COMPASS meetup vol. 48 Nexus Park対面開催

カードベース暗号と気まずくならない告白

宮原 大輝（情報学専攻 准教授）

2026. 12.3

12:15～12:45
（発表15分、Q&A15分）
Nexus Park（東11号館1階）



カードベース暗号は、トランプの表裏やシャッフルを利用して、秘密の情報を明かさずに計算を行う技術です。本発表では、オープンキャンパスで実施している体験キット「気まずくならない告白」を題材に、その仕組みをわかりやすく紹介します。また、より少ないカード枚数やステップ数で計算を実現するための研究を紹介します。さらに、秘密計算とプライバシー保護の関わりや、体験型の情報セキュリティ教育への応用、異分野連携の可能性についてもお話しします。秘密が守られたまま答えだけが出てくる、「えっ、本当に？」という感覚は、画面越しでは伝わりません。**ぜひ会場で、暗号ゲームを体感してください。**



研究分野	理論計算機科学
keyword	暗号プロトコル、秘密計算、ゼロ知識証明
対　象	電気通信大学教職員、学生
参加申込	右側のQRコードのフォームからご登録ください。

COMPASS meetupは、学内研究者がどんな研究をしているのかを知る機会として、お昼休みに定期的に開催しています。本学の教職員・学生はどなたでも聴講可能です。気軽にご参加ください。

【お問合わせ】
研究教育マネジメント推進室URA
compass@ura.uec.ac.jp