数理解析研究所講究録1361

符号と暗号の代数的数理

京都大学数理解析研究所

2004年4月

はしがき

この講究録は、2003年11月4日(月)から7日(木)までの4日間、京都大学数理解析研究所において行われた共同研究集会「符号と暗号の代数的数理」における諸講演を講演者自身の原稿をもとに作成した報告集であります。

この研究集会は、桂利行氏(東大数理)によって提案され、符号・暗号と代数幾何・数論との境界領域の開発を目指したものであります。幸いにも、大学や民間会社の研究者等数学や情報を専門とする人々が90名以上も参加され、集会は盛会でした。特に、院生等若い人達にとって、質の高い研究成果を広く知る機会ともなったことは幸いでした。

尚、この研究集会の講演者の旅費の一部を、桂利行氏の科研費基盤研究(A)(1)によって援助されました。ここに深く謝意を表します。

研究代表者
法政大学工学部　平松豊一

符号と暗号の代数的数理

京都大学数理解析研究所の共同研究事業の一つとして、下記のように研究集会を催しますので、ご案内申し上げます。なお、この集会は、この集会の提案者でもある桂利行氏を代表とする科研費基盤研究(A)(1)より助成を受けております。

研究代表者　平松豊一(法政大学工学部)

記

日時：2003年11月4日(火)10:00～11月7日(金)17:00
場所：京都大学数理解析研究所4階420号室
京都市左京区北白川追分町
市バス 京都大学農学部前または北白川前下車

プログラム

11月4日(火)
10：00～11：00　佐古和恵・古川潤（NEC インターネットシステム研）
ミックスネットについて～電子データをシャッフルする方法～
11：10～12：10　岡本龍明（NTT 情報流通研）・鹿島亮（東工大情報理工）
Resource Bounded Unprovability of Computational Lower Bounds (Part 1)
13：40～14：40　山本博資（東大情報理工）
秘密分散法とそのバリエーション
14：50～15：50　佐藤孝和（埼玉大理／東工大理工）
有限体上の楕円曲線の位数計算の最近の進展について
16：00～17：00　萩原学（東大生産研）・今井秀樹（東大生産研）
暗号研究の最新の動向　量子ワンタイムパッドの研究

11月5日(水)
10：00～11：00　川北素子（お茶の水大情報）
Some quotient curves of Fermat curves attaining Serre bound

11：10～12：10　酒井隆行（東大数理）
Primes is in P (after M.Agrawal, N.Kayal and N.Saxena)
13：40～14：40　和田秀男（上智大理工）
素因子分解と暗号
14：50～15：50　鈴木譲（阪大理）
三浦理論に基づく Kedlaya の位数計算の一般化
(Generalizing Kedlaya's order counting based on Miura theory)
16：00～17：00　小林欣吾（電通大情報通信工）・
森田啓義（電通大情報通信工）・星守（電通大情報通信工）
木情報源の符号化

11月6日(木)
10：00～11：00　渋谷智治（文科省メディア教育開発研）
BP 復号法に適した線形符号の設計
11：10～12：10　知念宏司（大阪工大工）・平松豊一（法政大工）
線形符号のゼータ関数とリーマン予想の類似
13：40～14：40　羽田充宏（阪府大理）・川添充（阪府大総合科学）・
高橋哲也（阪府大総合科学）
Formulae of the order of Jacobians for certain hyperelliptic curves
14：50～15：50　三浦晋示
ヤコビ群の加算アルゴリズム
16：00～17：00　坂内英一（九大数理）
種々の tight デザインの存在・非存在問題について

11月7日(金)
10：00～11：00　松本隆太郎（東工大集積システム）
量子符号の代数的構成法
11：10～12：10　内山智香子（山梨大工）
量子暗号の原理
13：40～14：40　水野弘文（イオンド大）
代数幾何符号の歩み
14：50～15：50　本間正明（神奈川大工）
Hermitian 曲線上の 2 点符号(予報)
16：00～17：00　藤沢匡哉（東京理科大工）・前田秀介（電通大情報通信工）・
阪田省二郎（電通大情報通信工）
複合誤り訂正符号について

符号と暗号の代数的数理
Algebraic Aspects of Coding Theory and Cryptography
研究集会報告集

２００３年１１月４日～１１月７日

研究代表者　平松　豊一 (Toyokazu Hiramatsu)

目　次