第７回代数幾何・数論及び符号・暗号研究集会

東京大学大学院数理科学研究科２１世紀 COE 協賛
日本応用数理学会 数理的技法による情報セキュリティ研究部会協賛

科学研究費補助金基盤研究 (A)(課題番号：15204001) により、下記のような研究集会を行いますので御案内いします。

記

日時： 2006 年 12 月 20 日 (水)–12 月 22 日 (金)
場所： 東京大学大学院数理科学研究科大講義室
(京王井の頭線駒場東大前駅下車徒歩 5 分)
世話人：岡本 龍明 (NTT), 桂 利行 (東大数理), 平松 豊一 (法政大工)

＜プログラム＞
１２月２０日（水）
10:00 – 11:00　藤原 洋（インターネット総合研究所）
インターネットの発展に数理科学が果たした役割
11:10 – 12:10　安田 雅哉（東大数理）
Torsion points of elliptic curves with good reduction
13:30 – 14:30　本間 正明（神奈川大工）
Hermitian 曲線上 2 点符号の第 2 一般化 Hamming 最小重みの決定
14:45 – 15:30　Eun Ju Cheon（山口大）
A characterization of some Griesmer minihypers and its application
15:45 – 16:45　斎藤 正顕（法政大工）・平松 豊一（法政大工）・松田 修三（法政大工）
被覆グラフの L-関数と符号

１２月２１日（木）
10:00 – 11:00　渡辺 曜大（国立情報学研）
量子暗号における秘匿性増強
11:10 – 12:10　鶴丸 豊広（三菱電機）
量子暗号実装と古典符号

13:30 – 14:30　笠井 健太（東工大）
　非正則 LDPC 符号アンサンブルの最小距離分布
14:45 – 15:45　和田山 正（名工大）
　2 元行列アンサンブルの平均見逃し誤り率について
16:00 —17:00　渋谷 智治（メディア教育開発センター）
　メッセージパッシングアルゴリズムの解析における線形計画からのアプローチ

１２月２２日（金）
10:00 – 11:00　萩谷 昌己（東大情報理工）
　数理的技法による情報セキュリティについて
11:10 – 12:10　住井 英二郎（東北大情報）
　spi 計算における暗号プロトコルの形式的検証について
13:30 – 14:30　萩原 茂樹（東工大情報理工）
　Abadi-Rogaway による暗号メッセージの解析手法とその健全性・完全性について
14:45 – 15:45　真野 健（NTT）
　ゲーム列による安全性証明の形式化と自動化
16:00 – 17:00　長谷部 浩二（産業技術総合研究所）
　BAN 論理から Protocol Composition Logic へ
　　〜セキュリティ・プロトコルの論理的分析法
17:30 – 19:00　懇親会

なお、この研究集会への事前の参加申し込みは不要です。

問い合わせ先
東京大学大学院数理科学研究科
桂　利行
e-mail: tkatsura@ms.u-tokyo.ac.jp