九州大学広報室
〒819-0395 福岡市西区元岡 744
TEL:092-802-2130 FAX:092-802-2139
MAIL:koho@jimu.kyushu-u.ac.jp
URL:http://www.kyushu-u.ac.jp

PRESS RELEASE（2015/4/24）

先進暗号数理デザイン室の開設
～暗号解読にチャレンジ！次世代暗号の開発へ～

概　要

マス･フォア･インダストリ研究所（以下 IMI）は、平成 27 年 4 月 1 日に新しい研究部門として、**先進暗号数理デザイン室**を開設しました。近年、暗号は盗聴を防ぐ目的だけでなく、サイバーセキュリティや仮想通貨に応用されるなど、現代社会には不可欠な技術となっています。本室では、世界最強の攻撃者を想定した解読技術により暗号の安全性を評価し、社会が求める多様な機能を持つ次世代暗号を開発することを目指します。暗号数理の研究推進により、IMI を産業数学の世界的な研究拠点に発展させる計画です。

■背　景

近年の暗号は、盗聴を防ぐ目的の利用だけでなく、サイバーセキュリティや仮想通貨に応用されるなど、ICT 社会には不可欠な技術となっています。暗号の用途の拡大とともに、暗号方式の構築とその安全性評価には、整数論（※1）のみならず従来にない数学理論が必要となっています。2013 年度ごろより世界は**ポスト量子暗号**（※2）―量子計算でも破れない暗号― の時代に突入し、新暗号方式の開発に利用される数学理論も格段に高度化かつ多様化し、数学側からの研究が求められています。

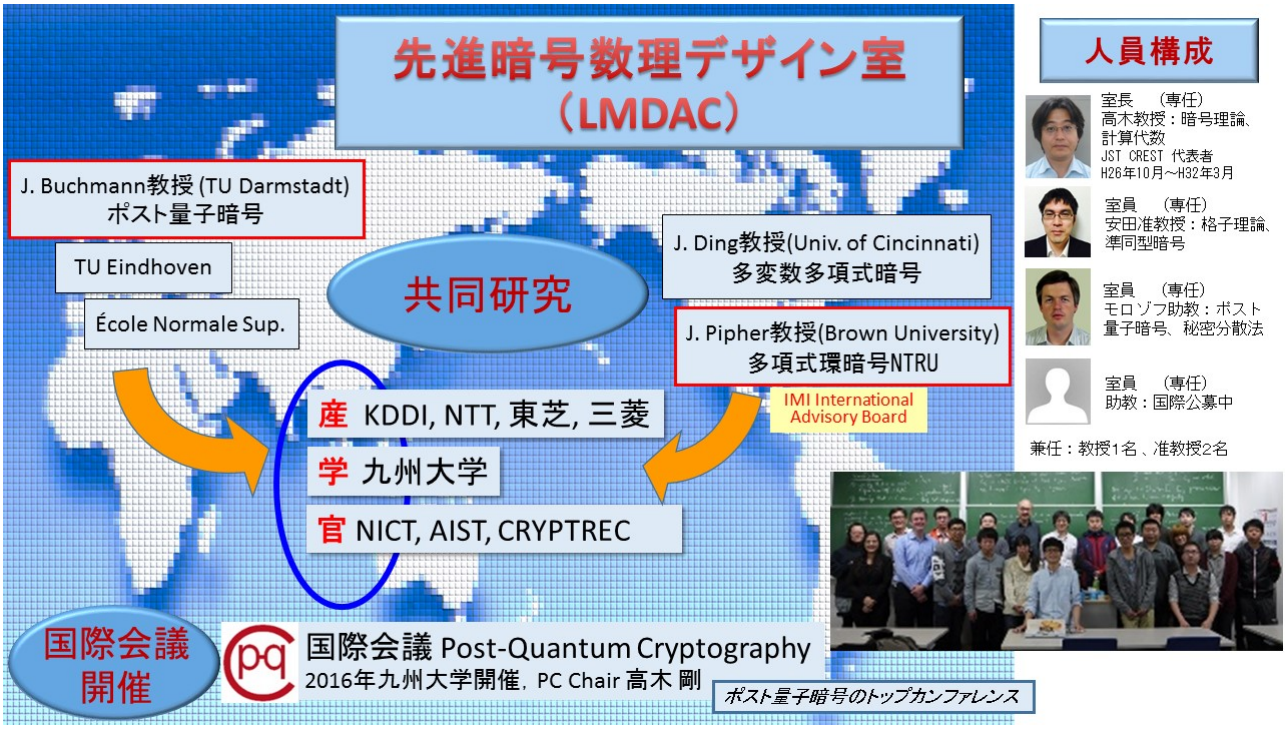
マス･フォア･インダストリ研究所（以下 IMI）では暗号理論に関して企業や政府機関と毎年数件の共同研究を推進してきました。室長の高木剛教授は、ペアリング暗号（※3）の解読世界記録達成などで活躍し、平成 26 年度日本学術振興会賞を受賞しました。また、数学・数理科学分野の JST CREST 研究領域「現代の数理科学と連携するモデリング手法の構築」に、高木教授を代表者として「次世代暗号に向けたセキュリティ危殆化回避数理モデリング」が採択され（H26.10～H32.3）、わが国の暗号研究の牽引役として大きな期待がかけられています。

■内　容

（1）平成 27 年 4 月 1 日に、平成 27 年度九州大学改革活性化制度により、IMI の新しい研究部門として、数学理論による次世代暗号の研究開発を目的とした**先進暗号数理デザイン室**を開設しました。平成 27 年度に新たに准教授 1 名と助教 1 名を雇用し、合計 4 名の専任教員（教授 1 名、准教授 1 名、助教 2 名）と 3 名の兼任教員を配置します。先進暗号数理デザイン室の主たる業務は以下となっています。

・暗号分野の研究の推進、特に暗号に利用可能な基礎数理の構築
・次世代暗号の安全性評価と国際標準化への貢献（堅牢で安全性の高い次世代暗号の提供）
・暗号分野における国内外の企業・官公庁等との共同研究の推進
・関連分野でのワークショップ等の開催、関連学会活動への参画
・暗号分野において国際的に活躍できる博士人材育成のコア支援（学生の教育、研究指導）
・共同利用・共同研究拠点の展開への積極的協力

（2） IMI 先進暗号数理デザイン室の開設記念行事として、平成 27 年 6 月 11 日（木）に、開設式・記念ワークショップを本学で開催します。産業界や大学から来賓をお迎えした開設式とともに、日本の暗号･情報セキュリティのキーパーソンによる最先端の研究に関するワークショップを行います。さらに、



先進暗号数理デザイン室の教員が指導する大学院数理学府の大学院生・ポスドクによるポスターセッションを実施して、ワークショップの参加者と交流を深めます。

■効　果

先進暗号数理デザイン室准教授・助教、各 1 名の新規雇用により、IMI の暗号分野における研究・教育活動がさらに強化される形で持続・発展していくための基盤が整備されます。そして、数学サイドから暗号分野へ大きく貢献できる世界的な研究教育拠点としての IMI が確立されることを目標とします。特に、国内外の企業や官公庁との数学をベースとする暗号分野における共同研究が飛躍的に伸び、セキュリティ脆弱化を阻止することで社会へ大きく貢献し、また九州大学の産学連携活動の推進役ともなることが期待されます。

■今後の展開

IMI 先進暗号数理デザイン室では、暗号設計における安全性評価指針を提案し、安全な次世代暗号の構築を目指します。更に、産学官の連携により暗号数理の研究を推進させ、次世代暗号方式の国際標準に関与し、IMI を産業数学の世界的な拠点に発展させる計画をしています。

【用語解説】

（※1）整数論：
整数や素数の性質を研究する数学の基礎分野。整数論において素因数分解問題が困難であることを利用した暗号技術は既に広く普及しています。

（※2）ポスト量子暗号：
量子計算機により素因数分解が簡単に計算できることが知られています。ポスト量子暗号とは、大規模な量子計算機が実現したとしても安全となる暗号のことです。

（※3）ペアリング暗号：
次世代暗号として産業界で活発に研究されており、標準化規格の設定がされ実用化が進んでいる暗号技術。

【お問い合わせ】
マス・フォア・インダストリ研究所 教授 高木 剛
電話：092-802-4401
FAX：092-802-4405
Mail：takagi@imi.kyushu-u.ac.jp

先進暗号数理デザイン室開設式・記念ワークショップ

日時：平成 27 年 6 月 11 日(木曜日)

場所：九州大学 共進化社会システムイノベーション施設

午前：開設式 10:30～12:20

司会：佐伯 修 (IMI 副所長)

開会挨拶　若山 正人 (九州大学 理事･副学長)

所長挨拶　福本 康秀 (IMI 所長)

来賓挨拶　Yvo Desmedt (University of Texas at Dallas, Distinguished Professor;
University College London, Courtesy Professor)

室長挨拶　高木 剛 (IMI 先進暗号数理デザイン室 室長)

基調講演　辻井 重男 (中央大学研究開発機構 教授)

招待講演　岡本 龍明 (NTT セキュアプラットフォーム研究所 岡本特別研究室 室長)

午後：記念ワークショップ 13:40～18:00

モデレーター：高木 剛 (IMI 先進暗号数理デザイン室 室長)

講演者リスト

秋山 浩一郎 (東芝 研究開発センター コンピュータアーキテクチャ・セキュリティラボラトリー 研究主幹)

清本 晋作 (KDDI 研究所 情報セキュリティグループ グループリーダー)

小暮 淳 (富士通研究所 ライフイノベーション研究所 イノベーションディレクター)

櫻井 幸一 (九州大学大学院システム情報科学研究院 教授、九州先端科学技術研究所 情報セキュリティ研究室 室長)

佐古 和恵 (NEC クラウドシステム研究所 技術主幹)

佐藤 尚宜 (日立製作所　研究開発グループ　システムイノベーションセンタ 主任研究員)

高島 克幸 (三菱電機 情報技術総合研究所 松井暗号プロジェクト G 主席技師長)

盛合 志帆 (情報通信研究機構ネットワークセキュリティ研究所 セキュリティ基盤研究室 室長)

17:00-18:00 学生･ポスドクによるポスター発表

18:00- 懇親会