# 格子暗号安全性評価のためのアルゴリズム高速化

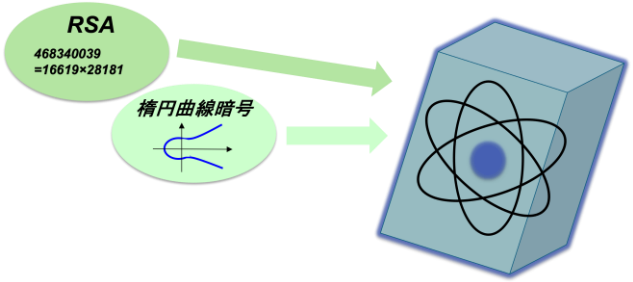
関連キーワード: 格子暗号，最短ベクトル問題，遺伝的アルゴリズム

## 研究内容

インターネットなどで現在広く使用されている公開鍵暗号としてRSAや楕円曲線暗号があります。これらの暗号は量子計算機によって解読されてしまうことが既に分かっているため、将来の量子計算機実現に備えて量子計算機に耐性のある暗号（耐量子計算機暗号）の社会実装は重要な課題です。今、耐量子計算機暗号の社会実装の準備が進められており、その中でも格子暗号は特に注目されている暗号です。暗号を使用する上で安全性評価は欠かせないものですが、格子暗号においてもこのことは当てはまります。

格子暗号の安全性は格子の最短ベクトル問題の難しさを根拠にしており、格子暗号安全性評価では最短ベクトル問題を解くアルゴリズムを使用します。安全性評価において必ずしも最速ではないアルゴリズムを使用すると、誤った安全性の見積もりをしてしまうことになります。そのため、安全性評価に使用するアルゴリズムの高速化を追求することは必要不可欠の課題です。

本研究では、最短ベクトル問題のアルゴリズムを高速化するために、遺伝的アルゴリズムを応用する研究を進めています。遺伝的アルゴリズムを活用する方法は、最短ベクトル問題のアルゴリズムの中では比較的新しいアイディアであり、まだ発展途上の段階ですが、遺伝的アルゴリズムは並列計算にも非常に相性が良いため、並列計算による高速化などにも取り組んでいます。




## 研究者プロフィール

- **工学部情報基盤工学科 准教授　深瀬 道晴**
- 専門分野：情報セキュリティ
- 研究分野：格子暗号
- 所属学会：情報処理学会
- 主な経歴：獨協大学特任助手、
  早稲田大学非常勤講師、秀明大学非常勤講師、東北学院大学講師、
  岩手大学非常勤講師

## 社会貢献に向けて

暗号の社会実装の過程においては、技術仕様や方式を公開し、広く公開された 形で様々な検討や議論がなされることが必要であり、近年では各種の研究においてもプログラムコードやリソースがオープンソースとして提供される事例も多くなっております。プログラムのリソースの公開については、ライセンス整備など難しい側面もありますが、本研究でも今後の公開を積極的に捉えています。

## 研究者への連絡先


- 産学連携推進センター
  Email srcenter@mail.tohoku-gakuin.ac.jp
  電話　022-354-8122


東北学院大学