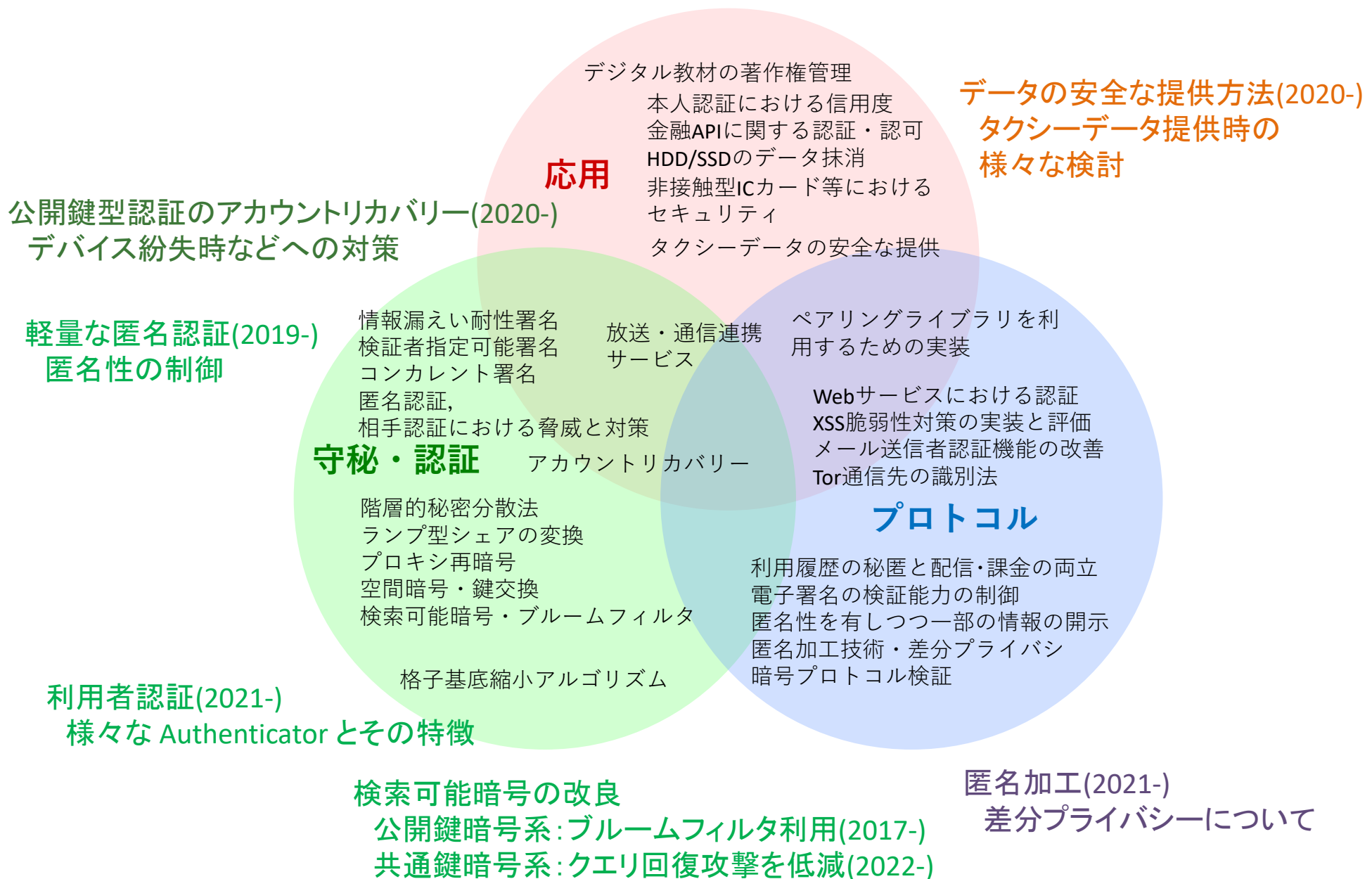


土井研究室

DOI Laboratory

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



高速な階層的秘密分散法の研究

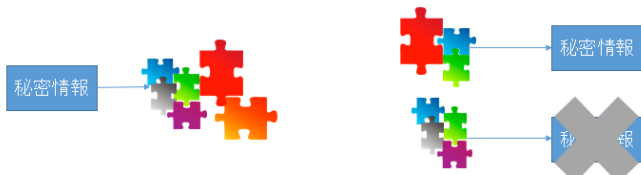
成果

- 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

例: 6 つの分散情報

3 つ以上の分散情報から秘密情報を復元できる
ただし、必須参加者1人が必要



- 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