平成　27　年度 共同利用研究報告書

平成 27 年 10 月 8 日

九州大学 マス・フォア・インダストリ研究所長 殿

所属・職名　　公益財団法人九州先端科学技術研究所・研究員
提案者 氏名（ふりがな）　　穴田 啓晃（あなだ ひろあき）

下記の通り共同研究の報告をいたします.　　記

	※整理番号			
1.研究計画題目	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			
2.種別（○で囲む）	a. 研究集会Ⅰ　(b. 研究集会Ⅱ)　c.短期共同研究　d.短期研究員			
3.研究代表者	氏名（ふりがな）	穴田 啓晃（あなだ ひろあき）		
	所属部局名	公益財団法人九州先端科学技術研究所 情報セキュリティ研究室	職名	研究員
	連絡先			
	e-mail		TEL	
4.研究実施期間	平成 27 年 9 月 1 日（火曜日）～平成 27 年 9 月 3 日（木曜日）			

5.参加者数・参加者リスト（＊別紙「共同利用研究報告書作成上の注意」参照）
(a,b は参加者数のみ記入し, 集会参加者リストを添付. c.の非公開プログラム参加者と d.は参加者リストに記入. c.は公開プログラムを含めた全参加者数を記入し，公開プログラム参加者リストを添付.）

参加者数：　33　人
参加者リスト（a,b は記入不要，c.は非公開プログラム参加者，d.は共同研究参加者を記入）

6.本研究で得られた成果の概要

まず，参加者の観点から，産学官別内訳は，学生を除く 28 名のうち産から 5 名，官から 8 名，学から 15 名であった．学からは九大の教員が多かった影響を差し引くと，およそ三つの業界の方々から満遍なく参加頂けた．また，賞味丸二日の開催期間に対し適切な人数であり，結果として，講演・聴講を通じて活発に交流頂くことが出来た．14 名の外国籍の方々に参加頂けたため国際会議として意見交換・交流できた点も，成果と考えている．

また，研究内容の観点から，本研究集会で実施された講演を次の三つのカテゴリに分類することができる．

A.　プライバシ保護暗号技術と数理構造
B.　分散型管理暗号技術と数理構造
C.　上記 A，B についてのパネルディスカッション

カテゴリ A は 5 件，カテゴリ B は 5 件，カテゴリ C は 2 件の講演を，各々トップレベルの研究開発者から頂くことが出来た.

より詳細については成果報告書に示す.

（以上）

平成 27 年度九州大学 IMI 共同利用研究・研究集会（II）

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

日時： 2015年9月1日（火）－9月3日（木）
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
URL： 公開プログラム：http://www.imi.kyushu-u.ac.jp/events/view/1640
組織委員 Web ページ：http://www.isit.or.jp/lab2/?p=3149

9 月 1 日(火)

14:00-14:10 開会

14:10-15:00 講演者: 岡田仁志（国立情報学研究所）
Social Implications of the Decentralized Virtual Currency: A Public Policy Standardization Perspective

15:10-15:20 休憩

15:20-16:00 講演者: Sushmita Ruj（インド統計研究所）
Attribute-Based Access Control in Mobile Clouds

16:00-16:40 講演者: 寺西勇(日本電気株式会社)
Order-Preserving Encryption Secure Beyond One-Wayness

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 講演者: Le Trieu Phong（情報通信機構）
Fast and Secure Linear Regression and Biometric Authentication with Security Update

10:40-11:00 休憩

11:00-11:40　講演者: Anirban Basu (株式会社 KDDI 研究所)
Homomorphic Encryption - are we there yet?

11:40-12:20　講演者: 吉野雅之(株式会社日立製作所)
Cryptography for Cloud Service

12:20-14:00　休憩

14:00-14:40　講演者: Sherman Chow (The Chinese University of Hong Kong)
Cryptography for Availability: The Case of Secure Cloud Storage

14:40-15:00　休憩

15:00-15:40　講演者: 高島克幸(三菱電機株式会社)
Decentralized Attribute-Based Cryptosystems

15:40-16:20　講演者: 花岡悟一郎(産業技術総合研究所)
Dynamic Threshold Public-key Encryption with Decryption Consistency from Static Assumptions

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　講演者: Samiran Bag (九州大学)
On the Application of Clique Problem for Proof-of-Work in Cryptocurrencies

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

2015-10-14

2015 年九州大学マス・フォア・インダストリ研究所共同利用研究集会(II)

“Next-generation Cryptography for Privacy Protection and Decentralized Control and Mathematical Structures to Support Techniques”
（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）

成果報告書

組織委員代表　公益財団法人九州先端科学技術研究所・研究員
穴田 啓晃

本報告書は, 2015 年の共同利用研究集会(II)て採択された上記表題の研究集会を開催し得られた成果を簡潔に報告することを目的とする.

はじめに，参加者についての成果を説明する．本研究集会は 33 名の参加者があった．参加人数の内訳を，国籍国内外別および産学官別で図 1 に示す．ただし後者については学生 5 名を除いている．本研究集会は，国外の国籍の参加者が 14 名（42%）であった．国際研究集会として交流できたものと考えている. また, 産からは 5 名(18%), 官からは 8 名(29%), 学からは 15 名（53%）であった．学からの参加者が約半分であったが，これは九州大学の教員が多かったためである．この影響を差し引くと，産学官からおよそ満遍なく参加頂けたと考えている.

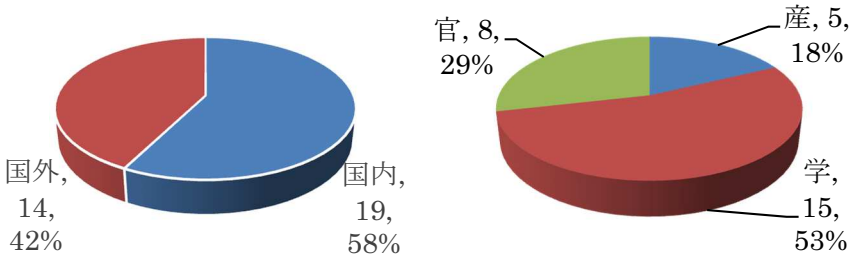

図 1　国籍国内外別（左）および産学官別（右）参加人数内訳（産学官は学生を除く）.

次に，研究内容についての成果を説明する．実施された講演は次の三つのカテゴリに分類される.

A. プライバシ保護暗号技術と数理構造
B. 分散型管理暗号技術と数理構造
C. 上記 A，B についてのパネルディスカッション

次ページ表 1 は上記カテゴリ別の実施講演一覧を示す．カテゴリ A は 5 件（計 200 分），カテゴリ B は 5 件（計 210 分），そしてカテゴリ C は 2 件（計 60 分）であった．このことから，本研究集会の応募時に計画したカテゴリ A およびカテゴリ B の研究主題について，件数および時間共に，賞味丸 2 日間の開催期間に対し十分な量の講演を頂けたと考えている．また，質の面では，表 1 に示されている講演者は業績の点で，産学官からのトップレベルの研究開発者である．加えて，カテゴリ C のパネルディスカッションにより，産業界への貢献の展望を，会場の参加者も巻き込み議論できたことが成果と考えている．

また，報告として，講演者の参加予算元について触れる．本研究集会では，九州大学マス・フォア・インダストリ研究所から本研究集会への予算により，表 1 における A1,A3,A4,A5,B1,B3,B4 の研究者を招へいすることができた．また，B2 の Sushmita Ruj 氏（インド統計研究所）および C の Masashi Une 氏（日本銀行）は，科研費により招へいすることができた（研究代表者：九州大学システム情報科学研究院・櫻井幸一教授，研究課題名：分権管理型暗号認証基盤の構築と応用システムの設計と解析，研究課題番号：15H02711）．また，A2 の Le Trieu Phong 氏は，国立研究開発法人情報通信機構からの出張費により参加頂いた. 残りの 2 名（B5 の Samiran Bag 特任助教および C の Kirill Morozov 助教）の方々には九州大学から参加頂いた．以上についてここに深謝申し上げる．

総括として，本研究集会では，上記カテゴリの講演 10 件，パネルディスカッション 2 件について，交流するのに適切な人数の方々（33 名）に参加頂き，結果として講演・聴講を通じて活発に交流頂くことが出来た．本研究集会が参加者に与えた影響については，九州大学マス・フォア・インダストリ研究所により行われるであろう《講演者のその後の関連論文数アンケート》に現れることを期待したい．

（以上）

表 1　カテゴリ別の実施講演一覧

No.	Name of Speaker	Affiliation
	Title	
A	Cryptography for Privacy Protection and its Mathematical Structures	
A1	Isamu Teranishi	NEC Corp.
	"Order-Preserving Encryption Secure Beyond One-Wayness"	
A2	Le Trieu Phong	Nat. Ins. Info. and Comm. Tech.
	"Fast and Secure Linear Regression and Biometric Authentication with Security Update"	
A3	Anirban Basu	KDDI R&D Lab.
	"Homomorphic encryption - are we there yet?"	
A4	Masayuki Yoshino	Hitachi, Ltd.
	"Cryptography for Cloud Service"	
A5	Sherman Chow	The Chinese Univ. of Hong Kong
	"Cryptography for Availability: The Case of Secure Cloud Storage"	
B	Cryptography for Decentralized Control and its Mathematical Structures	
B1	Hitoshi Okada	National Institute of Informatics
	"Social Implications of the Decentralized Virtual Currency: A Public Policy Standardization Perspective"	
B2	Sushmita Ruj	Indian Statistical Institute
	"Attribute based access control in mobile clouds"	
B3	Katsuyuki Takashima	Mitsubishi Electric Corp.
	"Decentralized Attribute-Based Cryptosystems"	
B4	Goichiro Hanaoka	Nat. Inst. of Adv. Ind. Sci. and Tech.
	"Dynamic Threshold Public-key Encryption with Decryption Consistency from Static Assumptions"	
B5	Samiran Bag	Kyushu University / ISI
	"On the Application of Clique Problem for Proof-of-Work in Cryptocurrencies"	
C	PANEL DISCUSSION　Invited Panelist: Masashi Une, Bank of Japan / Modelator: Kirill Morozov, IMI, Kyushu Univ.	
C1	"Mathematical structure behind decentralized cryptocurrencies: Formal? Robust? Secure?" (Panelists: Masashi Une, Sushmita Ruj and Hitoshi Okada)	
C2	"Multi-authority cryptographic primitives: Usability and practical impact" (Panelists: Masashi Une, Goichiro Hanaoka and Katsuyuki Takashima)	