NICT 等、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

国立研究開発法人情報通信研究機構（NICT）、慶應義塾大学、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。

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して、ショアのアルゴリズム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。

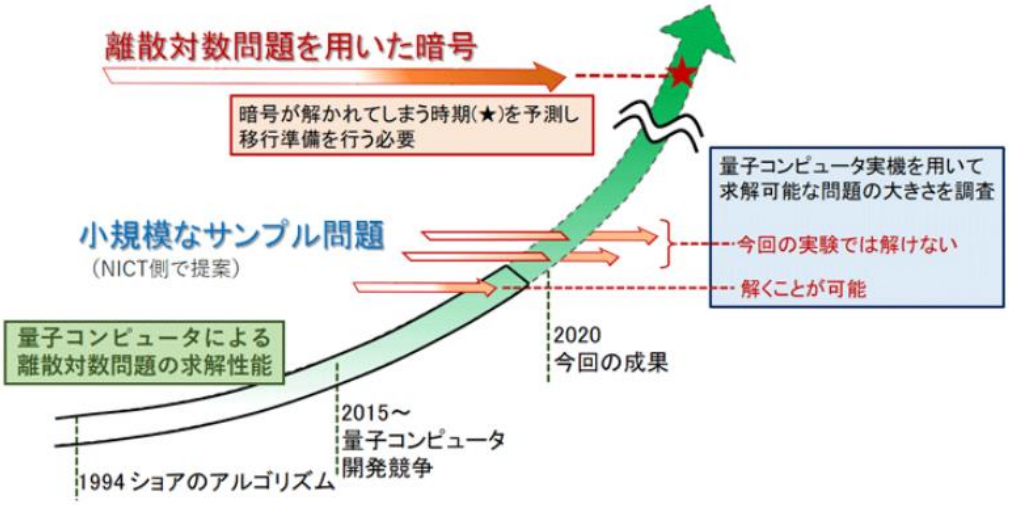

図 1 暗号の危殆化時期の予測に関する今回の成果を表す鳥瞰図

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。

実験では、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。

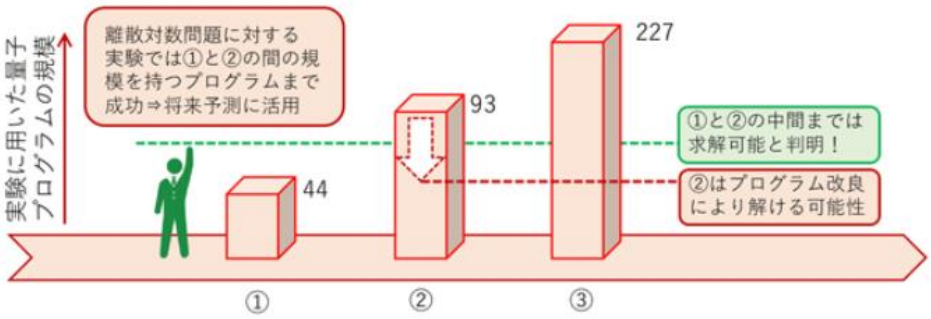

図 2 離散対数問題を解く量子コンピュータプログラムの規模と実験結果

日本語リリース
https://www.nict.go.jp/press/2020/12/09-1.html