国立研究開発法人
情報通信研究機構

プレスリリース
2020年12月9日
国立研究開発法人情報通信研究機構

量子コンピュータ実機を用いた離散対数問題の求解実験に成功

～次世代における暗号の安全性確保に向けて～

【ポイント】

- IBM 社の超電導量子コンピュータを用いた離散対数問題の求解実験に成功
- 離散対数問題の多様性のある特性を生かした量子コンピュータ向けプログラミング
- 現在の暗号への脅威の将来予測、耐量子計算機暗号への移行の第一歩に向けて

国立研究開発法人情報通信研究機構（NICT）、学校法人慶應義塾（慶應大学）、株式会社三菱 UFJ フィナンシャル・グループ（MUFG）、株式会社みずほフィナンシャルグループ（MHFG）は、IBM Q Hub at Keio University のある慶應義塾大学量子コンピューティングセンター（KQCC）において、量子コンピュータ時代における暗号の安全性確保のための第一歩として、クラウドからアクセス可能な量子コンピュータである IBM Quantum を使用した小規模離散対数問題の求解実験に成功しました。

離散対数問題は、現代の情報社会を支える暗号技術の安全性の根拠の一つとなっている極めて重要な問題であり、量子コンピュータ実機で解くことのできる離散対数問題の規模を知ることが重要な課題です。また、離散対数問題は、実験可能な量子プログラムの選択の幅が広く、暗号への脅威の将来予測のための量子コンピュータ実験に適しているのではないかという事前検討を踏まえ、実験を行いました。

本成果は、今後、量子コンピュータによる現代暗号の危殆化時期の予測検討に利用される予定です。

【背景】

現代の情報社会を支える暗号技術の安全性を保障する数学的な問題の一つに、離散対数問題（補足説明*1, 2 参照）があります。離散対数問題は、一定の性能を有する量子コンピュータを用いることで、高速に解かれてしまうことが理論的には証明されているため、量子コンピュータの性能向上により、暗号技術が危殆化することが懸念されています。対策として、一定の性能を持つ量子コンピュータの出現後も暗号の安全性を担保できると期待されている耐量子計算機暗号への移行に向けた検討が、米国国立標準技術研究所（NIST）を中心に世界的に進められています。その移行が必要となる時期を予測するため、現在利用可能な量子コンピュータを用いて、どの程度の規模の離散対数問題が解けてしまうのかを把握することが重要です。

【今回の成果】

今回、NICT ら 4 者のグループは、量子コンピュータ時代における暗号の安全性確保に向け、離散対数問題に

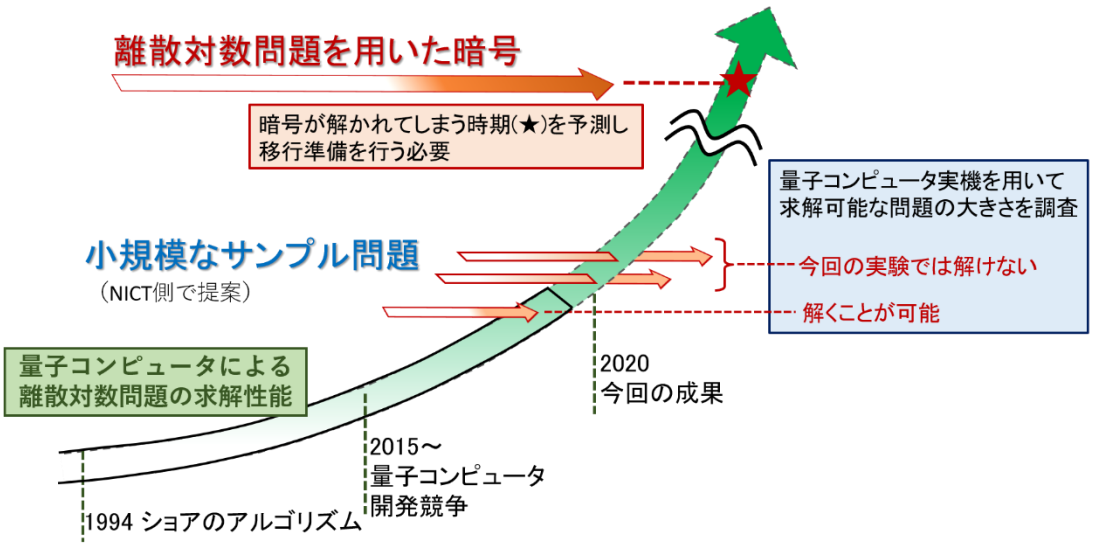

図 1 暗号の危殆化時期の予測に関する今回の成果を表す鳥瞰図

よって安全性が保障される暗号方式の危殆化時期評価に関する活動を開始しました。その活動の第一歩として、ショアのアルゴリズム（補足説明*3 参照）を離散対数問題用にプログラミングし、量子コンピュータ実機による離散対数問題の求解実験に世界で初めて成功しました。

今回の実験は、NICT が実験用の量子プログラムを設計した後、慶應大学、MUFG、MHFG により超電導量子コンピュータ IBM Quantum に合わせた効率化を行い、IBM Quantum の実デバイス上で実験を行いました。その出力結果の検討を 4 者で行ったところ、問題が解けているとの結論に至りました。

今回の成果は、まだ初歩的段階であるため、現在使われている暗号技術の安全性に脅威を与えることはありませんが、暗号技術の危殆化時期を予測する上で重要かつ貴重な一歩になったと考えています。

【今回の実験と結果の概要】

ショアのアルゴリズムは、素因数分解問題や離散対数問題を含む様々な問題に適用可能なため、それらの問題を安全性の根拠とする暗号技術への脅威となる可能性があることから、様々な研究が行われています。特に、RSA 暗号の安全性の根拠として利用されている素因数分解問題については、量子コンピュータを用いた様々な実験が行われてきました。一方、離散対数問題については、実験に成功したという報告はありませんでした。

暗号がいつ解かれてしまうのかを予測するために、その暗号の安全性の根拠となる問題がどの程度解かれてしまうのかを調べることは重要です。今回、ショアのアルゴリズムの暗号への影響を調査するため、両問題の実験について検討を行いました。その結果、離散対数問題の小規模なサンプル問題であれば、プログラミングを工夫することで、求解実験が成功する可能性があることが分かりました。

今回の実験のため、離散対数問題のいくつかのサンプル問題に対して量子コンピュータ向けのプログラミングを行い、そのプログラムの規模がどの程度までであれば、量子コンピュータ実機によって解くことが可能なのかを調べました。図 2 は、実験を行ったプログラムを規模（補足説明*4 参照）の順に並べ、量子コンピュータ実機で実験を行った結果をまとめたものです。今回実験を行った中で最も小さい規模の量子プログラム①の実行では、量子コンピュータ実機が十分に良い結果を出力しましたが、より大きな規模のプログラム②及び③では良い結果が出力されませんでした。

そのため、現在の技術により解くことのできる量子プログラムの規模は、図中①と②の間であるという結論を得ました。これは、離散対数問題を量子コンピュータ実機で解いた初めての成果となります。また、プログラム②の出力を検証したところ、プログラムの規模をより小さく改良することができれば、解ける可能性が残されているという結論に至りました。

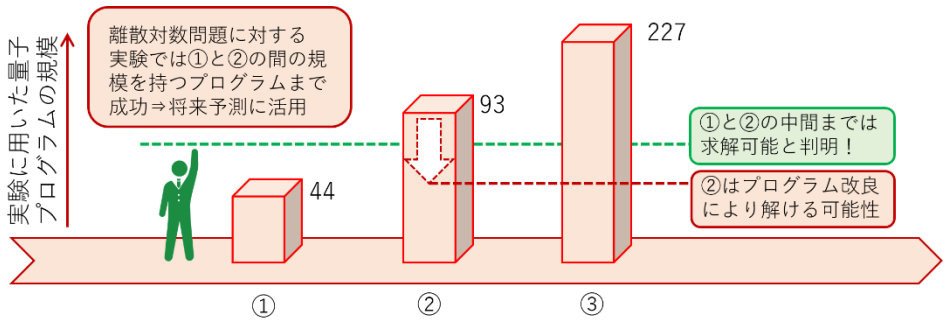

図 2 離散対数問題を解く量子コンピュータプログラムの規模と実験結果（数字の意味など詳細は補足説明 *4 参照）

【今後の展望】

今後も、量子コンピュータの性能の向上に合わせて定期的な実験報告を行うことで、現在用いられている暗号技術の危殆化時期をできる限り正確に見積もり、暗号技術の安全性評価の活動へとつなげていきます。

本研究成果について、2020 年 12 月 10 日（木）、11 日（金）にオンライン開催される第 43 回量子情報技術研究会（QIT43）にて発表する予定です。

＜発表情報＞

名称: 第 43 回量子情報技術研究会（QIT43）
日時: 2020 年 12 月 11 日（金）
タイトル: 超電導量子回路を用いた離散対数問題の求解実験

＜補足説明＞

*1 離散対数問題の位置付けと暗号の移行

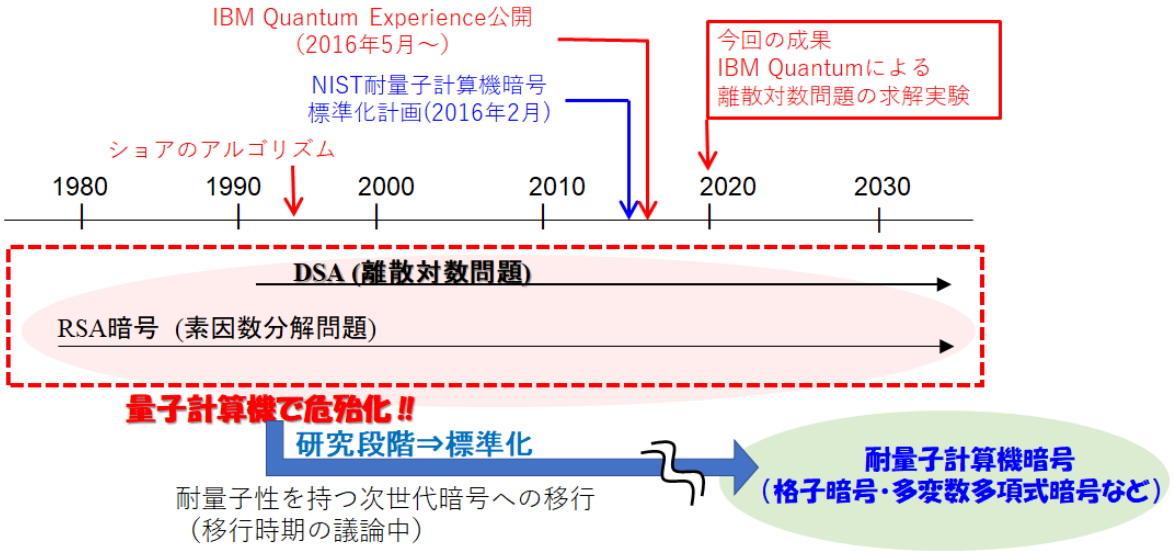

図 3 離散対数問題の位置付けと、危殆化による耐量子計算機暗号への移行

離散対数問題は、米国 NIST 標準のデジタル署名方式をはじめとする重要な暗号技術の安全性を保障する数学的な問題である。離散対数問題が解ければ秘密情報が漏洩してしまうという関係であり、それは、素因数分解問題が解ければ RSA 暗号が解けてしまうという関係と同様である。

一定の性能を持つ量子コンピュータにより、ショアのアルゴリズムを実行することで、離散対数問題と素因数分解問題が効率的に解けることが 1994 年に証明されている。つまり、量子コンピュータの性能の向上により、現在使われているいくつかの暗号の安全性が大きく低下することが予測される。これを暗号の危殆化と呼ぶ。

暗号の安全性を維持するためには、暗号の危殆化前に使用を中止し、量子コンピュータでも解くことが難しいと予測されている『耐量子計算機暗号（https://www.nict.go.jp/press/2018/01/11-1.html 参照）』の利用を開始する必要がある。これを暗号の移行と呼び、いつまでに移行を終えなければならないのかをできる限り正確に見積もる必要がある。今回の成果は、暗号の危殆化時期・移行のタイムリミットを予測する上で重要な一歩となる。

*2 離散対数問題と暗号技術

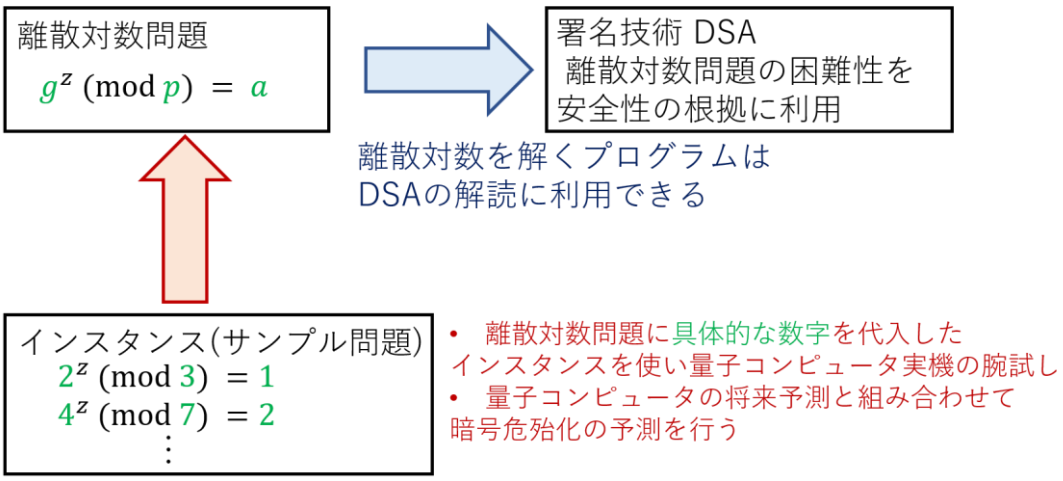

図 4 離散対数問題と代表的な署名技術 DSA の関係

離散対数問題は、電子署名 DSA の安全性の根拠として利用される方程式であり、3 つの自然数 g, a, p により、『$g^z \pmod p$=a』と表現される。これは、『$g^z \pmod p$が a となるような自然数 z を求めよ』という意味である。ここで、g^z は g を z 回掛け算したもので、$g^z \pmod p$はそれを p で割った余りを意味する。この問題を解くアルゴリズム(コンピュータプログラム)は暗号解読に利用可能であることから、長年研究されてきた。

暗号の危殆化時期を予測するためには、どの程度の大きさの離散対数問題が量子コンピュータ実機により解けるのかを継続的に調査する必要がある。そのためには、離散対数問題の g, a, p に具体的な数値を代入したインスタンス(サンプル問題)をつくり、コンピュータに解かせて腕試しをしてもらうことで、将来予測の基盤とすることができる。

*3 ショアのアルゴリズム

ショアのアルゴリズムでは、量子コンピュータの持つ、入力された関数の周期(繰り返しパターンの間隔)を発見する能力を利用し問題を解く。離散対数問題を解く際には、与えられたインスタンスに対応するある関数 F(x,y)を、F(x,y)=F(x+z,y+1)を満たすように手作業で構成する。ここで、z は問題の解となる自然数である。

例えば、g=2, a=6, p=13 を代入したインスタンス『$2^z \pmod{13}$=6』に対応する F(x,y)は F(x,y)=F(x+5,y+1)を満たすため、その値に応じて濃淡でプロットすると、図 5 のようになる。右に 5、上に 1 進むと、同じパターンが繰り返されるので、離散対数問題の答えが 5 であると読み取れる。通常のコンピュータを使うと、大量の F(x,y)の値を計算する必要から時間が掛かる。一方、ショアのアルゴリズムでは、量子コンピュータを用いて関数値 F(x,y)の各 x, y に対する重ね合わせを計算した後に、周期を計算することで、元の離散対数問題の解 z を高速に求めることが可能である。

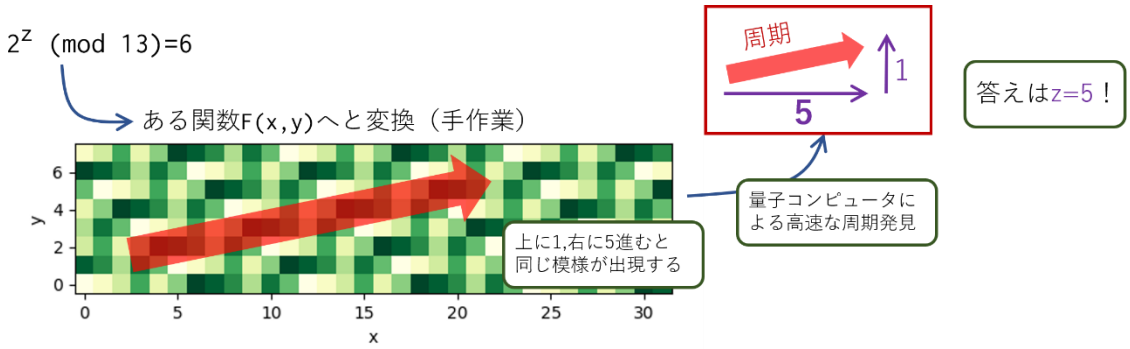

図 5 離散対数問題のインスタンス 2^z (mod 13)=6 に対応する周期の発見
上に 1、右に 5 進むと、同じ模様が出現するため、問題の解は z=5 であることが分かる。

*4 離散対数問題における量子プログラムの規模

素因数分解問題は、『自然数 N を素因数分解せよ』という問題であり、インスタンス（サンプル問題）の指定が 1 つの数で行われるのに対して、離散対数問題のインスタンスは、3 つの数 g ,a, p を用いて与えられる。後者の方が問題の設定変数に多様性があるため、それを生かすことで、量子コンピュータ実機での実験に適したインスタンスを選ぶことができると期待された。事前検討により、量子プログラミングの規模が小さい 3 つのインスタンス①$2^z \equiv 1$ (mod 3)、②$2^z \equiv 2$ (mod 3)及び③$4^z \equiv 2$ (mod 7)に注目した。

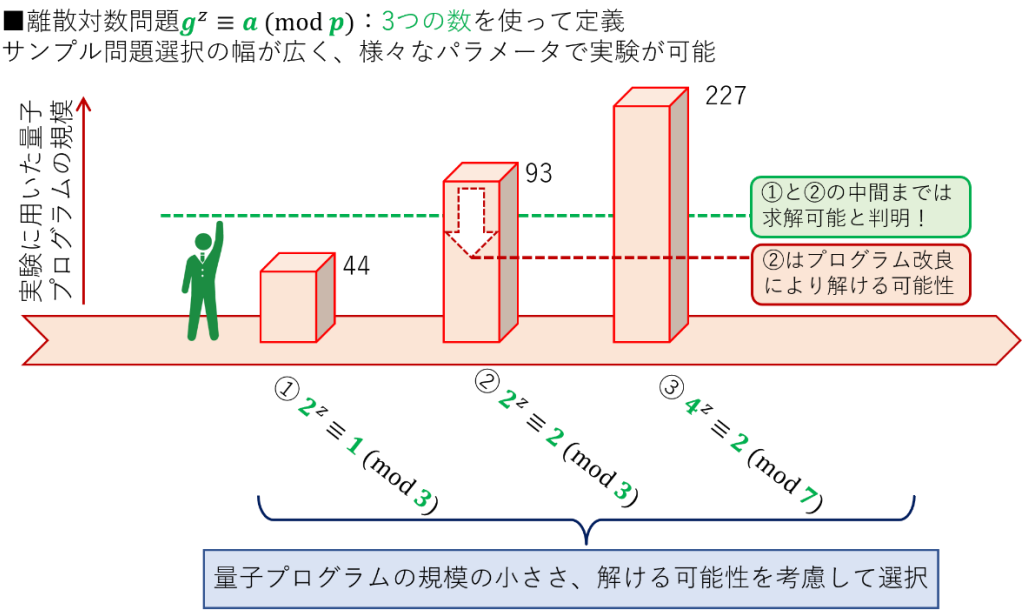

図 6 離散対数問題の選択の幅の広さと、単純な量子プログラミングが可能なインスタンスの選択

通常のコンピュータを用いて行ったシミュレータの出力と、量子コンピュータの実機を比較することで、実行結果の検証を行ったところ、①に関しては期待通りの出力を観測し、成功といえたが、②、③の出力は十分に良いものではなかった。このことから、現在の技術で解くことのできる離散対数問題は、①と②の間であると結論付けた。一方で、プログラム②の出力を詳細にシミュレータ出力と比較したところ、求解プログラムの規模をより小さくできれば、今回用いた量子コンピュータ実機によって解くことができる可能性があることも判明した。

量子コンピュータは、入力されるプログラムの規模が大きければ、その実行に時間が掛かるようになる。量子コンピュータの中で計算に用いられる量子状態は、時間が経つことでノイズが加わり、計算の役に立たないものへと変化してしまう。そのため、量子プログラムが複雑になり実行時間が延びると正しい計算結果を得ることが難しくなる。

図 2 及び図 6 のグラフにある数値は、プログラム内で指定された量子コンピュータが実行すべき量子的な操作の回数である。①のプログラムでは操作回数が 44 回であり、②のプログラムでは操作回数が 93 回であるため、②の方がプログラム規模が大きく、実行時に正しい出力を得ることが困難である。

共同研究機関:

・国立研究開発法人情報通信研究機構（NICT、理事長: 徳田 英幸）
・学校法人慶應義塾（慶應大学、塾長: 長谷山 彰）
・株式会社三菱 UFJ フィナンシャル・グループ（MUFG、代表執行役社長: 亀澤 宏規）
・株式会社みずほフィナンシャルグループ（MHFG、執行役社長: 坂井 辰史）

＜ 本件に関する問合せ先 ＞
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
青野 良範
Tel: 042-327-6594
E-mail: qsecdlp@ml.nict.go.jp

＜ 広報（取材受付）＞
広報部 報道室
廣田 幸子
Tel: 042-327-6923
E-mail: publicity@nict.go.jp