プライバシ保護・分散型管理の次世代暗号技術とこれを支える数理構造

開催時期　2015-09-01 14:00～2015-09-03 12:10

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

プライバシ保護・分散型管理の次世代暗号技術とこれを支える数理構造
Next-generation Cryptography for Privacy Protection and Decentralized Control and Mathematical Structures to Support Techniques
組織委員Webページ:http://www.isit.or.jp/lab2/?p=3149

※ 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　2015年9月1日(火) ～ 9月3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
アクセス情報

参加申し込み　参加費は無料です.
参加申し込み等詳しくは組織委員Webページをご覧ください.

【プログラム】
(全10講演)　9月1日(火)
14:00 - 14:10　開会

14:10 - 15:00
講演タイトル《**Social Implications of the Decentralized Virtual Currency: A Public Policy Standardization Perspective**》
講演者：岡田 仁志 (国立情報学研究所)

15:10 - 15:20　休憩

15:20 - 16:00
講演タイトル《**Attribute-Based Access Control in Mobile Clouds**》
講演者：Sushmita Ruj (インド統計研究所)
16:00 - 16:40
講演タイトル《**Order-Preserving Encryption Secure Beyond One-Wayness**》
講演者：寺西 勇 (日本電気株式会社)

16:40 - 17:00　フォトセッション

9月2日(水)

09:50 - 10:00　第二日開会

10:00 - 10:40
講演タイトル《**Fast and Secure Linear Regression and Biometric Authentication with Security Update**》
講演者：Le Trieu Phong (情報通信機構)

10:40 - 11:00　休憩

11:00 - 11:40
講演タイトル《**Homomorphic Encryption - are we there yet?**》
講演者：Anirban Basu (株式会社KDDI研究所)
11:40 - 12:20
講演タイトル《**Cryptography for Cloud Service**》
講演者：吉野 雅之 (株式会社日立製作所)

12:20 - 14:00　休憩

14:00 - 14:40
講演タイトル《**Cryptography for Availability: The Case of Secure Cloud Storage**》
講演者：Sherman Chow (The Chinese University of Hong Kong)

14:40 - 15:00　休憩

15:00 - 15:40
講演タイトル《**Decentralized Attribute-Based Cryptosystems**》
講演者：高島 克幸 (三菱電機株式会社)
15:40 - 16:20
講演タイトル《**Dynamic Threshold Public-key Encryption with Decryption Consistency from Static Assumptions**》
講演者：花岡 悟一郎 (産業技術総合研究所)

17:45 - 19:45　意見交換会

9月3日(木)

09:50 - 10:00　第三日開会

10:00 - 10:40
講演タイトル《**On the Application of Clique Problem for Proof-of-Work in Cryptocurrencies**》
講演者：Samiran Bag (九州大学)

10:40 - 11:00　休憩

11:00 - 12:00　**パネルディスカッション**
パネリスト：宇根 正志 (日本銀行金融研究所)，他
モデレータ：Kirill Morozov (九州大学マス・フォア・インダストリ研究所)
アジェンダ：
(a): Mathematical structure behind decentralized cryptocurrencies: Formal? Robust? Secure?
(b): Multi-authority cryptographic primitives: Usability and practical impact

12:00 - 12:10　閉会