情報科学研究科 重点プロジェクト

数学と諸分野の協働推進による
学際的・総合的な新領域研究の開拓

MATHEMATICS × EXTENSIVE SCIENCE

第14回講演会 兼 第61回応用数学連携フォーラム

日時 2017年6月1日（木）16時30分～17時30分

会場 東北大学 情報科学研究科棟 大講義室

講演者 水木敬明氏（東北大学 サイバーサイエンスセンター）

タイトル 秘密計算を実現するカードベース暗号

概要

仲良しグループが今度の土曜日にカラオケに行くかどうかを決めたい場面を考える。気まずくなるのを避けるため、各人の行きたいかどうかの気持ち（YES/NO）は秘密にしたまま、全員がYESであるか、それとも一人でもNOの人がいるのか、そのどちらであるかだけを知りたい。すなわち、全員の秘密のビット値の論理積（AND演算）の結果だけを知りたい。もしこのような「秘密計算」が可能であれば、前者の場合はもちろんカラオケに行くことにし、後者の場合は今回はやめておくことができる（後者のときも、誰がNOと思っているかわからないので、気まずくならない）。

本講演では、トランプのような物理的なカード組を使う「カードベース暗号」を用いると、上述のような秘密計算が簡単に実現できることを紹介する。特に、講演者らが考案した「ランダム二等分割カット」というシャッフルの登場により、論理積や排他的論理和（XOR）の秘密計算が少ないカード枚数や手順で実行できるようになり、カードベース暗号が急激に効率化され、人間が実際に実行できるレベルになっていることなどを含め、カードベース暗号の歴史と最近の動向を概観する。

http://www.math.is.tohoku.ac.jp/~project/