大学院集中講義開講通知

（数理科学専攻）

科目名　　応用数理特別講義１　　（博士前期課程：Ｒ００６１）
　　先端応用数理特別講義１　（博士後期課程：Ｒ００６２）

講　師　　大久保 美也子　（国立研究開発法人 情報通信研究機構）

日　程　　１１月２１日（火）　　３，４，５時限　　８号館６１８教室
　　１１月２２日（水）　　３，４，５時限　　８号館６１８教室

題　目　　ゼロ知識証明の基礎

簡単な内容

現代暗号は有用な数学の応用の一つであり、古典的な情報秘匿に加えて様々な機能を提供している。「ゼロ知識証明」は 1980 年代に基礎理論が構築され、近年のクラウドやブロックチェーン上の応用で改めてニーズが高まっている暗号技術である。公開された x に対して二項関係 $R(x,w)=1$ を満たす w を持つ証明者が、その関係が成り立つことをそれ以外の情報を一切明かさずに検証者に納得させることができるため、プライバシー保護や匿名性を必要とする応用において重要な役割を果たす。

本講義では、ゼロ知識証明の基本的な概念と構成を説明し、いくつかの応用を示す。

東京都立大学　理学研究科数理科学専攻

履修申請期間　２０２３年 １０月２４日 ～ １１月１４日

期間中に、下記ＵＲＬまたはＱＲコードから履修登録を行ってください

https://forms.office.com/r/xGgKp8m1i6