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

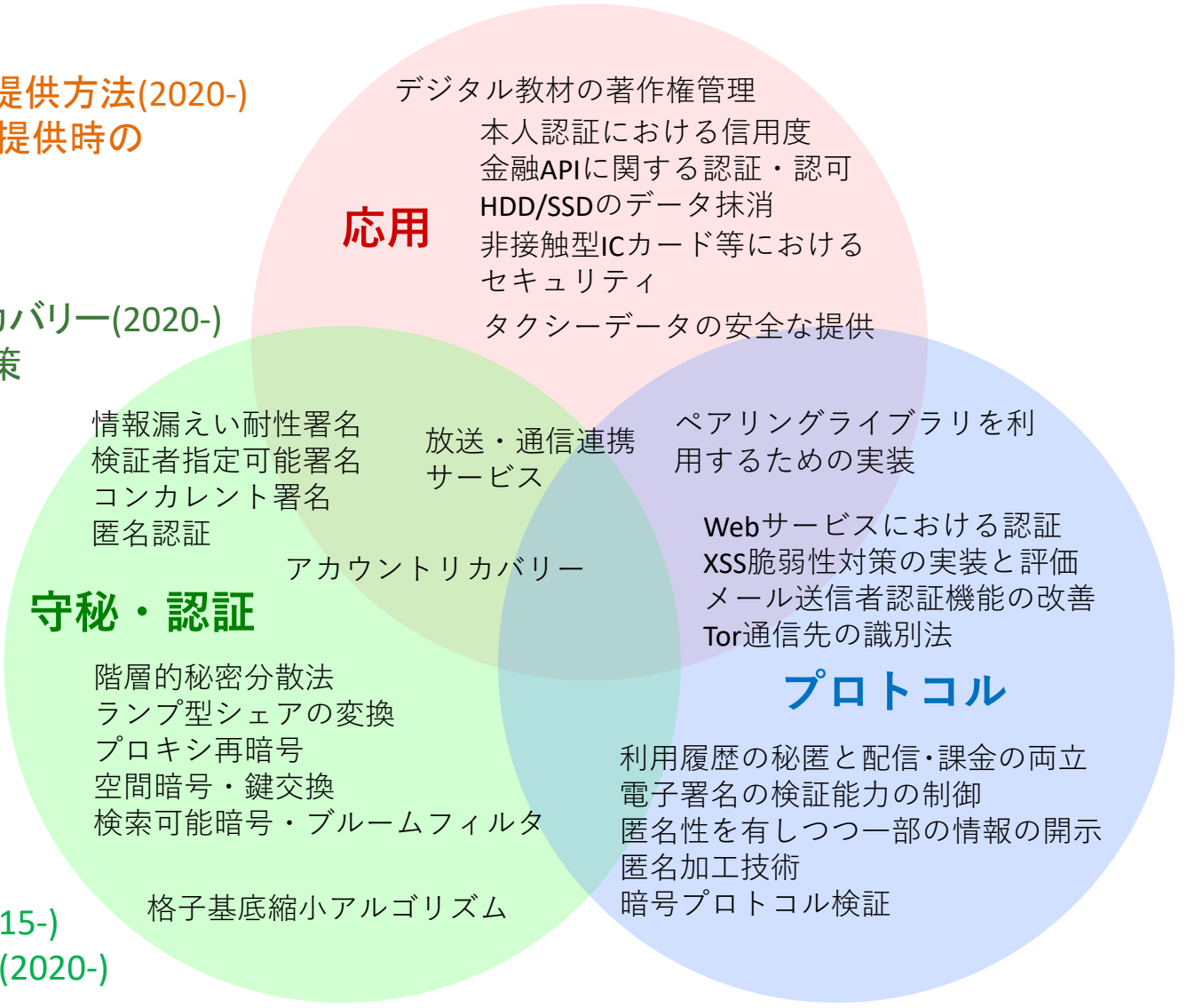
軽量な匿名認証(2019-)
匿名性解除

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-)

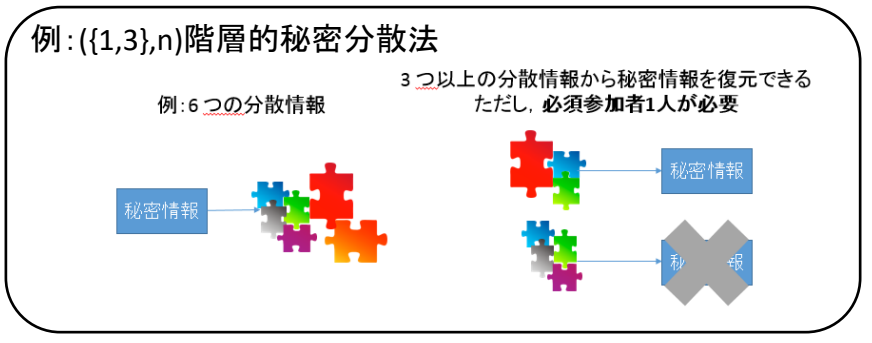
公開鍵検索可能暗号の改良(2017-)
ブルームフィルタの適用

匿名加工(2021-)
差分プライバシーについて



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