

MI Lecture Note Series

Volume No. : 53

Title : **Workshop on Algebraic constructions as a fundamental keystone of a safe and secure society—Mathematics for guaranteeing the reliability of the cyber-society—**

Editors : Yoshihiro SHIKATA, Kouichi SAKURAI, Takanori YASUDA, Xavier DAHAN

Written In : English

ISSN : 2188-1200

Published In : 2013年12月26日

Contents

27 August, 2013

Keynote Lecture

Cryptanalysis and Galois Theory Yoshihiro Shikata (Nagoya University Earthquake Research Institute)	1
--	---

Workshop

Connections Among Algebra, Statistical Designs and Secret Sharing Schemes Avishek Adhikari (University of Calcutta)	9
Galois Connection and Security (I) Taketoshi Sakuraba (HITACHI)	18
Abstracting Lattice Cryptography Phong Nguyễn (INRIA, France and Tsinghua University)	28
Attacks on the ECDLP using Groebner bases Xavier Dahan (Kyushu University)	33

28 August, 2013

Workshop

Galois Connection and Security (II) Taketoshi Sakuraba (HITACHI)	41
Rubik's for Cryptographers Christophe Petit (Université catholique de Louvain)	54
Design and Analysis of Public Key Cryptography using Non-commutative Algebra Takanori Yasuda (ISIT)	85
Applications of Algebraic Structures in Visual Cryptography Avishek Adhikari (University of Calcutta)	93

Efficient Implementation of Multiplication on Extension Field Using GPU
 Satoshi Tanaka (Kyushu University) 102

29 August, 2013

Workshop

Efficient Implementation of Multiplication on Extension Field Using GPU
 Satoshi Tanaka (Kyushu University) 113

On Cheater-Identifiable Secret Sharing Schemes Secure Against Rushing Adversary
 Kirill Morozov (Kyushu University) 122

Plaintext Checkable Encryption with Designated Checker
 Avishek Adhikari (University of Calcutta)..... 137

Improvement of Faugère *et al.*'s method to solve ECDLP
 Huang Yun-Ju (Kyushu University) 145