CRYPTRECシンポジウム2022

量子コンピュータと暗号

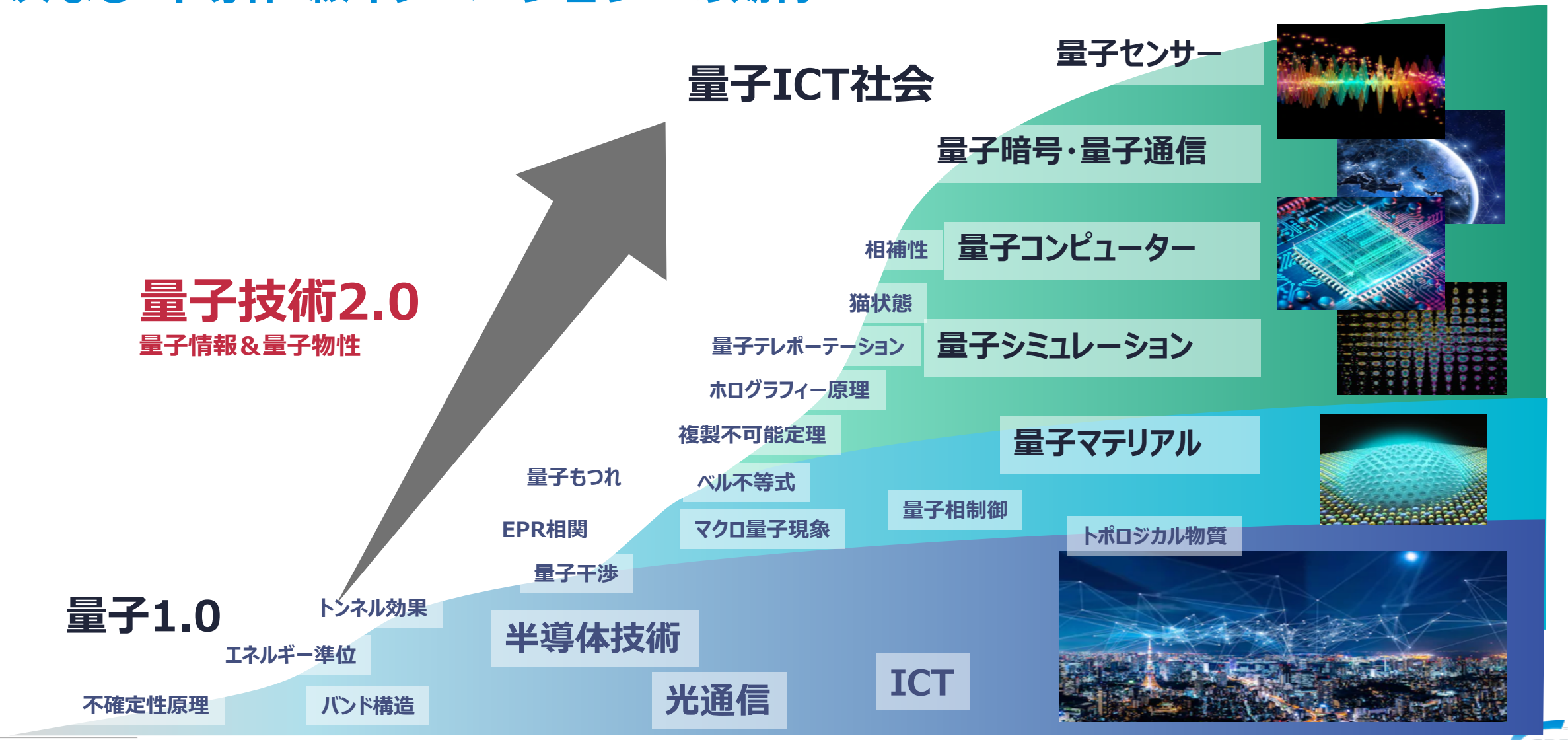
2022年7月5日

JST研究開発戦略センター(CRDS)
フェロー　嶋田 義皓

国立研究開発法人科学技術振興機構 研究開発戦略センター
Center for Research and Development Strategy Japan Science and Technology Agency

量子革命

次なる“半導体”級イノベーションへの期待



Google検索 “Quantum Computer will…”

2019/6/20	2021/6/24	2022/6/29
QC will **never work**	Will QC **destroy bitcoin**	QC will **be**
QC will **kill bitcoin**	Will QC **break bitcoin**	QC will **destroy bitcoin**
QC will **destroy bitcoin**	Will QC **be built**	QC will **never work**
QC will **fail**	Will QC **replace supercomputer**	QC will **break encryption**
QC will **be**	QC will **never work**	QC will **change the world**
QC will **not work**	QC will **be**	QC will **change everything**
How QC will **change the world**	**Why** QC will **fail**	QC will **not work**
What will a QC do	**When** will QC be available	QC will **never work reddit**

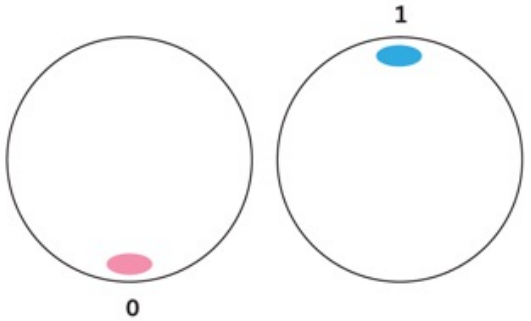
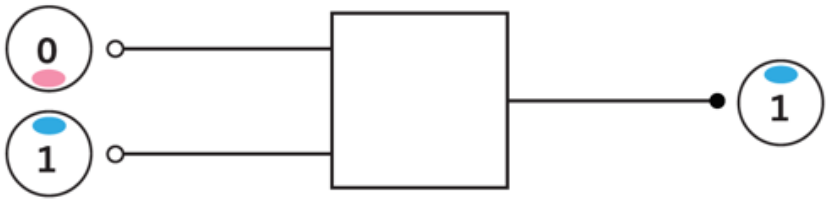
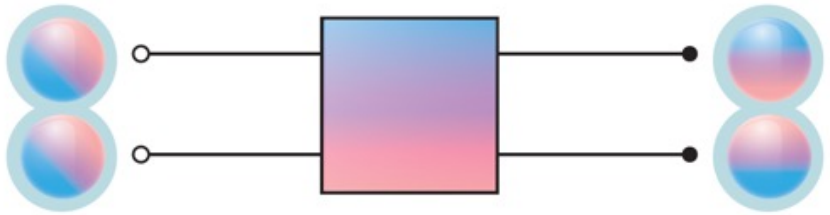
量子未来社会ビジョン

Designed by macrovector / Freepik

内閣府「量子未来社会ビジョン」（2022/4/22）
https://www8.cao.go.jp/cstp/ryoshigijutsu/ryoshi_gaiyo_print.pdf

1. 量子コンピュータの基礎

ビットと量子ビット

	コンピュータ	量子コンピュータ
	ビット	量子ビット
ビット	 $x \in \{0,1\}$	 $\|\psi\rangle = a\|0\rangle + b\|1\rangle$
	論理ゲート	量子論理ゲート
ゲート		
	• 0 または 1 • コピーが可能	• 0 と 1の重ね合わせ状態 • コピーは不可能 • 量子もつれ利用可能

A. Trabesinger, *Nature* 543, S2–S3 (2017)

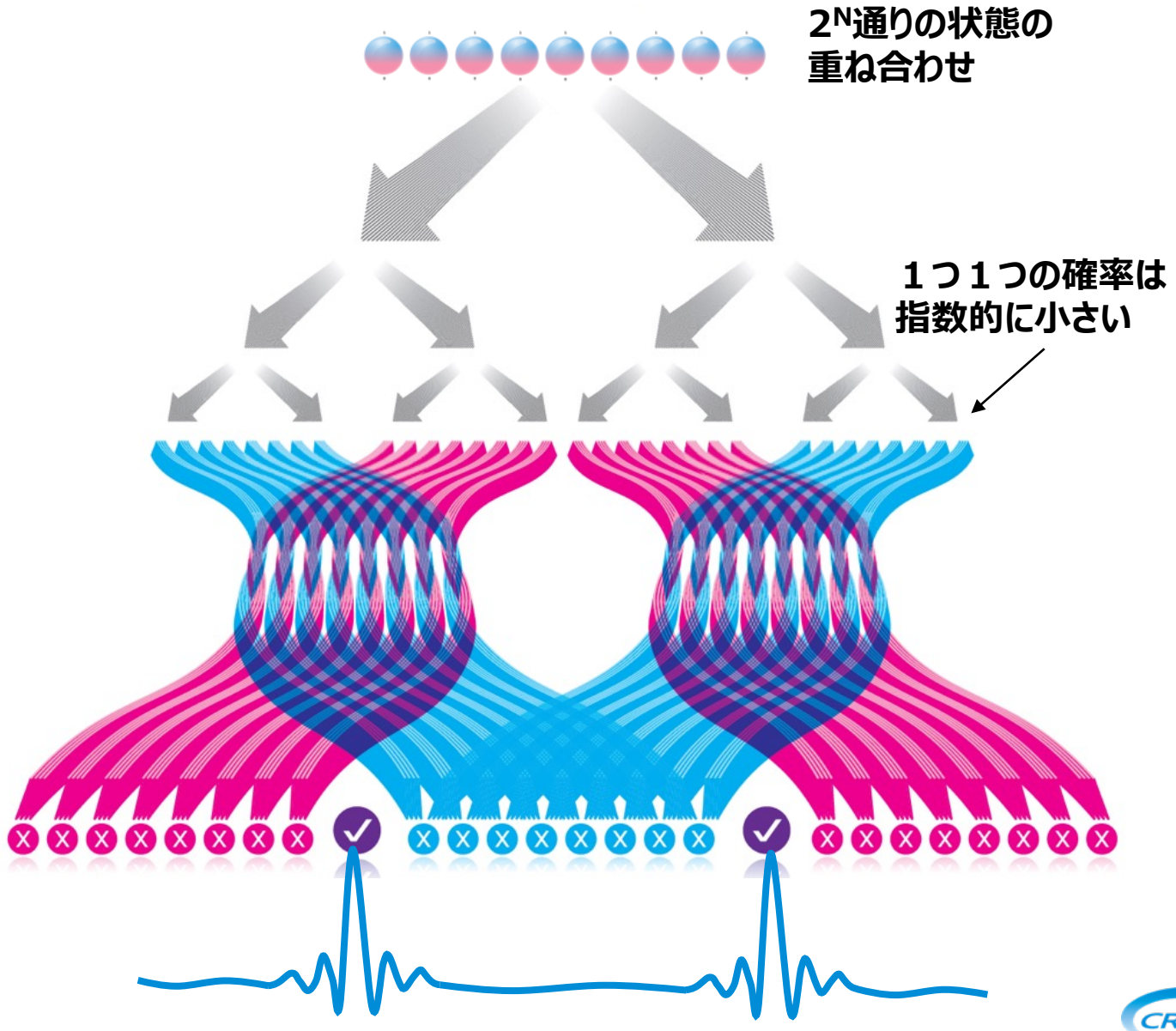
量子コンピュータの計算原理

0．初期化
指数的規模の組み合わせの超並列処理

1．超並列処理
重ね合わせ状態に対する量子ゲート操作

2．確率の波の干渉
正答確率の増幅（それ以外の答えの削減）

3．測定
量子ビットの状態を測定し、結果を取り出す



http://seedmagazine.com/content/article/cribsheet_15_quantum_computing

様々な量子アルゴリズム

*Noisy Intermediate-Scale Quantum

多数の量子アルゴリズムが知られているが、NISQ*では十分な性能が出ない

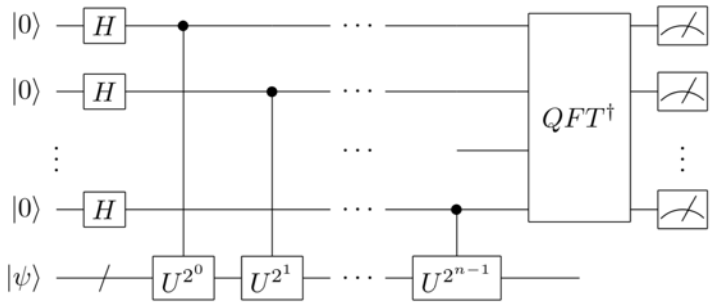
	アルゴリズム	サブルーチン	量子加速	データ
基本アルゴリズム	ショアの素因数分解 [Shor, 1994]	PEA	指数	古典
	量子化学計算（Full-CI）[Lanyon+, 2009]	PEA	指数	古典
	グローバー検索 [Grover, 1996]	AA	二次	量子
	線形連立方程式 [Harrow+, 2009]	PEA	指数	量子
教師なし機械学習	K-medians [Aimeur+, 2013]	AA	二次	古典
	階層的クラスタリング [Aimeur+, 2013]	AA	二次	古典
	K-means [Lloyd+, 2013]	(AA)	指数	量子
	主成分分析 [Lloyd+, 2013]	HHL	指数	量子
	主成分分析 [Kerenidis+, 2016]	HHL+QW	指数	量子
教師あり機械学習	NN [Narayanan+, 2000]	AA		古典
	SVM [Anguita+, 2003]	AA	二次	古典
	SVM [Rebentrost+, 2013]	HHL	指数	量子
	近傍法 [Wiebe, 2014]	AA	二次	古典
	回帰 [Bisio+, 2010]	-		量子

PEA: 位相推定
AA: 振幅増幅
QW: 量子ウォーク
HHL: Harrow-Hassidim-Lloyd

量子プログラムは量子回路で書かれる

量子アルゴリズムで利用される頻出サブルーチン

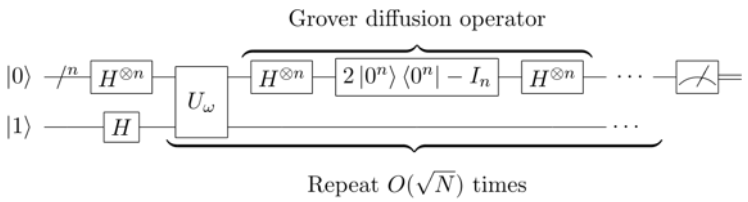
位相推定(PEA)



ユニタリー行列の固有値を求め補助量子ビットに二進小数で書き込む（固有値の二進小数表示n桁がn個の補助量子ビットに書き込まれる）

素因数分解
量子化学計算

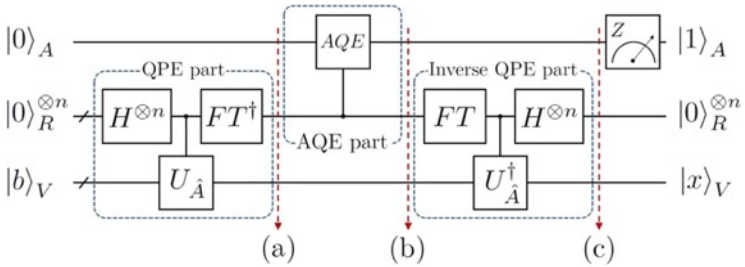
グローバー検索



N要素の未整序データベースの中から探索を行う（欲しい答えの固有状態をマーキングし、振幅増幅反転の繰り返しによって正答率を上げる）

検索
組み合わせ最適化
クラスタリング

HHL*



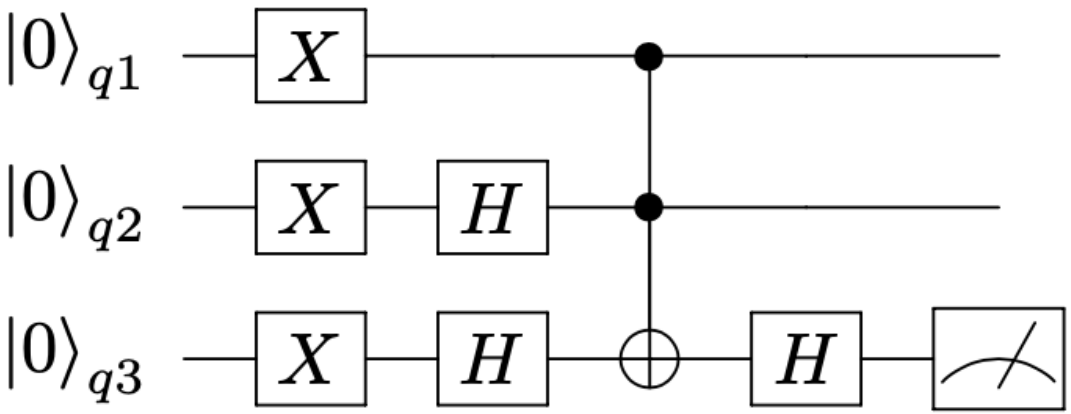
逆行列や行列積の演算を高速に行う（行列の固有値を位相推定で並列的に求め、それぞれの固有ベクトルを固有値で割る。行列積も同様）

連立方程式・線形回帰
主成分分析
サポートベクタマシン

*Harrow-Hassidim-Lloyd

量子回路＝量子ゲート列＝２Ｎ次元の行列

量子回路



ベクトル操作

$$\begin{bmatrix}1\\0\\0\\0\\0\\0\\0\\0\end{bmatrix} \xrightarrow{X} \begin{bmatrix}0\\0\\0\\0\\0\\0\\0\\1\end{bmatrix} \xrightarrow{H} \begin{bmatrix}0\\0\\0\\0\\0.5\\-0.5\\-0.5\\0.5\end{bmatrix} \xrightarrow{\text{Toffoli}} \begin{bmatrix}0\\0\\0\\0\\0.5\\-0.5\\0.5\\-0.5\end{bmatrix} \xrightarrow{H} \begin{bmatrix}0\\0\\0\\0\\0\\\frac{1}{\sqrt{2}}\\0\\\frac{1}{\sqrt{2}}\end{bmatrix}$$

3 量子ビット ＝ $\mathbf{2^3}$ 次元ベクトル

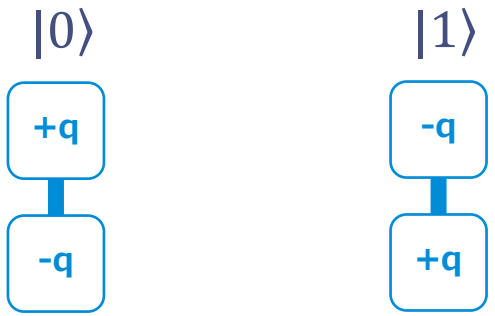
→ **量子回路**
＝ 2^n x 2^n のユニタリ行列

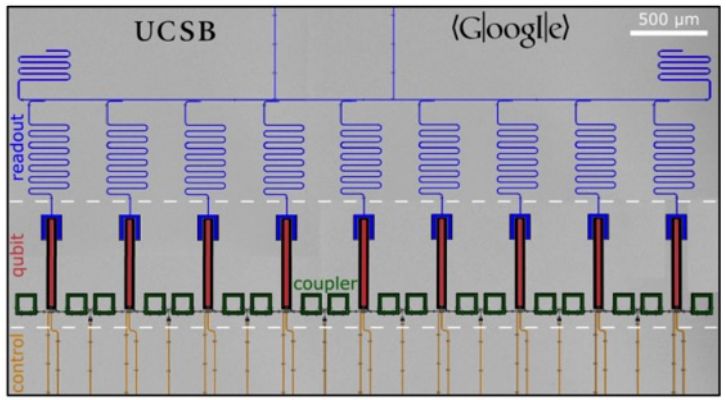
量子ビット実現方法

制御技術として一歩進んでいるのは主に２方式

ほかにも、NMR、Si量子ドット、光、冷却原子などの物理系も着実な研究が進められている

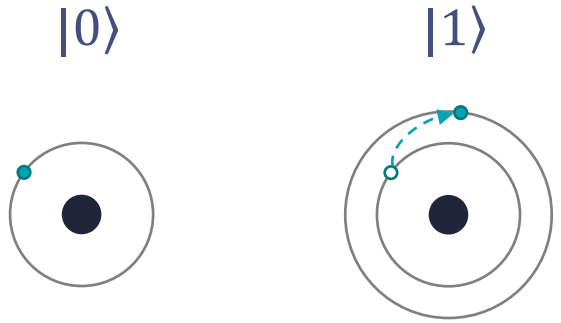
超伝導回路方式

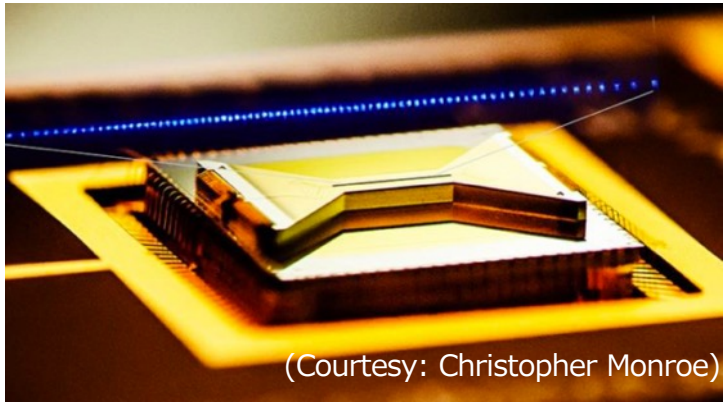




Google　IBM　rigetti　qci

イオントラップ方式





IONQ　Honeywell

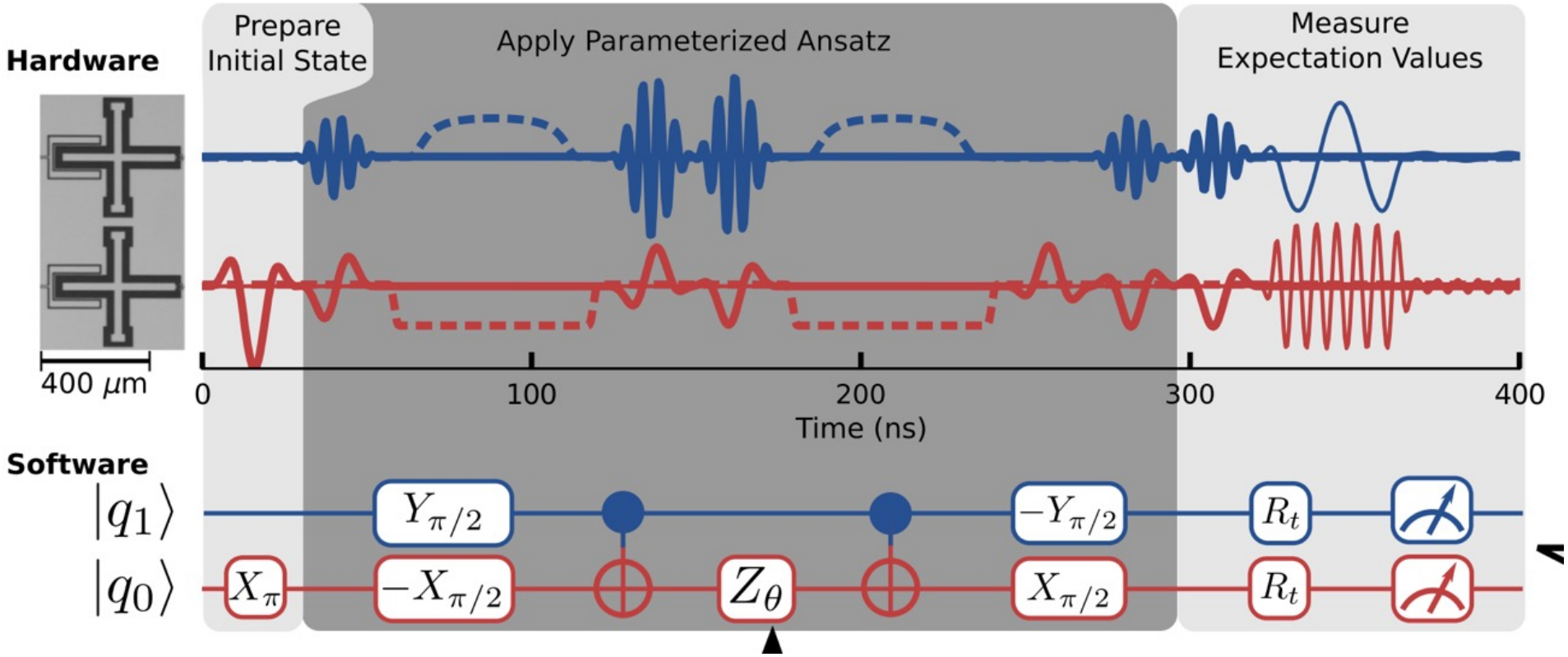
量子ゲートはソフトウェア

量子回路はソフトウェアであり、量子ゲートに物理的実体はない

超伝導の場合、量子ゲート操作＝高周波パルス（マイクロ波）

実際のパルス

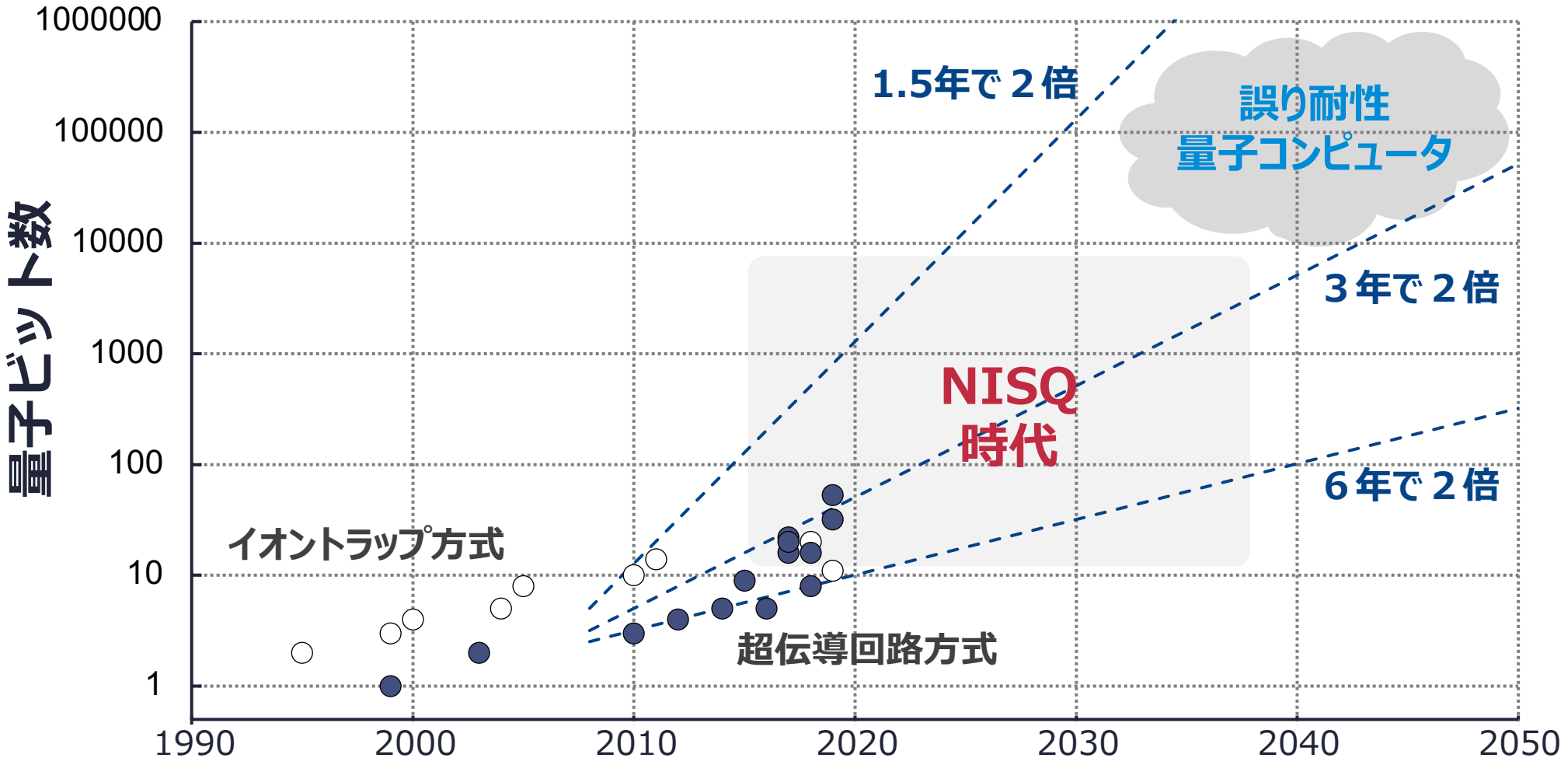
ゲート操作



P. J. J. O'Malley *et al.*, *Phys. Rev.* X **6**, 031007 (2016).

量子版ムーアの法則

集積度は上がってきている。NISQを如何に使いこなすかが鍵



NISQ（ニスク）時代の量子コンピュータ

フルの量子コンピュータ（誤り耐性QC）はまだ手に入らないが…

Noisy

ノイズあり
量子誤り訂正が不十分で、エラー率は高い。

Intermediate-**S**cale

中規模スケールの
50～100量子ビット程度

Quantum device

量子デバイス
量子効果を使うデバイス

John Preskill
(CalTech)

何かには使えそう。
限られたハードウェア資源を活かす知恵とソフトウェアが重要

John Preskill, “Quantum Computing in the NISQ era and beyond”, Quantum 2, 79 (2018).

キラーアプリケーション（の候補）

量子化学・量子多体系

問題設定がそもそも**量子力学で定式化**されているので、量子計算のほうが効率的なはず。

（例）
- 高精度の物性予測、分子・材料設計
- 反応・ダイナミクスのシミュレーション

機械学習・最適化

問題設定は**量子と無関係**だが、線形代数の構造や高次元の表現能力を上手に利用できそう。

（例）
- 巨大な行列の固有値・特異値
- サンプリング
- 主成分分析、クラスタリング、分類、SVM etc…

2. 量子コンピュータと暗号

Shorのアルゴリズム

量子位相推定アルゴリズムで周期発見を指数加速

i) 素因数分解したい整数 N と互いに素な整数 x を用意する *a).

ii) $a(=0,1,\cdots)$ を引数とした冪剰余 $f_{x,N}(a) := x^a \bmod N$ を計算する.

iii) $f_{x,N}(a)$ の周期 r（＝位数）を見つける（r が奇数なら 1 に戻る *a).

iv) $p = \gcd(x^{r/2}+1, N)$, $q = \gcd(x^{r/2}-1, N)$ が N の素因数.

---

*a ランダムに選んできた整数 x' に対して最大公約数 $\gcd(x', N) = 1$ であれば x' と N は互いに素です．$\gcd(x', N) \neq 1$ であれば，N の約数の 1 つが見つかったことになるので，今度は $N' = N/\gcd(x', N)$ の素因数分解問題を考えればよいことになります．

*a r は複数の近似値で得られるのでその中から偶数の r を選ぶか，それでもダメな場合はステップ 1 に戻り別の x で再度計算します．

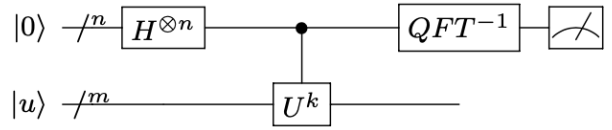
ユニタリ行列Uの固有値から位数を求められる

$$U_{x,N}\,|\alpha\rangle = |\alpha x \bmod N\rangle$$

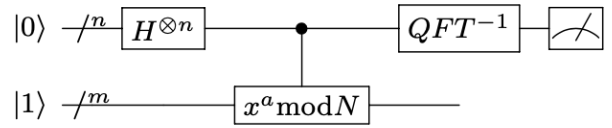
固有値

$$\exp\left(2\pi i \frac{s}{r}\right)$$

(a) 位相推定アルゴリズム



(b) 位数発見アルゴリズム



量子コンピュータと暗号

耐量子コンピュータ暗号

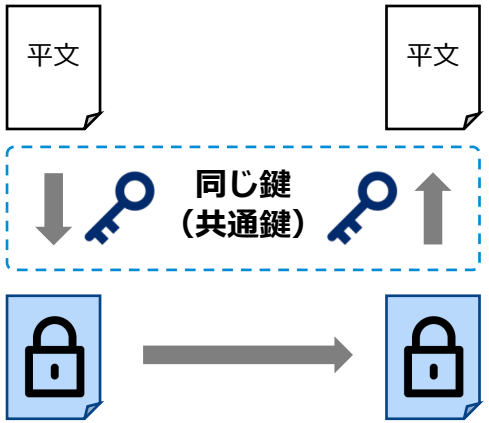
Post-quantum cryptography（PQC）。quantum-resistant / quantum-proof とも。

	代表例	量子アルゴリズム	対策
共通鍵暗号	**AES**	**グローバー検索** （共通鍵を総当たりで探索）	鍵長を２～３倍に延伸
公開鍵暗号	**RSA暗号** **楕円曲線暗号**	**ショアのアルゴリズム** （素因数分解・離散対数問題が多項式時間で解ける）	**耐量子コンピュータ暗号への移行**

（補足）QKDとPQC

量子暗号鍵配送（QKD）とPQCは似て非なるもの

共通鍵暗号

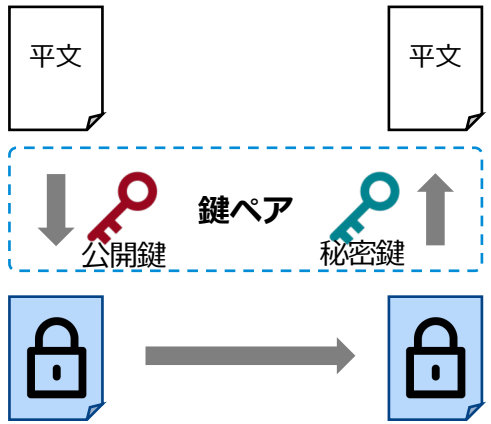


同じ鍵で暗号化・復号

暗号鍵の安全な共有が困難
（鍵配送問題）

量子暗号鍵配送（QKD）

公開鍵暗号



公開鍵で暗号化、**秘密鍵**で復号

鍵の事前共有は不要だが耐量子性に
課題（RSA、楕円曲線）

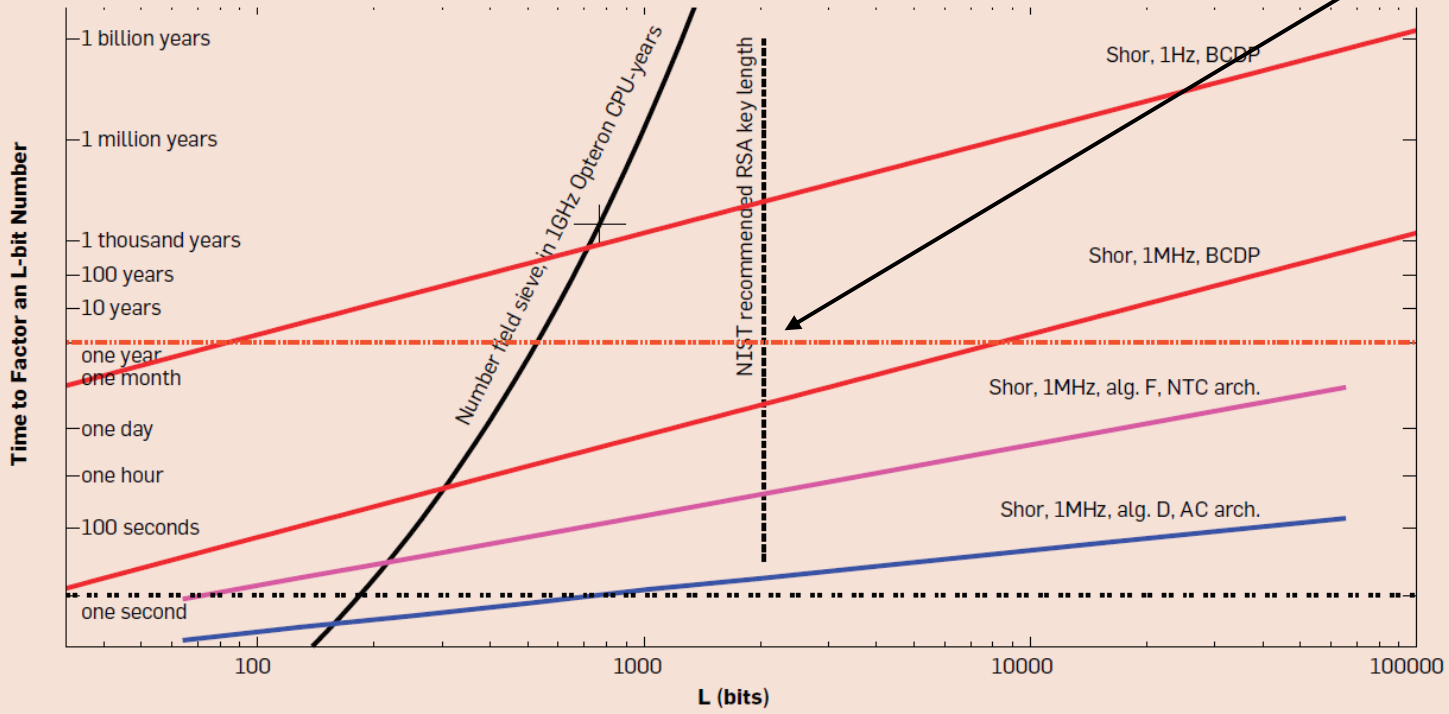
耐量子計算機暗号（PQC）

2048ビット整数の素因数分解にかかる時間

誤り耐性量子コンピュータのアーキテクチャに依存

数千万量子ビット、クロック10kHz程度で１年間連続動作が必要。アーキテクチャ最適化で計算時間は減少可能

The horizontal axis is the length of the number to be factored. The steep curve is NFS, with the marked point at $L = 768$ requiring 3,300 CPU-years. The vertical line at $L = 2048$ is NIST's 2007 recommendation for RSA key length for data intended to remain secure until 2030. The other lines are various combinations of quantum computer logical clock speed for a three-qubit operation known as a Toffoli gate (1Hz and 1MHz), method of implementing the arithmetic portion of Shor's algorithm (BCDP, D, and F), and quantum computer architecture (NTC and AC, with the primary difference being whether or not long-distance operations are supported). The assumed capacity of a machine in this graph is $2L^2$ logical qubits. This figure illustrates the difficulty of making pronouncements about the speed of quantum computers.



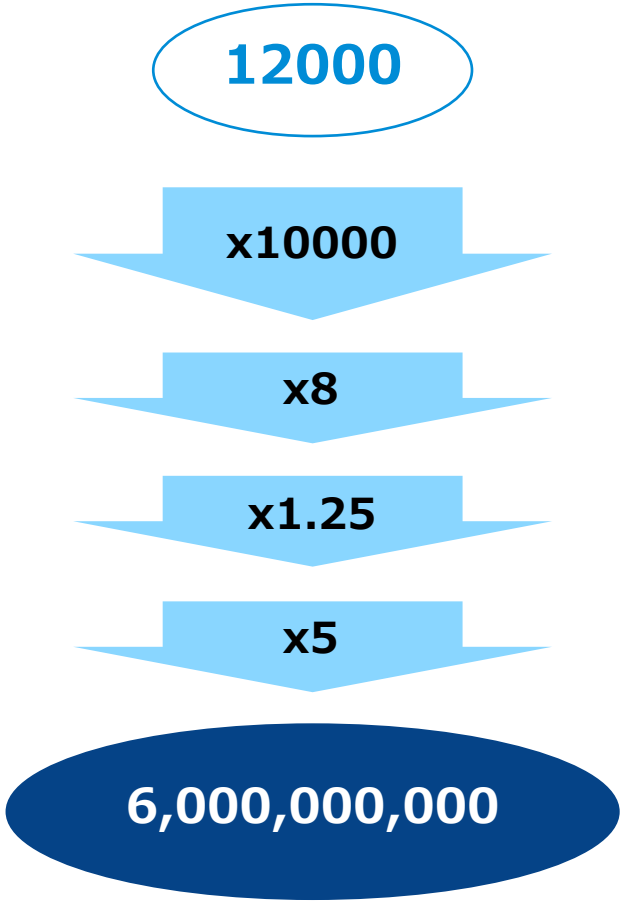
2048ビット整数を１年で素因数分解

クロック	アルゴリズム	アーキテクチャ
■ 1 Hz	BCDP	考慮なし
■ 1 MHz	BCDP	考慮なし
■ 1 MHz	F	NTC（近接のみゲート操作可能）
■ 1 MHz	D	AC（遠距離もゲート操作可能）

R. Van Meter, C. Horsman, “A blueprint for building a quantum computer”, Comm. of the ACM 56, 84 (2013).

量子誤り訂正符合によるオーバーヘッド

2048bitの数の素因数分解 → 60億量子ビット必要と見積もられる



論理量子ビット
実行効率を鑑みてやや余裕をもっている値

誤り訂正（表面符号、d＝56）
量子ビットのエラー率0.2%

魔法状態蒸留
（非クリフォード群ゲート利用のため）

量子ビットの配線

デバイスの歩留まり

物理量子ビット
現在の技術水準からみてかなり非現実的な値…

2000万量子ビットで
８時間という結果も
（エラー率10^{-3}, 表面符合サイクル1μs）

C. Gidney, M. Ekerå, “How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits”, Quantum 5, 433 (2021).

R. Van Meter, C. Horsman, “A blueprint for building a quantum computer”, Comm. of the ACM 56, 84 (2013).

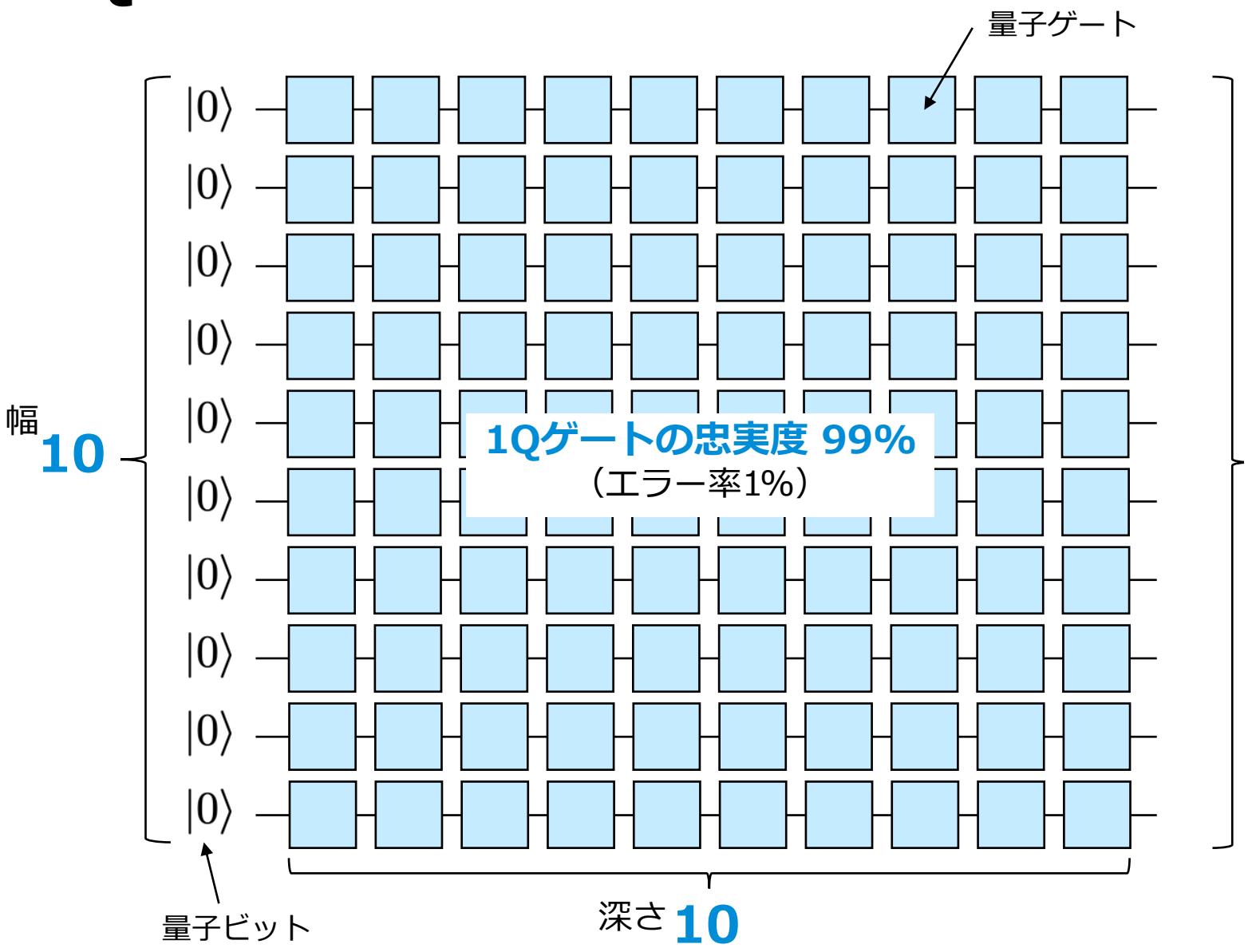
3. 今後の展望

クラウド提供が進むNISQ量子コンピュータ

			IBM	GCP	Azure	AWS	月間DL数
開発フレームワーク（SDK）	Qiskit (by IBM)		●	●			88881
	Cirq+TFQ (by Google)			●			25220
	Braket (by Amazon)					●	6279
	Pennylane (by Xanadu)			●			5372
	Tket (by CQC)			●			4306
	Q# (by Microsoft)				●		-
ハードウェア（QPU）	超伝導	IBM	●				
		Google		●			
		Rigetti				●	
		qci			●		
	イオントラップ	IonQ	●	●	●	●	
		Honeywell			●		
	QAマシン	D-wave				●	

Pypistat.org
(2021.5.18～6.18)

NISQのスケーラビリティ



結果の忠実度

$(0.99)^{100}$

$= 36.6\%$

単純計算で…

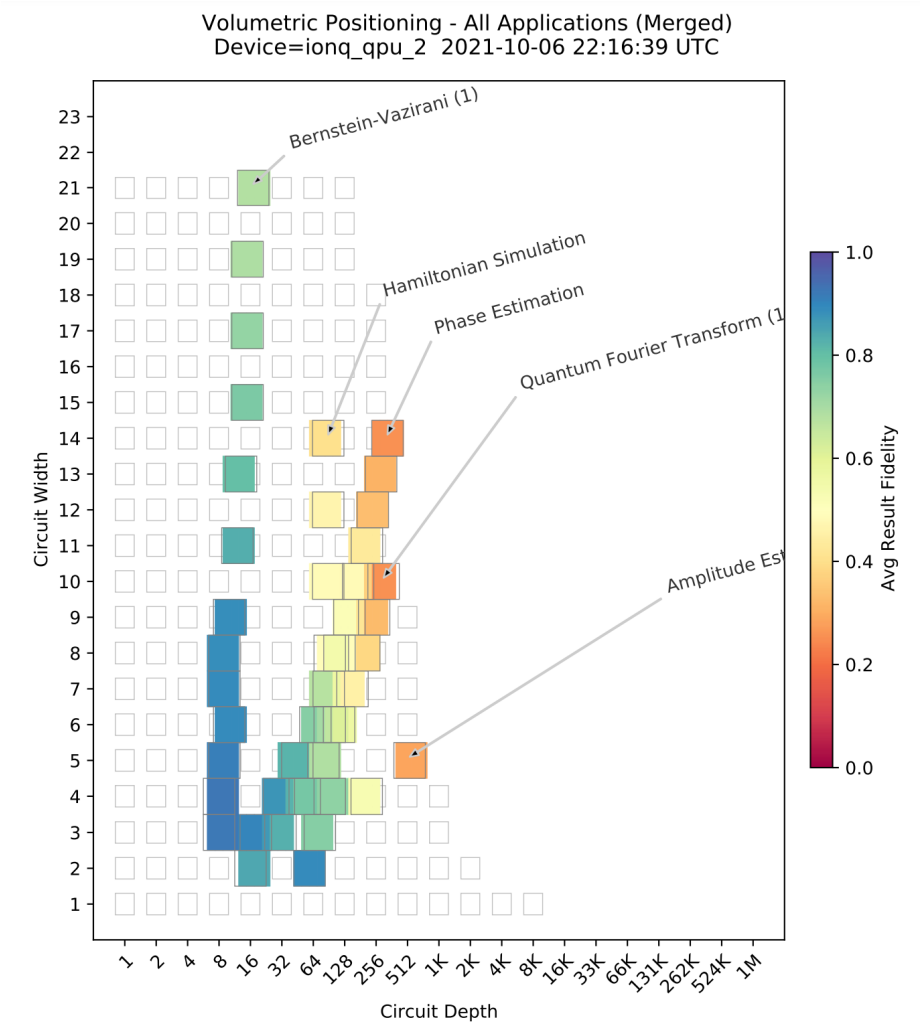
20Qなら**深さ5**

50Qなら**深さ2**

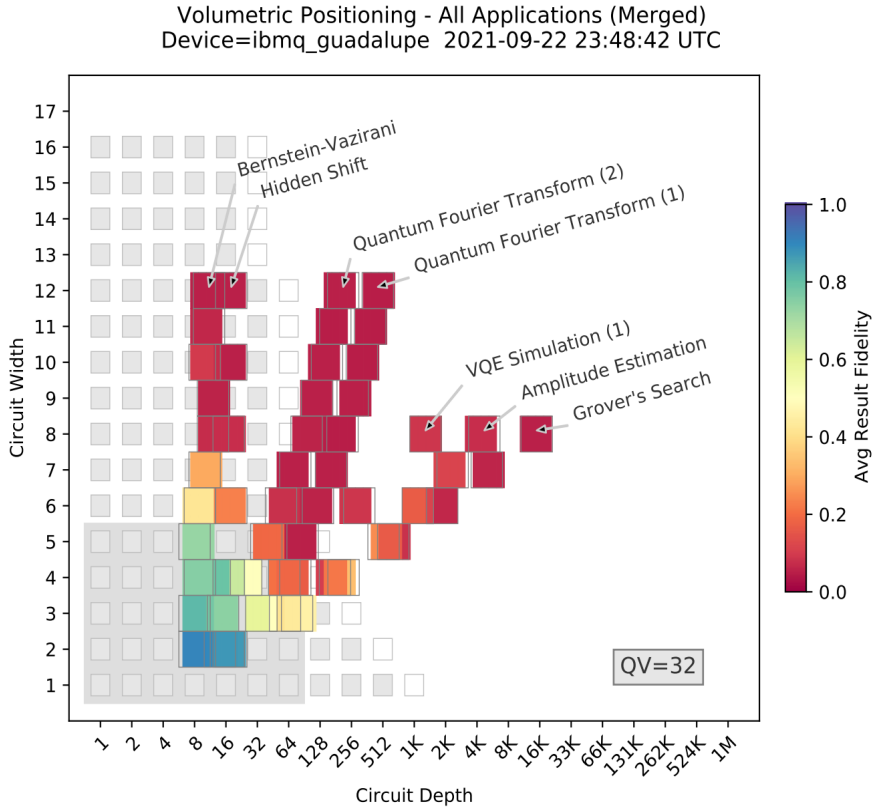
の計算までしか有効でない

NISQ量子コンピュータのベンチマーキング

IonQ（Latest, イオントラップ）



IBM（Guadalupe, 超伝導量子ビット）



T. Lubinski, et al., "Application-Oriented Performance Benchmarks for Quantum Computing", arXiv:2110.03137 (2021).

量子誤り訂正

量子ビットに冗長性をもたせ、エラーを検出・訂正する

古典コンピュータのハミング符合と同じ考え方

ただし「量子コンピュータ特有の事情」の考慮が必要

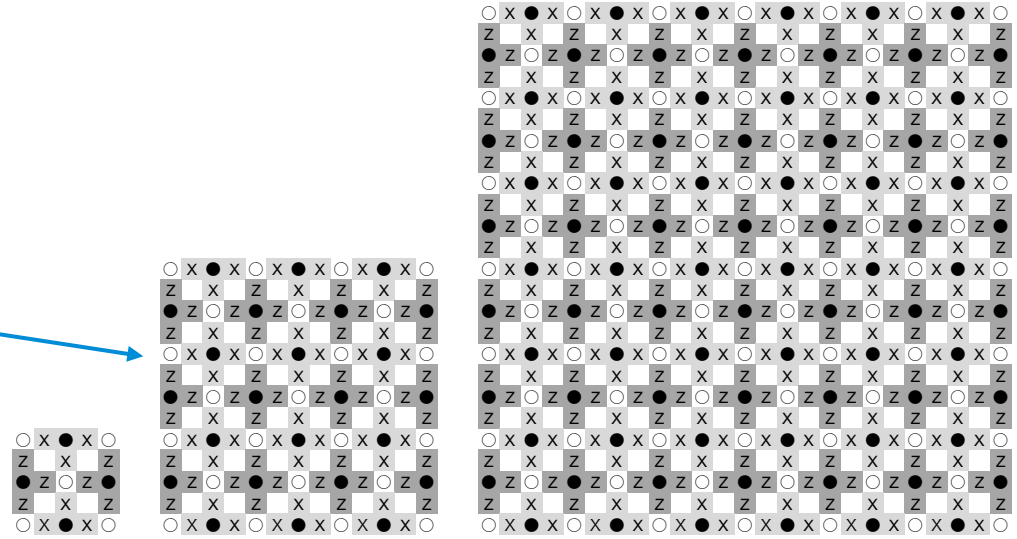
- ビット反転エラーに加えて位相反転エラーが存在
- 任意の量子状態のコピペは不可（No-Cloning定理）
- 計算実行中のレジスタを護る必要がある（符号化されたまま演算）→ 万能論理量子ゲート
- エラー検出・訂正に必要なゲート操作も高い確率で誤る → しきい値定理

量子の誤りを量子で訂正
「量子誤り訂正符号」

（例）２D表面符号 [[25,1,4]]

25物理量子ビット ＝ １論理量子ビット

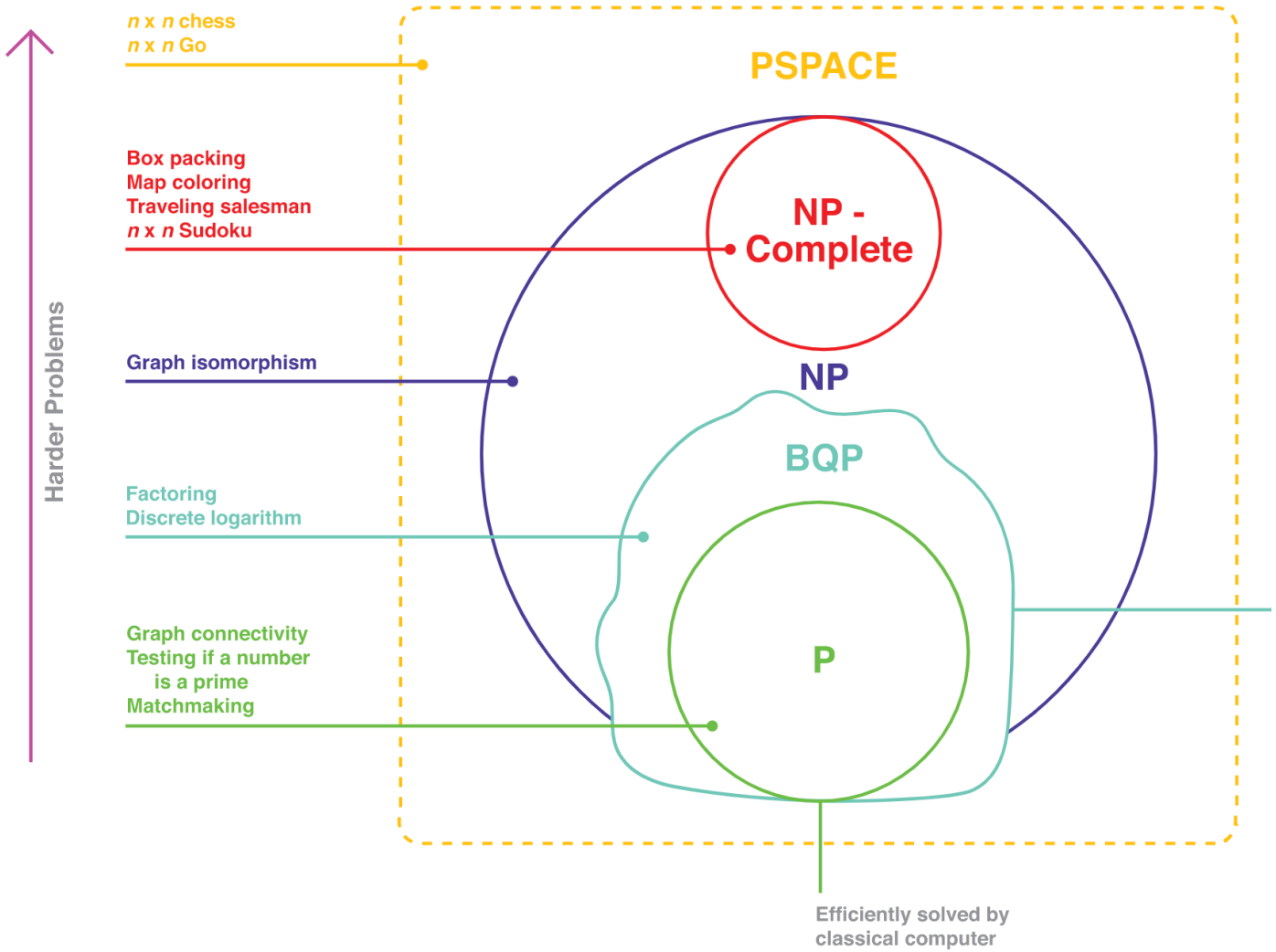
（符号距離d=4）



[[5,1,2]] [[25,1,4]] [[85,1,7]]

量子超越と計算複雑性

量子計算は古典計算より早いのか？



BQP
量子コンピュータで効率よく解ける問題のクラス

$$P \subseteq BPP \subseteq BQP \subseteq PSPACE$$

量子が古典より早いは「**BPP ≠ BQP**」を信じることになるが、示すのは困難

「“弱い”量子コンピュータを古典計算で効率的にシミュレート可能 → 多項式階層が崩壊」を使って示す

弱い量子コンピュータの例
IQP、ボソンサンプリング、one-clean-qubitモデル、ランダム量子回路

https://www.simonsfoundation.org/report2017/stories/scott-aaronson-quantum-and-classical-uncertainty/

量子技術の具体的な研究開発課題

量子コンピューティング 量子シミュレーション

NISQマシンのキラーアプリ探索
- 量子化学計算/機械学習
- 量子超越性
- 古典-量子ハイブリッドアルゴリズム

ゲート型量子コンピュータ実機の試作
- 超伝導量子ビット系

エラー耐性量子コンピューター基盤技術
- 量子ソフトウェア
- 量子誤り訂正方式
- 様々な量子ビット系

複雑系の計算が可能な量子シミュレータ開発

量子計測 センシング

ダイヤモンドNV中心作製技術
- 大型・高品質化（T_2向上）
- 新材料探索

ダイヤモンドNV中心と量子もつれ光センサの医療・診断応用
- プロトタイプ製作
- 脳磁計・心磁計
- イメージング技術

原子干渉計・光格子時計の実用性探索
- 小型化・可搬化
- 高精度化
- 「秒」の再定義・標準化

量子暗号・通信

QKDの社会実装と一般普及の促進
- BB84運用・品質保証
- 市場投入・キラーアプリ探索
- 低価格化

標準化活動への積極的寄与
- ETSI & ITU-T
- 耐量子-公開鍵暗号

高速化・長距離化に向けた量子中継技術、ネットワーク技術
- 量子メモリー・全光量子
- 量子望遠鏡
- 量子インターネット

量子マテリアル

トポロジカル量子物質
- トポロジカル量子コンピュータ
- トポロジカル絶縁体
- ワイル磁性体

スピントロニクス材料
- 半導体スピントロニクス
- スピンMOSFETデバイス

エネルギー変換材料
- スピン-ゼーベック効果
- スピン流

フォトニクス材料
- メタマテリアル
- シリコン／ナノフォトニクス

共通量子技術基盤

原子・分子・光科学
量子光学
量子エレクトロニクス

単一光子制御技術
- 効率化・室温動作・光子検出器
- 量子もつれ光子、多体量子もつれ制御

異種の量子ビット間結合（ハイブリッド量子科学）
- 固体量子ビット & 光 など

量子ビット基盤技術
- 様々な量子ビット系

材料設計・製造、計測技術

CRDS 量子技術関連のプロポーザル・報告書

CRDSのwebサイトから無料でダウンロード可能です

量子技術全般については…

量子2.0 ～量子科学技術が切り拓く新たな地平～

https://www.jst.go.jp/crds/report/CRDS-FY2019-SP-03.html

量子コンピュータについては…

みんなの量子コンピューター　～情報・数理・電子工学と拓く新しい量子アプリ～

https://www.jst.go.jp/crds/report/CRDS-FY2018-SP-04.html

量子マテリアルについては…

トポロジカル量子戦略～量子力学の新展開がもたらすデバイスイノベーション～

https://www.jst.go.jp/crds/report/CRDS-FY2016-SP-02.html