第８回「計算機を用いた数学研究」ＧＣＯＥセミナー

数学と情報セキュリティ科学を巡る知の循環、その実例として

11月12日(金) 14:30–16:30
11月13日(土) 10:00–12:00・14:00–16:00
京都大学理学部3号館110講演室
縫田 光司（産業技術総合研究所 情報セキュリティ研究センター）

RSA暗号や楕円曲線暗号のように、暗号・認証・電子署名などの技術を扱う情報セキュリティ分野において初等整数論や楕円曲線などの数学が応用されていることは比較的認知されているように見受けられる。本発表ではこれら「数学→情報セキュリティ」という波及効果と逆向きの、「情報セキュリティ→数学」という波及効果の実例として、情報セキュリティ分野の研究過程で見出した数学的研究テーマに関する話者のこれまでの研究について紹介する。特に、冒頭に紹介した初等整数論や楕円曲線のようなよく知られた（代数っぽい）題材に留まらず、凸集合の幾何学や確率不等式、組合せ論的数論など様々な分野の数学が登場することを強調しておきたい。

（なお、本発表においては情報セキュリティ分野についての予備知識は仮定せず、また各コマごとにself-containedな内容にする予定である。）

世話人：　阿部 拓郎（京都大学大学院工学研究科 機械理工学専攻）