第41回

愛媛大学 DS研究セミナー

愛媛大学データサイエンスセンター（CDSE）は、AI・統計解析・機械学習等の広義でのデータサイエンスと接点のある研究者、実務家、教育者を学内外から招聘し、講演していただくデータサイエンスセミナーを開催していきます。

多変数連立二次方程式を利用した暗号技術

現在広く普及している暗号技術（RSA暗号・楕円曲線暗号）は大規模な量子計算機によって危殆化することが知られています。そのため、量子計算機でも破ることができない暗号技術の開発のため耐量子計算機暗号（PQC）の研究が活発に行われています。これまで様々な数学問題に基づいたPQCが提案されている中、多変数連立二次方程式の求解困難性を安全性の根拠とする多変数多項式暗号（MPKC）が注目を集めています。この講演では、有力な方式であるUOV署名方式を通してMPKCの基本的な事柄について解説します。

参加無料

開催日時

2026年3月10日（火）
16:30〜17:30

開催方法

オンライン定員300名
（Zoom・Youtube同時配信）

申込締切

2026年3月6日（金）13:00

申込先

事前申し込み制となっております。
二次元コードまたは下記URLより
お申込みください。
https://forms.gle/AcwkuyZaqC7WArVRA

講演者

マス・フォア・インダストリ研究所准教授

池松 泰彦 氏

今回の資料は事前配布いたしませんので、あらかじめご了承ください。
アーカイブ視聴はございません。当日の配信のみとなっておりますのでご了承ください。
本セミナーは『数学談話会』としても開催しております。

主催 愛媛大学デジタル情報人材育成機構データサイエンスセンター

お問合せ先：愛媛大学デジタル情報人材育成機構データサイエンスセンター　E-mail: cdse@stu.ehime-u.ac.jp

CDSE
Center for Data Science, Ehime University