数理解析研究所講究録1420

符号と暗号の代数的数理

京都大学数理解析研究所

2005年4月

はしがき

この講究録は, 2004 年 11 月 8 日（月）から 11 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第 2 回目の共同研究集会「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された報告集であります.

この研究集会では, 符号・暗号理論に関係した代数学等の最近の発展についての諸講演と討論を通して, 代数幾何, 数論, 組合せ論にわたる広範な数学と符号・暗号理論との結びつきが明らかにされました. またゲノムをはじめとする数理生物学も一種の暗号的要素があり, その方面の専門家による講演もあり, 数学のさらなる応用の可能性を探ることもできました. 幸いにも大学や民間会社の研究者等 59 名の方々が参加され, 集会は盛会でした.

尚, この研究集会の講演者の旅費の一部に科学研究費補助金基盤研究 (A)(1) (15204001 代表者　桂利行) を使用しております.

2005 年 1 月

研究代表者
東京大学大学院 数理科学研究科
桂 利行

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、この集会には科学研究費補助金基盤研究(A)(1)(15204001 代表者　桂利行)を使用しております。

研究代表者　桂利行(東大数理)
研究副代表者　平松豊一(法政大工)

記

日時：2004 年 11 月 8 日(月) 10:00～11 月 11 日(木) 16:20
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 8 日(月)

10：00～11：00　加藤毅（京大理）
Interation states by iterating maps in molecular biology

11：10～12：10　O.R.Musin (Moscow State Univ.)
The kissing problem in four dimensions

13：30～14：30　宮野悟（東大医科研）
遺伝子ネットワーク推定とシュミレーション

14：40～15：40　池村淑道（総合研究大学院大学）
ゲノム配列に潜む多様なシグナルや暗号を明らかにする新規な数理的手法

15：50～16：20　多田秀樹（法政大工）・関田英太郎（日本獣医畜産大）
HIV-1（V3 loop）ウィルスとエントロピー

16：30～17：00　田辺隆人（数理システム）
Bioinformatics とソフトウェア

11 月 9 日(火)

10：00～11：00　有田正剛（情報セキュリティ大学院大学）
A Weil descent attack against elliptic curve cryptosystems over quartic extension fields
(長尾・松尾・志村氏との共同研究)

11：10～12：10　井坂元彦（関学大理工）
ターボ符号の構成と復号法

13：30～14：30　大矢雅則（東京理科大理工）
量子情報通信理論の基礎と最近の話題

14：40～15：40　小関道夫（山形大理）

Some small finite groups of linear transformations and their rings of invariants and from which the automorphic forms belonging to congruence subgroups are determined

15：50～16：20　坂川日出海（東大数理）

楕円曲線の有理点の height について

16：30～17：00　斎藤正顕（法政大工）・佐藤宏樹（東京理科大理）

Cartesian authentication codes from diagonal forms

11月10日(水)

10：00～11：00　本間正明（神奈川大工）

Hermitian 曲線の幾何と符号

11：10～12：10　宮地充子（北陸先端大学院大学）

Application of bilinear map to public-key encryption

13：30～14：30　吉田真紀（阪大情報）

電子透かしにおける最適な検出について

14：40～15：40　鈴木幸太郎（NTT）

ゲーム理論と暗号プロトコル

15：50～16：20　松田修三（法政大工）・平松豊一（法政大工）

円分数、暗号及び2次分割

16：30～17：00　藤原融（阪大情報）・安永憲司（阪大情報）

Some results on the local weight distribution of binary linear codes

11月11日(木)

10：00～11：00　松嶋敏泰（早大理工）

A classification of the probabilistic reasoning given distribution evidence and Kullback-Leibler information

11：10～12：10　趙晋輝（中央大理工）

超楕円暗号に関する最近の話題

13：30～14：30　野上保之（岡山大工）

XTR を用いた暗号とその高速実装

14：40～15：40　松井一（豊田工業大）・阪田省二郎（電通大）・栗原正純（電通大）

Fast parallel decoding on systolic array architecture for codes on a class of algebraic curves

15：50～16：20　渋谷智治（文科省メディア教育研）

周辺分布の高速近似計算と誤り訂正

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

２００４年１１月８日～１１月１１日

研究代表者　桂　利行 (Toshiyuki Katsura)
副代表者　平松　豊一 (Toyokazu Hiramatsu)

目　次