2021年度共同利用研究報告書

2022年01月07日

所属・職名 長崎県立大学情報システム学部情報セキュリティ学科・教授
穴田　啓晃

		整理番号		20210004
1.研究計画題目	秘密計算・秘密分散の数理と実用の探求			
2.新規・継続	新規			
3.種別	一般研究			
4.種目	研究集会(I)			
5.研究代表者	氏名	穴田　啓晃		
	所属 部局名	長崎県立大学情報システム学部情報セキュリティ学科	職名	教授
6.研究実施期間	2021年11月08日(月曜日)～2021年11月10日(水曜日)			
7.キーワード	数学モデリング，暗号，秘密計算，秘密分散，情報セキュリティ			
8.参加者人数	80人			

9.本研究で得られた成果の概要

講演については，暗号数理の業績で世界的に知られるBuchmann教授（ドイツ・ダルムシュタット工科大学）の講演"Cryptographic Long-term Security"（約60分）は期待以上であった．というのも，5Gや量子通信や量子計算機の研究開発が進む中，暗号数理が貢献できる可能性について，秘密分散共有法を例に挙げ，見解をお示し頂けたからである．また，秘密計算・秘密分散の数理の講演が5件，それらの実用への適用を3件講演頂けたのは，時間にして計4時間と長くはないものの，情報と示唆の多い充実したものとなった．実際，いずれの講演も，内容はトップレベルの国際会議で採択されている一連の研究の一端，もしくは最先端の研究の一端であった．

参加登録者については，80名超と，講演時間計5時間の研究集会として想定以上に興味を集めたものと考えている．参加者の内訳としては，40歳未満と40歳以上でおよそ同数（40名ずつ），また産からは25名（30%），学からは48名（60%），官からは8名（10%）と，産からの参加者が期待以上に多かった．この点も成果と考えている．

（以上）

2022 年 1 月 7 日

2021 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)

“Exploring Mathematical and Practical Principles of Secure Computation and Secret Sharing”

（秘密計算・秘密分散の数理と実用の探求）

成果報告書

組織委員

長崎県立大学・教授	穴田啓晃（代表者）
東京大学大学院新領域創成科学研究科・研究員	大畑幸矢
北陸先端科学技術大学院大学・助教	王 イントウ
九州大学マス・フォア・インダストリ研究所・教授	縫田 光司
九州大学マス・フォア・インダストリ研究所・助教	池松 泰彦

ウェブサイト

https://joint.imi.kyushu-u.ac.jp/research-reports/year-2021/

https://joint.imi.kyushu-u.ac.jp/post-1240/

本報告書は，2021 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て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 81 名の参加登録があった．参加人数の内訳を，年齢別及び産学官別でそれぞれ図 1 及び図 2 に示す．**図 1** から，40 歳未満と 40 歳以上でおよそ 40 名ずつであったことが判る．また図 2 から，産からは 25 名（30%），学からは 48 名（60%），官からは 8 名（10%）であったことが判る．学からの参加者が 6 割であったが，これは大学の教員・学生が多かったためである．

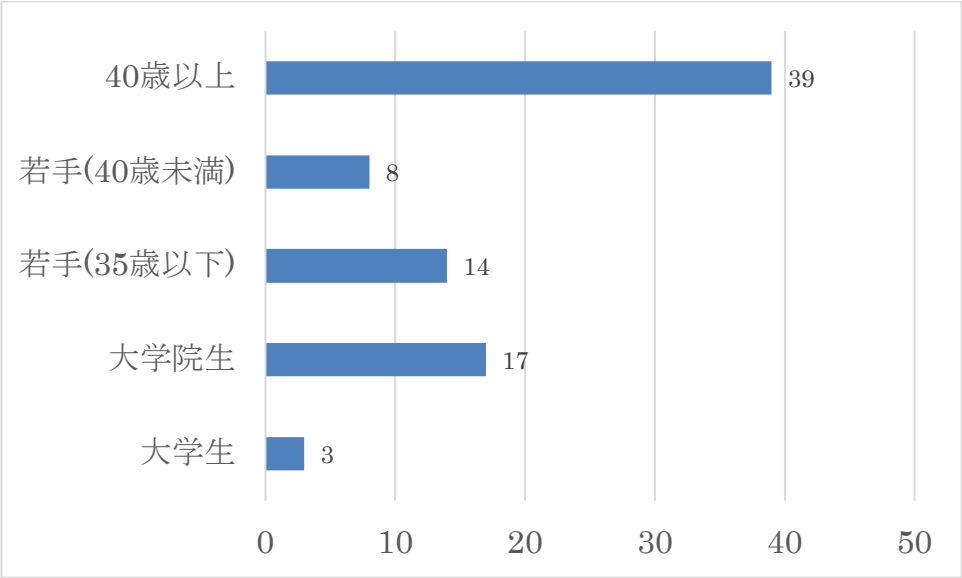

図 1　参加人数内訳．年齢別

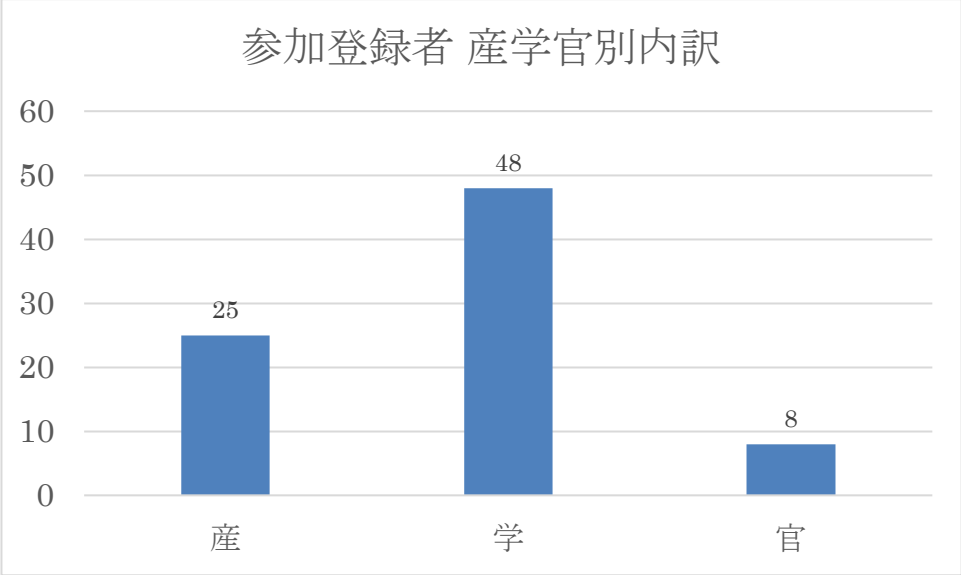

図 2　参加人数内訳．産学官別

次に，研究内容の成果を説明する．次ページに実施された講演の一覧を示す．講演は次の三つのカテゴリに分類される．

カテゴリA.　基調講演　　：講演 1)
カテゴリB.　数理　　：講演 2) 4) 7) 8) 9)
カテゴリC.　数理の実用への適用　　：講演 3) 5) 6)

このことから，本研究集会の研究題目「秘密計算・秘密分散の数理と実用の探求」に関し，件数及び時間の観点で数理と実用の双方をバランスよく講演頂けたものと考えている．

講演内容については，暗号数理の業績で世界的に知られる Buchmann 教授（ドイツ・ダルムシュタット工科大学）の講演"Cryptographic Long-term Security"（約 60 分）は期待以上であった．というのも，5G や量子通信や量子計算機の研究開発が進む中，暗号数理が貢献できる可能性について，秘密分散共有法を例に挙げ，見解をお示し頂けたからである．また，秘密計算・秘密分散の数理の講演が 5 件，それらの実用への適用を 3 件講演頂けたのは，時間にして計 4 時間と長くはないものの，情報と示唆の多い充実したものとなった．実際，いずれの講演も，内容はトップレベルの国際会議で採択されている一連の研究の一端，もしくは最先端の研究の一端であった．

最後に，本研究集会の開催に当たっては，九州大学マス・フォア・インダストリ研究所から支給頂いた予算を用いた．ここに深謝申し上げる．

（以上）

2022 年 1 月 7 日

実施された講演の一覧

第 1 日：11 月 08 日（月）

1) 16:05-16:55

Johannes Buchmann（Technische Universität Darmstadt）

“Cryptographic Long-Term Security”

2) 17:05-17:40

Yi Lu（Tokyo Institute of Technology / National Institute of Advanced Industrial Science and Technology）

“Efficient Two-party Exponentiation from Quotient Transfer”

3) 17:50-18:25

Hikaru Tsuchida（NEC Corporation）

“General-purpose Compiler for Secure Three-party Computation and Its Application to Prediction by Machine Learning Model”

第 2 日：11 月 09 日（火）

4) 09:05-09:55

Kirill Morozov（University of North Texas）

“Evolving Secret Sharing From Evolving Perfect Hash Families”

5) 10:05-10:40

Ibuki Mishina（NTT Social Informatics Laboratories）

“Secure-Computation AI：a Python Library for Machine Learning in Secure Computation”

6) 10:50-11:25

Kosuke Kaneko（Robert T.Huang Entrepreneurship Center of Kyushu University）

“Possibility of Secret Sharing using EtherCAT”

第 3 日：11 月 10 日（水）

7) 16:05-16:40

Yasuhiko Ikematsu（Institute of Mathematics for Industry）

“An Indeterminate Equation Scheme having Homomorphic Property”

8) 16:50-17:25

Reo Eriguchi（The University of Tokyo）

“Homomorphic Secret Sharing for Multipartite and General Adversary Structures Supporting Parallel Evaluation of Low-Degree Polynomials”

9) 17:35-18:10

Hiroaki Anada（University of Nagasaki）

“A Comparison of How to Garble Boolean and Arithmetic Circuits”

九州大学 IMI 共同利用・研究集会（I）

秘密計算・秘密分散の数理と実用の探求

Exploring Mathematical and Practical Principles of Secure Computation and Secret Sharing

日　　時：　2021 年 11 月 08 日（月）16:00 ～ 18:25
　　2021 年 11 月 09 日（水）09:00 ～ 11:25
　　2021 年 11 月 10 日（水）16:00 ～ 19:00
場　　所：　Zoom によるオンライン開催
組織委員　：
- Hiroaki Anada　(University of Nagasaki)　（研究代表者）
- Yasuhiko Ikematsu　(IMI, Kyushu University)
- Koji Nuida　(IMI, Kyushu University)
- Satsuya Ohata
- Yuntao Wang　(Japan Advanced Institute of Science and Technology)

プログラム

11 月 08 日（月）

16:00-16:05
オープニング

16:05-16:55
講演者：Johannes Buchmann (Technische Universität Darmstadt)
講演タイトル：“Cryptographic Long-Term Security”

17:05-17:40
講演者：Yi Lu (Tokyo Institute of Technology / National Institute of Advanced Industrial Science and Technology)
講演タイトル：“Efficient Two-party Exponentiation from Quotient Transfer”

17:50-18:25
講演者：Hikaru Tsuchida (NEC Corporation)
講演タイトル：“General-purpose Compiler for Secure Three-party Computation and Its Application to Prediction by Machine Learning Model”

11 月 09 日（火）

09:00-09:05
第 2 日オープニング

09:05-09:55
講演者：Kirill Morozov (University of North Texas)
講演タイトル：“Evolving Secret Sharing From Evolving Perfect Hash Families”

10:05-10:40
講演者：Ibuki Mishina (NTT Social Informatics Laboratories)
講演タイトル：“Secure-Computation AI ： a Python Library for Machine Learning in Secure Computation”

10:50-11:25
講演者：Kosuke Kaneko (Robert T.Huang Entrepreneurship Center of Kyushu University)
講演タイトル：“Possibility of Secret Sharing using EtherCAT”

11 月 10 日 (水)

16:00-16:05
第 3 日オープニング

16:05-16:40
講演者：Yasuhiko Ikematsu (Institute of Mathematics for Industry)
講演タイトル：“An Indeterminate Equation Scheme having Homomorphic Property”

16:50-17:25
講演者：Keitaro Hiwatashi (The University of Tokyo)
講演タイトル：(TBD)

17:35-18:10
講演者：Reo Eriguchi (The University of Tokyo)
講演タイトル：“Homomorphic Secret Sharing for Multipartite and General Adversary Structures Supporting Parallel Evaluation of Low-Degree Polynomials”

18:20-18:55
講演者：Hiroaki Anada (University of Nagasaki)
講演タイトル：“A Comparison of How to Garble Arithmetic and Boolean Circuits”

18:55-19:00
クロージング

最新情報及び参加情報は下記 URL(QR コード)のウェブサイトにて御確認下さい.
https://www.imi.kyushu-u.ac.jp/kyodo-riyo/research_meetings/view/30