PRESS RELEASE

東京大学

次世代暗号の「解読の限界」に挑む新アルゴリズムを開発

――従来より約 47,000 倍難しい MQ 問題を解読し、世界記録を達成――

発表のポイント

◆東京大学の研究グループは、次世代暗号の安全性に関わる MQ 問題を従来より高速に解く新しい計算方法を開発しました。

◆提案手法は、計算途中に現れる巨大な行列を小さく保つことで、従来より約 47,000 倍難しいとされる問題の解読に成功しました。

◆本成果は暗号研究の国際会議 CHES2026 に採択され、ポスト量子暗号の安全性評価への貢献が期待されます。

従来より約 47,000 倍難しいとされる MQ 問題を解読

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、次世代暗号の安全性評価に関わる「MQ 問題（注 1)」を高速に解く新しいアルゴリズムを開発しました。MQ 問題は、多変数の二次方程式を同時に解く問題であり、量子コンピュータでも解読が難しいと期待されるポスト量子暗号（注 2）の安全性を評価する上で重要です。従来の解読手法では、計算途中に巨大な行列が現れることが大きな課題でした。本研究では、ヒルベルト級数（注 3）と呼ばれる数理的な道具を用いて、計算に本当に必要な組合せを見極め、計算過程全体で行列を小さく保つ新手法を提案しました。その結果、従来記録より約 47,000 倍難しいとされる MQ 問題の解読に成功しました。本成果は、IACR Transactions on Cryptographic Hardware and Embedded Systems 2026（TCHES2026） に 2026 年 7 月 17 日付で掲載されました。暗号研究の国際会議 CHES2026（10 月 11 日～15 日開催）にて発表予定です。

図 1：次世代暗号の解読を高速化する新しい近道

従来手法では巨大な計算量の山を登るように多くの計算が必要でしたが、提案手法では「どの計算が本当に必要か」を事前に見極めます。さらに計算の後半でも、行列が大きくなりにくい計算だけを選ぶことで、全体を効率化しています。

発表内容

〈研究の背景〉

現在のインターネット通信や電子署名には、公開鍵暗号と呼ばれる暗号技術が広く使われています。しかし、将来、大規模な量子コンピュータが実現すると、現在使われている主要な公開鍵暗号の一部は短時間で解読される可能性があります。そのため、世界中で量子コンピュータにも耐えられる暗号、すなわちポスト量子暗号の研究開発と標準化が進められています。

ポスト量子暗号の候補の一つに、多変数多項式暗号（注 4）があります。この暗号の安全性は、多数の二次方程式を同時に解く「MQ 問題」の難しさに基づいています。したがって、MQ 問題をどこまで効率よく解けるかを明らかにすることは、暗号が本当に安全かどうかを評価するために不可欠です。

〈研究の内容〉

MQ 問題を解く代表的な方法として、F4 アルゴリズム（注 5）が知られています。しかし、従来の F4 アルゴリズムでは、計算途中に巨大な行列が現れ、膨大な計算時間とメモリが必要になることが課題でした。

本研究では、F4 アルゴリズムを MQ 問題に適した形に改良し、計算過程全体で行列を小さく保つ新しいアルゴリズムを開発しました。鍵となるのは、ヒルベルト級数という数理的な道具です。ヒルベルト級数を使うことで、各段階で本当に必要な計算量を見積もり、従来なら大量に生成していた不要な組合せを避けることができます。

さらに本研究では、計算の前半だけでなく後半にも着目しました。前半では、ヒルベルト級数に基づいて必要な組合せを選び、後半では、行列が大きくなりにくい組合せを優先的に選びます。これにより、計算の最初から最後まで、扱う行列を小さく保つことが可能になりました。

提案手法を用いた実験では、既存の代表的なソフトウェアの F4 より高速に MQ 問題を解けることを確認しました。また、MQ 問題の解読性能を競う Fukuoka MQ Challenge において新記録を達成しました(Type VI, m=24)。特に、今回解読した最大の問題は、従来記録と比較し，推定される計算困難性が約 47,000 倍難しいと見積もられています。これは、次世代暗号の安全性評価に関わる計算技術を大きく前進させる成果です。

〈今後の展望〉

暗号の安全性は、「現在知られている最も強い攻撃手法でも解けない」ことを根拠に評価されます。そのため、攻撃アルゴリズムの性能を正確に把握することは、安全な暗号パラメータを決める上で欠かせません。

今後は、提案アルゴリズムの適用範囲をさらに詳しく調べるとともに、より新しい CPU 命令や並列計算環境を活用した高速化を進めます。これにより、多変数多項式暗号を含むポスト量子暗号の安全性をより精密に評価し、将来の安全な情報通信基盤の設計に貢献することが期待されます。

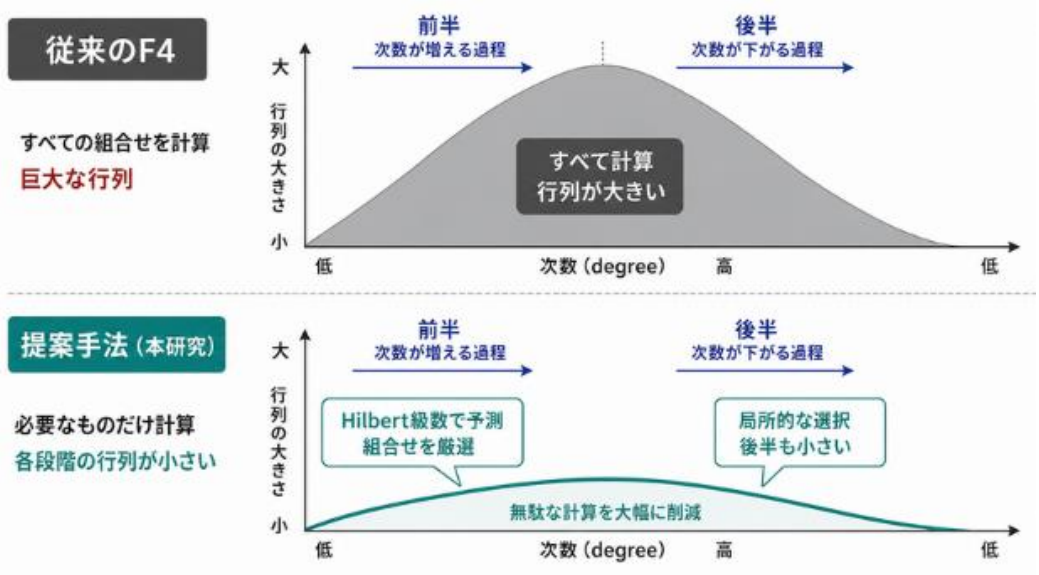

図 2：計算の前半・後半の両方で行列を小さく保つ新手法

MQ 問題を解く従来手法では、計算途中に巨大な行列が現れることが課題でした。本研究では、計算の前半ではヒルベルト級数に基づいて必要な組合せを選び、後半では行列が大きくなりにくい組合せを選ぶことで、計算過程全体で行列を小さく保ちます。

〇関連情報：

「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～」(2023/10/23)

https://www.i.u-tokyo.ac.jp/news/press/2023/202310232315.shtml

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

論文情報

雑誌名：IACR Transactions on Cryptographic Hardware and Embedded Systems 2026 (TCHES2026)
題　名：An Efficient Variant of F4 Algorithm for Solving MQ Problem（7 月 17 日付掲載）
著者名：Kosuke Sakata, Tsuyoshi Takagi
DOI：https://doi.org/10.46586/tches.v2026.i3.1284-1309
URL：https://tches.iacr.org/index.php/TCHES/article/view/13150

研究助成

本研究は、「JST 経済安全保障重要技術育成プログラム（課題番号:JPMJKP24U2）」,科研費「Hilbert 級数の解明による多変数多項式暗号の安全性解析の深化とその応用（課題番号:JP25K00140）」、の支援により実施されました。

用語解説

（注 1）MQ 問題
Multivariate Quadratic problem の略で、多数の二次方程式を同時に解く問題です。多変数多項式暗号の安全性評価で重要な役割を持ちます。

（注 2）ポスト量子暗号
量子コンピュータが実用化された後でも安全に使えることを目指して設計される暗号技術です。

（注 3）ヒルベルト級数
多変数方程式の代数的な構造を表す一変数の級数です。本研究では、前半の各段階で必要な計算を見積もるために使いました。

（注 4）多変数多項式暗号
多数の変数を含む多項式方程式を解くことの難しさを安全性の根拠とする暗号方式です。デジタル署名への応用が期待されています。

（注 5）F4 アルゴリズム
MQ 問題を高速に計算するための代表的なアルゴリズムです。