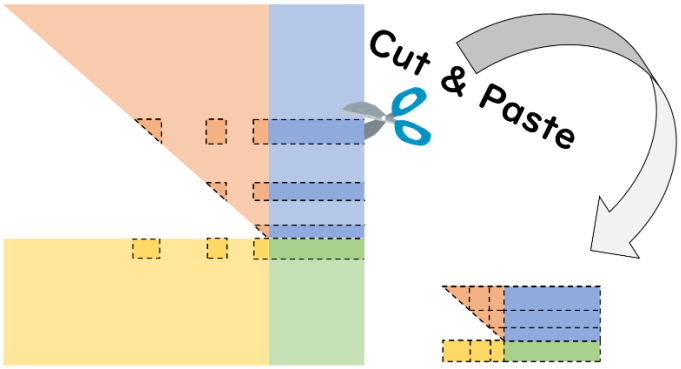
PRESS RELEASE

東京大学

次世代暗号の解読コンテストで世界記録を達成
――量子コンピュータも解読できないポスト量子暗号への挑戦――

発表のポイント

◆これまで解かれたことのない次元の暗号解読に成功しました。これは、量子コンピュータでも解読できない次世代暗号の安全性を評価する解読コンテスト「ＭＱチャレンジ」の世界記録となります。
◆本世界記録においては、解読問題の数理的な特性を利用した新しい高速アルゴリズムを提案し、大規模な並列計算機におけるプログラミング実装により解読記録を実現しています。
◆今後、この新しいアルゴリズムを詳細に評価することで、現在進められている次世代暗号の標準化規格に対して安全なパラメータの提案を進めます。



解読世界記録の達成へのアプローチ方法

概要

東京大学大学院情報理工学系研究科の坂田康亮特任研究員と高木剛教授は、次世代暗号の解読コンテストであるＭＱチャレンジにおいて、これまでに解かれたことがない次元の解読世界記録を達成しました。ＭＱチャレンジは、量子コンピュータでも解読できないポスト量子暗号の安全性を評価するための解読コンテストであり、特に多変数多項式を用いた暗号に関する解読問題が出題されています。今回、解読問題の数理的な特性を解明することで新しい高速アルゴリズムを提案し、世界記録を達成することができました。考案したアルゴリズムでは、計算途中に現れる巨大な行列のうち、出力結果に影響する最低限の領域だけを切り出し、解読に必要となる最小の行列を構成するよう工夫しました（図 1）。さらに、提案アルゴリズムを大規模な並列計算機にプログラミング実装することにより、これまでに解かれたことのない次元の暗号解読を可能としました。今後、この新しいアルゴリズムの詳細を評価し、現在進められている次世代暗号の標準化規格における安全なパラメータの提案を進めます。この研究成果は、情報処理学会主催のコンピュータセキュリティシンポジウム「Computer Security Symposium(CSS 2023)」(2023 年 10 月 30 日 - 11 月 2 日 福岡開催)で発表しました。

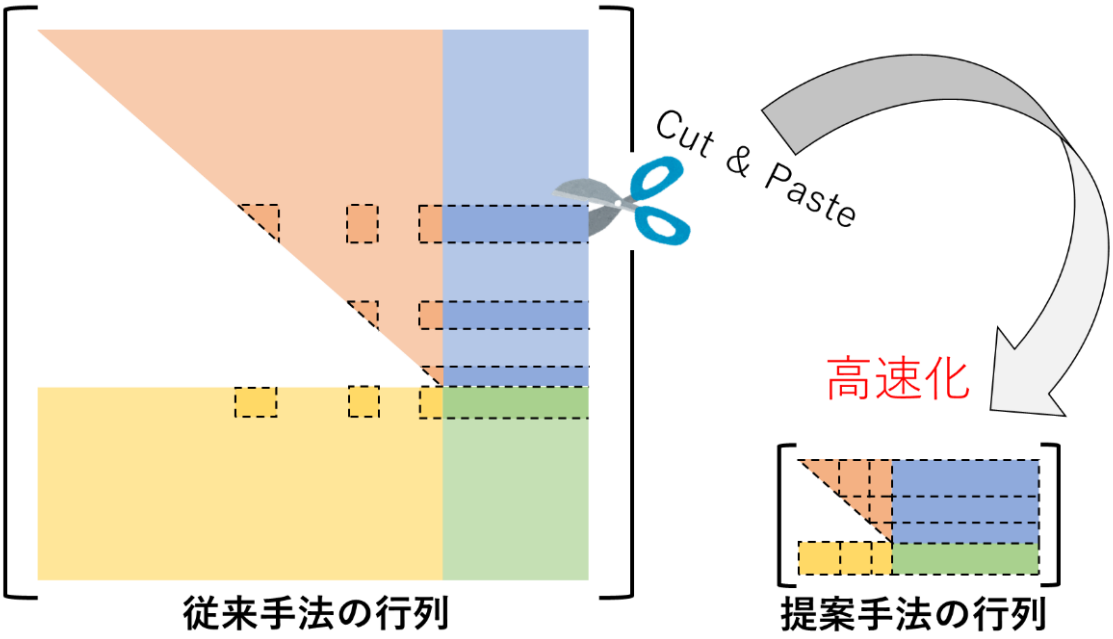


図１：提案アルゴリズムのイメージ図

発表内容

〈研究の背景〉

現在の私たちの生活にはいたるところに暗号技術が使用されています。しかし、量子コンピュータが実用的なレベルで完成すると、現在使用されている暗号は簡単に解読されてしまうことが知られています。そこで、米国標準技術研究所（ＮＩＳＴ）は量子コンピュータでも解読が困難な暗号である、安全な耐量子計算機暗号の選定を進めています。これらの耐量子計算機暗号の安全性を保障するため、攻撃者の計算限界を解明することを目標に、最も効率的な攻撃アルゴリズムを評価する研究が進められています。

図２は暗号の解読問題の難度と攻撃アルゴリズムの計算量を示したグラフです。青線で示したグラフのように、暗号パラメータを大きくすることで解読問題の難度を上げることができます。ここで、攻撃手法の研究が進み、最も効率的な攻撃アルゴリズムが青線から赤線のように変わると解読問題の難度は下がり、攻撃者により解かれてしまう危険があります。このような状況は暗号の危殆化と呼ばれ、情報漏洩などにより犯罪に悪用されることが危惧されます。暗号の危殆化を回避するためには、想定されうる最も効率的な攻撃アルゴリズムを解明し、その攻撃アルゴリズムを基に暗号パラメータを決定する必要があります。

〈研究の内容〉

耐量子計算機暗号の一つに、多変数多項式暗号（注 1）という暗号方式があり、その解読問題は連立二次多変数多項式の求解問題（ＭＱ問題）です。ＭＱ問題の困難性を評価するために、解読コンテスト「ＭＱチャレンジ」が行われています。今回は、これまでに解読されていない最も難しいレベルである問題（Type VI、次元 31、方程式数 21）の解読に約 9 時間で成功しました。

ＭＱ問題を解く標準的な手法としては、グレブナ基底（注 2）を計算するアルゴリズムであるＦ４（注 3）が知られており、解読には巨大な行列を計算する必要がありました。そこで本研究では、ＭＱ問題が持つ数理的特性をヒルベルト級数（注 4）により解明し、計算する多項式の数を最小化するアルゴリズムを構築しました。その結果、Ｆ４が生成する行列の中から、計算に本質的な領域のみを取り出した小さな行列を計算することで、高速化に成功しました（図3）。実際、計算する行列を小さくしても、グレブナ基底計算の観点では全く同等な結果となっています。

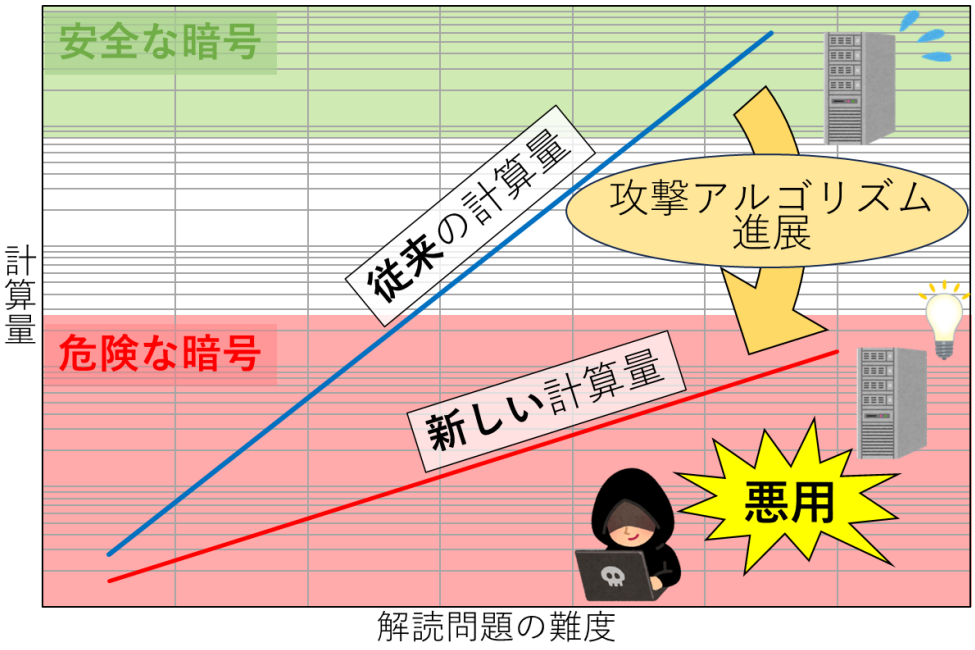


図 2：解読問題の難度と問題の計算量の関係

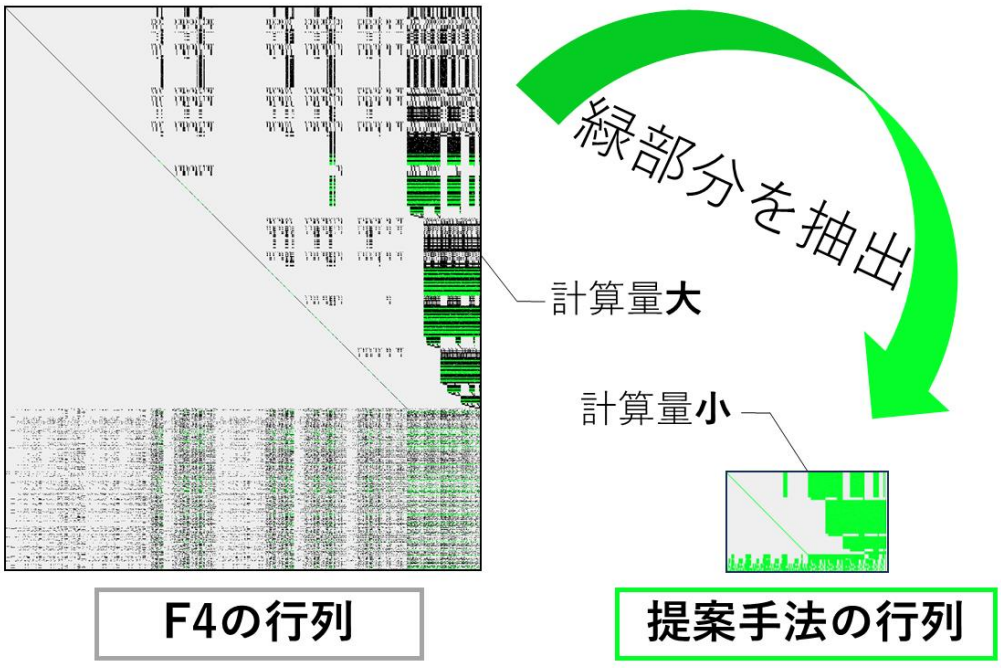


図 3：次元 10 のＦ４（従来）と提案アルゴリズムの比較

〈今後の展望〉

現在、ＮＩＳＴでは次世代デジタル署名暗号の標準化の選定が進められており、主要な候補の中に多変数多項式暗号があります。今回解読に成功した問題の種類は、多変数多項式暗号によるデジタル署名に現れるＭＱ問題と一致します。今後、この新しいアルゴリズムを詳細に評価することで、現在進められている次世代暗号の標準化規格に対して安全なパラメータの提案を進めます。

発表者・研究者等情報

東京大学大学院情報理工学系研究科数理情報学専攻
坂田　康亮　特任研究員
高木　剛　　教授

学会情報

学会名：コンピュータセキュリティシンポジウム 2023（CSS2023）
題　名：Hilbert 級数を用いたＭＱ問題の高速解法とその実装
著者名：坂田　康亮*、高木　剛

研究助成

本研究は、総務省の「電波資源拡大のための研究開発（JP000254）」における委託研究「安全な無線通信サービスのための新世代暗号技術に関する研究開発」の支援により実施されました。

用語解説

（注 1）多変数多項式暗号
連立二次多変数多項式の求解問題(ＭＱ問題)を安全性の根拠とする暗号方式であり、デジタル署名に応用した場合、署名サイズが小さくなることが特徴です。

（注 2）グレブナ基底
多変数の連立方程式を解くときに使用されるなど、幅広い応用を持つことで知られています。特に、多変数多項式暗号の安全性を評価する際にも、この理論が使用されています。

（注 3）　Ｆ４
高速にグレブナ基底を求めることが可能なアルゴリズムであり、多くの代数計算ソフトで使用されています。ＭＱ問題を解読するときには、標準的なアルゴリズムとされています。

（注 4）　ヒルベルト級数
多変数多項式の集合に対して定義できる一変数の級数であり、その集合の代数構造の情報を持っています。これまでの暗号理論では、グレブナ基底の計算による攻撃をしたときに現れる多項式の最大の次数を計算するために使用されてきましたが、本研究では各次数において最低限計算する必要がある多項式の数を算出するために使用しています。