TOKYO METROPOLITAN UNIVERSITY
首都大学東京

国立研究開発法人
情報通信研究機構

プレスリリース
2019年6月27日
公立大学法人首都大学東京
国立研究開発法人情報通信研究機構

耐量子計算機暗号の安全性評価で世界記録を達成

～量子コンピュータを使用しても解読が困難な"多変数公開鍵暗号"の実用化に向けて～

【ポイント】

- 耐量子計算機暗号の一つとされる多変数公開鍵暗号の安全性評価のコンテストで世界記録達成
- 従来の解読方法より計算が5倍速く、メモリ使用量を8分の1に削減することに成功
- 量子コンピュータ時代でも安全かつ高速な暗号技術の実用化に期待

首都大学東京（学長: 上野　淳）と国立研究開発法人情報通信研究機構（NICT、理事長: 徳田　英幸）サイバーセキュリティ研究所の研究グループは共同で、量子コンピュータを使用しても解読が困難な"多変数公開鍵暗号"[*1]の安全性の根拠とされている連立二次多変数代数方程式[*2]を解くコンテスト（Fukuoka MQ Challenge プロジェクト[*3]）において、Type II 及び III に分類される方程式について、まだ誰にも解かれていない37という多くの変数の方程式を、世界で初めて解くことに成功しました。

多変数公開鍵暗号は効率的な暗号処理方法を持つことから、実用的な耐量子計算機暗号[*4]として期待されています。今回の成果は、多変数公開鍵暗号を安全に運用するために必要な変数の個数の算出に利用されます。

【背景】

公開鍵暗号は、現代の情報通信システムの安全性を支える基盤技術であり、具体的には、RSA 暗号及び楕円曲線暗号[*5] が広く使用されています。しかし、実用的な量子コンピュータが開発されると、これらの公開鍵暗号の安全性が大きく低下することが懸念されています。そのため、量子コンピュータでも、現在のコンピュータでも、解読が困難な暗号が必要とされており、そのような暗号技術は、耐量子計算機暗号と呼ばれています。

特に近年、世界各国及び国内において耐量子計算機暗号の研究開発及び標準化に向けた準備が進められています。耐量子計算機暗号の有力な候補の一つに多変数公開鍵暗号があり、その安全性の根拠とされる連立二次多変数代数方程式を解く研究が重要な課題として活発に進められています。

【今回の成果】

多変数公開鍵暗号を安全に利用するためには、連立二次多変数代数方程式が何変数まで解けるのかを評価する必要があります。

量子コンピュータを使用しても解読が困難な"多変数公開鍵暗号"の安全性の根拠とされている連立二次多変数代数方程式を解くコンテスト Fukuoka MQ Challenge において、6タイプ（Type I～VI）の方程式が設定されており、各タイプにおいて解かれた最大の変数の個数が報告されています。

首都大学東京大学院理学研究科の内山成憲教授と NICT サイバーセキュリティ研究所の伊藤琢真研究員、篠原直行主任研究員らは共同で、Fukuoka MQ Challenge において、Type II 及び III に分類される連立二次多変数代数方程式に特化したアルゴリズムとプログラムを開発し、従来よりも計算が約5倍速く、メモリ使用量を最良の場合では8分の1に節約する

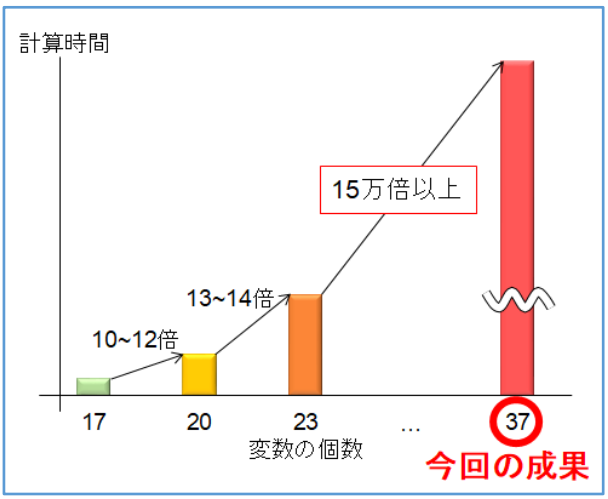

図1 連立二次多変数代数方程式の求解の難しさ

ことに成功しました。本手法を使用して、まだ誰にも解かれていない 37 変数の問題に挑戦しました。この 37 変数の問題を解くためには、MQ Challenge の資料を参考にすると、23 変数の問題を解く場合の約 15 万倍の時間がかかり、汎用ソフトを使用した場合は 4～16 年はかかると考えられます。

しかし、我々の開発したアルゴリズムとプログラムを汎用サーバ（CPU: Intel® Xeon® CPU E5-4669 v4 (2.20GHz/22Core)×4、メモリ: 1TB）で使うことで、Type II の 37 変数については 75.7 日、Type III の 37 変数については 56.1 日で解くことに成功し、3 年近く更新されていなかった世界記録を更新しました。

【今後の展望】

今後は、多変数公開鍵暗号の実用化に向けて、他のタイプの連立二次多変数代数方程式についても解読アルゴリズムを開発し、安全性の評価を実施していきます。

なお、本研究成果について、2019 年 8 月 28 日（水）から 30 日（金）に開催される情報セキュリティに関する国際会議 IWSEC2019（The 14th International Workshop on Security）にて発表する予定です。

＜用語解説＞

***1 多変数公開鍵暗号**

連立二次多変数代数方程式を解く計算の困難性を暗号の安全性の根拠とする公開鍵暗号。多変数公開鍵暗号で使用される連立二次多変数代数方程式が解けると多変数公開鍵暗号は解読されてしまう。多変数公開鍵暗号は暗号処理がシンプルで、具体的には、二次多項式への代入演算、すなわち、高々三つの小さい値の積とそれらの和の計算によって暗号処理が実現できるため、計算コストが小さく効率的な暗号であることが期待されている。
米国立標準技術研究所（NIST）の耐量子計算機暗号の標準化プロジェクトにおいて、4 つの多変数公開鍵暗号（GeMSS、LUOV、MQDSS、Rainbow）が耐量子計算機暗号候補とされている。

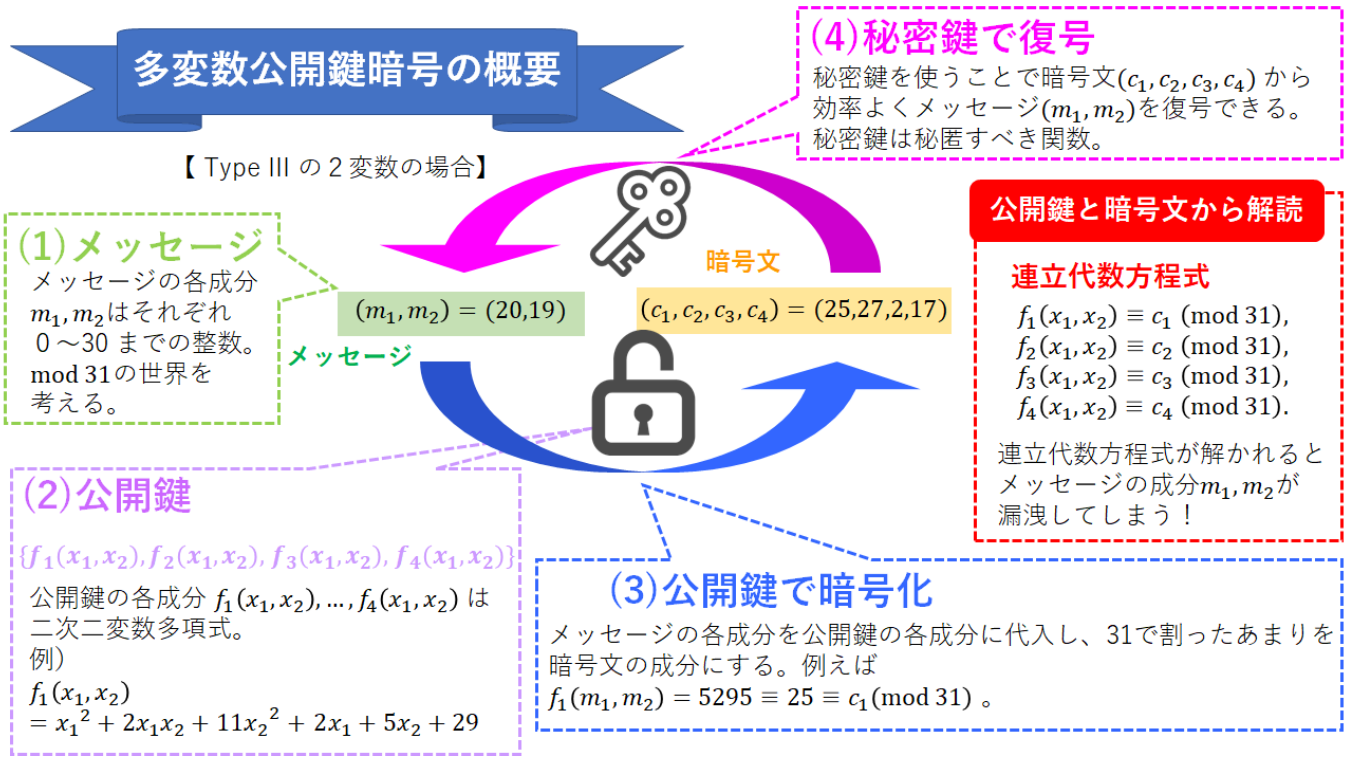

図 2 多変数公開鍵暗号の概要

***2 連立二次多変数代数方程式**

図 3 は、扱う数値が mod 31 の世界における 2 変数の場合の連立二次代数方程式である。それぞれの方程式は、2 個以下の変数を掛け合わせたものを足した形をしている。一般に、変数の個数が多くなるほど、この全ての方程式を満たすような答えを見つけるのは難しくなる。

$$f_1(x_1,x_2) = {x_1}^2 + 2x_1x_2 + 11{x_2}^2 + 2x_1 + 5x_2 + 29 \equiv 25 \pmod{31}$$
$$f_2(x_1,x_2) = 5{x_1}^2 + x_1x_2 + 2{x_2}^2 + 10x_1 + 2x_2 + 4 \equiv 27 \pmod{31}$$
$$f_3(x_1,x_2) = 6{x_1}^2 + 5x_1x_2 + 5{x_2}^2 + 3x_1 + 6x_2 + 16 \equiv 2 \pmod{31}$$
$$f_4(x_1,x_2) = 11{x_1}^2 + 13x_1x_2 + 17{x_2}^2 + 19x_1 + 23x_2 + 29 \equiv 17 \pmod{31}$$

図 3 連立二次多変数代数方程式の例

***3 Fukuoka MQ Challenge プロジェクト**

安田貴徳（岡山理科大）、ダハン・グザヴィエ（お茶の水女子大学）、黄筠茹（ASTRI）、高木剛（東京大学）、櫻井幸一（九州大学）らが主催する、多変数公開鍵暗号に使用される連立二次多変数代数方程式を解く国際的なコンテスト。6 タイプの方程式が用意されており、現在までに、計 4 か国の参加者が研究成果をこのプロジェクトで報告している。https://www.mqchallenge.org/

今回のプレスリリースは、Type II 及び Type III に分類される方程式に関するものであり、図 4 は、MQ Challenge の Type II、III に関するこれまでの成果を表し、どの変数の問題が解かれて、いつこのプロジェクトに報告されたかを表す。

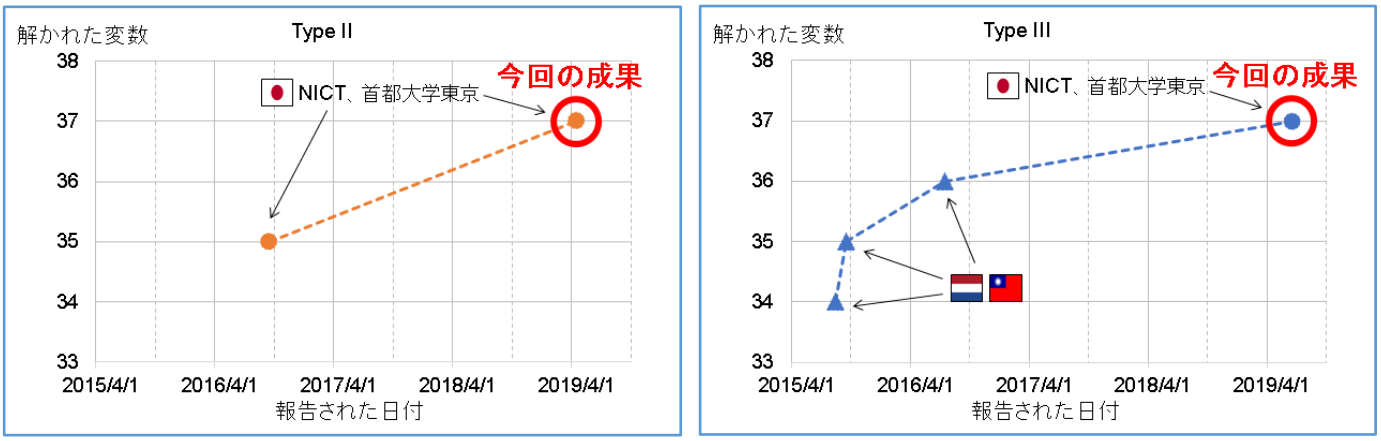

図 4 Fukuoka MQ Challenge Type II、III の成果

***4 耐量子計算機暗号**

量子コンピュータでも現在のコンピュータでも解読が困難な暗号。現時点では、「整数を素因数分解する計算の困難性」及び「離散対数問題を解く計算の困難性」を安全性の根拠としない暗号が耐量子計算機暗号の候補とされ、その代表的なものとして多変数公開鍵暗号、格子暗号、符号暗号、同種写像暗号、ハッシュ関数署名などの研究開発が世界的に活発に進められている。

特に近年、NIST において耐量子計算機暗号の標準化プロジェクトが進められており、現時点では多変数公開鍵暗号を含む 26 件の候補の安全性が検証されている。

https://csrc.nist.gov/projects/post-quantum-cryptography/round-2-submissions/

***5 RSA 暗号と楕円曲線暗号**

現在広く使用されている公開鍵暗号。RSA 暗号や楕円曲線暗号は耐量子計算機暗号ではない。その理由は、RSA 暗号の安全性が整数を素因数分解する計算の困難性を根拠とし、楕円曲線暗号の安全性は離散対数問題を解く計算の困難性を根拠としていることである。これら二つの計算問題は、量子コンピュータによって高速に解けることが知られている。

補足資料

＜今回の成果のポイント＞

連立代数方程式を効率良く解くために、方程式を構成する多項式の集合をグレブナー基底と呼ばれる集合に変換するアルゴリズムが広く採用されています。その代表的なアルゴリズムとして、F4-style アルゴリズム、M4GB などが挙げられます。F4-style アルゴリズムは、M4GB と比べてメモリを節約して計算できる可能性が大きく、並列した計算に適した性質を持っています。そのため、今回我々は、F4-style アルゴリズムを基に、連立二次多変数代数方程式を解くための高速化及びメモリ使用量の削減を行いました。

このアルゴリズムを用いて問題を解く場合、多項式の割り算を大量に行う必要があります。しかし、その計算の中には、不要な割り算を実行してしまうケースが多く存在します。そのため、不要な割り算をしないようにするための判定法を開発することで、計算の回数を削減しました。演算も最適化することで、M4GB よりも約 5 倍速くすることに成功しました。さらに、メモリを節約する方法も開発し、最良の場合では、メモリ使用量を M4GB の 8 分の 1 にすることに成功しました。

この改良した方法を用いて、Fukuoka MQ Challenge の Type II 及び III の問題に挑戦し、その世界記録を更新しました。

図 5　Fukuoka MQ Challenge: https://www.mqchallenge.org/

＜ 本件に関する問い合わせ先 ＞
首都大学東京
大学院理学研究科
内山 成憲
Tel: 042-677-1111（代表）
E-mail: mqc-query@tmu.ac.jp

国立研究開発法人情報通信研究機構
サイバーセキュリティ研究所
セキュリティ基盤研究室
伊藤 琢真、篠原 直行
Tel: 042-327-5343
E-mail: mpkc@ml.nict.go.jp

＜ 広報 ＞
公立大学法人首都大学東京
管理部 企画広報課 広報係
Tel: 042-677-1806
E-mail: info@jmj.tmu.ac.jp

国立研究開発法人情報通信研究機構
広報部 報道室
廣田 幸子
Tel: 042-327-6923
E-mail: publicity@nict.go.jp