代数的手法による数理暗号解析

開催時期　2018-02-05 13:00～2018-02-07 11:45

場所　〒814-0002 福岡市早良区西新2-16-23 九州大学 西新プラザ 大会議室A

代数的手法による数理暗号解析
Workshop on analysis of mathematical cryptography via algebraic methods

※ この研究集会はマス・フォア・インダストリ研究所 共同利用研究の公開プログラムです.

開催期間　2018年2月5日(月) ～ 2月7日(水)

開催場所　〒814-0002 福岡市早良区西新2-16-23
九州大学西新プラザ 大会議室A, アクセス

【プログラム】
(全11講演)

2月5日(月)

13:00　開場
13:15 - 13:25　開会式

13:30 - 14:30
講演者：Mehdi Tibouchi (NTT)
講演タイトル：**Physical attacks on lattice-based schemes**
Abstract

14:45 - 15:45
講演者：Kim Taechan (NTT)
講演タイトル：**Use of algebraic subfield structure in cryptanalysis**
Abstract

16:00 - 17:00
講演者：玉置 卓 (京都大学)
講演タイトル：**Fine-grained complexity and cryptography: A personal survey**
Abstract

2月6日(火)

9:00　開場

9:30 - 10:30
講演者：黒田 匡迪 (北海道大学)
講演タイトル：**On monomial GAPN (Generalized Almost Perfect Nonlinear) functions and their classification**
Abstract

10:40 - 11:40
講演者：相川 勇輔 (北海道大学)
講演タイトル：**Elliptic curve method with complex multiplication method**
Abstract

13:10 - 14:10
講演者：中島 規博 (東京電機大学)
講演タイトル：**A modification of the discrete Fourier transform for the code defined by Garcia-Stichtenoth tower**
Abstract

14:20 - 15:20
講演者：Carlos Cid (Royal Holloway, University of London)
講演タイトル：**Code-based cryptography: design and security**
Abstract

15:30 - 16:30
講演者：高安 敦 (東京大学)
講演タイトル：**Solving RSA and factoring problems using LLL reduction**
Abstract

16:40 - 17:40
講演者：縫田 光司 (産業技術総合研究所/JST さきがけ)
講演タイトル：**Towards fully homomorphic encryption without ciphertext noise from group theory**
Abstract

18:10頃から　懇親会

2月7日(水)

9:00　開場

9:30 - 10:30
講演者：橋本 康史 (琉球大学)
講演タイトル：**A survey on multivariate public key cryptosystem**
Abstract

10:45 - 11:45
講演者：奥村 伸也 (大阪大学)
講演タイトル：**On the Security of Homomorphic Encryption Schemes Based on Ring-LWE Problem over Decomposition Fields**
Abstract

世話人　阿部 拓郎 (九州大学)
高島 克幸 (三菱電機)

縫田 光司 (産業技術総合研究所/JST さきがけ)
安田 雅哉 (九州大学)