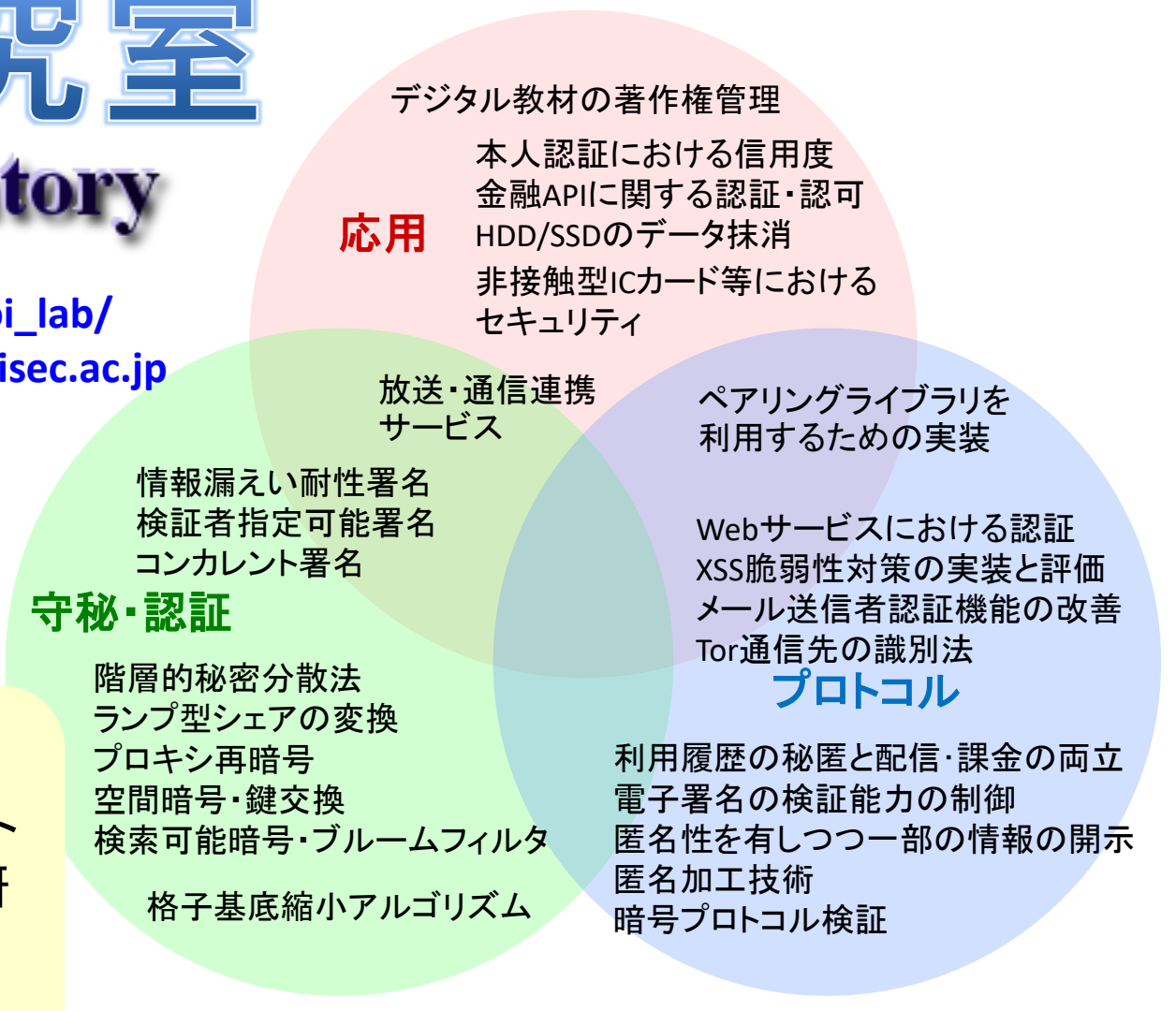
土井研究室
DOI Laboratory

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



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

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

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
    - IPSJ Outstanding Paper Award 受賞

2020年度の研究テーマ例

- 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