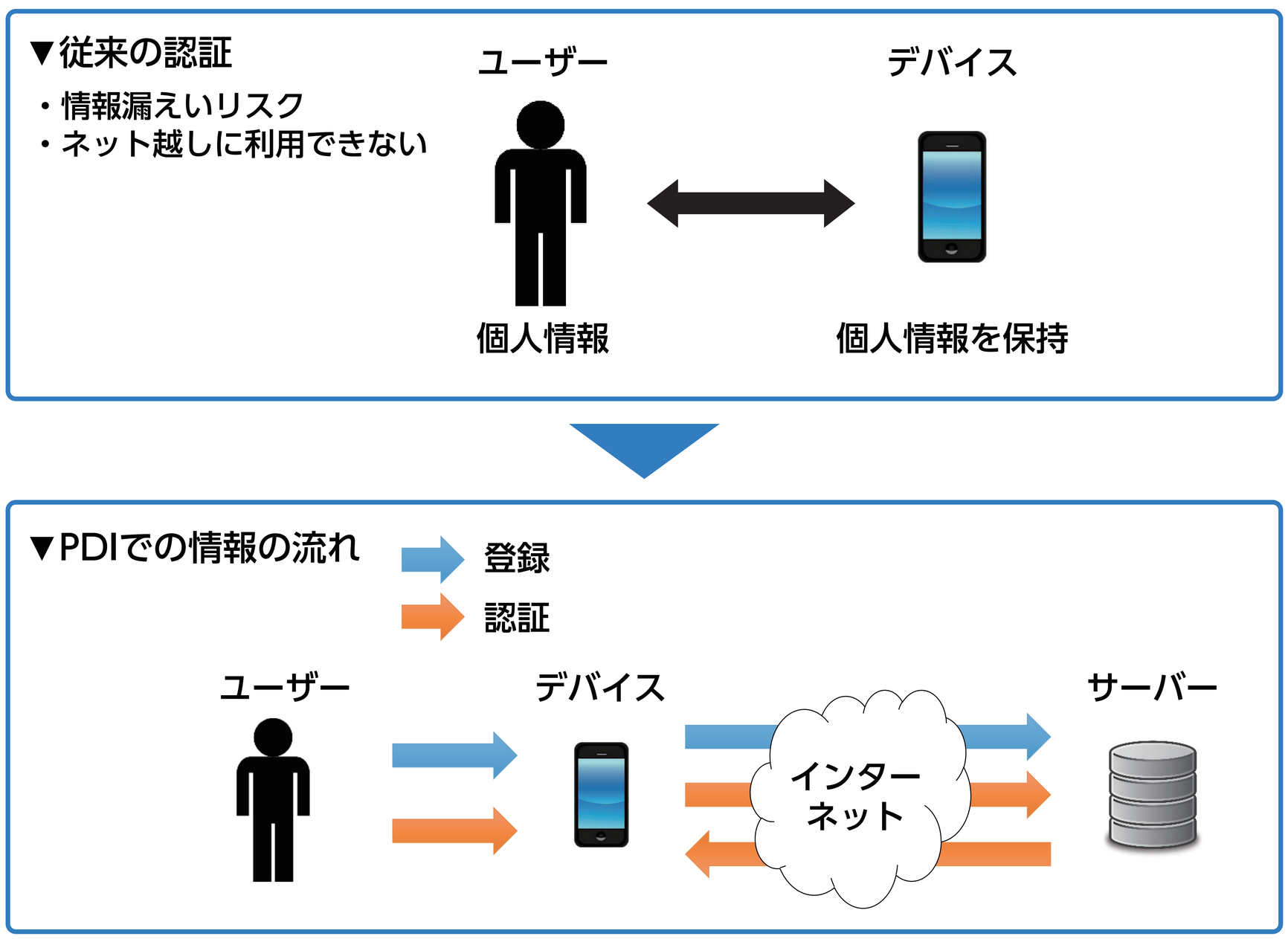
情報を暗号化して復号せずに照合する革新的暗号処理システム

Authentication Based on Verifiable Encryption with Private Digital Identity

研究概要

認証で使われるDigital Identityは情報漏洩に備え暗号化して保護されていますが、認証時に情報を復号する際に情報漏洩のリスクがあります。本研究では、個人情報のネット上でのセキュアで安全な利用のため、情報を暗号化したまま照合できる高速かつ安全な認証システムの開発を行っています。



*PDI:Private Digital Identity

Point

- 鍵交換の必要がない
- 復号化する必要がないため漏洩リスクが低減
- 処理速度の高速化に成功
- 内部メモリ削減の達成

「情報を暗号化して復号せずに照合する革新的暗号処理システム」　東京理科大学　理工学部　情報科学科　入山　聖史

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/

2018.8

情報通信
Information Science

東京理科大学　理工学部　情報科学科
Department of Information Sciences, Faculty of Science and Technology, Tokyo University of Science

入山　聖史　講師

Satoshi IRIYAMA　Junior Associate Professor

現状

- 一元的なデータ管理による個人情報漏洩のリスクがある
  There is a risk of personal information leakage due to unified data management.
- 準同型暗号を用いた検索可能暗号は処理速度が遅い
  Searchable encryptions using homomorphic cryptography are slow.
- 使用メモリが膨大
  The memory used is enormous.
- 利用範囲が限定的
  Usage range is limited.

新技術

- **Private Digital Identity（PDI）の提案**
  Proposal of Private Digital Identity (PDI).
- **任意のDigital Identityを外部に知らせることなく認証に用いる技術**
  It is possible to authenticate without informing any Digital Identity to a third party.
- **暗号化したまま認証が可能**
  It can authenticate with encryption.
- **鍵交換を行わない**
  Key exchange is not required.
- **使用メモリが少ない**
  The memory used is very small.
- **処理速度が速い**
  The processing speed is fast.

今後

活用例

- IoT鍵管理システム（宿泊施設の予約/入退室管理/宅配ボックス/カーシェアリング等）
  IoT key management system: accommodation facility reservation, entrance management, delivery box, car sharing, etc
- 認証システム
  Authentication system
- イベント会場でのチケット管理/入場管理
  Ticket management / entrance management
- 公共Wi-Fiのセキュリティの向上
  Improving security of public Wi - Fi

課　題

- 実際の使用場面を想定したユーザーインターフェースと専用デバイスが未完成
  User interfaces and dedicated devices assuming actual use situations are incomplete.
- 使用場面を想定した全体のシステム構築と実証実験
  Overall system construction and demonstration experiment assuming the situation of use are incomplete.
- 魅力的なサービスの試作品の開発
  Development prototypes of attractive services.

「情報を暗号化して復号せずに照合する革新的暗号処理システム」　東京理科大学　理工学部　情報科学科　入山　聖史

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/

2018.8