[様式 1.3.]

AIMaP 研究集会等実施報告書

(Part 1/4) 名称・重点テーマ・キーワード等

項目	内容
名称	「Special Session of Mathematics and Information Security (M&IS)」(IWSEC2019)
採択番号	2019K003
重点テーマ	重点領域「セキュリティ安全性の確保・保証」 情報処理学会・電子情報通信学会
キーワード	暗号理論, プライバシー保護, ブロックチェーン, ゼロ知識証明, 数学キャリアパス
主催機関	九州大学・マス・フォア・インダストリ研究所
運営責任者	溝口佳寛 (九州大学・マス・フォア・インダストリ研究所)
開催日時(開始)	2019/8/28 09:40
開催日時(終了)	2019/8/30 17:10
開催場所	東京工業大学 (大岡山キャンパス)

(Part 2/4) 最終プログラム・参加者数

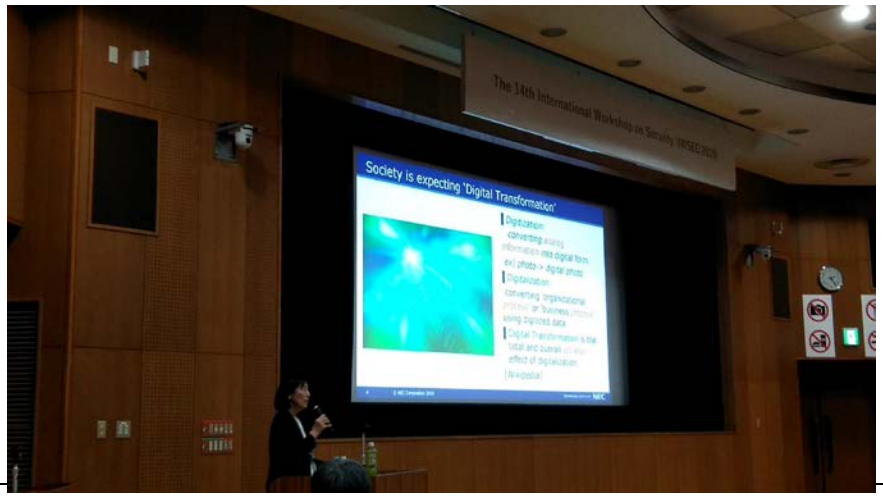
項目	内容
最終 プログラム	プログラムウェブページ (https://www.iwsec.org/2019/program.html) AIMaP 特別セッション (https://www.iwsec.org/2019/aimap.html) (1) 8 月 29 日(水) 14:10-15:10 Mathematics and Cryptography for Society 佐古和恵 (NEC セキュリティ研究所, AIMaP 運営委員) (2) 8 月 30 日(木) 10:55-11:55 Domain Specific Ciphers Carlos Cid 教授 (Royal Holloway, University of London, Director of Centre for Doctoral Training in Cyber Security) (3) 8 月 28 日(水) 17:30-19:30 Poster Session
参加者数	数学・数理科学:35 人, 諸科学: 50 人, 産業界: 44 人, その他: 10 人

(Part 3/4) 論点・現状・今後の展開

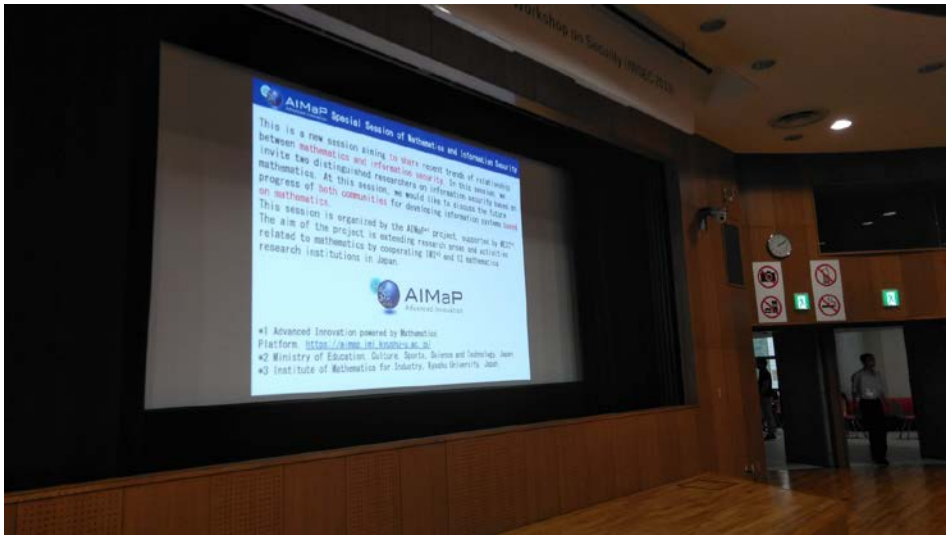
項目	内容
当日の論点	IWSEC2019 は，情報処理学会コンピュータセキュリティ研究会（CSEC）および電子情報通信学会情報セキュリティ研究会（ISEC）が共催の暗号を含む情報セキュリティ分野における日本で毎年開催の国際会議である．日本における情報セキュリティ研究の発展と国際化を目的とすると共に，国内外の最新の研究発表ならびに研究動向に関する研究者同士の情報交換の場を提供している．本年度の開催では，AIMaP 特別企画として情報セキュリティ研究の中での数学研究の役割，および，数学理論の考え方がいかに必要とされているかを数学科出身で暗号研究の第一人者である欧米応用暗号研究者に基調講演をしてもらい，具体的な事例を紹介して頂いた．日本人研究者らと討論を行い，日米のキャリアパスの違いを明らかにし，その改善策を探った．さらに，情報セキュリティ研究者らの講演セッション，ポスターセッションにおいて，数学理論，応用技術などの発表者を交えて，今後の数学応用の可能性を模索し，実現方法の手順を具体化するための討論を行なった．
研究の現状と課題（既にできていること、できていないことの切り分け）	海外と日本における数学者のキャリアパスの違い，暗号研究への取組方法の違いが紹介された．日本国内においては，社会情報システム構築の基幹としての情報セキュリティ技術への取組の中での数学研究の重要性を若手研究者へ伝える機会が少なかった．暗号理論の基礎数学としての数論，セキュリティプロトコルの基礎理論としての数理論理学，など応用分野の中の基礎理論ではなく，基礎数学研究者が，どのような視点から取り組み，新たな応用技術開発に貢献したのか，学問のつながりでだけでなく，人と組織と方法の多様なキャリアパスを紹介し，暗号研究分野における数学研究の意義を周知することが課題である． Carlos Cid 氏の基調講演では，英国政府により設立された産官学連携の PhD プログラムを実施する博士課程サイバーセキュリティセンター(Center for Doctor Training in Cyber Security)が紹介された．そこでは，企業へのキャリアパスを見据えた，大学院博士課程としての数学と情報セキュリティ強化教育プログラムが実現されている．
新たに明らかになった課題	日欧の数学キャリアパスの傾向の違い，応用技術の中の要素技術としての数学理論ではなく，数学理論に内在する考え方から生まれた新技術の紹介などは，研究そのものの紹介ではないため，今まで実現が難しかったが，今回の AIMaP 支援により，日本における情報セキュリティの一流会議においての基礎数学研究者と暗号応用研究者との合同企画が実現できたことは，広報の視点からも情報セキュリティ分野内に限らず非常に効果的であった．この企画での新しい交流機会を活かし，新しい視点からの研究課題への取り組みへと導くことが課題である.具体的には，量子計算機による暗号解読に耐性のある次世代暗号技術である「耐量子計算機暗号」は格子・符号・多変数多項式・楕円曲線上の同種写像などの数学を基にしており，数学と情報セキュリティの両分野のより密な交流が必要であることが分かった．さらに，ビットコインの仮想通貨以外のビジネス展開が強く期待されるブロックチェーンなどの技術においても，量子情報社会に向けた次世代暗号の組み込みが必要なため，耐量子計算機暗号の社会実装に向けても数学が重要となっている．
今後解決すべきこと、今後の展開・フォローアップ	量子計算機でも解読困難な数学問題を応用した耐量子計算機暗号の最新動向とその社会的重要性に関して企業暗号研究者に強い興味を持って頂いた．特に，耐量子計算機暗号の攻撃・実装手法の調査と考察においては，九大 IMI と企業間で共同研究テーマと各役割について定期的な議論を開始することとなった．

(Part 4/4) 写真

[様式 1.3.]

項目	内容
添付写真 1	
添付写真 2	
添付写真 3	

[様式 1.3.]

添付写真 4	
添付写真 5	

(20190422a)