量子コンピュータはスパコンを超えるか？

量子ゲート方式の量子コンピュータ

- アダマールゲート (H)、回転ゲート (π/8)、制御 NOT ゲート (CNOT) という 3 種類のゲートの組み合わせで、汎用的な量子計算が可能
- Google は、53 量子ビットの量子プロセッサー「Sycamore」を使用して スパコンで 1 万年かかる処理を 3 分 20 秒で解いたと発表
- 量子コンピュータに有利な「ランダム量子回路サンプリング」で検証
- 量子ゲートマシンは理論的には、従来型コンピュータをシミュレート可能

- 特定の計算しかスパコンに勝てない
- 量子ビットのエラー訂正技術が未対応
- 理論上は、既存の暗号化技術は将来破られる
- SHA-256 などの解読はまだまだ実現が困難
- 量子コンピュータの計算結果の検証が困難
- 量子ビットは壊れやすいため冷却設備が必要

2019 年 10 月 Google が、量子コンピュータによって最先端のスーパーコンピューターでも 1 万年かかるとされる処理を、200 秒で実行でき量子超越性（quantum supremacy）を実現したと科学誌「Nature」に掲載された論文で発表し、これに対し、IBM は、世界最速のスパコン「Summit」なら、2 日半で完了できるという反論もあり話題になりました。
今回該当する量子コンピュータは、すでに実用化された「D-Wave」で知られている組合せ最適化問題に特化している「量子アニーリング方式」ではなく、どんな計算問題を解けると期待されている「量子ゲート方式」です。そのため、スパコンよりも高速処理を量子コンピュータが実現したとなると、公開鍵やビットコインの暗号がいずれ破られてしまうのではないかという不安が増大し、世間を賑わせる結果になりました。以前から、理論上は量子コンピュータが実用化されれば、短時間で暗号解読が可能になり、現在主流の暗号方式ではセキュリティが守られないと懸念されていました。
ただ、残念ながら今回の計測は、量子コンピュータに乱数を生成する量子回路を実装し、実際にビット列の乱数を生み出し、それに並行して既存方式のスパコンでも同様の構成の量子回路をシミュレーションし、同じように乱数を生成して競わせるという、量子コンピュータにとって圧倒的に有利な「ランダム量子回路サンプリング」という実用では全く利用価値のない特殊な計算でした。
量子コンピュータは量子力学の原理に従って動作し、量子力学の基礎方程式を元に、量子コンピュータの動作を従来のコンピュータでシミュレーションすることが可能です。但し、量子ビット数が 50 を超えるような量子コンピュータをシミュレーションするには、スパコンでもとても長い処理時間がかかるということです。
今回は、53 ビットの量子ビットのコンピュータだったため、スパコンより優位に立てたわけですが、このレベルでは、とても RSA 暗号や、仮想通貨で使用されている SHA-256 などのハッシュ関数を解読することは到底無理です。
量子を安定させるために絶対零度近く（-273℃）まで冷却する設備もかなりの投資ですが、量子ビットのエラー訂正技術を実現するには数百万個から数億個の量子ビットが必要とされるというのも非現実的に思えます。
量子コンピュータの高度な計算結果は量子コンピュータでしか検証できないということに加え、このエラー訂正の問題があるため出てきた答えが正解なのかどうか証明することはとても困難であるという事実が、量子コンピュータが本当に実社会で利用可能になるのかどうか、まだまだ不安にさせています。