3-3　暗号技術の安全性評価
3-3　Security Evaluation of Cryptographic Technologies
3-3-1　量子コンピュータによる現代暗号の安全性評価
3-3-1　Estimating the Security Strength of Cryptography with Quantum Computers

青野 良範　篠原 直行
AONO Yoshinori and SHINOHARA Naoyuki

素因数分解問題・離散対数問題の計算困難性は現在インターネット上で用いられる多くの暗号の安全性と関連している。ショアのアルゴリズム [1] により量子コンピュータを用いて効率的に解かれてしまうため安全性が脅かされるとされているが、現実的なパラメータを持つ暗号を解くためには巨大な規模の量子回路が必要であり、実際の脅威には遠いとされてきた。近年の商用を中心とした量子コンピュータの普及と性能進化に伴い、この脅威について調査し実際の暗号が解かれるのがいつ頃になるのかを予測する必要がある。セキュリティ基盤研究室では、実際の量子コンピュータを用いて暗号の解読実験を行った実験データを基に、将来の脅威を予測する枠組みを提案した。

Since Shor demonstrated that polynomial-size quantum circuits can efficiently solve the integer factoring problem and discrete logarithm problem, the development of quantum computers has posed a threat to modern cryptography. However, solving such problems with actual cryptosystems requires large-scale quantum computers, which remain inadequately developed. To anticipate when these quantum threats might materialize, we have been monitoring the progress of quantum computer development. This paper details our experiments using IBM quantum computers to solve discrete logarithm problems and proposes a framework for predicting future quantum computer advancements and associated threats.

1　まえがき

現在インターネット上での通信をはじめとする情報の保護に用いられる RSA 暗号、楕円曲線暗号 [2] はそれぞれ素因数分解問題・離散対数問題を解くことで解読される*1 ことが知られており、古典コンピュータでそれらの問題を効率的に解くアルゴリズムが長年発見されていないという事実がその安全性を保証している。しかし一方で、nビットの素因数分解問題・離散対数問題は$O(n)$論理量子ビット、$O(n^3)$論理量子ゲート程度の量子回路によって解かれてしまうことが知られている [3]。これらの量子回路を実際に構成すると、論理量子ビット・ゲートを実現するための量子誤り訂正により規模が数千倍に膨らみ、例えば 2,048 ビットの RSA 暗号を解く場合には 2 千万量子ビット、27 億量子ゲート程度となる [4]。その一方で、2024 年現在開発されている量子コンピュータの中で最大の量子ビット数を持つものは 1,000 量子ビット程度であり、最近出版されたサーベイ論文 [5] によれば実際の計算機実験で用いられる量子ビットはほぼ10以下である。今後数十年以内には量子コンピュータの性能進化と量子アルゴリズムの改良により現実的な脅威となるという予測も存在するものの、量子誤り訂正・量子メモリ等、2024 年現在では実用化されていない技術の開発速度が未知数であることから具体的な年代の予測は困難であると考えられる。

セキュリティ基盤研究室では、慶應義塾大学、三菱 UFJ フィナンシャル・グループ、みずほフィナンシャルグループとの共同研究により、量子コンピュータとショアのアルゴリズムを用いた暗号解読の枠組みを整

*1　量子とは直接関係が無い話題だが、素因数分解・離散対数計算以外の解き方があるかどうかは知られておらず、暗号分野の重要な未解決問題である。

理し、IBM の量子コンピュータ実機を用いた実験を通じて現代暗号危殆化に関する将来予測の基礎とした [6]。

2 量子コンピュータでの計算の枠組み

図 1 に量子コンピュータを用いた計算の枠組みを示す。大まかに①量子回路設計、②実機への投入、③測定結果の後処理の 3 段階に分かれる。2024 年現在量子コンピュータの利用環境は整備されつつあるものの、FPGA･GPGPU 等のようなアクセラレータ的な使い方が主流である。NISQ（Noisy Intermediate-Scale Quantum）デバイスの名のとおり量子デバイスの実行にはノイズが多く、対処のため前処理・後処理に関して古典計算機を使う部分はまだまだ多い。

以下、離散対数問題を解くためのショアのアルゴリズムを例にこの枠組みを解説する。本稿で扱う離散対数問題は有限体上のものであり、整数(g, a)と素数pに対して$g^z \equiv a \pmod p$を満たす整数zを求める問題である。暗号で利用される離散対数問題の性質により、本稿では 1 以上$p-1$未満の任意の整数kに対しては$g^k \not\equiv 1 \pmod p$が成り立つとする。このとき、関数

$$f(x, y) = g^x a^{-y} \pmod p \qquad (1)$$

が 2 つの周期$(p-1, 0), (z, 1)$を持ち、その片方が解zの情報を含んでいることから、ショアのアルゴリズムの周期発見能力を利用することができる。実際の実験では離散対数問題の意味のあるインスタンス*2の中で最も単純な$2^z \equiv 1 \pmod 3$を用いて解の$z = 2$を求めた。

2.1 量子回路設計

解きたい問題に合わせて量子コンピュータ上で実行される量子回路を設計する。離散対数問題に対するショアのアルゴリズムでは入力のg, a, pに対して、以下の図 2 の量子回路図で示される計算と測定を行う。

実験では$(g, a, p) = (2, 1, 3)$に対応する量子回路を Qiskit フレームワーク上のプログラミング言語で記述した。図 2（下）で示した回路は論理レベルの記述である。古典コンピュータ上でのシミュレーションはこのまま実行可能であるが、量子コンピュータ実機上での実行のためにはさらに、デバイスの量子ビット配置と

*2　離散対数問題$g^z \equiv a \pmod p$に具体的な数値を代入した$2^z \equiv 1 (\mathrm{mod} 3)$のような計算問題のことを、問題のインスタンスと呼ぶ。

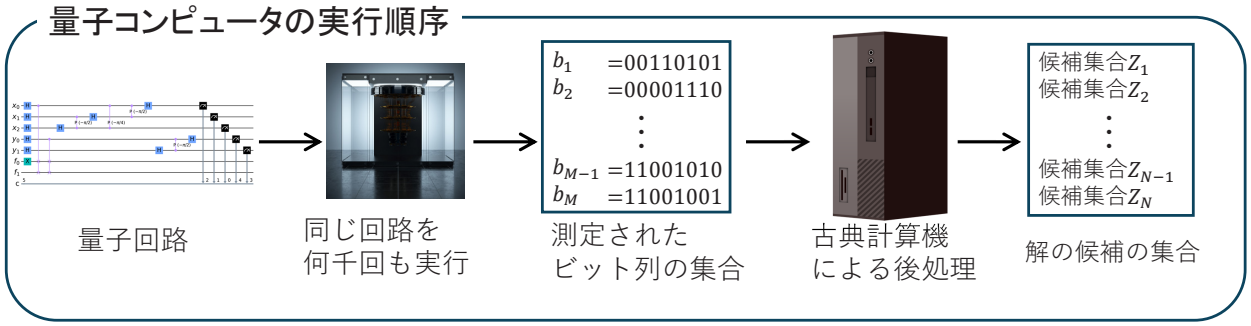

図 1　量子コンピュータの実行順序

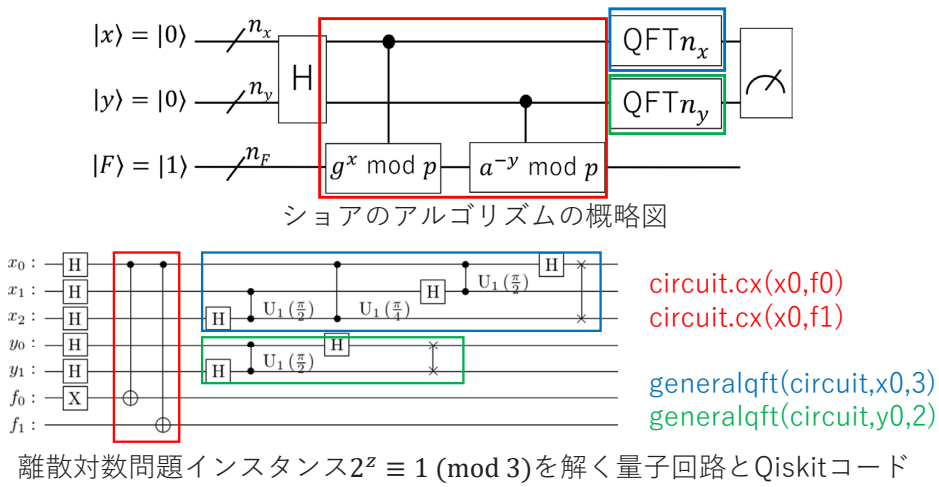

図 2　離散対数問題を解くショアのアルゴリズムの概念図（上）及びインスタンス$2^z \equiv 1 \pmod 3$を解く量子回路及び Qiskit コード（下）

実行可能ゲートのセットに合わせ古典コンピュータ上での変換を行う必要がある。この変換操作をトランスパイルと呼ぶ。

我々の実験では IBM Quantum [7] の ibm_kawasaki デバイスを用いたため、それに合わせてトランスパイルを行い、さらに手動でゲート数の最適化を行った。

2.2　実機への投入と結果の回収

量子回路を記述したトランスパイル後の回路コードを量子コンピュータに投入する。このとき、回路の実行回数Mを指定することで複数回の実行が行われ、M個のビット列$b_1, \ldots, b_M$を得る。

我々の実験では IBM クラウドサービスのインターフェースを通じて回路情報を転送した。実行回数は M=8,192 とした。回路の実行自体は数十μ秒で終了するが、待ち時間は数時間から数十時間かかることもあり、手元のシミュレーターで十分にデバッグを行ってから実機に投入する必要がある。このあたりの事情はスーパーコンピュータのような共用設備の利用と同様であるが、一方で量子コンピュータがまだ開発の初期段階であるという特有の困難もある。まず、回路実行前に量子デバイス上の量子ビットを初期化する必要があるが、量子力学の原理から完璧な$|0\rangle^n$状態を作り出すことはできず、僅かなゆらぎが残る。この影響で実験中の量子ノイズの乗り方が時々刻々と変化するため、結果の確率分布もそれに合わせて変化し、厳密な意味での実験の再現性はなくなる。また、量子デバイス自体のアップデートも頻繁に行われ、論文が出版される頃には実験に用いたデバイスがアクセス不可能となることもあった。

2.3　出力ビット列の後処理

量子デバイスから出力されたビット列$b_1, \ldots, b_M$はそのままでは計算問題の解とはならないため、後処理を行う必要がある。例えばショアのアルゴリズムでNの素因数分解を行う場合、出力ビット列b_iを実数$r_i \in [0,1]$と解釈しなおしてその近似分数d/cを求め、分子dから$\gcd(a^{\frac{d}{2}} \pm 1, N)$を計算して素因数の候補を求めるといった複雑な操作が必要であり、この部分は古典コンピュータで行われる。

離散対数問題の計算においてもこの状況は同様であり、古典コンピュータでかなりの後処理を行う必要がある。図 2 の量子回路を実行して得られるビット列b_iを量子フーリエ変換のサイズに従い 2 つの部分に分割し、それぞれを実数q_i, r_iとして解釈する。このとき、点(q_i, r_i)は以下の行列 D の行ベクトルによって張られる格子内の点の何れかを近似したものとなる。この D は量子フーリエ変換の性質から$f(x, y)$の周期に対応する行列 B で張られる格子の双対格子であり、離散対数問題の後処理では双対格子の点から元の格子の基底を復元する問題を解く。

$$B = \begin{bmatrix} p-1 & 0 \\ z & 1 \end{bmatrix} \qquad D = \frac{1}{p-1}\begin{bmatrix} 1 & -z \\ 0 & p-1 \end{bmatrix} \quad (2)$$

復元の標準的な手法は、k個の(q_i, r_i)の組からk次元格子を構成し、格子の短いベクトルを列挙することで解zの候補集合Zを求めるというものである。これは、量子ノイズの影響が全くない場合には非常に高い確率で離散対数問題を解くことが知られているが、現在の NISQ デバイスのように計算に大きなノイズが含まれる場合にどのような挙動を示すのかは知られていなかった。

2.4　計算問題が解けたことの基準

我々が研究を開始した時点で、量子コンピュータからどのような出力が得られれば離散対数問題が実機で解けたと主張できるのかについて、どのような基準を用いるのかというコンセンサスはなかった。図 1 に示したように、現在利用可能な量子コンピュータでの計算は同じ量子回路を何度も実行し複数個のビット列$b_1, \ldots, b_M$を得たのちに、それらを後処理し解の候補集合$Z_1, \ldots, Z_N$を出力するという枠組みから成る。このときにb_iとZ_iのどちらの情報を用いてどのような基準を作るのかということが問題となっていた。

離散対数問題に限らず、現在の量子コンピュータで実行可能な暗号に関する計算問題のサイズは小さい。仮に量子コンピュータのノイズが非常に大きく、出力がほぼランダムビット列であったとしても後処理アルゴリズムはかなりの高確率で正解を出力してしまうが、そのような場合に量子コンピュータが上手く動いていると主張するのは不自然である。

実際の実験では例えば$M = 8{,}192$個のビット列を得たのちに、$K = 4$個ごとにまとめて後処理アルゴリズムに入力すると 2,048 個の解の集合が得られるが、ターゲットの離散対数問題$2^z \equiv 1 \pmod 3$はzが偶数であれば正解、奇数であれば不正解であるため、ランダムな出力でも正解率は 50 % となる。解候補の集合Z_iは多くの元を含むため、実際には 60 % 程度の後処理が正解を含む。

このような状況の下、先行研究では一般論として、シミュレーターにより計算された量子ノイズのない場合の確率分布、実機出力の確率分布、一様ランダム分布をダイバージェンスなどの指標を用いて比較することで解けたか否かを判断していた。しかし、この手法では問題サイズが大きくなるに従い量子ノイズのない場合のシミュレーションが困難となるためスケーリン

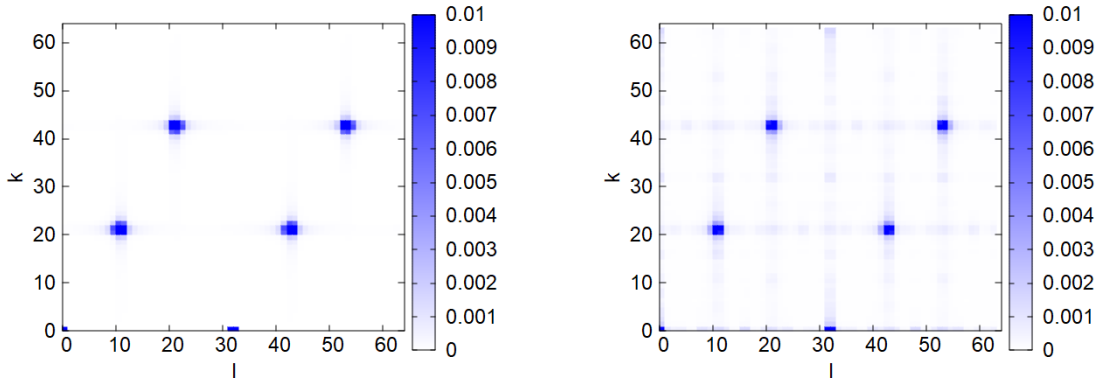

図 3　離散対数問題 $3^z \equiv 4 \bmod 7$ を解く量子回路の出力確率分布のシミュレーション結果。左：P_{ideal} 量子ノイズがない場合のシミュレーション、右：P_{noise} 僅かに量子ノイズがある場合のシミュレーション。

グが難しい。また、ダイバージェンスの非対称性から来る結果の矛盾や、僅かな値のずれが最終的な正解率に大きく影響することがシミュレーションから判明したために確率分布を用いない別の手法を模索した。

後者の問題点を説明する。図 3 は Qiskit フレームワークにより量子ノイズがある場合の回路シミュレーションを行った出力の確率分布である。定量的な指標として確率分布間のダイバージェンスを用いて判断を行うとする。このとき、一様ランダム分布を $P_{uniform}$ としてダイバージェンスを比較すると $D(P_{ideal}||P_{noise}) < D(P_{noise}||P_{uniform})$ となり P_{noise} が P_{ideal} に近いため成功しているように見えるが、変数を反対にすると $D(P_{uniform}||P_{noise}) < D(P_{noise}||P_{ideal})$ となり、P_{noise} が $P_{uniform}$ に近いため失敗しているかのように見える。つまり、距離の測り方によって実験が成功とも失敗とも解釈できてしまう。

様々な先行研究を検討した結果、最終的に IBM の研究者が量子コンピュータの性能指標の一つとして提案した量子体積（Quantum Volume）[8] の考え方を参照し、以下の定量的な基準を提案した：

$$\frac{p_{ideal} + p_{uniform}}{2} \leq p_{device} \qquad (3)$$

であれば、離散対数問題は解けていると判断する。ただし、各量は以下で計算される。

- p_{ideal}：後処理アルゴリズムにシミュレーターで計算した量子ノイズのないビット列を入力したときの正解率
- p_{device}：後処理アルゴリズムにデバイスの出力ビット列を入力したときの正解率
- $p_{uniform}$：後処理アルゴリズムにランダムビット列を入力したときの正解率

この基準の長所は以下の 2 点である。問題サイズが小さい場合には $p_{ideal}, p_{uniform}$ はそれぞれ量子シミュレーターの出力を後処理アルゴリズムに入力することで計算可能である一方、シミュレーターを動かすことが困難であるほどに大きな問題サイズに対しては $p_{ideal} \approx 1, p_{uniform} \approx 0$ と近似できるため、$p_{device} \geq 0.5$ を基準とでき、NISQ 領域とより大きな量子コンピュータでの実験領域をシームレスにつなぐことができると期待される。

また、p_{device} の値は与えられた解候補を順番に離散対数問題に代入すれば効率的に計算可能であるため、あらかじめ答えを知らないランダムインスタンスの計算実験にこの枠組みを適用することでベンチマークとして用いることができる。この関係は計算量クラス NP に属する任意の計算問題に対して適用可能であり、素因数分解、他の群での離散対数問題、一般的な暗号解読問題も取り扱うことができる。

一方で、問題点として離散対数問題を解く場合に後処理アルゴリズムに入力するビット列の個数をいくつに取れば良いのかが不明であるという点、現在の格子ベースの後処理アルゴリズムがビット反転のような量子的ノイズに非常に弱いという点などがあり今後の課題である。研究を進めるにあたりより大きな離散対数問題を用いてシミュレーションを行うことが必要であるが、整数演算回路の複雑さから適切な規模のベンチマーク問題を構成することが難しいという課題も挙げられる。

3　量子コンピュータを用いた離散対数問題の計算実験

本節では IBM Quantum の量子コンピュータ ibm_kawasaki を用いて離散対数問題の計算機実験を行った結果について紹介する。まず、ターゲットとした離散

対数問題は(a) $2^z \equiv 1 \pmod 3$ 及び(b) $2^z \equiv 2 \pmod 3$ であり、考えられる中で最小のインスタンスである。これらは右辺のaが1か2かの違いしかないが、図2の $a^{-y} \bmod p$ の計算が省略可能であるかどうかにより回路の複雑さが異なり、トランスパイル後の回路における CNOT ゲート数がそれぞれ(a) 15 個と(b) 30 個と2倍の違いが出る。

3.1　実験結果と成功の判定

トランスパイル後の回路を 2021 年 7 月 21 日に量子コンピュータに投入し得られた 8,192 個のビット列からランダムにk個のビット列をサンプリングし後処理アルゴリズムに入力、出力の解候補集合に正解が含まれているかどうかの判定を行うことでp_{device}を計算した。シミュレーターの出力ビット列、ランダムビット列は生成した順にk個をまとめて後処理アルゴリズムに入力しp_{ideal}と$p_{uniform}$を計算した。(a) のインスタンスに対してはkの値によらずほぼ$p_{ideal} = 1$となり、離散対数問題が解けていることが主張できる一方で、(b) のインスタンスに関しては図 4 に示すとおり成功確率(灰色線)が基準値(赤点線)を大幅に下回るため、提案した基準に照らし合わせると解けていないという判断を下した。

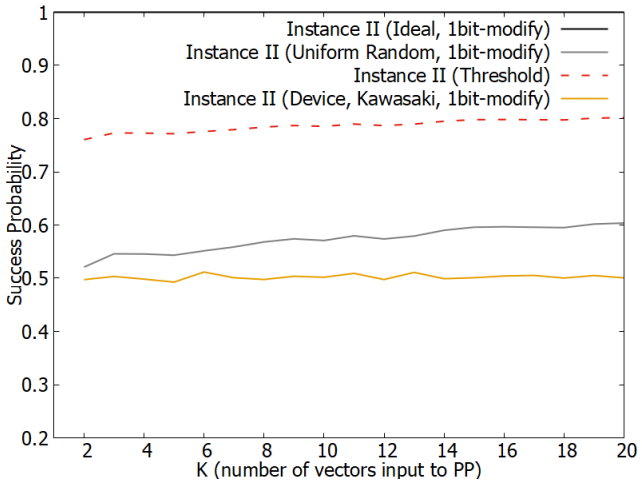

図 4　インスタンス (b) の実験結果。横軸は後処理アルゴリズムに入力するビット列の個数kである。黒線：p_{ideal}、黄線：$p_{uniform}$、赤点線：基準値$(p_{ideal} + p_{uniform})/2$、灰色線：$p_{device}$ デバイス出力の成功確率が基準値に届いていないため、実験成功を主張できない。

3.2　将来予測

(b) のインスタンスの計算実験は 2021 年当時の量子コンピュータでは成功しなかったが、性能進化によりいつ頃解けるのかという将来予測を行った。ノイズの大きさeを指定し、シミュレーターの出力を後処理アルゴリズムに入力したときの正解率をp_eとする。シミュレーション結果により$e = 0.07$のときに$p_{device} \approx p_{0.07}$となることが確認でき、ノイズが$e = 0.04$よりも小さい場合には(3)式の基準$(p_{ideal} + p_{uniform})/2 \leq p_e$を満たすことが確認できた。つまり、現在のノイズレベルが約半分になればインスタンス(b)が解けることが期待される。

次に、実機のノイズレベルが半分になるまでの時期を予測した。IBM が公表した過去の量子デバイスのリリース日と CNOT ゲートにおける平均ノイズレベルの一覧表 [9] を参考に、1 年で半分になる傾向が得られたため、(b) を解く量子コンピュータがリリースされるのは 2022 年の後半と予測でき、実際に 2022 年末の追試では解けていることが確認できた。

他のインスタンス$4^z \equiv 2 \pmod 7$、$3^z \equiv 4 \pmod 7$に対してノイズ付きの回路シミュレーションと成功率

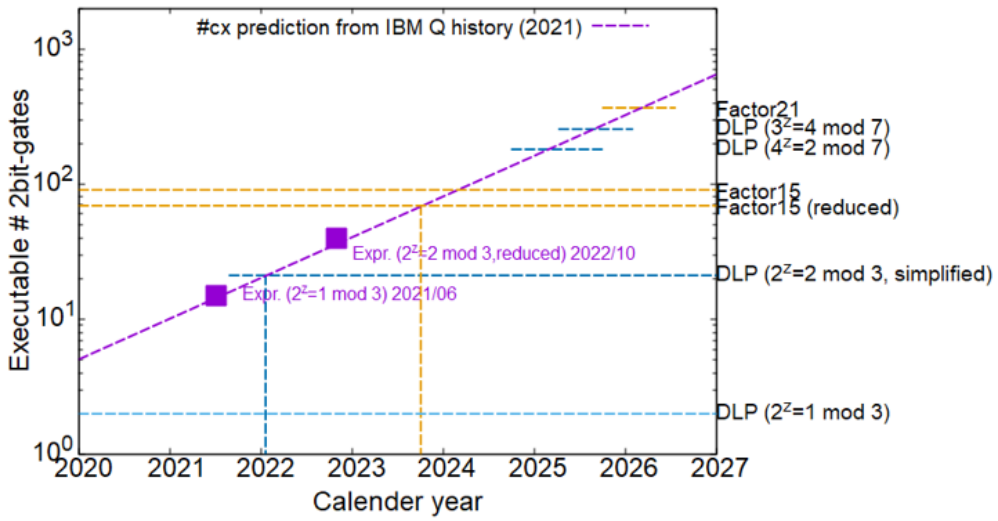

図 5　量子コンピュータ実機によるショアのアルゴリズムの実験結果と将来予測。紫の四角は実機での実験結果、点線が文献 [6] による 2021 年末時点でのトレンド予測である。

の比較を行ったところ、必要なノイズレベルeとトランスパイル後の CNOT ゲート数cの間に大体$e < 1/c$の関係があることが判明した。これはショアのアルゴリズムが非常にノイズに弱く、実行中に 1 回でもゲート操作にエラーが起きればその測定結果から問題の解を復元することが困難であることを示す。

しかしながら、たとえノイズに弱いとしても上記量子ノイズの傾向を合わせて考えると実行可能な CNOT ゲートの数が毎年 2 倍になることが予想される。この傾向に従うと、15,21 の素因数分解はそれぞれ 2023 年、2025 年頃に十分な成功率で可能になることが予測された。(図 5) そのため、2020 年代後半からショアのアルゴリズムの実験的研究が急速に進展する可能性がある。

ただし、小さい数を扱うショアのアルゴリズムの回路は数に合わせて極端に最適化されている一方で汎用的な数を扱う回路は最低でも数万ゲートを必要とするため現在の量子コンピュータのカバーする範囲からはほど遠い。この差を埋めるためには適度な大きさのベンチマーク問題を生成する必要があり、今後の課題のひとつである。

上記傾向をそのまま引き延ばすことで、2,048 ビットの RSA 暗号が 2050 年には解読可能となるという予測は可能であるが、冒頭で述べたとおりに量子誤り訂正・量子メモリ等の技術開発により大幅にずれる可能性はある。今後も技術動向に注目しつつ、研究を続けていきたい。

【参考文献】

1 P. Shor, “Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer,” SIAM J. Comput.,vol.26, no.5, pp.1484–1509.
2 NIST FIPS 186-5, “Digital Signature Standard (DSS),” https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-5.pdf
3 N Kunihiro, “Quantum Factoring Algorithm: Resource Estimation and Survey of Experiments, International Symposium on Mathematics, Quantum Theory, and Cryptography.” Mathematics for Industry, vol.33, pp.39–55, 2021.
4 C. Gidney and Martin Ekerå, “How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits,” Quantum 5, 433, 2021.
5 T. Ichikawa et al., “Current numbers of qubits and their uses,” Nature Reviews Physics, vol.6, pp.345–347, 2024.
6 Y. Aono et al., “The Present and Future of Discrete Logarithm Problems on Noisy Quantum Computers,” IEEE Transactions on Quantum Engineering, 3, pp.1–21, 2022.
7 IBM Quantum, https://docs.quantum.ibm.com/support
8 A.W. Cross et al. “Validating quantum computers using randomized model circuits,” Phys. Rev. A, vol.100, Iss.3, 032328.
9 https://research.ibm.com/blog/heavy-hex-lattice

青野 良範 （あおの よしのり）

サイバーセキュリティ研究所
セキュリティ基盤研究室
主任研究員
博士 (理学)
公開鍵暗号の安全性評価

【受賞歴】
2023 年　IEEE Signal Processing Society Best Paper Award
2021 年　科学技術分野の文部科学大臣表彰 若手科学者賞
2017 年　情報処理学会コンピュータセキュリティ研究会 (CSEC) 優秀研究賞

篠原 直行 （しのはら なおゆき）

サイバーセキュリティ研究所
セキュリティ基盤研究室
室長
博士 (数理学)
暗号に関する数理学

【受賞歴】
2019 年　The 14th International Workshop on Security (IWSEC 2019) Best Paper Award
2013 年　第 12 回 (2013 年) ドコモ・モバイル・サイエンス賞先端技術部門優秀賞
2008 年　日本数式処理学会第 17 回大会 2008 年度奨励賞