情報を暗号化して復号せずに照合する暗号処理システム

東京理科大学　理工学部　情報科学科
講師　入山 聖史

従来技術とその問題点

検索可能暗号とは

暗号化された文章中に，検索キーワードがあるか，暗号化したまま検索する技術

データベースを暗号化しておけば，サーバに侵入があっても漏洩リスクが小さい

処理速度が遅い

利用範囲が限定的

等の問題により，実用化に課題がある

新技術の特徴･従来技術との比較

- 従来技術の問題点であった，速度と使用メモリを大幅に改善した
- 従来は速度と使用メモリが莫大なため，応用範囲が限られていたが，速度が1sec以下，メモリ数MB以下となったため，様々な用途へ応用が可能となった
- 本技術の適用により，情報漏えいリスク低減，暗号化されたデータの活用が見込まれる

想定される用途

- 本技術の特徴を生かすためには，データベース管理や認証技術へ適用することで，高速処理とセキュリティ向上のメリットがある
- 上記以外に，データの改ざん防止にも応用が可能である
- また、達成された処理速度に着目すると，任意の個人所有の磁気カードを用いた入退室管理システムにも展開できる

応用例：カギのIoT すべてのカードをカギに．便利な入退室

特徴

- ✓ 全ての非接触磁気カード（クレジットカード，SUICA，メンバーカード等）を入退室のカギとして使える
- ✓ スマートフォン不使用
- ✓ 個人情報は全てワンタイムキーで保護され安全

活用シーン

- ◆ 民泊などでの鍵管理の簡略化
- ◆ ビジネスホテルでのフロント業務の簡略化
- ◆ アミューズメント施設の入場管理
- ◆ 子供や高齢者などスマホに馴染みがない方々

使用方法

登録：直接PCで読み込むか，インターネットを通じて登録
入室：登録されたカードを扉の読取機にかざすだけ
削除：アプリからいつでも削除

ユーザーのメリット

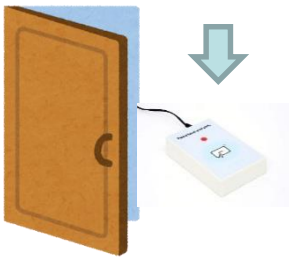
- ◆ すでに所有しているカードがカギになるため余分なものが増えない
- ◆ 民泊のフロントでの不都合が解消

事業者のメリット

- ◆ インターネット予約でもカギを作成できるため，直接渡す必要がなくなり，フロント業務を簡略化できる
- ◆ 扉に機器を取り付け，PCにアプリをインストールすることで使用可能
- ◆ データは全て暗号化されているので，サーバ等は第三者に委託できる

①磁気カードを登録

②登録されたカードをかざせばロックが開く



実用化に向けた課題

- 現在，PCと通常のUSBデバイスで実装済み．しかし実際の使用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不十分
- 今後，実際の使用場面を想定した全体のシステム構築とその実証実験が必要
- 実用化に向けて，導入しやすさと使いやすさについて検討が必要

企業への期待

- 実証実験については，パートナー企業と協力することで克服できると考えている
- 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
- 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る.

本技術に関する知的財産権

- 発明の名称 :東京理科大学
- 出願番号　　:出願準備中
- 出願人　　:東京理科大学
- 発明者　　:入山　聖史、木原　眞紀

お問合せ先

東京理科大学
研究戦略・産学連携センター
担当URA　是成 幸子

ＴＥＬ ０３－５２２８－７４４０
ＦＡＸ ０３－５２２８－７４４１
e-mail ｕｒａ@ａｄｍｉｎ.ｔｕｓ.ａｃ.ｊｐ