



Global COE Seminar

第21回 離散幾何解析セミナー

日 時： 2012年1月13日(金) 13:00~14:30
場 所： 京都大学理学研究科3号館552号室
講 演 者： 縫田 光司 (産業技術総合研究所)
題 目： 離散的な関数族間の距離の評価と暗号分野への応用

話者らの最近の研究で、有限な定義域と値域を持つ二つの関数族どうしの距離を評価する問題が、暗号分野の研究と関連を持つことが明らかとなった。本発表では、このような関数族間の距離の評価の具体例と、暗号分野におけるハッシュ関数および擬似乱数の研究との関連を紹介し、さらに今後の発展的な研究についての展望を議論する。なお、本発表は京都大学の阿部拓郎・前野俊昭両氏、山口大学の鍛冶静雄氏、東京大学/JST CRESTの沼田泰英氏との共同研究に基づくものである。