

# 土井研究室

## DOI Laboratory

URL [http://lab.iisec.ac.jp/~doi\\_lab/](http://lab.iisec.ac.jp/~doi_lab/)  
 問い合わせ [doi-lab-query@iisec.ac.jp](mailto:doi-lab-query@iisec.ac.jp)

### 研究テーマ

電子署名, 認証, 暗号プロトコル等の安全性に関する研究と, その電子社会システムへの応用研究など

### 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

放送・通信連携サービス

ペアリングライブラリを利用するための実装

### 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

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

### プロトコル

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

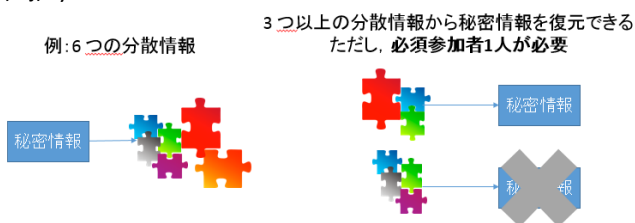
利用履歴の秘匿と配信・課金の両立  
 電子署名の検証能力の制御  
 匿名性を有しつつ一部の情報の開示  
 匿名加工技術  
 暗号プロトコル検証

## 2020年度の研究テーマ例

### 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ICISC 2018(Seoul)で発表
- 標数2の有限体上の $(k,n)$ 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
    - IPSI Outstanding Paper Award 受賞

- 階層的秘密分散法の研究
  - 巡回行列の性質を利用した証明法
- 秘密分散法
  - 情報のライフサイクルを考慮した拡張法の検討
    - ランプ型秘密分散法の拡張
- 検索可能暗号
  - 公開鍵検索可能暗号に適したブルームフィルタの検討
- 認証プロトコル
  - 利用者の負担を低減可能な方式の検討

### ランプ型シェアの変換

