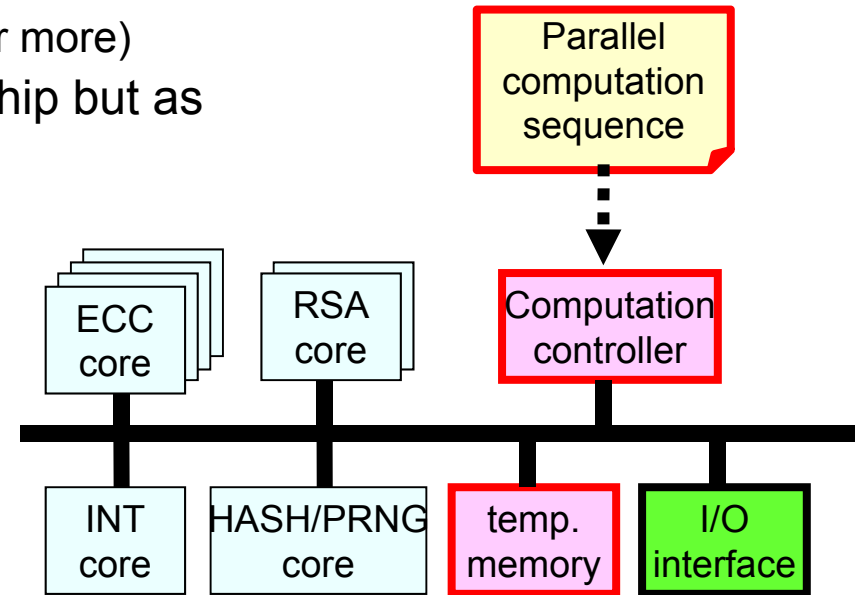
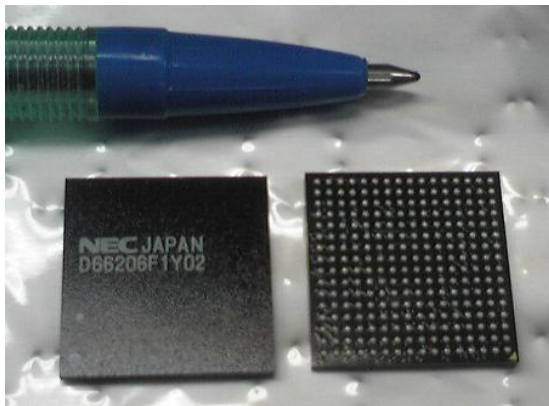
Complexities of these procedures differ large depending on schemes. Especially, that of revocation of attributes/users and update of attributes.

No scheme provides all procedures that are perfectly efficient. Hence, the practicality of schemes depends on the choice of concrete applications and **we are not sure** if any anonymous credential can be useful. Therefore, **pilot experiments** are necessary for the next significant step.

Tools

An LSI for group signatures (2010)

- Fast signature generation/verification speed.
 - 0.1 seconds at 150MHz clock
 - Same speed with S/W on 3GHz clock PC
- Low power consumption.
 - Less than 0.6W at 150MHz clock
 - 1/100 or less power compared to PC (60W or more)
- Usable not only as an independent LSI chip but as an IP core ($2mm^2$)



Anonymous credential with fast attribute updates

- Very efficiently attribute updatable

Summary for Attribute-based Authentication

■ Attribute-based authentication will be necessary if individuals need to access many services that verifies each one's attributes.

■ Anonymous credential can be an answer for this problem. But whether or not its efficiency is enough is not clear and we need **a good pilot experiment** for the next significant step. This will further teach us lessons in real-life implementation.

NECグループビジョン2017

人と地球にやさしい情報社会を
イノベーションで実現する
グローバルリーディングカンパニー



Empowered by Innovation

NEC

Part of results presented in these slides
were sponsored by Japanese Ministry of
Internal Affairs and Communications.