通信・情報処理

暗号データ処理システム、及びプログラム

Authentication Based on Verifiable Encryption with Private Digital Identity

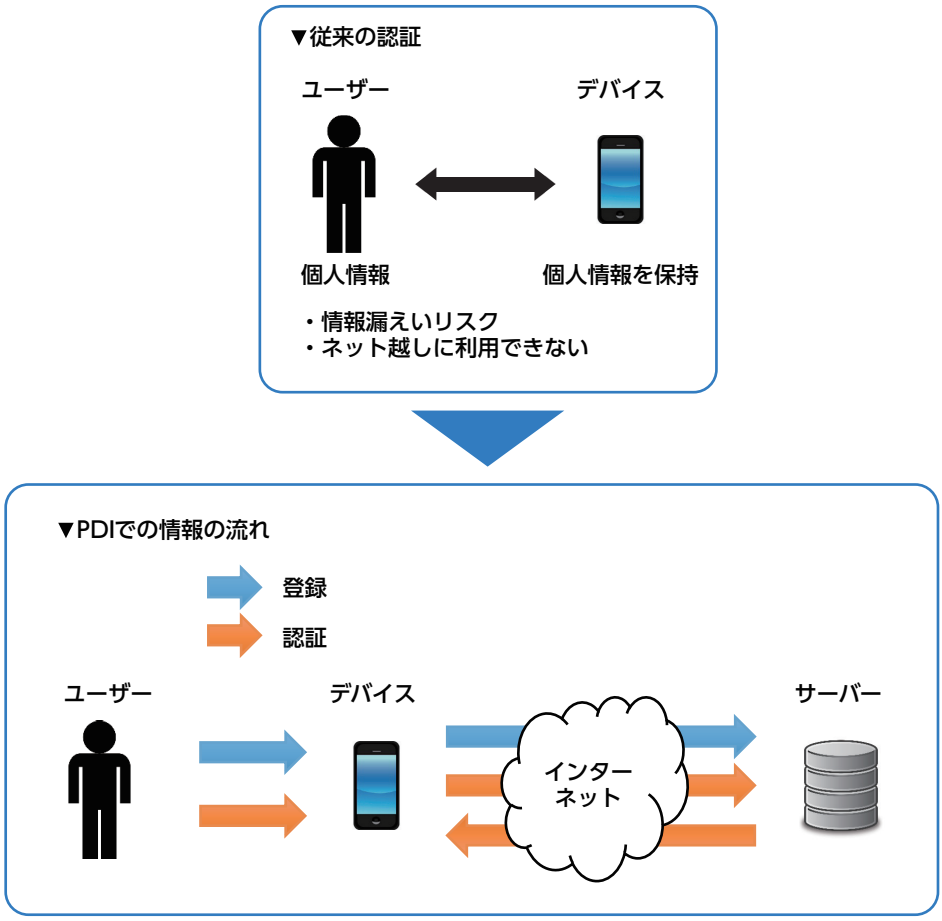
入山　聖史　Satoshi IRIYAMA（東京理科大学　理工学部　情報科学科　准教授）

研究の目的

情報通信技術の発展によって、インターネット販売等で様々な商品やサービスを購入することが可能になりました。その際に購入者は、自分の名前、年齢、住所等の個人情報を企業に提供する場合がありますが、それによって、望まない過剰な広告の配信や、企業のデータベースからの個人情報漏えい等のリスクがあることが問題です。

研究の概要

本研究は、プライバシー保護と利便性との両立を目的とし、ユーザー自身が自己を特定するものとして選択した情報を暗号化し、暗号化したまま高速で照合可能な独自技術を開発したものです。



*PDI：Private Digital Identity

従来・競合との比較

従来：暗号化された情報に対して、復号化せずに処理する方法は存在した。

従来の課題
- ・個人情報（生体情報, PIN等）が集約して保管されているため, 情報漏洩のリスク
- ・安全性を追求するために処理速度を犠牲にする

本技術：処理速度, 安全性, 内部メモリ削減の達成

想定される用途

- ・民泊、ホテルのフロント、コワーキングスペース、ホームセキュリティでの業務軽減
- ・イベント会場での入場管理、公共WiFiのセキュリティ向上
- ・子供や高齢者などスマートフォンになじみのない方の利用

実用化に向けた課題

- ・現在：実験室での実装を完了しているが、実際の利用を想定した実証実験が未実施
- ・課題：どのような利用形態がふさわしいか等のビジネスモデルの構築

企業へ期待すること

データベースまたは個人認証の技術を持つ企業との共同研究を希望します。また, IoT製品を開発中の企業, クラウド分野への展開を考えている企業には, 本技術の導入が有効と思われます。

POINT

- ・鍵の受け渡しの必要がなくなる
- ・個人情報は暗号化され、復号化されないため漏洩リスクが低減
- ・サーバーを第三者に委託できるため、参入コストが低い
- ・スマートフォン不使用

■知的財産権　：PCT/JP2018/45505「暗号データ処理システム、及びプログラム」
■試作品　　：あり

東京理科大学 産学連携機構

〒162-8601　東京都新宿区神楽坂一丁目３番地　TEL：03-5228-7440　E-MAIL：ura@admin.tus.ac.jp

2022.04