平成２９年度 共同利用研究報告書

平成 ３０年 ３ 月 １５ 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　北テキサス大学コンピュータサイエンス工学科・准教授
提案者 氏名(ふりがな)　モロゾフ・キリル

下記の通り共同研究の報告をいたします.　　記

	※整理番号		20170021	
1.研究計画題目	ネットワークストレージを安全にするための暗号技術とその数学モデリング			
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)	モロゾフ　キリル		
	所属部局名	University of North Texas Dept. of Computer Science and Engineering	職名	准教授
	連絡先			
	e-mail		TEL	
4.研究実施期間	平成 29 年 6 月 12 日（月曜日）～平成 29 年 6 月 13 日（火曜日）			

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：　４４　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）

氏名(ふりがな)	所属	職名	氏名(ふりがな)	所属	職名
－	－	－	－	－	－

6.本研究で得られた成果の概要

秘密分散法や秘匿計算は情報漏洩や情報損失に対し安全なストレージや情報処理を実現するための解決策として学術及び産業界で盛んに研究開発されている．本研究集会が参加者数 44 名と想定以上の関心を集めたのはこの傾向を反映したものと考える．産学官別の内訳は，産から 7 名，学から 33 名，官から 4 名であり，三つの業界の各々から参加頂けた．また，この参加者数は二日間の開催期間に対し多い数字であり，結果として講演・聴講を通じ活発に期待以上に交流頂くことが出来た．更に，10 名の外国籍の方々に参加頂き，国際会議として意見交換し交流頂くことも出来た.

研究内容の観点からは，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出来る.

カテゴリA.　秘密分散法の数学モデルと適用
カテゴリB.　秘匿計算の数学モデルと実装
カテゴリC.　秘密分散法及び暗号技術の応用
カテゴリD.　A, B, C についてのパネルディスカッション

カテゴリ A は 4 件，カテゴリ B は 3 件，カテゴリ C は 2 件，カテゴリ D は 1 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）

"Workshop on Cryptographic Technologies for Securing Network Storage and Their Mathematical Modeling"
Program

Date/Time				Lectures			
Date	Start	End	Time	No.	Event/Lecturer	Affiliation	Title
Jun 12	10:00	10:10	0:10	1	Opening Address	-	-
	10:10	10:50	0:40	2	Amos Beimel	Ben-Gurion University, Israel	Graph Secret Sharing
	10:50	11:10	0:20	-	Coffee Break	-	-
	11:10	11:50	0:40	3	Yvo Desmedt	The University of Texas at Dallas, USA	Human Recomputable Secret Shares and their Applications in E-Voting
	11:50	14:00	2:10	-	Lunch (Self)	-	-
	14:00	14:40	0:40	4	Mitsugu Iwamoto	The University of Electro-Communications, Japan	Secret Sharing Schemes under Guessing Secrecy
	14:40	15:00	0:20	-	Coffee Break	-	-
	15:00	15:40	0:40	5	Naruhiro Kurokawa	Bank of Japan, Japan	Function Secret Sharing Using Fourier Basis
	15:40	16:00	0:20	-	Coffee Break	-	-
	16:00	16:30	0:30	6	Panel Discussion	-	-
	16:40	17:00	0:20	7	Photo Session	-	-
	17:30	20:00	2:30	8	Banquet	-	-
Jun 13	10:10	10:50	0:40	8	Eyal Kushilevitz	Technion, Israel	Ad-hoc MPC
	10:50	11:10	0:20	-	Coffee Break	-	-
	11:10	11:50	0:40	9	Takeshi Koshiba	Waseda University, Japan	Secure Message Transmission against Rational Adversaries
	11:50	14:00	2:10	-	Lunch (Self)	-	-
	14:00	14:40	0:40	10	Kazuma Ohara	NEC Corporation, Japan	Optimized Honest-Majority MPC for Malicious Adversaries - Breaking the 1 Billion-Gate Per Second Barrier
	14:40	14:50	0:10	-	Coffee Break	-	-
	14:50	15:30	0:40	11	Ryo Kikuchi	NTT CORPORATION, Japan	Key components in MEVAL
	15:30	15:40	0:10	-	Coffee Break	-	-
	15:40	16:20	0:40	12	Bernardo David	Tokyo Institute of Technology, Japan	A Provably Secure Proof-of-Stake Blockchain Protocol
	16:20	16:30	0:10		Closing Remarks	-	-

(Ver. Jun 5, 2017)

2018 年 3 月 15 日

2017 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(I)

“Cryptographic Technologies for Securing Network Storage and Their Mathematical Modeling”

（ネットワークストレージを安全にするための暗号技術とその数学モデリング）

成果報告書

組織委員

北テキサス大学・准教授	モロゾフ・キリル（代表者）
長崎県立大学・准教授	穴田啓晃
㈱インターネットイニシアティブ・シニアエキスパート	須賀祐治

本報告書は，2017 年の共同利用研究集会(I)で採択頂いた上記の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 44 名の参加者があった．参加人数の内訳を，国内外（国籍）別および産学官別で図 1 に示す．本研究集会は，外国籍の参加者が 10 名（23%）であった（図 1，左）．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 7 名（16%），学からは 33 名（75%），官からは 4 名（9%）であった（図 1，右）．学からの参加者が約 4 分の 3 であったが，これは大学の教員・学生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．

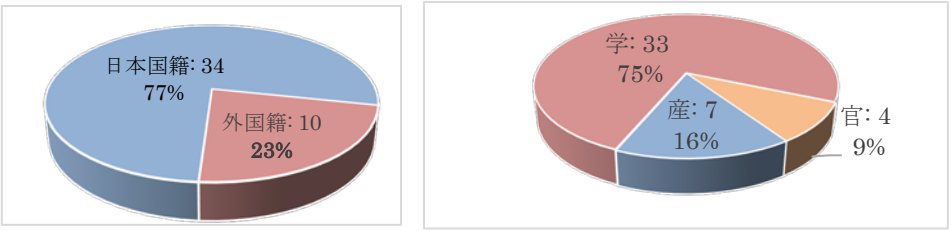

図 1　外国籍・日本国籍別（左）および産学官別（右）参加人数内訳．

次に，研究内容の成果について説明する．実施された講演は次の四つのカテゴリに分類される．

カテゴリA. 秘密分散法の数学モデルと適用

カテゴリB. 秘匿計算の数学モデルと実装

カテゴリC. 秘密分散法及び暗号技術の応用

カテゴリD. A, B, C 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 4 件（計 160 分），カテゴリ B は 3 件（計 120 分），カテゴリ C は 2 件（計 80 分），そしてカテゴリ D は 1 件（計 30 分）であった．このことから，本研究集会の研究題目「ネットワークストレージを安全にするための暗号技術とその数学モデリング」に対して，件数および時間共に， 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．なお，カテゴリ D のパネルディスカッションは，聴講者も巻き込んだディスカッションがなされた．このパネルディスカッションの動画を “Youtube”を利用し参加者へ配信し，かつ，会議録 “MI Lecture Note” に URL を掲載した．

講演者の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支給頂いた予算を用い，表 1 における A3，A4，B2，B3，C1，C2 の研究者を招へいすることができた．ここに深謝申し上げる．

総括として，本研究集会では，講演 9 件，パネルディスカッション 1 件について，交流するのに想定（40 名）以上の方々（44 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．なお，本研究集会が参加者に与えた研究開発上の影響については，九州大学マス・フォア・インダストリ研究所により例年行われる《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

A.　秘密分散法の数学モデルと適用		
A1	Amos Beimel	Ben-Gurion University, Israel
	“Graph Secret Sharing”	
A2	Yvo Desmedt	The University of Texas at Dallas, USA
	“Human Recomputable Secret Shares and their Applications in E-Voting”	
A3	Mitsugu Iwamoto	The University of Electro-Communications, Japan
	“Secret Sharing Schemes under Guessing Secrecy”	
A4	Naruhiro Kurokawa	Bank of Japan, Japan
	“Function Secret Sharing Using Fourier Basis”	
B.　秘匿計算の数学モデルと実装		
B1	Eyal Kushilevitz	Technion, Israel
	“Ad-hoc MPC”	
B2	Kazuma Ohara	NEC Corporation, Japan
	“Optimized Honest-Majority MPC for Malicious Adversaries - Breaking the 1 Billion-Gate Per Second Barrier”	
B3	Ryo Kikuchi	NTT CORPORATION, Japan
	“Key components in MEVAL”	
C.　秘密分散法及び暗号技術の応用		
C1	Takeshi Koshiba	Waseda University, Japan
	“Secure Message Transmission against Rational Adversaries”	
C2	Bernardo David	Tokyo Institute of Technology, Japan
	“A Provably Secure Proof-of-Stake Blockchain Protocol”	
D.　PANEL DISCUSSION Moderator: Kirill MOROZOV, Tokyo Institute of Technology, Japan.		
D1	Panelists: Bernardo David, Yvo Desmedt, Mitsugu Iwamoto, Ryo Kikuchi, Naruhiro Kurokawa, Eyal Kushilevitz, Kazuma Ohara	
	“Secret Sharing and Multi-Party Computation: Perspectives for Industrial Applications”	