PQCヒアリング
誤り耐性型量子コンピュータ（FTQC)
について

内閣府 2025.9.8

大阪大学 量子情報・量子生命研究センター センター長
北川 勝浩

北川 勝浩

1983-93 日本電信電話公社武蔵野電気通信研究所/NTT基礎研究所
1993-96 大阪大学 助手 基礎工学部
1996-97 大阪大学 講師 基礎工学部
1997-03 大阪大学 助教授 大学院基礎工学研究科
1999-05 CREST 核スピンネットワーク量子コンピュータ
（日本初の量子コンピュータ研究プロジェクト）
2003-24 大阪大学 教授 大学院基礎工学研究科
2005-11 CREST 分子スピン量子コンピュータ
2009-14 FIRST 量子情報処理プロジェクト
2009-14 新学術 量子サイバネティックス
2014-16 量子の冬
2016-22 CREST 室温超核偏極と量子符号化による超高感度生体MRI/NMR
2018 (株)QunaSys 共同創業
2018-20 先導的学際研究機構 量子情報・量子生命研究部門長
2020- ムーンショット目標6 プログラムディレクター
2020- 内閣府量子技術イノベーション会議 構成員
2020-21 先導的学際研究機構 量子情報・量子生命研究センター長
2020- COI-NEXT量子ソフトウェア研究拠点 プロジェクトリーダー
2021- 世界最先端研究機構 量子情報・量子生命研究センター長
2021 キュエル(株) 共同創業

Physical Review A 50th Anniversary Milestones

PHYSICAL REVIEW A

Squeezed spin states
Masahiro Kitagawa and Masahito Ueda
Phys. Rev. A **47**, 5138 (1993)

本日の内容

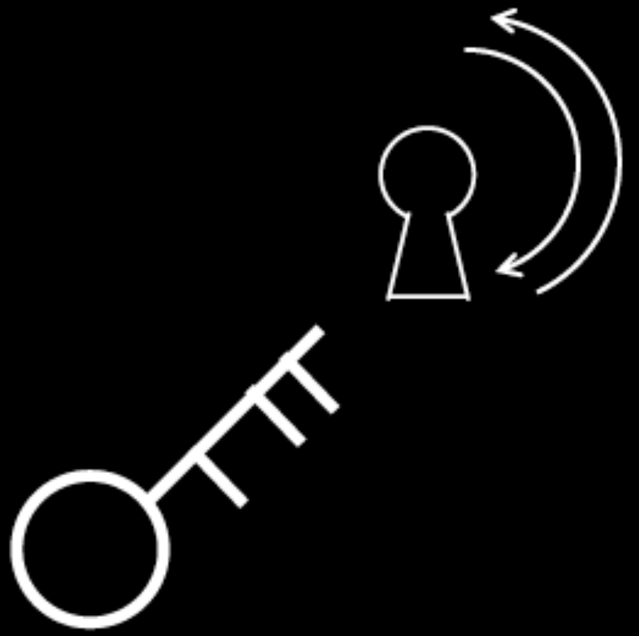
- 公開鍵暗号と量子コンピュータ
- 量子コンピュータの現状
- 誤り耐性量子コンピュータに向けた開発競争

量子技術

- 量子コンピュータ
  - NISQ　誤りがある中小規模の量子コンピュータ（計算規模に限界）
  - FTQC　　誤り耐性型量子コンピュータ（大規模計算可能でスパコンを凌駕）
- 量子暗号・量子セキュリティ
  - 量子鍵配送（量子暗号）量子コンピュータでも破れない暗号（物理）
  - 耐量子計算機暗号（PQC）量子コンピュータでも破れない暗号（数理）
- 量子計測・センシング
  - 光格子時計　精度18桁（100億年に1秒の誤差）、重力センサ数cm
  - 量子ジャイロ（原子波干渉計）GPSに依らない航法（北極海潜水）
  - ナノ量子センサ（NVダイヤモンド）
  - 超偏極MRI
- 量子生命科学　（長期的）
  - 量子ジャイロ（渡り鳥の目の地磁気コンパス）
  - 光合成、窒素固定など生物の酵素反応の解明と模倣

暗号

- 共通鍵暗号

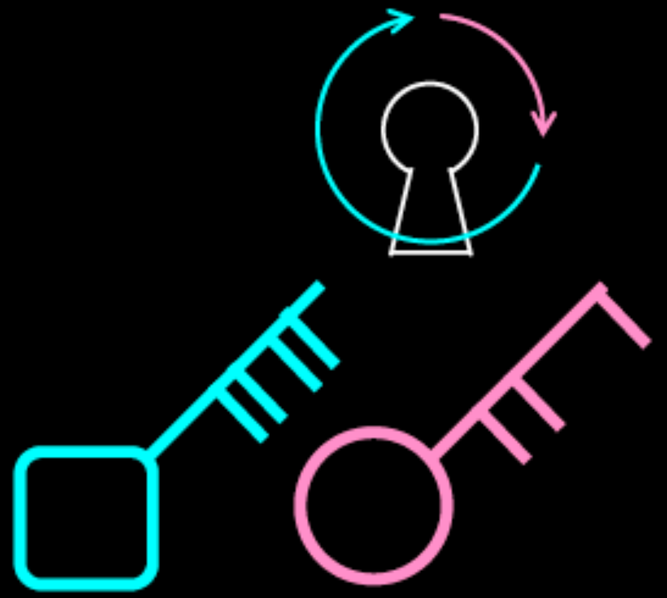


共通鍵

暗号化
復号化

鍵の配送が困難

- 公開鍵暗号



秘密鍵　　公開鍵

復号化　　暗号化

米 デフィー、ヘルマン 1976

米 リベスト、シャミア、エイデルマン 1979

RSA公開鍵暗号

(リベスト,シャミア,エイデルマン 1979)

英GCHQ エリス1969・コックス 1973

アリス Alice

- 大きな素数p, qを選ぶ
- $N=pq$を計算する
- Nとランダム数eを公開
- $ed=1 \pmod{(p-1)(q-1)}$ となる秘密鍵dを保管
- $c^d=x^{ed}=x^{1+k(p-1)(q-1)}$ $=x \pmod{N}$ で、暗号文を解読

公開鍵 N, e

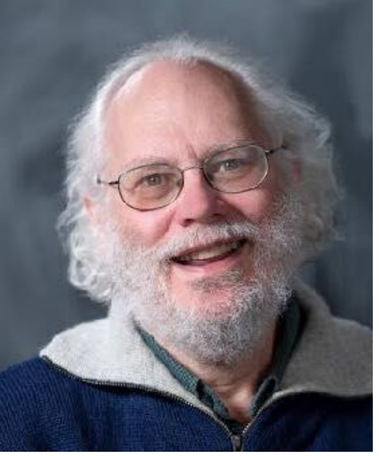
暗号文 c

ボブ Bob

- アリスの公開鍵N,eで通信文xを暗号化する $c=x^e \pmod{N}$
- cをアリスに送信

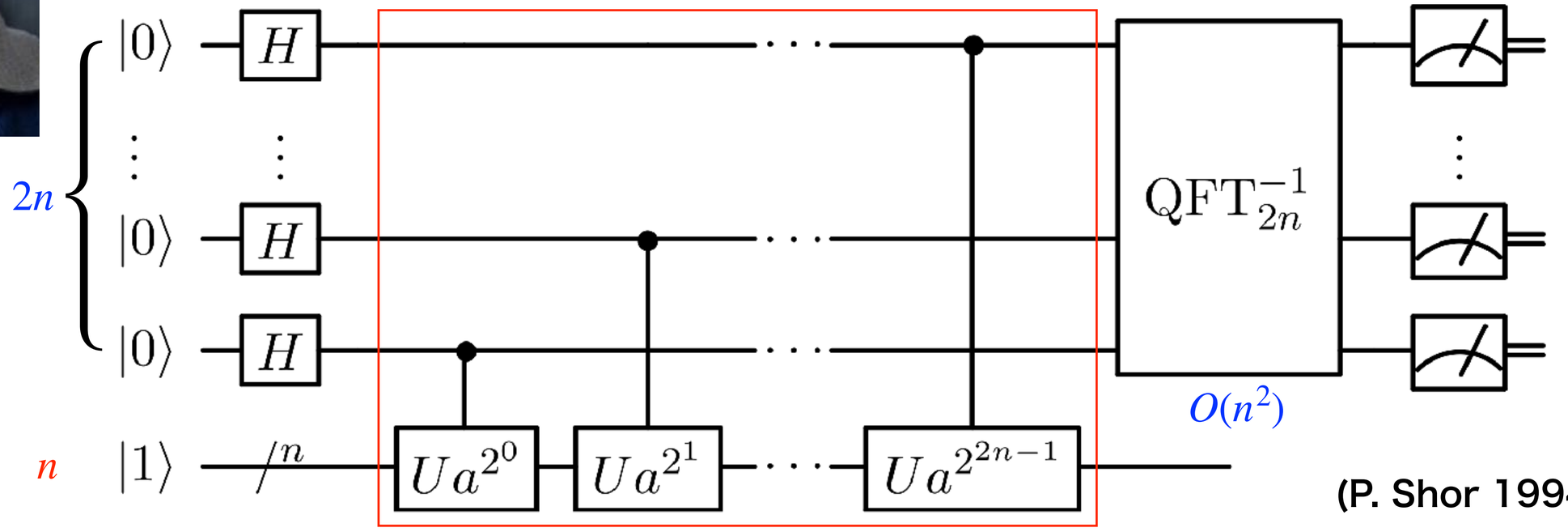
盗聴者イブ Eve

- 公開鍵N,eを入手
- 盗聴によってcを入手
- Nさえ因数分解できれば…



Shorの量子アルゴリズム

n bitの整数の素因数分解　＝周期を求めるアルゴリズム



(P. Shor 1994)

古典で最速の
アルゴリズム
数体ふるい法

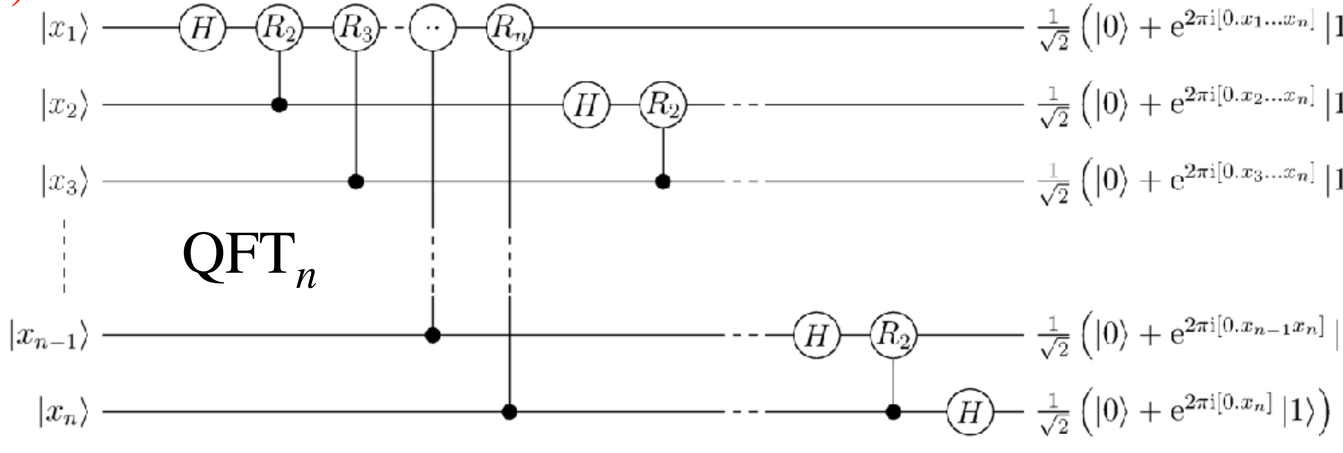
$\exp(cn^{1/3}(\log n)^{2/3})$

手に負えない

2048 bitの素因数分解

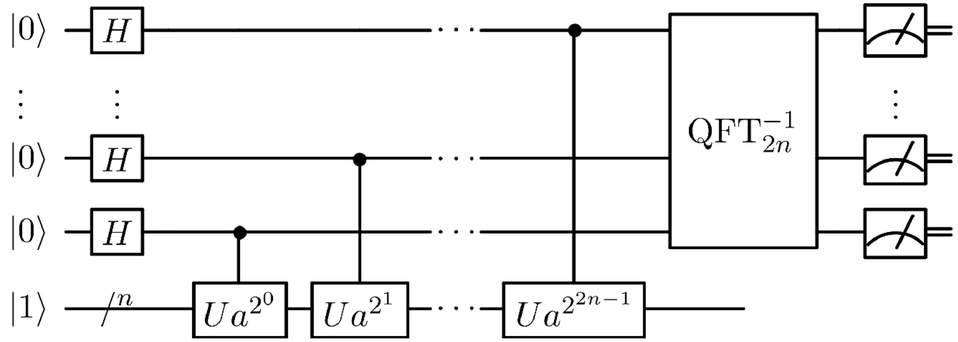
$3n \approx$ 6k qubits

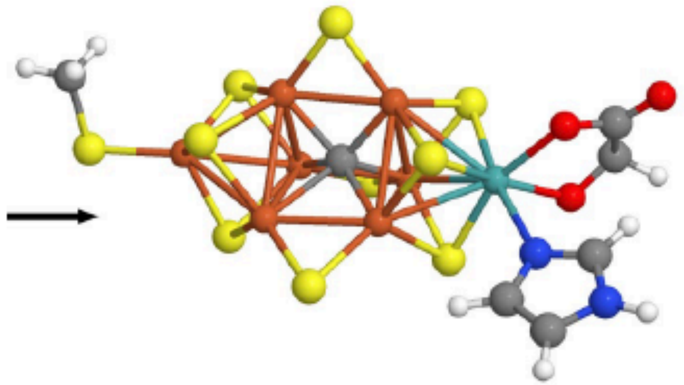
$O(n^3) \approx$ 8G gates



量子ビット数n、ゲート数g、誤り率$p < 1/g$

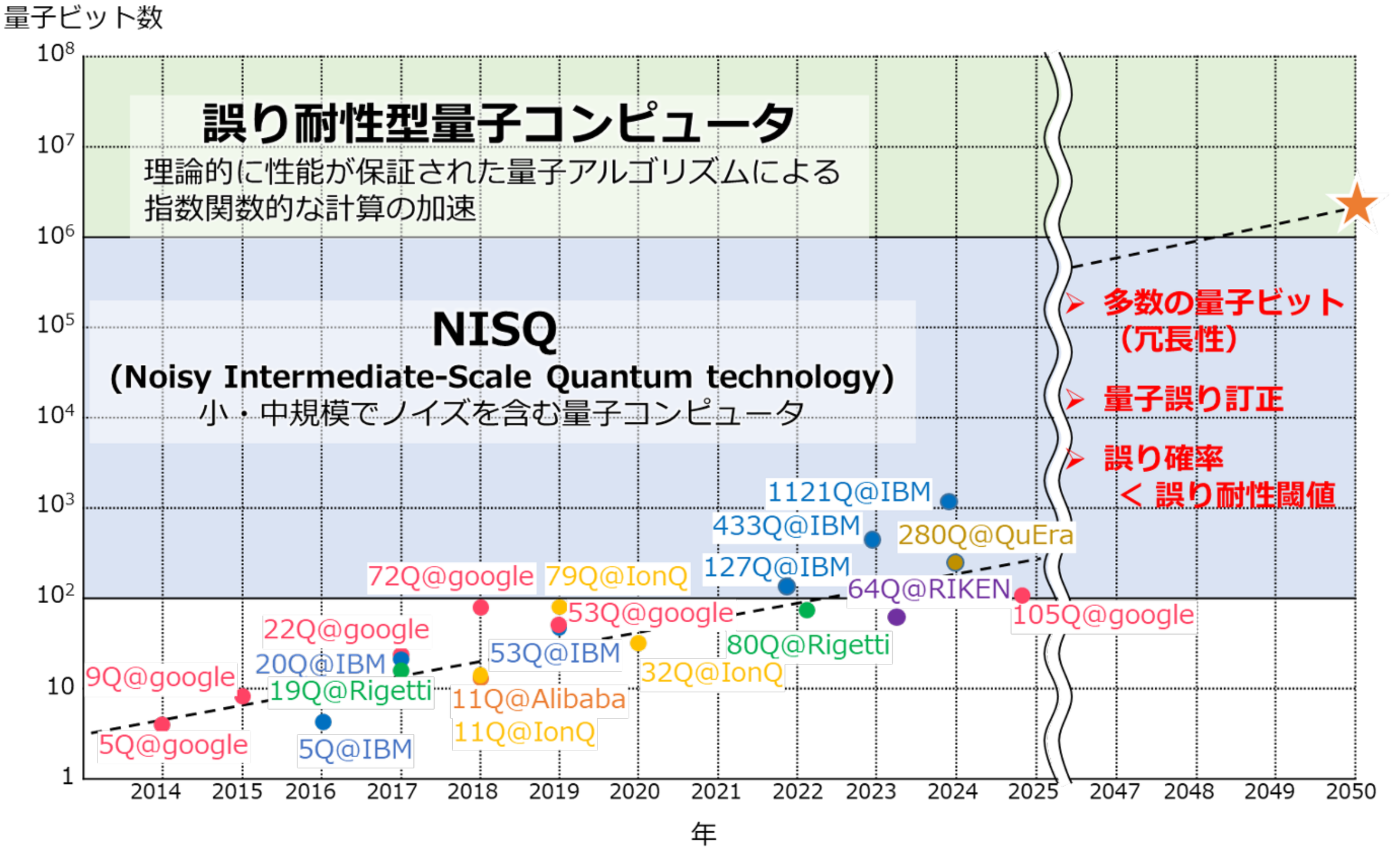
- 2048ビットの因数分解
  - $n = 6\text{k}$, $g \approx 8\text{G}$, $p \approx 10^{-10}$
- FeMocoの精密量子化学計算
  - $n = 2\text{k}$, $g \approx 5.3 \times 10^9$, $p \approx 10^{-10}$





本日の内容

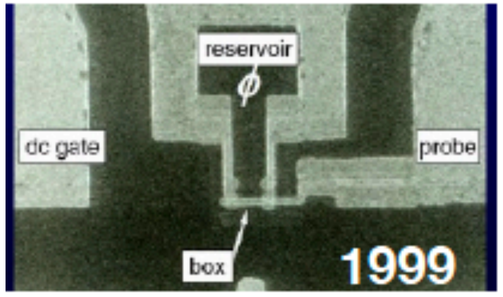
- 公開鍵暗号と量子コンピュータ
- 量子コンピュータの現状
- 誤り耐性量子コンピュータに向けた開発競争


量子ビット数
10^8
10^7
10^6
10^5
10^4
10^3
10^2
10
1
誤り耐性型量子コンピュータ
理論的に性能が保証された量子アルゴリズムによる
指数関数的な計算の加速
NISQ
(Noisy Intermediate-Scale Quantum technology)
小・中規模でノイズを含む量子コンピュータ
➢ 多数の量子ビット
（冗長性）
➢ 量子誤り訂正
➢ 誤り確率
＜ 誤り耐性閾値
1121Q@IBM
433Q@IBM
280Q@QuEra
127Q@IBM
64Q@RIKEN
105Q@google
72Q@google
79Q@IonQ
53Q@google
22Q@google
20Q@IBM
53Q@IBM
80Q@Rigetti
9Q@google
19Q@Rigetti
32Q@IonQ
11Q@Alibaba
11Q@IonQ
5Q@google
5Q@IBM
2014
2015
2016
2017
2018
2019
2020
2021
2022
2023
2024
2025
2047
2048
2049
2050
年

野心的なロードマップ

- 超伝導
  - IBM https://www.ibm.com/quantum/technology.　https://www.ibm.com/roadmaps/quantum/
  - Google https://quantumai.google/roadmap
- イオントラップ
  - Quantinuum https://www.quantinuum.com/press-releases/quantinuum-unveils-accelerated-roadmap-to-achieve-universal-fault-tolerant-quantum-computing-by-2030
  - IonQ https://ionq.com/blog/ionqs-accelerated-roadmap-turning-quantum-ambition-into-reality
- 中性原子 QuEra, Atom Computing, Infleqtion, Pasqal, Yaqumo
  - QuEra https://www.quera.com/qec
  - Pasqal https://www.pasqal.com/technology/roadmap/
- 光量子 PsiQuantum, Xanadu, OptQC
- 半導体 Intel, Silicon Quantum Computing, Quantum Motion, Equal1, etc.

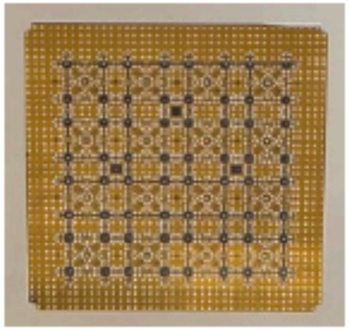
世界初の超伝導
量子ビット



超伝導量子コンピュータ
国産初号機

64-qubit
(53-qubit)

March 27, 2023



第53回
日本産業技術大賞
内閣総理大臣賞

理化学研究所
産業技術総合研究所
情報通信研究機構
国立大学法人 大阪大学
富士通株式会社
日本電信電話株式会社

企業名	方式	量子ビット
IBM（米）	超電導	433
Rigetti Computing（米）	超電導	84
Google（米）	超電導	72
理化学研究所	超電導	64
百度（中国）	超電導	36
Oxford Quantum Circuits（英）	超電導	32
IonQ（米）	イオントラップ	29

（出所：NIKKEI Tech Foresightが作成、23年8月時点）

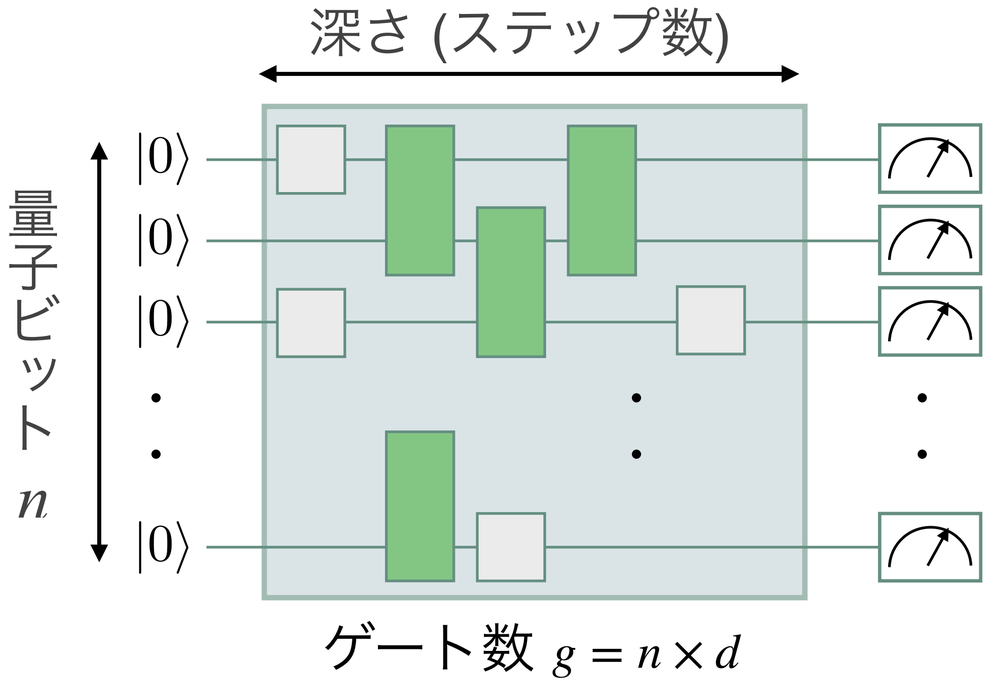
理化学研究所　NICT　FUJITSU
産総研　大阪大学 OSAKA UNIVERSITY　NTT

2023年は国産量子コンピュータ元年

量子ビット数 n、ゲート数 g、誤り率 p

- **現状ベスト**

量子ビット数 $n \approx 100$, **誤り率** $p \approx 0.001$ (0.1%)



- **計算の成功確率**（全てのゲートで演算が成功）

ゲート数 g = 量子ビット数 n × 深さ d

$g = 1000$　$(1-p)^g = 0.999^g = 0.367...$　37%は成功　$(n = 50,\ d = 20)$

$g = 10000$　$(1-p)^g = 0.999^g = 0.000045...$ ほぼ無理　$(n = 50,\ d = 200)$

$p \leq 1/g$ でないと有意な確率で成功しない

量子ビット数 n、ゲート数 g、誤り率 p の関係

- **現状ベスト** 量子ビット数 $n \approx 100$, **誤り率** $p \approx 0.001$ (0.1%)

- 計算の成功確率（全ての演算が成功する確率）
  $g = 1000$　$(1-p)^g = 0.999^g = 0.367...$　有意な確率37%で成功
  $g = 10000$　$(1-p)^g = 0.999^g = 0.000045...$　無理
  $p \leq 1/g$ でないと有意な確率で成功しない

- **アプリケーションからの要求**
- 2048ビットの因数分解
  - $n = 6\text{k}$, $g \approx 8\text{G}$, $p \approx 10^{-10} \leq 1/g$
- FeMoCoの精密量子化学計算
  - $n = 2\text{k}$, $g \approx 5.3 \times 10^9$, $p \approx 10^{-10} \leq 1/g$

量子ビット、量子ゲートの
物理的な改善だけでは埋められない

誤り率のギャップ

量子誤り訂正 QEC
誤り耐性量子計算 FTQC
（ムーンショット目標６）

本日の内容

- 公開鍵暗号と量子コンピュータ
- 量子コンピュータの現状
- 誤り耐性量子コンピュータに向けた開発競争

Google 誤り耐性閾値以下での量子誤り訂正に成功

105物理量子ビットの超伝導QPUで、表面符号をリアルタイムにデコードして誤り訂正を行った。
符号距離 $d = 5$ に比べて$d = 7$ の方が１サイクル当たりの論理誤り率が1/2.14に下がった。
寿命も2.4倍となり、明確にブレークイーブンを下回った。

nature

Explore content ⌄ About the journal ⌄ Publish with us ⌄

nature › articles › article

Article | Open access | Published: 09 December 2024

Quantum error correction below the surface code threshold

Google Quantum AI and Collaborators

Nature **638**, 920–926 (2025) | Cite this article

大きなブレークスルー
しかし、
・論理量子ビットが1つできただけ
・論理誤り率も0.143%/サイクル
なので、量・質ともに全然足りない

↓

物理量子ビットの
・数を飛躍的に増やす
・誤り率を下げる
ことが必要

著作権の関係で、下記URLをクリックしてご覧ください。

論文 https://www.nature.com/articles/s41586-024-08449-y

Blog https://research.google/blog/making-quantum-error-correction-work/

2048-bitの数を因数分解するには

- 6k 論理量子ビット、5G 論理量子ゲート、論理誤り率 $P_L \approx 10^{-10}$

- $p = 10^{-3}$ (0.1%) の場合
  - $d = 15, \quad 2d^2 - 1 = 449$ 物理量子ビット
  - 3M（300万）物理量子ビット
- $p = 10^{-4}$ (0.01%) の場合
  - $d = 7, \quad 2d^2 - 1 = 97$ 物理量子ビット
  - 600k（60万）物理量子ビット

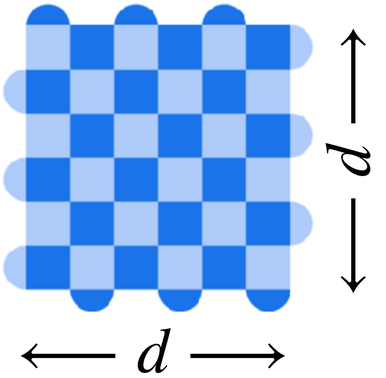
表面符号

誤り耐性閾値 $p_{th} = 0.01$

符号距離 d

論理誤り率

$$P_L = p_{th}\left(\frac{p}{p_{th}}\right)^{(d+1)/2}$$



物理量子ビット数/論理量子ビット

$2d^2 - 1$

物理量子ビットは質（誤り率）も量（ビット数）も全然足りない

ここから、新・未来へ

MOONSHOT
RESEARCH & DEVELOPMENT PROGRAM

ムーンショット目標６

2050年までに、経済・産業・安全保障を飛躍的に発展させる誤り耐性型汎用量子コンピュータを実現











量子ハードウェア

超伝導	イオントラップ	光量子	半導体 量子ドットアレイ	半導体 スパースマトリクス	中性原子 2次元アレイ	中性原子 ナノファイバー
山本剛PM (NEC)	高橋PM (OIST)	古澤PM (東大)	水野PM (日立)	樽茶PM (理研)	大森PM (分子研)	青木PM (早大)

量子通信ネットワーク

小坂PM (横国大)
山本俊PM (阪大)
永山PM (慶大)

超伝導と通信の連携

光検出器で連携

分散QC連

量子ビット接続で連携

量子ネットワークシステム技術

誤り耐性

小芦PM (東大)
小林PM (京繊大)

量子誤り訂正・誤り耐性理論／ソフトウェア

誤り訂正システム（古典部分）実装

研究開発体制図： プログラムポートフォリオ

黒枠は2020年度採択
赤枠は2022年度採択

理論・ソフトウェアプロジェクトにおいて、マルチレイヤー協調設計モデルを構築し、研究開発の指針を得る。
内外の研究開発の活発化に対応し、2022年度にプログラムの強化・アップデートを実施。

スーパーコンピュータでは、複雑に絡み合う量子状態の計算は困難

大規模な量子状態の厳密計算を可能とする
「誤り耐性型汎用量子コンピュータ」を実現する

2050 大規模化を達成し、誤り耐性型汎用量子コンピュータの実現

2040 中規模な誤り耐性量子コンピュータの実現（スパコンを超える有用計算が可能）
~~分散処理型NISQ量子コンピュータの実証 量子誤り訂正下での有用タスク計算~~

2030 小規模または部分的な誤り耐性をもつ量子コンピュータの実現（PoC）
~~一定規模のNISQ量子コンピュータの開発と量子誤り訂正の有効性実証~~

＜量子コンピュータシステム＞
量子ビット、量子ゲート、量子誤り訂正（エラーシンドローム測定等量子部分）を開発し、量子誤り訂正システム（古典部分）と合わせて、誤り耐性量子コンピュータシステムを開発。

公募を通し
実現可能性・将来性
のあるPJを見極める

超伝導・イオントラップ・光量子・半導体・中性原子などの物理量子ビット７PJ

＜量子バス・量子通信ネットワーク＞
ハードウェア単体の物理限界を超えて誤り耐性量子コンピュータの規模を拡大する量子接続技術（量子バス、量子インターフェイス、量子通信ネットワーク等）を開発。

公募を通し
共通基盤技術
開発に絞り込む

３PJ

＜量子誤り訂正・誤り耐性理論＞
誤り耐性量子コンピュータ開発のための理論（量子誤り訂正符号、誤り耐性、アーキテクチャ、モデル化、設計法、指針等）。

＜量子誤り訂正システム（古典部分）＞
誤り耐性量子コンピュータの量子誤り訂正システム（古典部分）（エラーシンドローム解析、量子ハードウェアとのインタフェース）を開発。

＜アプリケーション＞
誤り耐性量子コンピュータのアプリケーション（量子アルゴリズム、ソフトウェア）の開発、実行条件（論理量子ビット数・論理誤り率）の緩和、アプリケーション開発環境の開発、ELSI問題の研究。

公募により新規PJ採択

世界に伍する成果に向かって研究開発