

第5回 RCMS サロン「ランダム性の数理」

2019年12月18日(水) 15:15 ~ 18:00 (Tea Time を含む)

筑波大学 総合研究棟 B 棟 1 階 0110 号室

■15:15 ~ 15:30 Tea Time

■15:30 ~ 16:00 縫田 光司 (東京大学 情報理工学系研究科)

タイトル. 「暗号技術における乱数の活用例と落とし穴」

概要. 暗号技術は情報の安全性を守る技術であり、その実現には乱数の利用が不可欠である。乱数を巧みに用いることで暗号技術をより効率化できる場合もあるが、一方で、暗号技術の理論設計で想定している理想的な乱数を現実の装置の中で発生させることは困難であり、暗号技術の実装においては乱数周りで「事故」が起りやすい傾向にある。この発表では、現代の暗号技術における乱数の役割やその活用例について紹介するとともに、暗号理論における理想的な乱数と現実的な乱数との差異が及ぼす影響に関する発表者の最近の研究について紹介する。

■16:15 ~ 16:45 秋山 茂樹 (筑波大学 数理物質系)

タイトル. 「乱数と力学系の生成点」

概要. 人工的に生成された「乱数」は、それ自体が形容矛盾のようにみえる。しかしながら、このような人工の疑似乱数は現代情報化社会で非常に大きな役割を果たしている。今回は乱数のさまざまな数学的な定義の試みを紹介し、さらに乱数と力学系の生成点との繋がりに関する私たちの最近の共同研究を紹介する。

■17:00 ~ 17:30 羽田野 祐子 (筑波大学 システム情報系)

タイトル. 「ランダム性と環境問題」

概要. 環境中に現れる計測値を簡単な確率過程でモデル化し10年後の汚染レベルを予測した例を紹介する。合わせて非整数階微分方程式を福島事故における大気中セシウム濃度の予測に用いた例を紹介する。

■17:30 ~ 18:00 Tea Time

お問い合わせ先

世話人：佐垣 大輔 (筑波大学 数理物質系)

sagaki@math.tsukuba.ac.jp