資料16－3

量子コンピュータと その暗号技術への影響

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
野島 良

国立研究開発法人
情報通信研究機構
National Institute of Information and Communications Technology

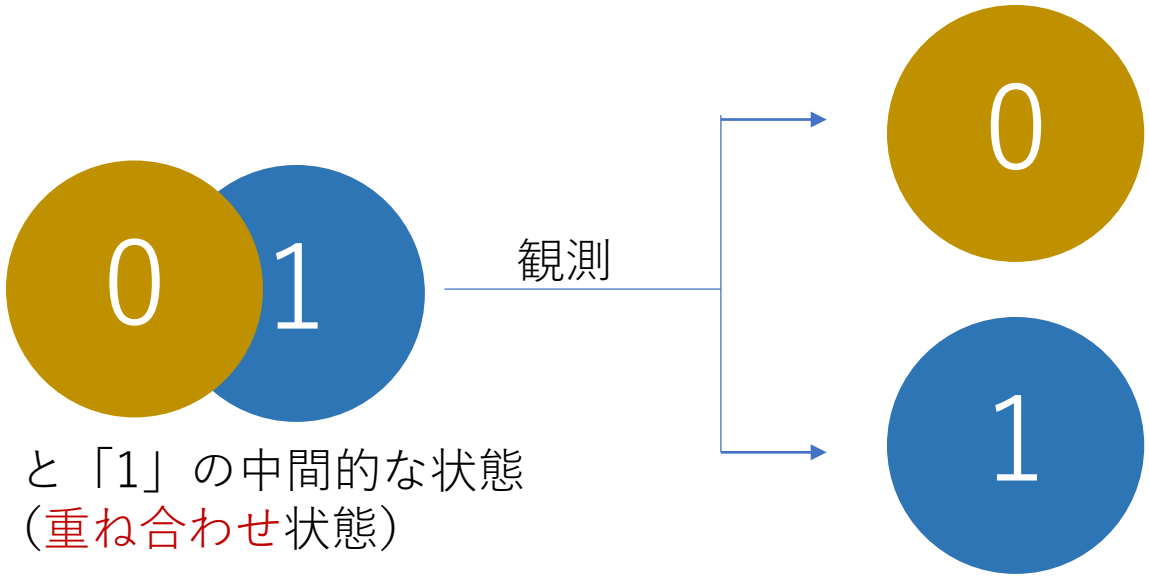
背景

- Google が Sycamoreプロセッサ を開発
  - 量子コンピュータ
  - 53量子ビットを使い”量子超越性”を実証
    - 世界最速のスーパーコンピューターで1万年かかる計算を200秒で完了
- 大規模な量子コンピュータが出現すると …
  - 新薬の開発、機械学習など、さまざまな分野への応用が期待される
  - まだ道のりは遠いが、主要な公開鍵暗号（素因数分解、楕円曲線ベース）を破ることができる

量子と古典の本質的な違い: 量子メモリ

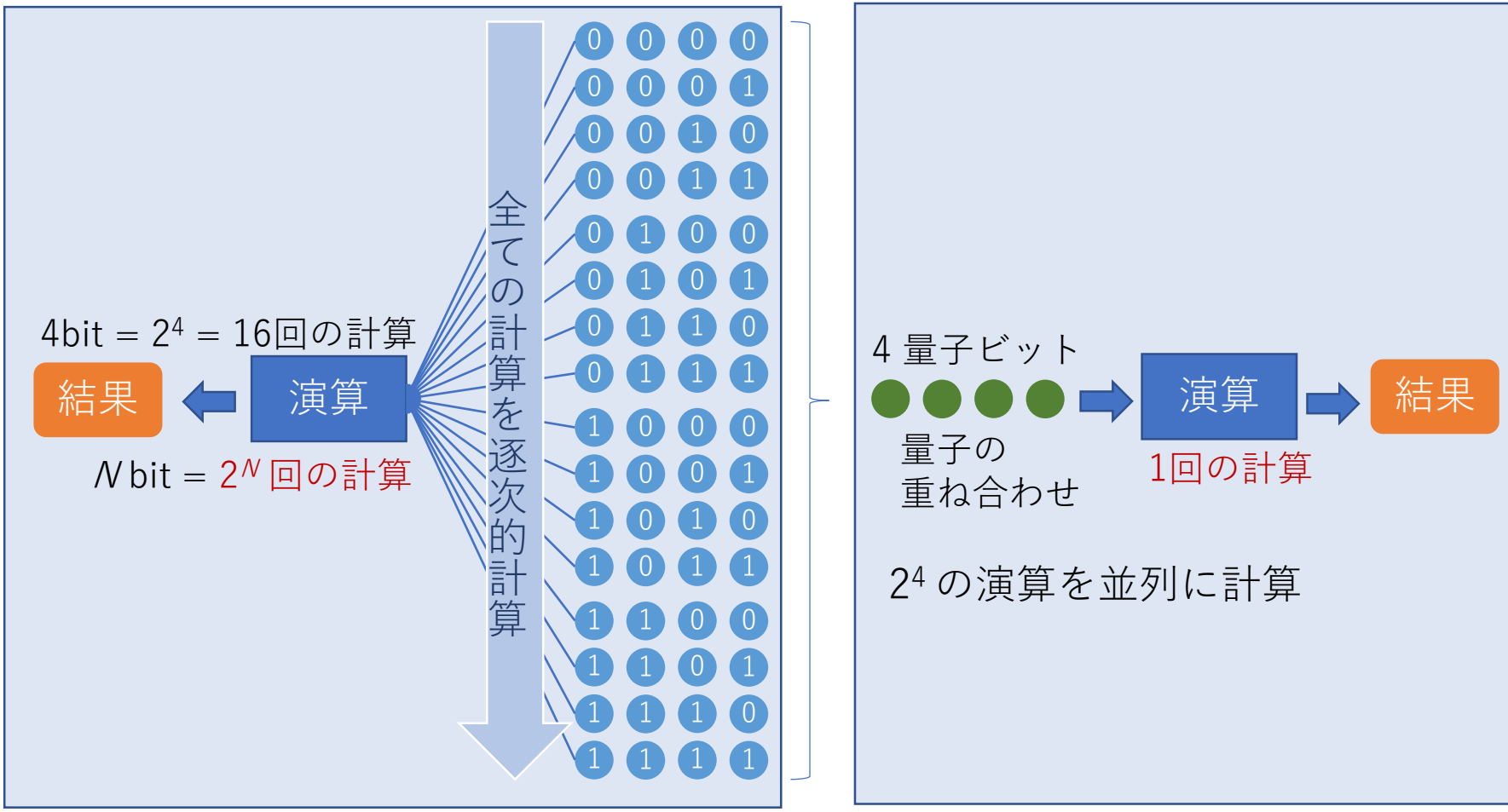
- 通常のコンピュータでの情報の最小単位 は**ビット**

- 量子コンピュータでの情報の最小単位 は**量子ビット**



量子コンピュータの優れているところ

- 量子重ね合わせにより、超並列計算を実現



量子超越性の意味するところ

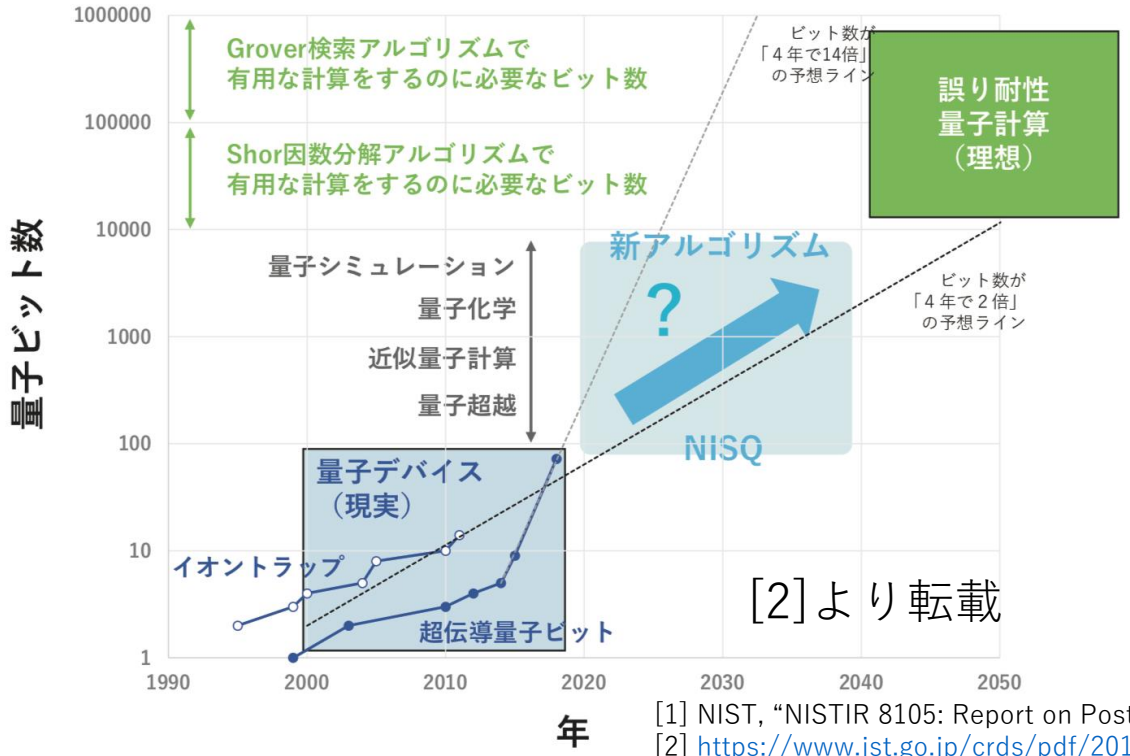
- 量子コンピュータの量子メモリはまだ小さいため、古典コンピュータよりも優れていることを示すことは困難
  - 量子コンピュータが得意とする素因数分解でも、まだ 15 (=3×5) や 21 (=3×7) が解ける段階

- 量子超越性は重要なマイルストーン:
  - （どのような演算でもよいため）量子コンピュータが古典よりも速く処理できることを示すこと。

- 今回の量子超越性の達成では、ランダム量子回路サンプリングを採用
  - 量子コンピュータが出力する結果を予測するという演算
  - メモリサイズがある程度大きく、エラー率が低いため達成できたか

量子コンピュータ今後の展開

- ある種の計算に役立つ量子コンピュータについては、5～10年で商業化（ジャーロッド・マクレーン博士、10/29 毎日新聞）
- 米国では、2030年頃までに公開鍵長2,048ビットのRSA暗号を解読可能な量子コンピュータが実現し得ることを想定[1]
- 科学技術未来戦略ワークショップ報告書[2]からは、RSA暗号の危殆化は2025年～2050年と推察される

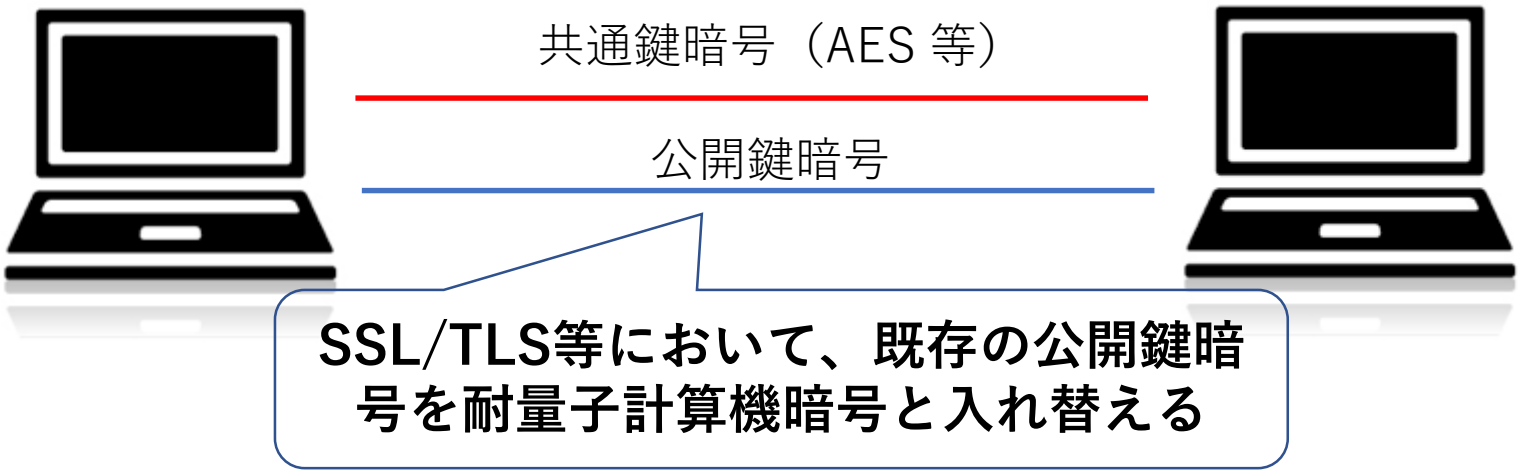


[2]より転載

[1] NIST, “NISTIR 8105: Report on Post-Quantum Cryptography,” April, 2016.
[2] https://www.jst.go.jp/crds/pdf/2018/WR/CRDS-FY2018-WR-09.pdf

まとめ：今後の対策

- 現在使っている公開鍵暗号から耐量子計算機暗号(PQC)に移行することで対応可能
  - PQCとして、格子暗号、多変数多項式暗号など世界中で研究開発・標準化が進んでいる



- 長期的視点に立つと、量子鍵配送という選択肢もある