量子コンピューティング ユースケース集

RSA暗号の解読可能性評価

富士通



国立研究開発法人新エネルギー・産業技術総合開発機構（NEDO）

富士通：RSA暗号の解読可能性評価　【2023/01】　1／2

検証

産業領域	その他
手法	暗号解読
プロセス	–
技術分類	ゲート*

取組の背景

- 現在普及している**公開鍵暗号（RSA暗号等）の安全性は素因数分解問題の困難性**に立脚し、2,048ビットの合成数が広く利用されている
  - ✓ 現在古典コンピューターで解読可能な合成数は829ビットのため*1
  - ✓ 素因数分解の合成数N＝p x q（p、qは異なる素数）
- **古典コンピューターによる素因数分解を効率的に解く研究**も進められているが、現在最も漸近的に高速なアルゴリズムである数体ふるい法では、**合成数Nの桁長に対して準指数時間が必要となり解読が困難**
  - ✓ 2,048ビットの合成数の素因数分解に数体ふるい法を適用しスパコンを利用しても、最も高速なスパコン（Linpack性能1018FLOPS）でも数十年以上必要と推算される*2
- ところが、**量子コンピューターと高速計算可能なShorアルゴリズムの出現によりRSA暗号の現実的な時間内での解読可能性が示され**、理論的に解読された状態にある
  - ✓ **Shorアルゴリズムの計算量は合成数Nの桁長の多項式**時間となり、**古典コンピューターの計算時間から指数加速**されている

解決したい課題・モチベーション

- **量子コンピューターの出現により暗号の安全性が危殆化されるが、実際にどれくらいの量子コンピューターの計算リソースがRSA暗号の解読に必要かを検証した実験事例が少なく見積もりは困難な状況**
- よって、**富士通は量子シミュレータを活用し、2,048ビットのRSA暗号の安全性を評価するための素因数分解を実証した**

*1：「[Cado-nfs-discuss] Factorization of RSA-250」（https://web.archive.org/web/20200228234716/https:/lists.gforge.inria.fr/pipermail/cado-nfs-discuss/2020-February/001166.html）
*2：電子情報通信学会「量子計算機時代のセキュリティ―耐量子計算機暗号の動向―」（https://app.journal.ieice.org/trial/106_11/k106_11_966/index.html）
参考：富士通株式会社「量子シミュレータを活用したRSA暗号の安全性評価に成功」（https://pr.fujitsu.com/jp/news/2023/01/23.html）
*ゲート（gate-based）＝ 量子ビットに対して順に演算を適用することで計算を行う方式。通常のコンピュータにおける論理回路に近い考え方で、幅広い問題に対応可能。

富士通：RSA暗号の解読可能性評価　【2023/01】　2／2

検証

産業領域	その他
手法	暗号解読
プロセス	–
技術分類	ゲート*

量子コンピューターとしての問題設定

- 現在一般的に用いられている**2048ビットのRSA暗号を解読するために必要とされる量子コンピューターのリソース評価**を行った
- 計算機実験は、**入力された合成数を素因数分解する量子回路を生成する汎用的なプログラムをShorのアルゴリズムを活用して量子シミュレータに実装**した上で、**10ビットから25ビットのいくつかの合成数を素因数分解する量子回路を実際に生成**した
- **その際必要だった計算リソースから、2,048ビット合成数の素因数分解に必要な量子回路の計算リソース推定**を実行
- 自社開発の**39量子ビットの量子シミュレータを活用**し素因数分解を実行
  - ✓ 量子シミュレータはスパコン「富岳」のCPU「A64FX」の高速性と富士通が持つ大規模並列計算技術を活用

期待されるビジネス効果

- **N=15からN=511までの96個の素因数分解に成功**し、汎用的なプログラムが正しい量子回路を生成できることを確認した
- 10ビットから25ビットのいくつかの合成数を素因数分解する量子回路で必要な計算リソースから、2,048ビットの合成数を素因数分解するには**下記のスペックを持つ量子回路を使用しても104日間の計算量**が必要であることを示した
  - ✓ 量子ビット数: およそ1万量子ビット
  - ✓ ゲート数: およそ2兆2,300億
  - ✓ 量子計算のステップ数: およそ1兆8,000億回
- ただし、大規模かつ長時間（104日間量子ビットを誤りなく保持すること）にわたり**安定稼働するFTQCを短期的に開発することは困難**なことから、**2,048ビットのRSA暗号はShorアルゴリズムに対して安全**である、と評価

参考：富士通株式会社「量子シミュレータを活用したRSA暗号の安全性評価に成功」（https://pr.fujitsu.com/jp/news/2023/01/23.html）
*ゲート（gate-based）＝ 量子ビットに対して順に演算を適用することで計算を行う方式。通常のコンピュータにおける論理回路に近い考え方で、幅広い問題に対応可能。

WEBサイトにて、その他の事例も公開しています。ぜひご覧ください。
https://www.quantum-computing-use-cases.nedo.go.jp

他の事例を見る

国立研究開発法人 新エネルギー・産業技術総合開発機構（NEDO）
AI・ロボット部（e-mail：quantum_ai@ml.nedo.go.jp）

本ユースケース集は、国立研究開発法人新エネルギー・産業技術開発機構（NEDO）の委託業務「量子・古典ハイブリッド技術のサイバー・フィジカル開発事業／量子技術に関するユースケース事例調査」および「ポスト５Ｇ情報通信システム基盤強化研究開発事業（量子産業化）／量子コンピュータの産業化促進に向けた包括的調査」の成果として、得られたものです。