社会基盤としての高機能暗号とその楕円曲線及び格子による実現

開催時期　2014-09-09 14:00～2014-09-11 12:30

場所　九州大学 産学官連携本部 産学官連携イノベーションプラザ 2階セミナールーム

社会基盤としての高機能暗号とその楕円曲線及び格子による実現
Functional Encryption as a Social Infrastructure and its Realization by Elliptic Curves and Lattices
※ 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　2014年9月9日(火) ～ 9月11日(木)

開催場所　〒814-0001 福岡市早良区百道浜3丁目8-34
九州大学 産学官連携本部 産学官連携イノベーションプラザ 2階セミナールーム
アクセスマップ

【プログラム】
(全12講演)

9月9日(火)

14:00 - 14:10　開会

14:10 - 14:50
講演者：辻井 重男 (中央大学研究開発機構), (講演協力者: 山口 浩 (中央大学研究開発機構), 五太子 政史 (中央大学研究開発機構))
招待講演«Advanced Concept of Information Security in Organizational Communications and Realization of Organization Encryption Systems with Elliptic Curves Cryptosystem»

15:10 - 15:50
講演者：HENG, Swee-Huay (Multimedia University, マレーシア)
海外招待講演«Recent Development in Identification»

15:50 - 16:30
講演者：MOROZOV, Kirill (九州大学IMI)
講演«On Identity-Based Identification from Codes»

18:00 - 20:00　意見交換会

9月10日(水)

09:50 - 10:00　第二日開会

10:00 - 10:40
講演者：CHENG, Chen-Mou (国立台湾大学, 台湾)
招待講演«Efficient Implementation of Elliptic-Curve and Lattice-Based Cryptography»

11:00 - 11:40
講演者：安田 貴徳 (ISIT)
講演«Efficient Pairing Instantiations Using Fixed Coefficients»

11:40 - 12:30
講演者：高島 克幸 (三菱電機(株))
基調講演«Functional Encryption from Dual Pairing Vector Spaces»

14:00 - 14:40
講演者：DAHAN, Xavier (ISIT)
講演«On a New Matrix Variant of NTRU»

15:00 - 15:40
講演者：有田 正剛 (情報セキュリティ大学院大学)
招待講演«Some Applications of the Multilinear Map»

15:40 - 16:20
講演者：安田 雅哉 ((株)富士通研究所)
招待講演«Practical Applications of Somewhat Homomorphic Encryption Using Lattices»

9月11日(木)

09:50 - 10:00 第三日開会

10:00 - 10:40
講演者：穴田 啓晃 (ISIT)
講演«Attribute-Based Signatures without Pairings»

11:00 - 11:40
講演者：寺西 勇 (日本電気(株))
招待講演«Anonymous Credential with Attributes Certification after Registration»

11:40 - 12:20
講演者：WENG, Jian (暨南大学, 中国)
招待講演«Verifiable Outsourcing of the Decryption of Ciphertext-Policy Attribute-Based Encryption»

[協賛] 公益財団法人九州先端科学技術研究所(ISIT)
九州大学システム情報科学研究院 櫻井研究室