東北大学

産学連携によるカードベース暗号の数理的未解決問題と新課題の整理

クロージング

10:00-11:30　オープニング、セッション1

水木 敬明（東北大学 サイバーサイエンスセンター）
ANDプロトコルにまつわる未解決問題

宮原 大輝（電気通信大学 情報理工学研究科）
カードベースZKPプロトコル

標準モデル等

13:00-14:30　セッション2

中井 雄士（豊橋技術科学大学）
秘匿置換を用いたカードベース暗号

真鍋 義文（工学院大学 情報学部情報科学科）
無開示性を持つカードベース暗号プロトコルについて

プライベート
モデル

15:00-17:15　セッション3、クロージング

品川 和雅（茨城大学 理工学研究科）
カードベース暗号に登場するさまざまなカード組と符号化

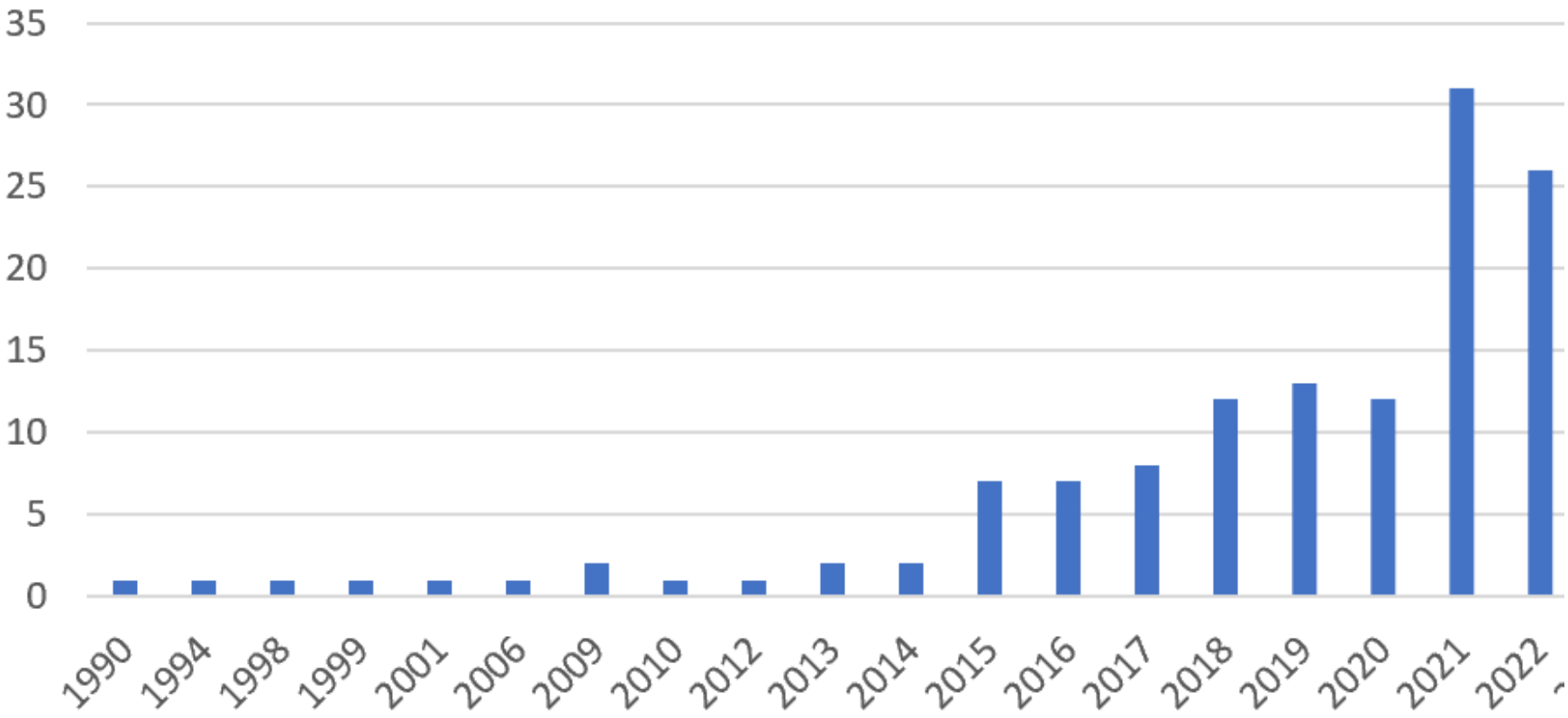
須賀 祐治（株式会社インターネットイニシアティブ）
デッキ分割法とアソシエーションスキーム

縫田 光司（九州大学マス・フォア・インダストリ研究所）
カードベース暗号に現れる数学

カード組と符号化

数学とのかかわり

カードベース暗号分野の Scopus掲載論文数の推移



本日のスライド資料は、後日九州大学IMIのサイトに掲載予定です。

カードベース暗号の研究に取り組んでみませんか？

今回示された課題や未解決問題を解くなどして、論文を出版される場合、この研究集会を引用していただく必要はございませんが（元論文を引用ください）、この研究集会がきっかけであることを謝辞にご記載いただけると嬉しいです。

本研究は九州大学マス・フォア・インダストリ研究所 共同利用・共同研究拠点の支援を受けた.（2023年度短期共同研究「産学連携によるカードベース暗号の数理的未解決問題と新課題の整理」（2023a020）
This work was supported by Institute of Mathematics for Industry, Joint Usage/Research Center in Kyushu University. (FY2023 Short-term Joint Research “Organizing open problems in card-based cryptography through industry-academia collaboration” (2023a020).)

東北大学

ご質問などありましたら、代表者の水木＠東北大までお願いします。（内容に応じて、適切な講演者等に転送します。）

mizuki+imicard［AT］tohoku.ac.jp