行動する知性。
中央大学

中央大学 理工学研究所 2015年度 第1回 特別講演会

最近の暗号理論の進展

講師

おかもと　たつあき
岡本　龍明 氏

日本電信電話株式会社　サービスイノベーション総合研究所
セキュアプラットフォーム研究所　岡本特別研究室　室長
中央大学研究開発機構　客員研究員（機構教授）

参加費無料
事前申込不要

日時：2016年1月25日（月）16:30～18:00

会場：中央大学 後楽園キャンパス 5号館1階5134号室

講演概要

この数年間における暗号分野の理論進展には目を見張るものがある。その一つが、21世紀になり急速に研究が進んだIDベース暗号の概念をより発展させ一般化した関数型暗号（functional encryption）に関する研究の進展である。特に、2013年にその実現例が発見され、その応用が一躍脚光を浴びるようになった識別不可難読器（indistinguishability obfuscation）と関数型暗号の密接な関係が見いだされ、この分野の研究はより一層深まりを見せている。また、2009年にその実現方式が発表された完全準同型暗号も、暗号の新しい応用を開くものとして、活発な研究が行われてきた。

これらいずれの方向の進展も、ネットワークの進展と深く関係している。最近、ネットワーク利用の広がりの中で、クラウドコンピュータやビッグデータ、IoT などが注目を集めている。そのような中で、セキュリティやプライバシの問題を杞憂する声も多く聞かれるようになり、最近のネットワーク利用環境下でのセキュリティやプライバシ問題を解決する新たな技術の展開が待望されている。上で述べた新しい暗号理論の進展はこの要望に応えるものであり、一言でいうと、暗号化したまま高度な情報処理や検索を行う機能を提供する。この機能を使うことにより、機密情報を保護（暗号化）した形で様々な高度なネットワークサービスを受けることが可能となる。

本講演では、上記のような最近の暗号理論の進展を、特別な前提知識を必要としないで平易に解説する。

参加費：無料
定　員：100名
主　催：中央大学 理工学研究所
問合先：112-8551
東京都文京区春日1-13-27
中央大学 研究支援室
（後楽園キャンパス3号館10階）
TEL：03-3817-1602　FAX：03-3817-1677