九州大学マス・フォア・インダストリ研究所　共同利用研究集会

安全・安心社会基盤構築のための代数構造

～サイバー社会の信頼性確保のための数理学～

期間：8 月 26 日（月）～8 月 30 日（金）
会場：九州大学西新プラザ　中会議室

プログラム

8 月 26 日（月）

15:00—15:10　開会
15:10—17:00　研究交流会
- 研究集会の趣旨説明
- 参加者の自己紹介

8 月 27 日（火）

10:00—11:00　基調講演　四方義啓（名古屋大・名誉教授）
暗号解析とガロア理論

11:30—12:30　Avishek Adhikari（カルカッタ大学・インド）
Connections Among Algebra, Statistical Designs and Secret Sharing Schemes

14:00—15:00　櫻庭健年（日立製作所）
ガロア接続を用いた動的秘密情報の管理 I

15:15—16:15　Phong Nguyen（INRIA, France and Tsinghua University, China）
Abstracting Lattice Cryptography

16:30—17:30　Xavier DAHAN（九州大学）
楕円曲線上の離散対数問題のグレブナー基底計算に基づく攻撃

8 月 28 日（水）

10:00—11:00　櫻庭健年（日立製作所）
ガロア接続を用いた動的秘密情報の管理 II

11:15—12:15 Christophe Petit（Universite catholique de Louvain）
Rubik's for Cryptographers

14:00—15:00 安田貴徳（九州先端科学技術研究所）
非可換代数を用いた公開鍵暗号の設計と解析

15:15—16:15 Avishek Adhikari（カルカッタ大学・インド）
Applications of Algebraic Structure in Visual Cryptography

16:30—17:00 田中哲士（九州大学）
Efficient Solving of Multivariate Quadratic Polynomial System using GPU

8 月 29 日（木）

10:00—10:30 田中哲士（九州大学）
Efficient Implementation of Multiplication on Extension Field using GPU

10:40—11:10 Kirill Morozov（九州大学）
On Cheater Identifiable Secret Sharing Schemes Secure Against Rushing Adversary

11:20—11:50 Avishek Adhikari（カルカッタ大学・インド）
Plaintext Checkable Encryption with Designated Checker

14:00—16:00 パネル討論会
ECDLP への攻撃手法について

8 月 30 日（金）

10:00—12:00 討論会