中村　周平（Shuhei Nakamura）

所属（Domain）　情報科学領域（Domain of Computer and Information Sciences）

●研究テーマ（Research theme）

①連立代数方程式問題の解法に関する研究

（英文）Research on solving algorithms for systems of algebraic equations

②代数的攻撃からの暗号の安全性解析

（英文）Algebraic cryptanalysis for cryptography

③次世代暗号に向けた数理技法の開発

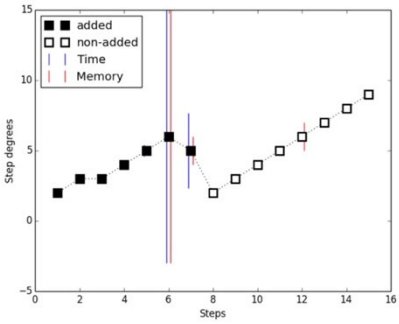
（英文）Development of mathematical techniques for next-generation cryptography

---

① 連立代数方程式問題は、多くの分野で応用される問題であり、その解法の改良と実装は重要な課題となっています。当研究室では、情報通信分野における応用を考慮し、有限体上での連立代数方程式問題の解法について研究しています。

$$\begin{cases} 2x^2+3y^2-5z^2-6w^2 &= 10 \\ x^2-4y^2+7z^2+2w^2 &= -3 \\ 3x^2+2y^2+8z^2-w^2 &= 1 \\ 4x^2-6y^2-2z^2+9w^2 &= 12 \end{cases}$$

Systems of algebraic equations are widely used problems in various fields, and improving their solution methods and implementing them is an important task. In our research lab, we are investigating systems of algebraic equations over finite fields.

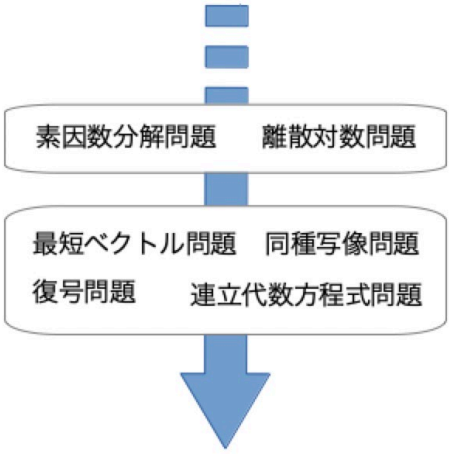


② 公開鍵暗号は、数学問題の困難性に基づいて通信の安全性を確保することを目的としています。当研究室では、暗号で利用される問題を連立代数方程式問題に帰着させる様々な攻撃手法の効率性を調べるため、それらの計算量評価を行っています。

Public-key cryptography aims to ensure the security of communication based on the difficulty of mathematical problems. In our research lab, we are estimating the complexity of various attacks that reduce the problems appeared in cryptography to systems of algebraic equations.

③ 現在、大規模な量子計算機による攻撃への対策として、最短ベクトル問題、復号問題、同種写像問題、連立代数方程式問題などの新しい数学問題を基にした公開鍵暗号が検討されています。当研究室では、高度化する情報社会の基盤技術となりうる様々な数学的対象に取り組み、次世代の暗号に向けた数理技法の開発に取り組んでいます。

Currently, public-key cryptography based on new mathematical problems such as the shortest vector problem, the decoding problem, the isogeny problem, and MQ-problem is being considered to counter an attack using quantum computers. In our research lab, we are tackling various mathematical objects as the foundation technology for an advanced information society and developing mathematical techniques for next-generation cryptography.



キーワード（Keyword）	代数的アルゴリズム(Algebraic Algorithm)
専門分野（Specialized Field）	情報学基礎論(Information theory)
共同研究可能技術（Possible Technology of Cooperative research）	暗号理論(Cryptography)
関連論文・特許情報 website（Related articles･patent information）	https://info.ibaraki.ac.jp/Profiles/128/0012742/profile.html
研究設備（Research Facility）	
研究室URL（Lab. URL）	
E-mail	shuhei.nakamura.fs71@vc.ibaraki.ac.jp