第11回

愛媛大学
DS研究セミナー

2021.9.28（火） 16:30-18:00
オンライン開催

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。

定員 先着300名

参加費 無料　事前登録制
Zoom定員先着300名
YouTube同時配信

セミナー

「量子コンピュータ時代に向けた次世代暗号技術」

講演者 ／ 相川 勇輔 氏（三菱電機情報技術総合研究所）

古代より主に軍事目的で利用されてきた暗号技術は、コンピュータ通信の進展に伴い1970年代に公開鍵暗号の概念が登場し大きく発展を遂げました。以降、大学や民間企業を中心に研究および開発が進められるようになった暗号技術は社会全体に広く実用されていき、今や私たちの生活はそれなしでは成り立ちません。これら公開鍵暗号の安全性は、例えば素因数分解問題のような計算量的に一方向性を持つと期待される数学的問題が支えています。

しかし、1994年にShorはこれらの問題を効率良く解く量子アルゴリズムを発見しました。これは十分に規模の大きい量子コンピュータを利用すると、これらの暗号を効率的に解読できることを意味します。

そこで、量子コンピュータの実現した未来へ向けて、それを利用した解読にも耐えうる新たな暗号の研究が進められています。これらの暗号は耐量子計算機暗号と総称され、現在NISTによる技術標準化活動も進められています。

今回は、暗号の基本的な仕組みからはじめ、耐量子計算機暗号の研究動向を皆様と共有します。そののち、講演者が主に研究に取り組んでいる耐量子計算機暗号の一つである同種写像暗号についてお話させていただきます。この同種写像暗号の研究においては、楕円曲線と呼ばれる数学的対象の整数論が本質的な役割を果たします。このような数学的な内容もお話いたします。

申込締切
9.27（月）
12:00

事前登録制としています。参加を希望する方は
右記QRコードからお申込みください。
もしくは下記URLよりGoogleフォームからお申し込みください。
https://forms.gle/tXonmwh4913U3ayR8

主催／ 愛媛大学データサイエンスセンター

お問い合わせ／愛媛大学データサイエンスセンター（石川、西岡）
E-mail: cdse@stu.ehime-u.ac.jp
H　P :http://www.cdse.ehime-u.ac.jp/