AIMaP Special Session of Mathematics and Information Security

This is a new session aiming to share recent trends of relationship between mathematics and information security. In this session, we invite two distinguished researchers on information security based on mathematics. At this session, we would like to discuss the future progress of both communities for developing information systems based on mathematics.

This session is organized by the AIMaP*1 project, supported by MEXT*2. The aim of the project is extending research areas and activities related to mathematics by cooperating IMI*3 and 12 mathematics research institutions in Japan.

AIMaP
Advanced Innovation

*1 Advanced Innovation powered by Mathematics Platform. https://aimap.imi.kyushu-u.ac.jp/
*2 Ministry of Education, Culture, Sports, Science and Technology, Japan.
*3 Institute of Mathematics for Industry, Kyushu University, Japan.

Dr. Kazue Sako
Distinguished Researcher, Security Research Laboratories,
Central Research Laboratories, NEC Corporation
https://www.nec.com/en/global/rd/people/kazue_sako.html

Mathematics and Cryptography for Society

Abstract

In the age of digital transformation, not only industry but also society as a whole will be largely impacted from information and communication technology (ICT). Yet these technologies can be misused to harm individuals and society, by being insecure or unfair. In the physical world, we had been using physical objects and its limitation to disable malicious activities to achieve more security and fairness. However, in the digital world, these limitations are useless and thus the system is apt to be misused. Cryptography provides a tool to create such limitations in the digital world, as it studies mechanisms to control information flow or restrict procedures in digitalized systems. Therefore it is important to design secure and fair systems for society using cryptography. Mathematics is necessary to to make sure that cryptographic protocols and primitives achieve the designed criteria.

In this presentation, we will discuss the design of blockchain technology used in Bitcoin as an example of societal system that decentralizes power to achieve fairness, together with some of the activities within Japan to bridge mathematics and cryptography.

Prof. Carlos Cid
Professor in Information Security,
Royal Holloway University of London, UK,
and Simula UiB, Norway
http://www.isg.rhul.ac.uk/~ccid

Domain Specific Ciphers

Abstract

In this talk we discuss symmetric-key algorithms specifically designed for use in particular domains or novel applications. While block ciphers are perhaps the best understood and widely used class of cryptographic algorithms, most conventional algorithms have been designed to encrypt bit-string messages for transmission and storage. Furthermore, they aimed for efficient implementation on standard CPUs and in hardware. Recent advances in cryptography have on the other hand increased the number and range of applications in which symmetric-key ciphers can be used, or required: for example, a block cipher may be needed to encrypt messages respecting a specific format; they may be used as building block of applications which would benefit from low multiplicative circuit depth; or have features that facilitate secure obfuscation. Despite its attractive features, AES and most conventional block ciphers may not be particularly suitable for these applications or platforms.

We provide an overview of the main recent developments in this area, focusing mainly on the design and analysis of algebraic ciphers proposed for supporting advanced applications, such as Zero-Knowledge proofs. These ciphers aim to minimize the number of multiplications on a large field, in order to improve performance of ZKPs. However their simple algebraic structure may make them particularly vulnerable to algebraic attacks.

AIMaP Advanced Innovation

Please give us your feedback.

2019K003

「AIMaP 特別セッション（IWSEC2019）」(2019/8/28-8/30)

文部科学省科学技術試験研究委託事業 AIMaP アンケート

このワークショップは文部科学省科学技術試験研究委託事業「数学アドバンストイノベーションプラットフォーム(AIMaP)」の支援を受けて開催されています。今後の参考にさせていただくため、アンケートにご協力ください。

●あなたのご所属
- □大学等研究者（数学・数理科学分野）
- □大学等研究者（数学・数理科学以外の分野）
  （分野名：　　）
- □産業界の研究者・技術者
  （業界：　　）
- □ポスドク（数学・数理科学分野）
- □ポスドク（数学・数理科学以外の分野）
  （分野名：　　）
- □学生（数学・数理科学分野）
- □学生（数学・数理科学以外の分野）
  （分野名：　　）
- □その他（具体的に：　　）

●このワークショップを知ったきっかけ
- □AIMaP のチラシ
- □AIMaP のホームページ
- □ワークショップのホームページ
- □ワークショップのポスター・チラシ
- □学会等のホームページ
- □学会等のメーリングリスト
- □twitter, facebook などの SNS
- □関係者からの連絡（含：講演依頼）
- □その他（具体的に：　　）

●ワークショップにおけるあなたの役割
- □主催者
- □講演者・討論者
- □参加者
- □その他（具体的に：　　）

●このワークショップには何を期待して参加されましたか。
- □今後の自分の研究に役立つかもしれない、新たな発想や視点を得たい。
- □新たな人脈を得たい。
- □共同研究につながるきっかけを得たい。
- □分野を異にする人との連携・協力。
- □その他（具体的に：　　）

●実際のワークショップはいかがでしたか。
- □期待以上
- □期待通り
- □期待以下

その理由：

●【数学・数理科学以外の分野あるいは産業界からご参加の方にお伺いします。】AIMaP 事業では、数学・数理科学の特定のテーマに関するチュートリアルを計画しています。数学・数理科学の特定の分野や手法の中でより詳しく知りたいものがあれば、以下に挙げてください。

※差し支えなければ、お名前、ご所属、ご連絡先をお書きください（AIMaP 事業の他、文部科学省が今後実施する事業に関してご連絡を差し上げます。以前のワークショップ等で既に登録されている方はご記入不要です。）

お名前：

ご所属：

ご連絡先（メールアドレス）：

2019K003

AIMaP Program Questionnaire

This workshop is being held with a support by AIMaP (Advanced Innovation powered by Mathematics Platform) Program of the Ministry of Education, Culture, Sports, Science and Technology. Please help us serve you better by taking a couple of minutes to tell us about the workshop.

● You are:
- ☐ Researcher in academia (in mathematics)
- ☐ Researcher in academia (in other discipline) (Discipline:)
- ☐ Researcher or Engineer in industry (Category:)
- ☐ Post-doctoral fellow (in mathematics)
- ☐ Post-doctoral fellow (in other discipline) (Discipline:)
- ☐ Student (in mathematics)
- ☐ Student (in other discipline) (Discipline:)
- ☐ Other (Describe:)

● How did you know the workshop?
- ☐ Flyer of AIMaP
- ☐ Website of AIMaP
- ☐ Website of the workshop
- ☐ Poster or flyer of the workshop
- ☐ Website of an academic society
- ☐ Mailing lists
- ☐ SNS such as twitter, facebook
- ☐ Direct contacts by organizers of the workshop
- ☐ Other (Describe:)

● Your role in the workshop:
- ☐ Organizer
- ☐ Speaker or panelist
- ☐ Participant
- ☐ Other

(Describe:)

● What was your expectation for the workshop (before attendance)?
- ☐ New ideas or insights that may be helpful to your own research
- ☐ Making personal acquaintance
- ☐ Chance leading to a cooperative research
- ☐ Cooperation with others in a different discipline
- ☐ Other (Describe:)

● How was the workshop (after attendance)?
- ☐ more than expected
- ☐ as expected
- ☐ less than expected

Please specify the reason:

●【For those who are in academia in a discipline other than mathematics or those working in industry】We are planning to organize some tutorial sessions on specific topics of mathematics. Please specify mathematical topics you are now most interested in?

If you wish to receive latest information on AIMaP Program, please fill in the following form (unless already registered).

Name:
Institution:
Email address

AIMaP 事務局 aimap@imi.kyushu-u.ac.jp HP: http://aimap.imi.kyushu-u.ac.jp

AIMaP Advanced Innovation

Advanced Innovation powered by Mathematics Platform

http://aimap.imi.kyushu-u.ac.jp/

A project in
MEXT: Ministry of Education, Culture, Sports, Science and Technology, JAPAN.

文部科学省 文部科学省委託事業

AIMaP
Advanced Innovation

数学アドバンストイノベーションプラットフォーム

九州大学 KYUSHU UNIVERSITY

Secretary Organization
Institute of Mathematics for Industry
Kyushu University

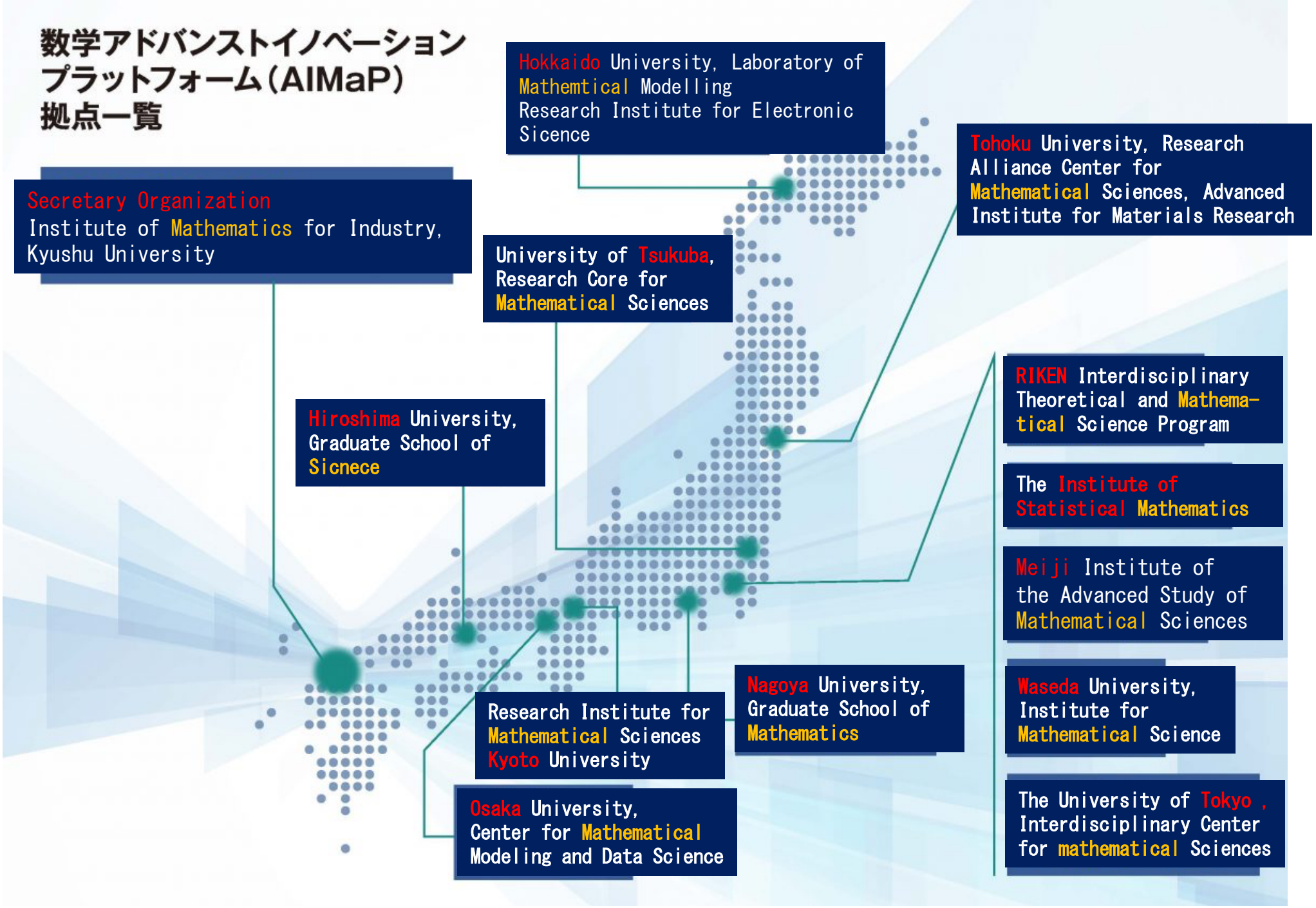
後援 日本数学会、JSIAM 日本応用数理学会、統計関連学会連合

Supporting Associations:
- The Mathematical Society of Japan
- The Japan Society for Industrial and Applied Mathematics
- Japanese Federation of Statistical Science Associations

AIMaP
Advanced Innovation

AIMaP Organizations (2019/04/01)

数学アドバンストイノベーション プラットフォーム(AIMaP) 拠点一覧



Mathematics session in other societies

30 sessions in 2017, 34 sessions in 2018 and 26+α sessions in 2019

cf. https://aimap.imi.kyushu-u.ac.jp/wp/2019list

○【Tohoku】 2017/9/10 Japan Radiological Society @ Matsuyama

Functional Analysis of blood flow and geometric characteristic, etc.

○【Osaka】 2017/12/6 Consortium of Biological Sciences @ Kobe
Mathematical analysis of cell membrane molecule interaction, etc.

○【Kyushu】2018/3/17 The Japan Society for Precision Engineering

Geometric approach to precision engineering

○【RIKEN】 2018/3/22-25 The Physical Society of Japan

Persistent homology and its application to randomness in physics

○【Kyushu】 2019/8/28-30 International Workshop on Security @ TIT

Special Session of Mathematics and Information Security (M&IS)

IWSEC2019 in Tokyo

AIMaP Advanced Innovation

Mathematics and Mathematical Science researches collaborating with industry and other sciences (1/4)

Describe a mechanism of complex phenomenon using Mathematics

複雑な現象のメカニズムを数学で記述

製鉄高炉内の変化予測による効率化

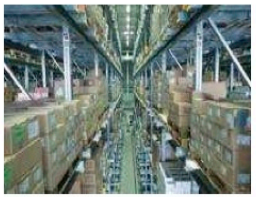
現象のメカニズムの数理モデル化により結果から原因を推定する「**逆問題**」という数学的手法を利用して、**製鉄高炉における温度変化を数理モデル化**した。

これにより、高炉の炉底煉瓦に埋設された2つの温度計の温度差データから、**高炉内の温度変化を高精度に推測**できるようになり、**異常状態の予兆の検出、高炉の制御の効率化**による生産量upとコスト削減、CO2排出量の削減、高炉の寿命延長にも貢献している。

※中川淳一(新日鐵住金(株))より提供

渋滞メカニズムの解明と解消

数学モデルにより、渋滞発生メカニズムを解明し、渋滞の要因(車間距離、速度等)を適切にコントロールすることによる渋滞解消法を提唱して、**高速道路での実証実験によりその有用性を証明**。羽田空港貨物ターミナル設計、工場の製造行程設計、物流倉庫内における商品の最適配置、商店街や店舗デザイン、カーナビシステムにも幅広く応用。

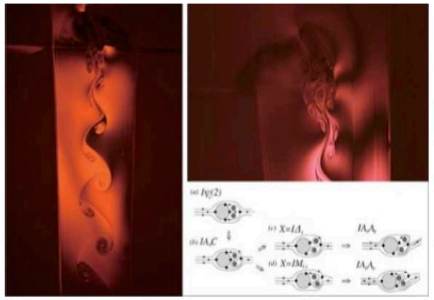


左)中央道での実証実験の様子

右)物流倉庫の商品の最適配置

※西成活裕(東京大学先端科学技術研究センター教授)より提供

流れの文字化と渦閉じ込め機構の解明

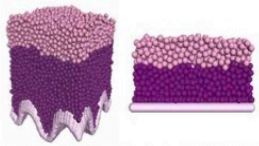


上から下に流れ落ちる石鹸膜に細い板を差し込むと**美しい規則的な渦の列(左の写真)ができる**現象について、**トポロジー(位相幾何学)**を使って背後にある**複数の数学的メカニズムを抽出**(右下の模式図と式)。

本手法と数理流体力学により、渦の物体まわりへの「閉じ込め」理論を展開、渦の有効をする全く新しい流体機器、例えば**高い飛行性能を持つ新しい渦翼デザイン**の開発が期待される. 現在では、本成果をベースにした「位相流線解析」による**企業コンサルタント**も始まっている。

※坂上貴之(京都大学大学院理学研究科教授)より提供

皮膚構造の数理モデル化と疾患解明



真皮に凹凸が生まれると表皮が厚くなり、バリア機能が強化される。(抗老化対策へのヒント)

表皮構造の数理モデル化により, 傷ついた皮膚が回復する有様をシミュレートし、**皮膚のバリア機能を評価**できるようになった。

バリア機能強化の視点から老化を抑えるための**化粧品**開発の可能性や皮膚疾患の発症要因の解明にも役立つ可能性がある。

簡単な病態の再現(魚の目の形成)

※長山雅晴(北海道大学電子科学研究所附属社会創造数学研究センター教授)より提供

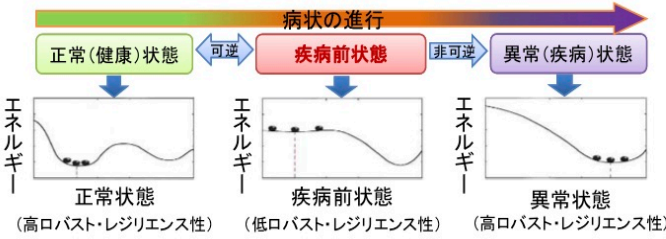
2016年7月15日 文部科学省・戦略的基礎研究部会資料「数学イノベーション推進に必要な方策について」より

Mathematical formulations of fluctuation estimations and predictions

数学による将来の変動の予測、予兆の解明

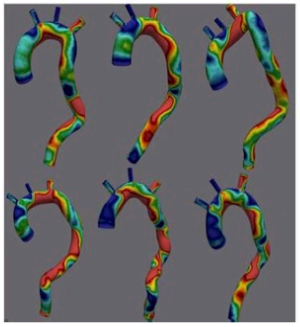
疾病状態に至る前の予兆を検出

健康状態から疾病状態に分岐する直前の**疾病前状態（遷移状態）**において**生体分子ネットワークの不安定化プロセスを数学的に解析**し、**動的ネットワークバイオマーカー**として検出。超早期診断・治療が期待できる。



※合原一幸（東京大学大学院生産技術研究所教授）より提供

大動脈瘤治療後の変化の予測



胸部大動脈における血流解析

大動脈における血流の解析を通して、血管壁にかかる内圧や摩擦力の分布と個人差の大きい形状の特徴の関係を数理モデル化することにより、**患者ごとの大動脈瘤の治療後の変化**を予測。

大動脈の形状の**幾何学的特徴に着目**することで、各々の患者への適切な治療が期待できる。

※水藤寛（岡山大学大学院環境生命科学研究科教授）より提供

熟練者の経験による判断の定式化、数学による記述

シャフトの歪み解消機の劇的な改善

品質管理指標の大幅な改善

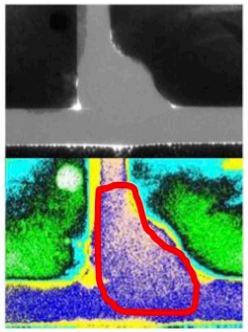
※30%以上は品質保証上改善が必要

自動車のエンジンの動力を車輪に伝える**「シャフト」の歪みを解消する機械の制御ソフトウェアの設定**は、これまで**現場の経験と勘に頼っていた**が、シャフト形状のモデル化と数学的アプローチに基づき、**自動化・高精度化を実現**。

品質管理指標が従来の20-28%から8-15%となり大幅に改善された。

※山本昌宏（東京大学大学院数理科学研究科教授）より提供

X線透過画像からの溶接部位の抽出



X線透過画像（上図）では溶接部と基材部の差はほとんどなく、**熟練工が肉眼判定**していた。

この画像に前処理をした上で、対象領域の輝度分布をいくつかの正規分布に分ける手法（混合ガウス分布）を適用し、**溶接部と基在部の輝度の差を表すことができ、溶接部（下図の赤線内）を抽出**。今後、医療画像への応用も期待できる。

※鈴木貴（大阪大学大学院基礎工学研究科教授）より提供

Mathematical formulations of decision processes of skilled technicians

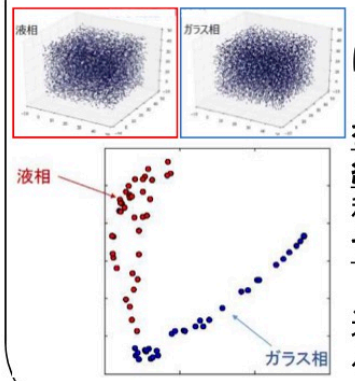
AIMaP Advanced Innovation

Mathematics and Mathematical Science researches collaborating with industry and other sciences (3/4)

Extraction and reconstruction of data in another Mathematical space

データからは直接見えないものを抽出・可視化

データ科学的視点からガラスの構造を抽出

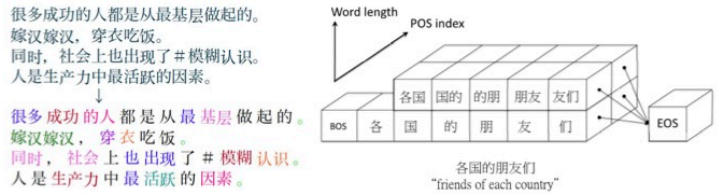


シリカの液層とガラス相の構造は見た感じでは区別できないが（上図）、**位相幾何学(トポロジー)を活用したデータ解析と確率論・統計学**を融合することで、データ科学的視点から**構造変化を抽出することに成功**した（下図）。

本手法はタンパク質の立体構造の分類問題などにも応用できる。

※平岡裕章（東北大学原子分子材料科学高等研究機構教授）より提供

言語の文字列から単語と品詞を自動判別

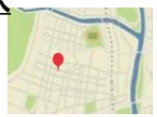


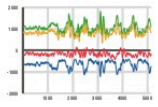
デンソーITラボラトリ(東京)との共同研究により、様々な言語で書かれているどんな文章でも、その**大量の文字列データのみから単語を抽出し、その品詞を同時に推定する手法**を開発。自然言語処理の基礎的な技術であり、例えば会話する次世代カーナビなどへの応用が考えられる。

※持橋大地（統計数理研究所准教授）より提供

スマホの加速度データで道路の凸凹を検知

位置（GPS）　　揺れ（加速度）



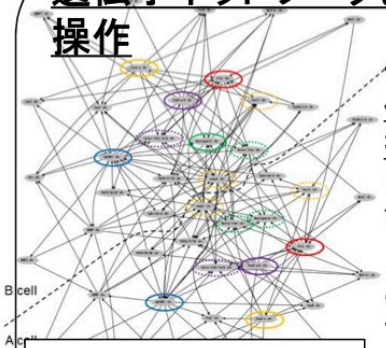


道路パトロール車にスマホを搭載し、**車両加速度の時系列データ**を取得する。このデータをパターン認識し、,GPSの位置情報と合わせて、**道路の凸凹（劣化状況）を診断する**（ウェーブレットシュリンケージ、SVM、変化点解析、周波数解析を活用）。

※西井龍映（九州大学マス・フォア・インダストリ研究所教授）より提供

複雑な構造を適切に単純化

遺伝子ネットワークを少数遺伝子で捉えて操作



ホヤの遺伝子ネットワーク（実線で囲まれたものが操作すべき遺伝子）

※望月敦史（理化学研究所 主任研究員）より提供

複雑な遺伝子ネットワーク全体のダイナミクスが、**一部の遺伝子の振る舞いで捉えられ、操作できる**こと、重要な遺伝子はネットワークの形だけから決まることを**数理的に証明**。

100近くの遺伝子を含むホヤの細胞分化ネットワークにおいて、5つの遺伝子の活性を人工的に操作するだけで、ホヤの**すべての細胞分化状態を再現できると予測。**

Reconstruction of a network structure in another Mathematical space

AIMaP Advanced Innovation

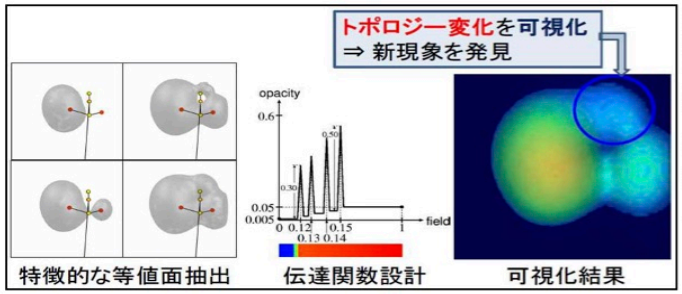
Mathematics and Mathematical Science researches collaborating with industry and other sciences (4/4)

Visualization of topological changes

データからは見えないものを抽出・可視化

陽子と水素原子の衝突現象の可視化

陽子と水素原子の衝突の際のエネルギー分布関数の数値シミュレーション結果について、**トポロジーが変化する等値面を強調する**ように伝達関数を設計することで、その部分が強調されて**可視化**される。

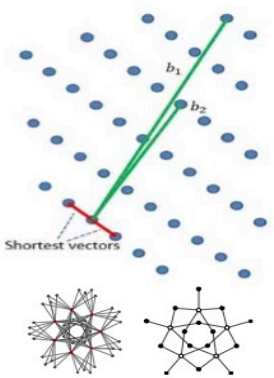


※佐伯修（九州大学マス・フォア・インダストリ研究所教授）より提供

Information Security

次世代の情報セキュリティの確保

ポスト量子暗号−次世代高機能暗号−



サイバーセキュリティを支える暗号は、計算機性能向上や量子計算機の進歩など、**恒常的に新たな攻撃の脅威**に晒されている。

想定される最強の攻撃者をモデル化して、**最先端の数学理論（格子理論、表現論など）**を用いることにより、予想困難な未来の**セキュリティ危殆化を回避するための数理モデリング**が必要となる。

※高木 剛（九州大学マス・フォア・インダストリ研究所教授）より提供

Computer Graphics

数学を直接活用した豊かな表現

CGによるリアルな表現

引用：Zaragoza大学、Diego Gutierrez教授

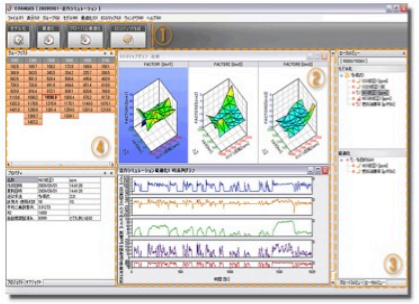
レンダリング方程式と呼ばれる積分方程式をリアルタイムで解く手法で生成された架空の顔。 **多層構造を持つ皮膚を、リアルかつ効率的に表現**するために、モンテカルロ法を応用した数理モデルを利用している。

※安生健一（(株)オー・エル・エム・デジタル）より提供

Convex Optimization

数学を活用した実験の効率化

エンジンの適合試験の効率化



提供：株式会社小野測器

凸最適化とよばれる幾何学的な手法を用いて、10以上あるパラメータを制御することが求められる**自動車エンジンの適合試験等を効率化**。国産ソフトウェアに実装されている。

※伊藤聡（統計数理研究所教授）より提供

AIMaP Advanced Innovation

Exchange meetings for companies and students studying mathematics
The University of Tokyo, Komaba Campus, 2019/10/26(Sat)

日本数学会が設けた産官学の有識者からなる社会連携協議会が中心となり、2014年以降毎年開催。
2018年11月に第5回の交流会を開催。産官学から226名が参加。

- ポスター発表を行った数学専攻学生（主に博士課程学生）：60件
- 企業等34社からの参加者:91名
- その他（大学教員、大学生・大学院生、企業、高校教員等）

数学・数理科学専攻若手研究者のための 異分野・異業種研究交流会２０１９

日時：2019年10月26日（土）10：00 － 19：30　場所：東京大学駒場1 キャンパス

プログラム【第一部】

10：00 ～10：15 開会挨拶 寺杣友秀（日本数学会理事長）

10：10 ～10：45

基調講演 「デジタルトランスフォーメーションに向けたMUFGの取り組み ～数学を通じた社会貢献に向けて～」
亀澤宏規氏（三菱UFJフィナンシャル・グループ代表執行役副社長 ）

【第二部】

10：45 ～12：15 協力企業・研究所紹介

13：15 ～15：00 若手研究者によるポスター発表

15：10 ～15：40 リクルートセミナー（学生のみ対象）青沼君明氏 （明治大学教授）

15：45 ～17：45 個別交流会 （若手研究者が企業ブースを訪問）

【第三部】

18：00 ～19：30 表彰式・情報交換会（優れた発表には「ベストポスター発表」を授与し表彰する）

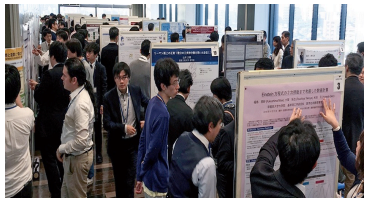
協力企業・研究所：40社

アイシン・エィ・ダブリュ,アイシン精機,IBM東京基礎研究所,アクサ生命保険,アクセンチュア,Arithmer,C-ENGINE,AGC,NEC中央研究所,NTT研究所,アルトナー,光電製作所,シナモン,東芝研究開発センター,とめ研究所,ニコン,富士通研究所,三井住友銀行,グローバルヘルスコンサルティング・ジャパン,厚生労働省,構造計画研究所,コマツ,ジブラルタ,生命保険,スローガン,総務省統計局,大同生命保険,中部電力技術開発本部エネルギー応用研究所,TDSE,トヨタ自動車,日本製鉄先端技術研究所,日本ユニシス,富士通,方正,MathWorks Japan,マツダ技術研究所,三菱電機,三菱UFJ銀行,三菱UFJモルガン・スタンレー証券,ヤフー,有限責任監査法人トーマツ

参加大学等：

茨城大学,大阪大学,お茶の水女子大学,金沢大学,関西学院大学,関西大学,九州大学,京都大学,慶應義塾大学,神戸大学,埼玉大学,首都大学東京,上智大学,情報・システム研究機構統計数理研究所,中央大学,筑波大学,東京工業大学,東京大学,東京理科大学,東北大学,名古屋大学,日本大学,広島大学,北海道大学,明治大学,理化学研究所,立命館大学,早稲田大学

Keynote Talk (2018)



Poster Session (2018)

Best Poster Award (2018)