Communication and information processing

Authentication based on verifiable encryption with private digital identity

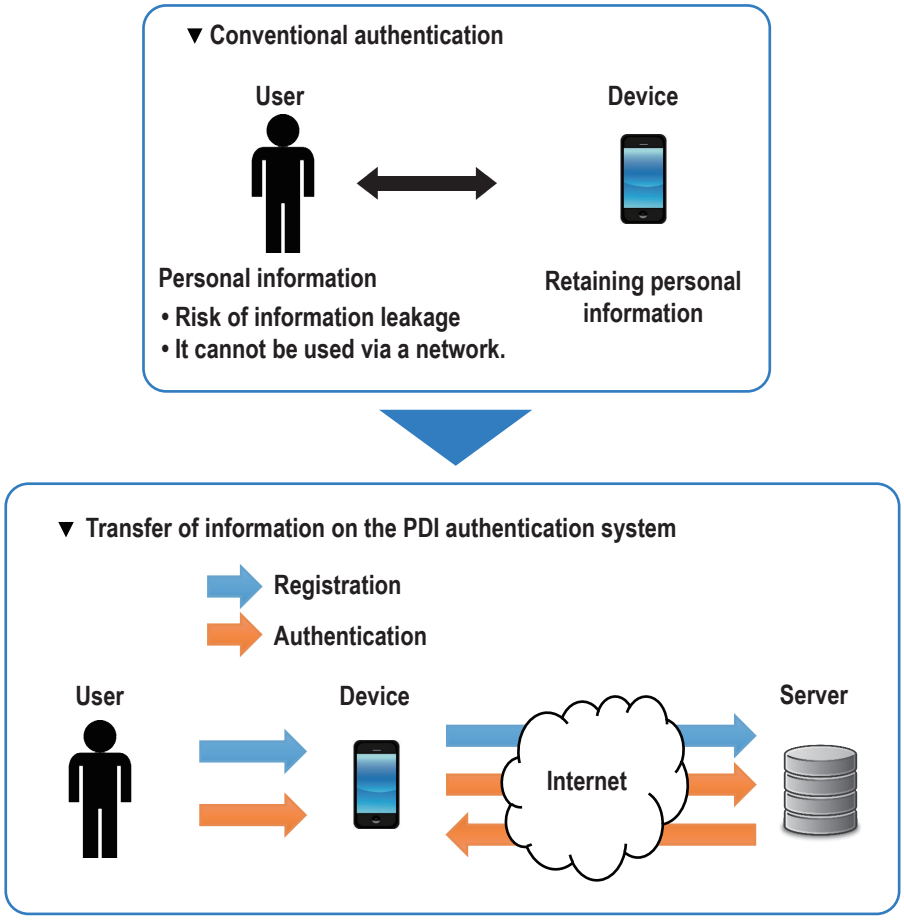
Satoshi IRIYAMA (Associate Professor, Department of Information Sciences, Faculty of Science and Technology, Tokyo University of Science)

Purpose of Research

As information communication technology has advanced, it has become possible to buy all sorts of products and services remotely through the Internet. In these cases, users have to give their personal information such as name, age, and address to service providers. This may cause problems such as unwanted distribution of excessive advertisements and personal data leakage from companies' databases.

Summary of Research

Aiming to simultaneously protect privacy and retain convenience, in this research we have developed an original technology that encrypts information selected by the user as his/her identification and carries out rapid verification using its secure algorithm without any decryptions.



*PDI: Private Digital Identity

Comparison with Conventional or Competitive Technologies

Conventional situation: Some processing methods have encrypted information without decryption.

Problems with conventional systems:

- There is a risk of information leakage because personal data (such as biometric data and PINs) are placed together and stored in a single place.
- Safety is pursued at the expense of data processing speed.

This new technology: It assures sufficient processing speed, safety, and reduction in internal memory use.

Expected Applications

- Reduction in workload at front desks of private lodgings and hotels, coworking spaces, and home security services
- Admission control at event venues and improvement in public Wi-Fi security
- Use by people such as children and seniors who are not familiar with smartphones

Challenges in Implementation

- Current status: The system is working in the laboratory, and some pilot systems with server and core SDK are ready.
- Tasks to do: Create a business model such as an appropriate form of use.

What We Expect from Companies

We hope to conduct joint research with a company that has database or personal authentication technology. In addition, this technology would be useful for companies developing IoT products and companies planning to venture into Cloud services.

POINT

- **No need to exchange keys**
- **The risk of information leakage is reduced because personal information is encrypted and not decrypted**
- **The entry cost is low because the server can be entrusted to a third party**
- **Does not use smartphones**

■ Intellectual Property: International Patent Application
No.PCT/JP2018/45505 "Encrypted Data Processing System and Program"
■ Prototype: Present

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