# ビッグデータの有効活用とプライバシー保護を実現する個人制御可能な秘匿計算システム

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

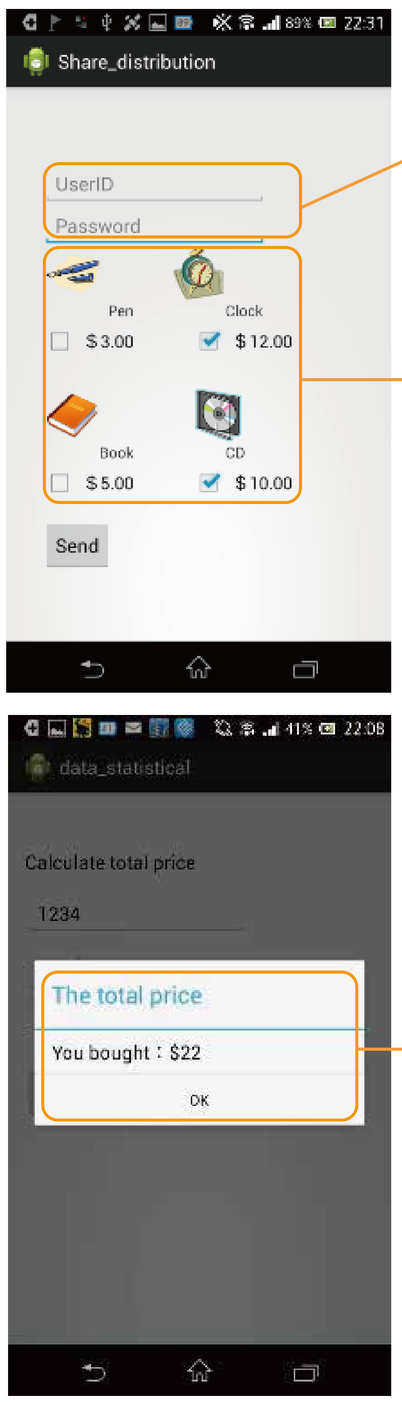
## 研究概要

ビッグデータにおけるプライバシー保護を実現する秘匿計算は、一般に処理が重く、データが膨大であるため、容易に利用できません。本研究では、加減算のみで分散・復元処理が可能な高速の秘密分散法により、データを鍵情報1つに集約することが可能となり、スマートフォン等による利用者が制御可能な秘匿計算が実現できます。

## スマートフォンを用いたライフログシステム

Life log system using a smartphone

**軽量&小容量なのでスマートフォンで自分の記録（ライフログ）を秘匿管理するアプリケーションが可能**




## Point

- ○ 膨大なデータを記憶することなく秘密鍵から生成
- ○ 加減算のみで実現可能な高速の秘密分散処理
- ○ 秘密情報のオーナが秘匿計算を制御可能

「ビッグデータの有効活用とプライバシー保護を実現する個人制御可能な秘匿計算システム」　東京理科大学 工学部第一部 電気工学科　岩村 恵市

TOKYO UNIVERSITY OF SCIENCE University Research Administration Center

東京理科大学 研究戦略・産学連携センター

http://www.tus.ac.jp/ura/

2015.08

# 情報通信

Information and Communication


東京理科大学 工学部第一部 電気工学科

Tokyo University of Science,Department of electrical engineering

**岩村 恵市 教授**

Keiichi IWAMURA　　Professor



## 現状

- ビッグデータを活用する秘匿計算は
一般に処理が重くかつデータが膨大であるため
容易に利用できない

  Privacy preserving data mining for big data is generally processed heavy and data is not readily available for a huge

- 1業者にクラウド管理を委託する場合、
秘密分散された情報を収集・復元されるかもしれない
という不安がある。

  When a user entrusts management of secret information to one Cloud contractor, there is the uneasiness that the secret information may be restored by collecting the shares by secret sharing

## 新技術

- **膨大なデータを鍵情報1つに集約でき
利用者が管理可能**

  Users can manage their own huge data in person since vast amounts of data can be aggregated to one key

- **加減算のみで分散・復元処理が可能な
高速の秘密分散法**

  High-speed secret sharing scheme is realized only by addition and subtraction

## 今後

**活用例**

- 家計簿のネット管理

  Internet management of household account book

- ライフログアプリケーション

  Life log application

- 医療分野などで個人情報を秘匿したまま統計処理

  In the medical field, statistical processing while concealing personal information

## 課　題

- 具体的な演算等に対する実用性の検討

  Consideration of practicality for specific computation




TOKYO UNIVERSITY OF SCIENCE University Research Administration Center

東京理科大学 研究戦略・産学連携センター

http://www.tus.ac.jp/ura/

2015.08