

土井研究室

DOI Laboratory

URL http://lab.iisec.ac.jp/~doi_lab/
問い合わせ doi-lab-query@iisec.ac.jp

データの安全な提供方法(2020-)
タクシーデータ提供時の
様々な検討

公開鍵型認証のアカウントリカバリー(2020-)
デバイス紛失時などへの対策

軽量の匿名認証(2019-)
匿名性解除

利用者認証(2021-)
様々な Authenticator と特徴

階層的秘密分散法の研究(2015-)
識別子割り当て問題の解決(2020-)

公開鍵検索可能暗号の改良(2017-)
ブルームフィルタの適用

匿名加工(2021-)
差分プライバシーについて

応用

デジタル教材の著作権管理
本人認証における信用度
金融APIに関する認証・認可
HDD/SSDのデータ抹消
非接触型ICカード等における
セキュリティ
タクシーデータの安全な提供

守秘・認証

情報漏えい耐性署名
検証者指定可能署名
コンカレント署名
匿名認証
放送・通信連携
サービス
アカウントリカバリー
階層的秘密分散法
ランプ型シェアの変換
プロキシ再暗号
空間暗号・鍵交換
検索可能暗号・ブルームフィルタ
格子基底縮小アルゴリズム

プロトコル

ペアリングライブラリを利用するための実装
Webサービスにおける認証
XSS脆弱性対策の実装と評価
メール送信者認証機能の改善
Tor通信先の識別法
利用履歴の秘匿と配信・課金の両立
電子署名の検証能力の制御
匿名性を有しつつ一部の情報の開示
匿名加工技術
暗号プロトコル検証

高速な階層的秘密分散法の研究

- 秘密分散法とは秘密情報を分散管理するための方法
 - 分散情報の一部が漏えいしても秘密情報は安全
 - 分散情報の一部が紛失しても秘密情報は復元可能

例: $(\{1,3\},n)$ 階層的秘密分散法



成果

- XORベースの高速な階層的秘密分散法
 - 国際会議IWSEC2018(仙台)で発表
- IDAを利用した階層的秘密分散法
 - 国際会議ICISC2018(Seoul)で発表
- 標数2の有限体上の階層的秘密分散法
 - 論文誌 Journal of Information Processing で発表
 - 標数2の (k,n) 階層的秘密分散法を初めて達成
 - IPSJ Outstanding Paper Award 受賞
- XORベースの秘密分散法と巡回行列の関係
 - 論文誌 Journal of Information Processing で発表