Telecom-munications

An individual controllable secrecy computation system realizing effective use and privacy protection of big data

Keiichi IWAMURA (Professor, Department of Electrical Engineering, Faculty of Engineering, Tokyo University of Science)

Purpose of Research

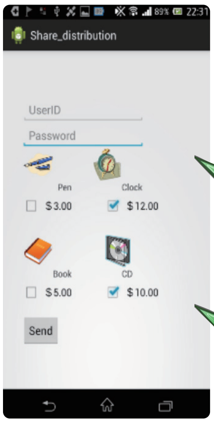
The effective use of big data is one of the keywords in the present technology. However, because big data includes personal and confidential information, there is a need to protect privacy while using this data. One of the technologies for realizing this is secrecy computation. However, because the data is processed while being kept secret, the processing is generally heavy, and due to the huge amount of data, conventional technology cannot be easily used. Thus, I am researching a method that can be controlled by even a smartphone.

Summary of Research

When users store data in the cloud, it is encrypted in order to protect the data. However, when it is time to use the data, the data must decrypt itself, so it cannot be processed in the cloud. In recent years, much research has been conducted into secrecy computation, which utilizes the secrecy sharing scheme to enable processing in the cloud using secret data while maintaining the secrecy of the data. However, when management of the cloud is outsourced to a single company, users cannot escape the insecurity that the secretly shared data may be collected and decrypted. Therefore, I propose a system in which secrecy computation using the secrecy sharing scheme cannot be performed without the data that is managed by the user. Even for a huge volume of data, as long as the user manages a single key, the system realizes high-speed secrecy computation.

Life log system using a smartphone

Because of the light weight and small volume, it is possible to create an application that secretly manages an individual's own records (life log) on a smartphone



Share_distribution

UserID

Password

Pen □ $3.00

Clock ☑ $12.00

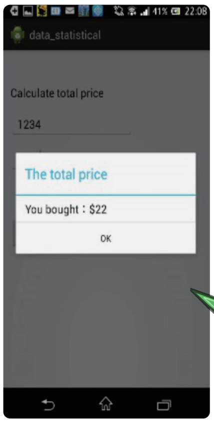
Book □ $5.00

CD ☑ $10.00

Send

User enters his/her ID and password

Select a product



data_statistical

Calculate total price

1234

The total price

You bought : $22

OK

Even if the user stores the large purchase history on a management system, it is possible to manage the history, total amounts, etc. without the contents of the data being made known.

Points

- **Generate a huge volume of shares from a secret key without storing the data**
- **High-speed secret sharing scheme can be realized using just addition and subtraction**
- **Owner of the secret data can control the secrecy computations**

Comparison with Conventional or Competitive Technology

- The huge volume of data that should be managed on the server can be consolidated into a single key data that the user can manage.
- Proposing a high-speed secrecy sharing scheme that enables sharing and restoration through just addition and subtraction.
- Because the user only needs to manage a single key, secrecy computations using smartphones and other similar devices are possible.

Expected Applications

- Managing household expenses online (can average and tabulate monetary amounts, which is personal information, while maintaining the secrecy)
- Life log application (every time data is created, it can be shared, secretly computed and decrypted using a smartphone)
- Statistical processing while maintaining the secrecy of the personal information in the medical and other fields (enables both a reduction in record volumes and statistical processing)

Challenges in Implementation

The basic secrecy calculations has been realized, but study needs to be conducted into the practical applications.

What We Expect from Companies

Companies that want to use this research for a specific application are asked to contact me.

Future Developments

October 2015:
Demonstration at the Computer Security Symposium 2015
2016~2017 : Research on secrecy computation.
2018~ : Study for practical applications for secrecy sharing schemes and secrecy computation.

■ Associated System:	Grants-in-Aid for Scientific Research, Basic Research (C)
■ Intellectual Property:	Patent application filed in Japan
■ Awards:	Fellowship from the Information Processing Society of Japan

TOKYO UNIVERSITY OF SCIENCE Organization for Innovation and Social Collaboration

1-3, Kagurazaka, Shinjuku-ku, Tokyo, 162-8601, Japan E-MAIL: ura@admin.tus.ac.jp
2022.04