情報科学系セミナー（第2回）

テーマ

「Practical Impact of Tight Security Reductions」

講演者： NTT セキュアプラットフォーム研究所

上席特別研究員　阿部　正幸　氏

日　時： 平成29年7月7日（金）15：30～17：00

場　所： 情報科学系研究棟Ⅲ棟5階

コラボレーションルーム7

講演要旨：

暗号やディジタル署名のような暗号方式の安全性は離散対数問題など難しいと考えられている問題への帰着によって示される。帰着の効率は攻撃の難しさと帰着された問題の難しさの間の距離に相当するため、両者の間に乖離のないタイトな帰着を示すことが望ましい。しかしながらタイトな帰着を示すことは容易ではなく、また、それが示せないことで直ちに攻撃可能であるとも言えない。本講演では、ペアリングに基づく署名方式およびハッシュベース署名を例に挙げてタイト帰着が実用性に与えるインパクトについて論じる。

講演者略歴：

1990(H.02).3 東京理科大学工学部電気工学科卒業
1992(H.04).3 同大学院電気工学専攻科修士課程修了、NTT 情報通信網研究所勤務
1996(H.08).9-1997(H.09).8 スイス連邦工科大学チューリッヒ校(ETH Zurich) 客員研究員
1999(H.11).1 NTT 情報流通プラットフォーム研究所勤務
2003(H.13).4 同 研究所 特別研究員
2004(H.16).4 IBM T. J. Watson Research Center 勤務
2012(H.24).4 NTT セキュアプラットフォーム研究所 主幹研究員・特別研究員
2013(H.25).4 同研究所 主幹研究員・上席特別研究員（現職）

参加申込・予約は不要です。直接会場にお越しください。

お問合せ先：共通事務管理課共通事務第二係（E-mail：is-secr）