Campus Mail

For all the students

FIT Fukuoka Institute of Technology 福岡工業大学
この件のお問い合わせは広報課へ
TEL ：092-606-0607
MAIL：kouhou@fit.ac.jp

掲示期間 2025-073
7 月 22 日～8 月 8 日

情報工学部　情報通信工学科　工藤　桃成　准教授

日本応用数理学会 2024 年度年会において「若手優秀講演賞」 受賞

情報工学部　情報通信工学科　工藤桃成准教授が、日本応用数理学会　2024 年度年会（2024 年 9 月開催）において、「若手優秀講演賞」 を受賞しました。受賞した研究発表のタイトルは「Gröbner 基底の計算量理論の定式化－暗号の安全性解析に向けて－」です。
工藤准教授は計算代数幾何学（特に正標数の代数幾何学におけるアルゴリズムに関する研究）を主な専門としており、今回はグレブナー基底の計算量とその暗号解析への応用について検討したものが評価されました。

情報工学部　情報通信工学科　　工藤　桃成　准教授

※熊本出身の工藤准教授は、くまモンの熱心なサポーターです！

タイトル：Gröbner 基底の計算量理論の定式化－暗号の安全性解析に向けて－

1960 年代に Bruno Buchberger と廣中平祐によって独立に導入された Gröbner（グレブナー）基底は、代数幾何学・可換代数といった数学分野における重要な研究対象の一つです。Gröbner 基底は、連立代数方程式の求解をはじめ、暗号解読や誤り訂正符号にも利用されるなど、数学以外の分野への応用も多く知られています。一方で、Gröbner 基底の計算量（＝アルゴリズムの実行時間を表す関数）を精密に評価することは一般には非常に難しい問題であり、特に Gröbner 基底計算によって解読が可能となる暗号プロトコルの安全性を評価する上で、極めて重要な課題となっています。

本講演ではまず、Gröbner 基底の計算量を測る指標である「求解次数（solving degree）」について、先行研究で混同されてきた複数の定義を整理し、数学的に厳密な形で再定義しました。次に、暗号の安全性解析でよく仮定される「半正則性」という性質に着目し、Hilbert 級数の理論を用いることで、半正則に"近い"構造をもつ多項式列を「一般化された半正則列」として定式化しました。さらに、一般化された半正則列に対する求解次数の上界評価と、Gröbner 基底の計算量の漸近評価式を証明しました。これにより、Gröbner 基底計算を用いた暗号解読の有効性検証のための、新たな理論的枠組みを提供することができました。