社会数理コロキウム

10 月 19 日（木）17:00〜18:30　数理科学研究科棟 056 号室

高島 克幸 氏

（三菱電機　情報技術総合研究所）

格子と同種写像に関するアルゴリズムの耐量子暗号への応用

■ 講演アブストラクト

量子計算機の出現に備えて、量子計算機でも効率的に破れない公開鍵暗号の研究が活発に行われています。本講演では、その候補である格子暗号と同種写像暗号について紹介します。Shor の量子アルゴリズムにより、素因数分解問題や離散対数問題が効率的に解けます。更に、Shor アルゴリズムにより、より広いクラスである有限アーベル群に対する隠れ部分群問題が効率的に解けるので、それを避ける数学構造及びその上の計算量仮定、そしてその仮定に基づいた（効率的な）暗号構成が必要になります。本講演では、特に、格子と（楕円曲線間）同種写像という数学構造を利用する方法について概説します。

学生時代に、楕円曲線が暗号に応用されていることを知りました。そして、会社に入って楕円曲線暗号に携わり始めたのは 97 年でした。それから、世の移ろいと共に、楕円曲線暗号に対する要求も変わり、研究トレンドも変わりました。最近、活発に研究されている耐量子暗号である同種写像暗号は、その一例です。耐量子暗号の重要な候補である格子暗号とともに、最近の研究動向をいささかなりともお伝えするのが、本講演の目的です。

■ 講演者プロフィール

京都大学大学院理学研究科数学・数理解析専攻修士課程を終えて、1997 年に三菱電機株式会社に入社。その後、暗号理論の研究開発に従事。2009 年に、京都大学大学院情報学研究科で博士取得。2013 年度から、九州大学マス・フォア・インダストリ研究所客員教員。2016 年度から、日本応用数理学会副会長。

18:30 から 2 階コモンルームで高島氏を囲んで情報交換会を予定しております。