本人による匿名性解除が容易で軽量な匿名認証の研究

A Study of Lightweight Anonymous Authentication that Issuers Can Easily Open

山田崇晴・ネットワーク分科会・情報セキュリティ大学院大学

Nowadays, many organizations are collecting people’s active history from their ordinary life outside of the Internet. If personal data is collected with pseudonyms, they can identify this data with already collected personal data by matching the content of some databases. I have proposed an anonymous authentication scheme which can prevent linking between databases and has three features(1. Lightweight calculation. 2.Easy to open anonymity for members. 3. No privileged organizer who can open any anonymity.)

なぜ匿名認証か？

昨今の情報社会においてプライバシー保護は重要なテーマ。本研究では、匿名かつリンク不可能な識別子を用いた認証スキームを考案し、外部データベースの突き合わせに耐性を持たせた。

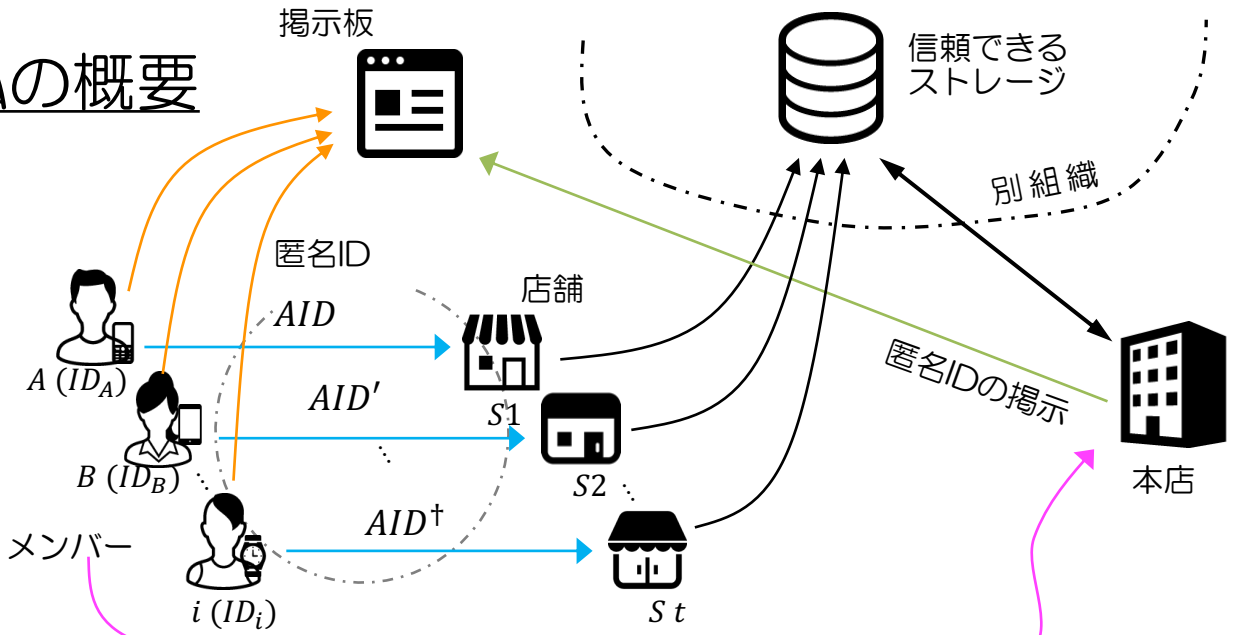
特徴は？

軽量な計算量 ⇒ ハッシュ関数を使用

簡単な匿名性解除 ⇒ 短期個別鍵を渡す

特権的な管理者が不在 ⇒ メンバーが自ら名乗り出る

スキームの概要



まとめ

匿名認証のスキームを提案し、このスキームを使ったアプリケーション(当たりくじモデル)を提示した。また匿名性の安全性も定義した。