

量子コンピュータの最新動向 とShorのアルゴリズム

湊 雄一郎（みなと ゆういちろう）

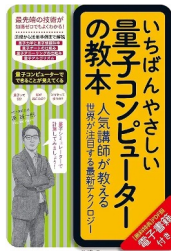
東京都世田谷区生まれ
東京大学工学部卒業
隈研吾建築都市設計事務所を経て、
2008年にMDR（現blueqat）株式会社設立

2015年 総務省異能vation最終採択
2017~19年 内閣府ImPACT山本プロジェクトPM補佐
2019~2021年 文科省さきがけ量子情報領域アドバイザー
2022年~ SEMI量子コンピュータ協議会委員長





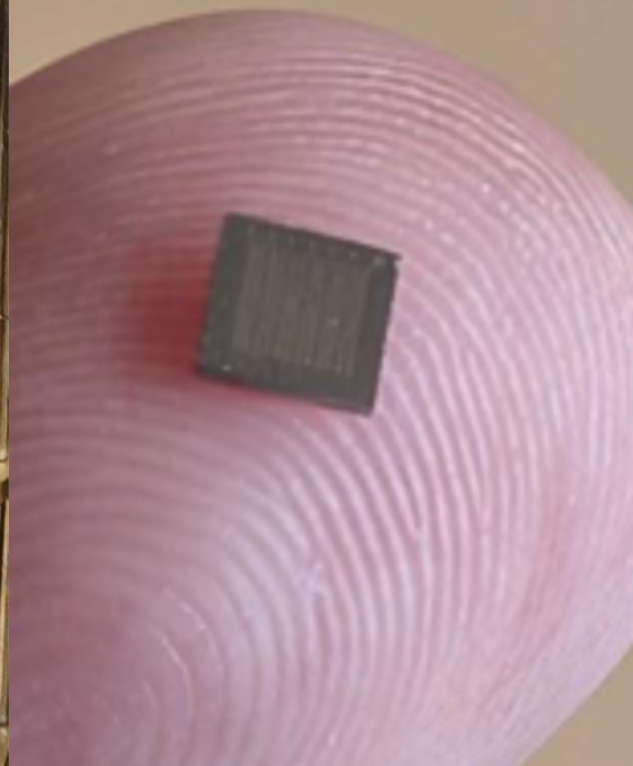
会社名	blueqat株式会社（英語表記：blueqat Inc.）
代表者	湊 雄一郎（みなと ゆういちろう）
設立日	2008年12月12日
所在地	渋谷スクランブルスクエア 39F
資本金	2億6,310万円
事業内容	・ 量子コンピュータ開発 ・ 生成AI・量子機械学習サービス



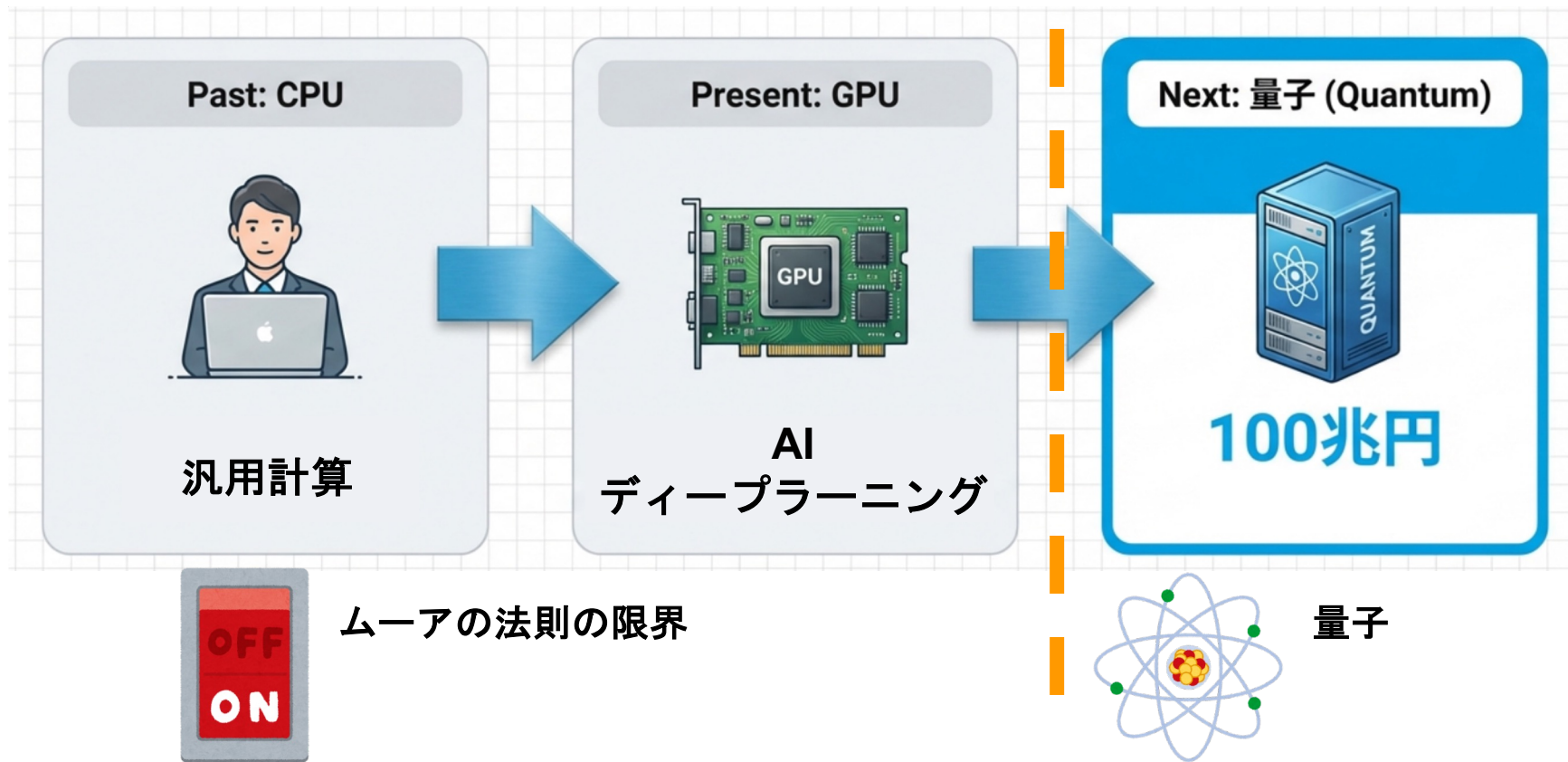
NVIDIA量子パートナー
Amazon量子パートナー



blueqat

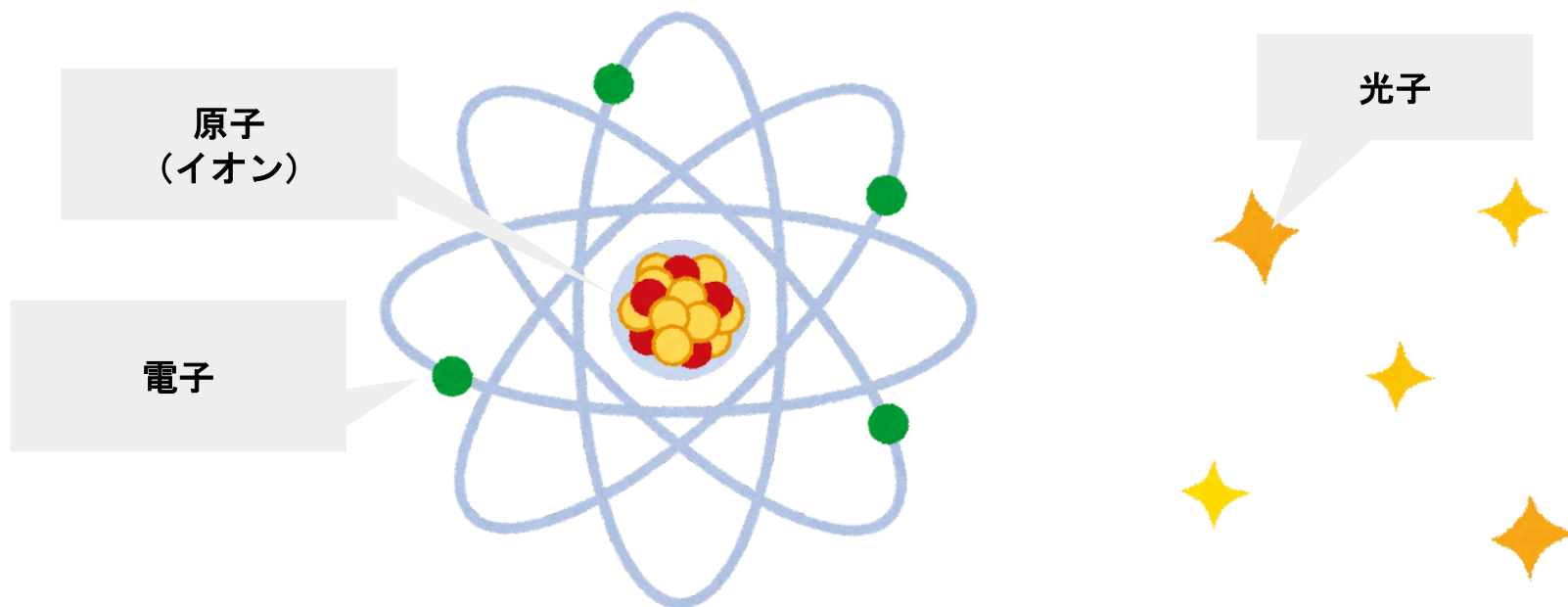


計算100兆円市場とQPUの時代



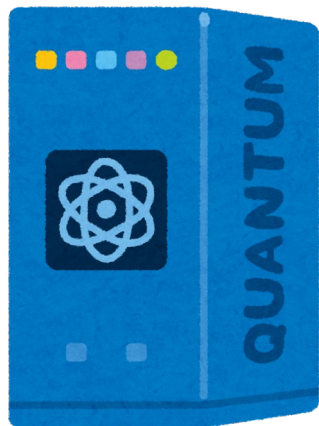
量子とは？

ナノサイズのものすごい小さいエネルギーや物質などの総称



量子を利用した新しい技術が開発中

量子の小さなサイズの世界では物理法則が変わる。量子力学を利用した新しい技術が登場し、実用化に向けて開発が進む。



量子コンピュータ

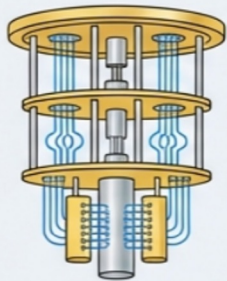


量子センサー

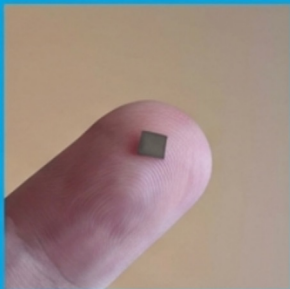


量子インターネット

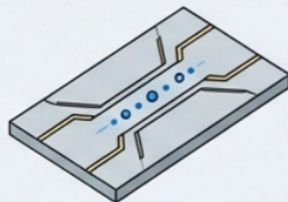
量子コンピュータの5大方式



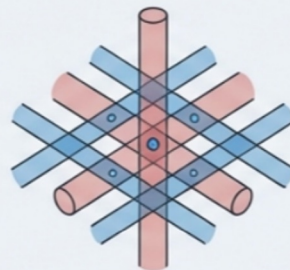
超伝導
(Superconducting)



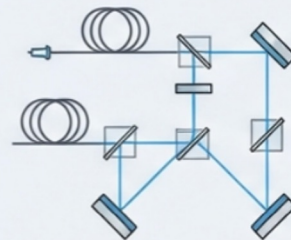
半導体
(Semiconductor)



イオントラップ
(Ion Trap)

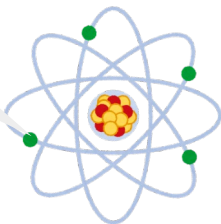


中性原子
(Neutral Atom)

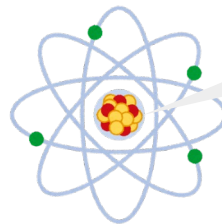


光量子
(Optical)

電子



原子



光子



量子コンピュータの4大アプリ

シミュレーション
化学・材料

シミュレーション
金融・流体他

最適化

AI

暗号

マーケット・ロードマップ

段階的な技術発展とともに市場規模が爆発的に増大しており、開発も加速している。

1、NISQ時代：量子と既存コンピュータのハイブリッド利用

全世界市場規模：7500億円程度 / 2015年-

2、量子超越時代：量子コンピュータの性能がスパコンを凌駕

全世界市場規模：7.5兆円程度 / 2021年-

現在位置

3、FTQC時代：量子コンピュータが完成し市場が爆発的に拡大

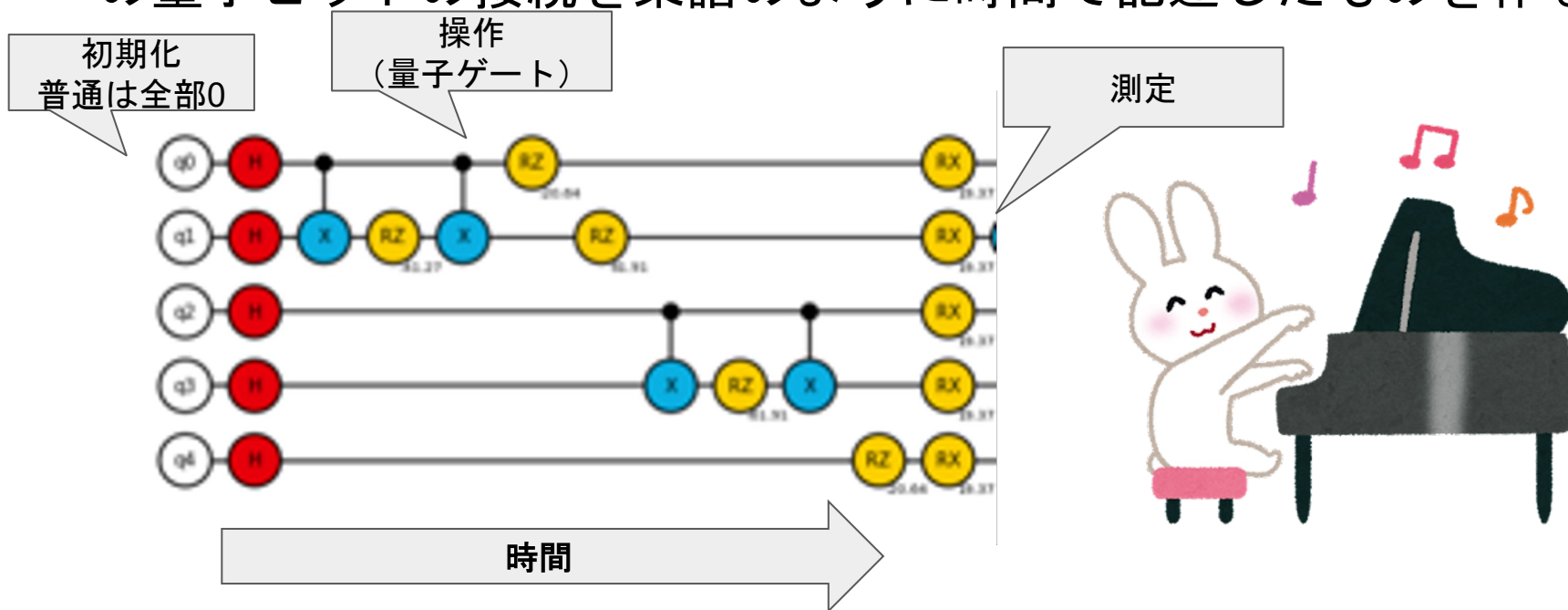
全世界市場規模：100兆円程度 / 2035-40年ごろ？

Where Will Quantum Computers Create Value—and When? BCG Report

<https://www.bcg.com/publications/2019/quantum-computers-create-value-when.aspx>

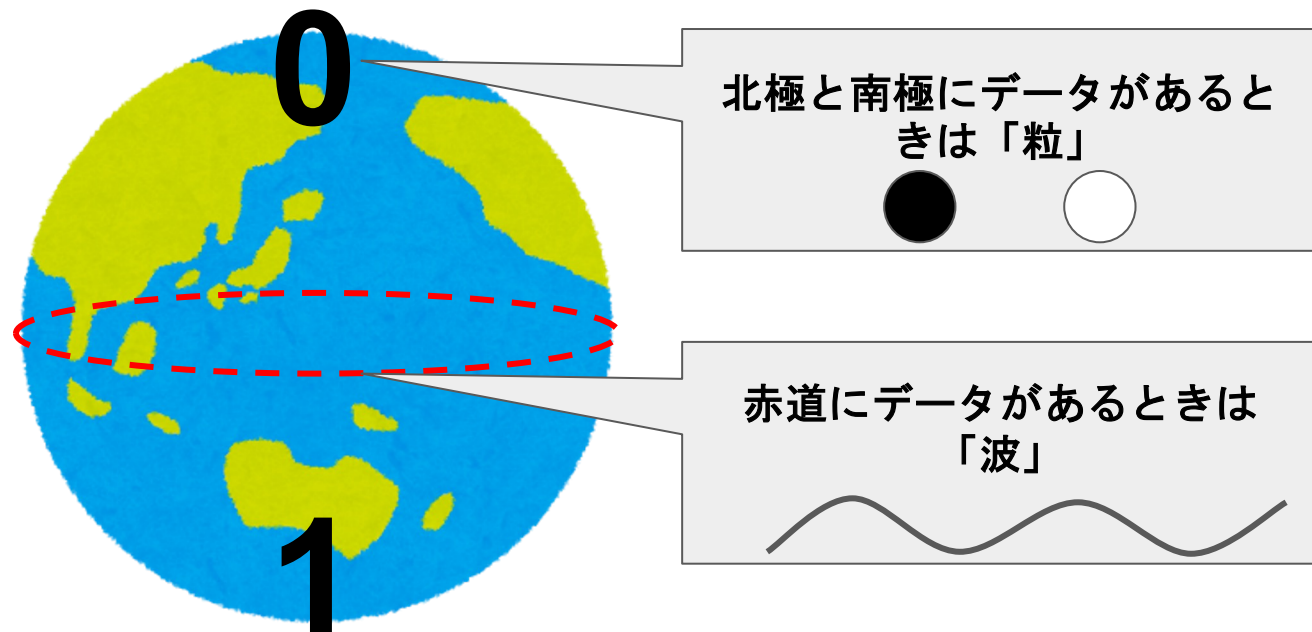
量子回路

量子コンピュータのプログラミングは、データの回転操作や二つの量子ビットの接続を楽譜のように時間で記述したものを作る



デジタルと波を切り替えて計算できる

これまでの計算機はデジタルの01だけを利用してきた。波を使うと計算の幅が広がる。



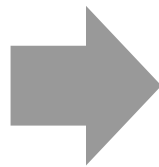
使い分けて
プログラミング
shorでは主に波の
性質を使って計
算する。

Shorのアルゴリズム

ShorのアルゴリズムとPQC

Shorの脅威

量子計算により、
RSAや楕円曲線暗号
などの現行公開鍵暗号
が無効化される。



PQCへの移行

量子でも解きづらい数
学（格子等）に基づく
「耐量子暗号」への早
期移行が急務。

Shorのアルゴリズムの全体像

大きな目的は「**巨大な数 N を素因数分解すること**」ですが、Shorのアルゴリズムはこれを直接行うのではなく、「**周期発見問題**」へ変換して解きます。**ソフトウェア自体はすでにあり**、ハードの開発が進行中。

[古典・前処理] 素因数分解を周期発見という数学的課題に言い換える



[量子部分] 量子コンピュータで、巨大な選択肢から周期 r を見つける



[古典・後処理] 得られた周期 r から簡単な計算で素因数を取り出す

[古典・前処理] 周期発見問題

やること

解きたい数 N （例: 15）に対して、ランダムな整数 a （例: 7）を選びます。

狙い

$f(x) = a^x \pmod{N}$ という関数の周期 r を見つける問題にセットアップします。

mod N は N で割った
余りのこと

その他多少の判定あり

【量子部分】 周期 r を見つける

例

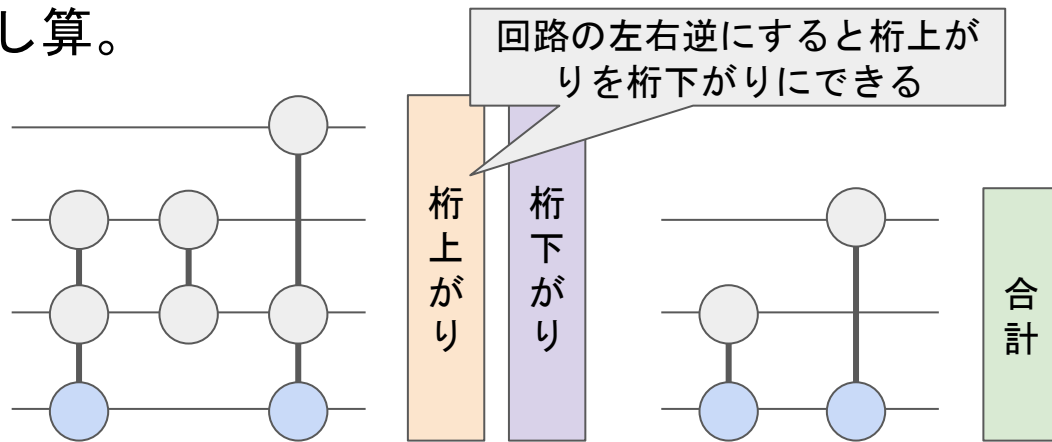
$N=15, a=7$

x	a^x	$a^x \pmod{N}$
1	7	7
2	$7*7=49$	4
3	$7*7*7=343$	13
4	$7*7*7*7=2401$	1
5	$7*7*7*7*7=16807$	7

4回ごとにパターンが繰り返すため、周期 $r=4$ となります。数字が巨大になると古典ではこの r を探すのに途方もない時間がかかります。

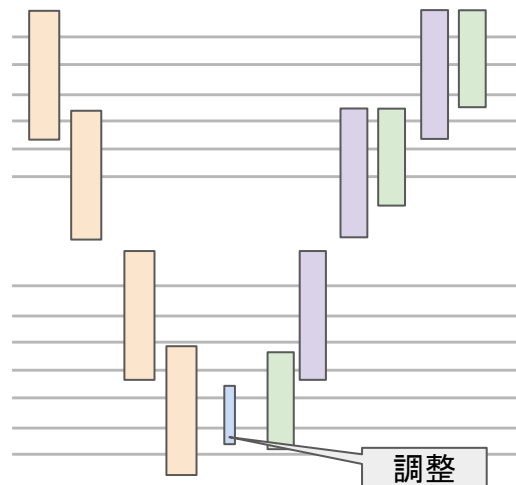
[量子] 量子足し算

意外と最後まできちんと量子コンピュータでのshorを実装した人がいないので、blueqatSDKで全部作ってみた。量子コンピュータの計算はすべて入れ子状になっているため、パーツを一つずつ作っていく。最初は足し算。



桁上がり量子回路

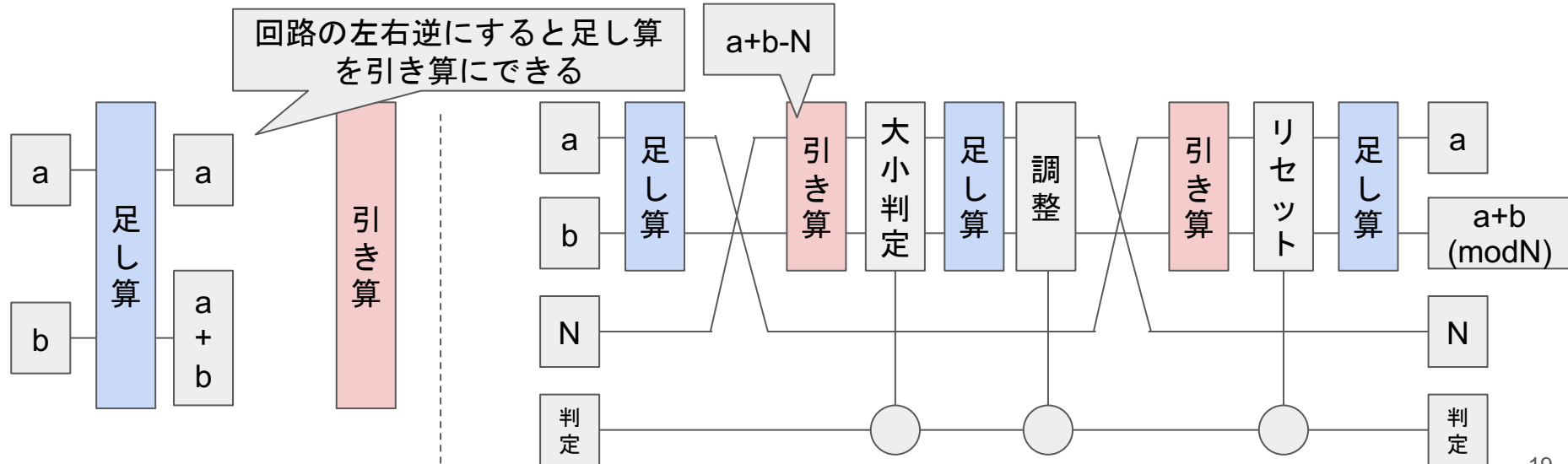
合計量子回路



足し算量子回路

[量子] 量子足し算した後余りを求める

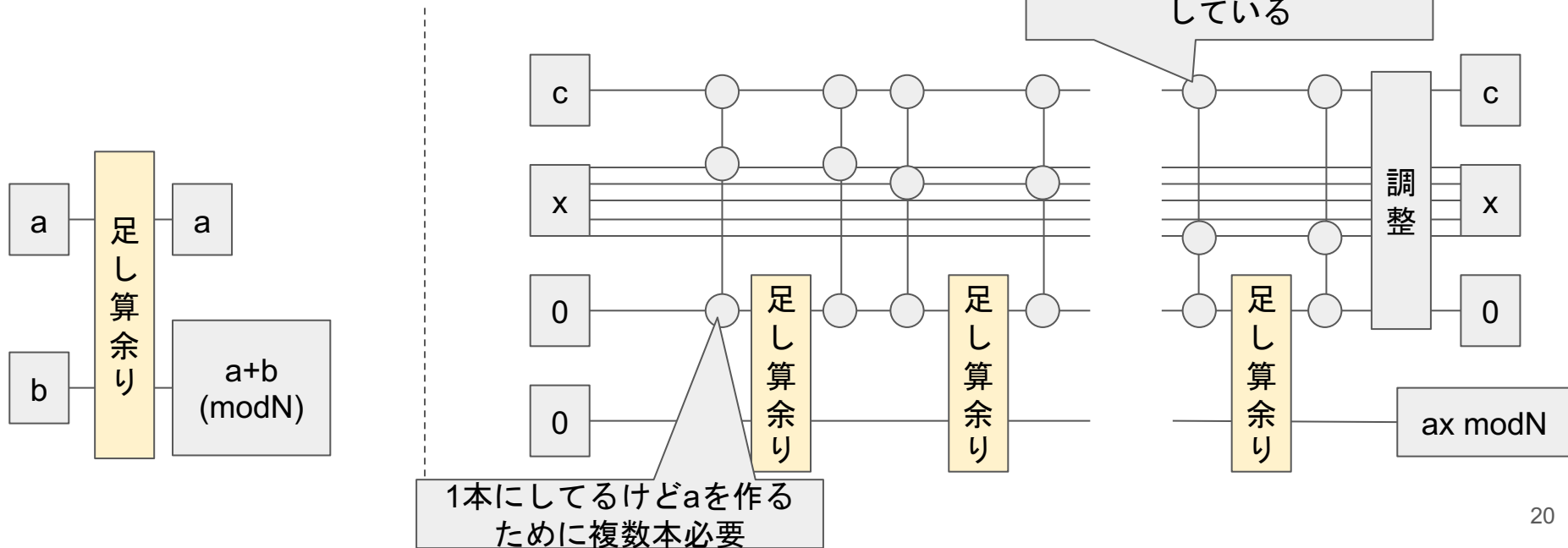
作った足し算回路を利用して、二つの数を足した後にあまりを求める量子回路を作る。 $a + b - N$ するだけだけど、 **N が $a+b$ を超える場合と、そうでない場合で量子回路的にはややこしい。**



[量子] 制御つき掛け算の筆算

最後のパーツに行く前に、そのベースとなるパーツを作る。

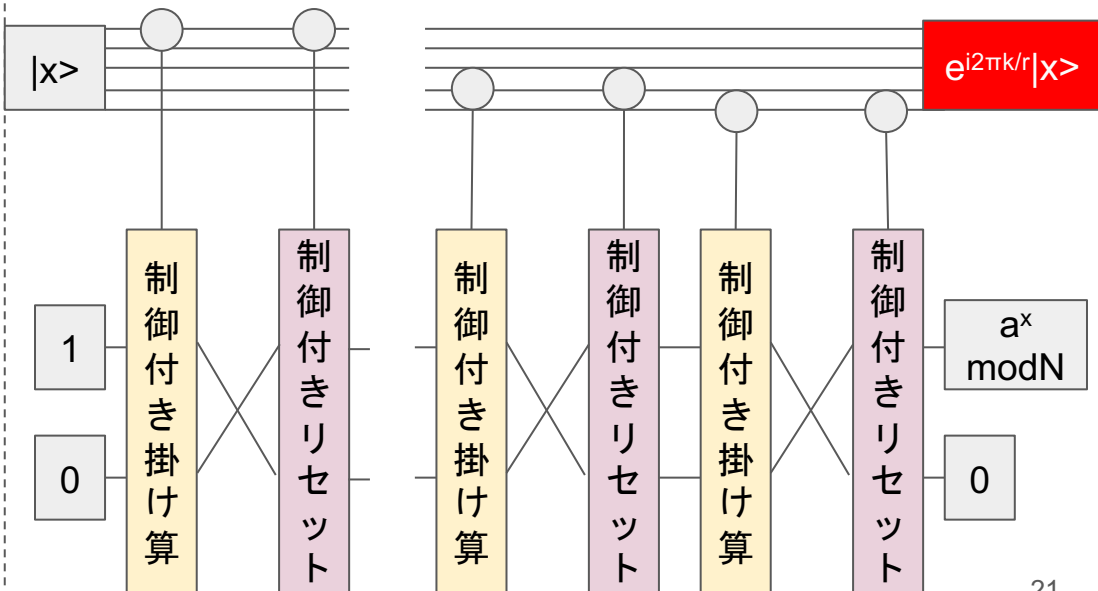
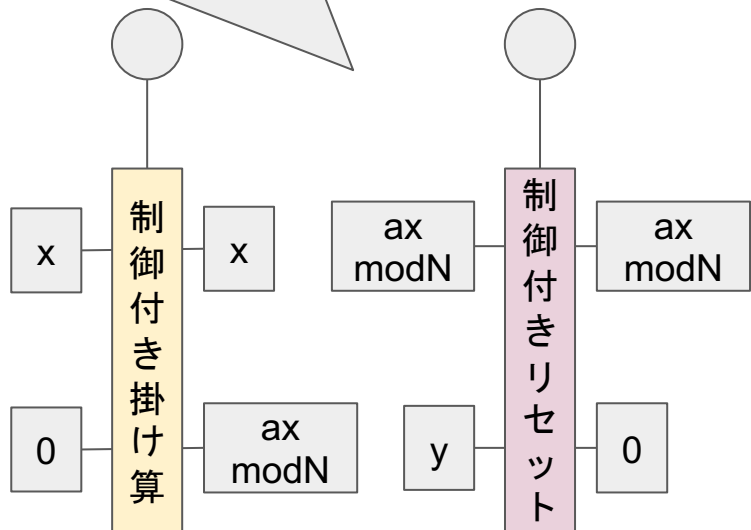
$c=1$ の時に $2^i a \pmod{N}$ を読み込む量子回路



[量子] 制御つき累乗計算

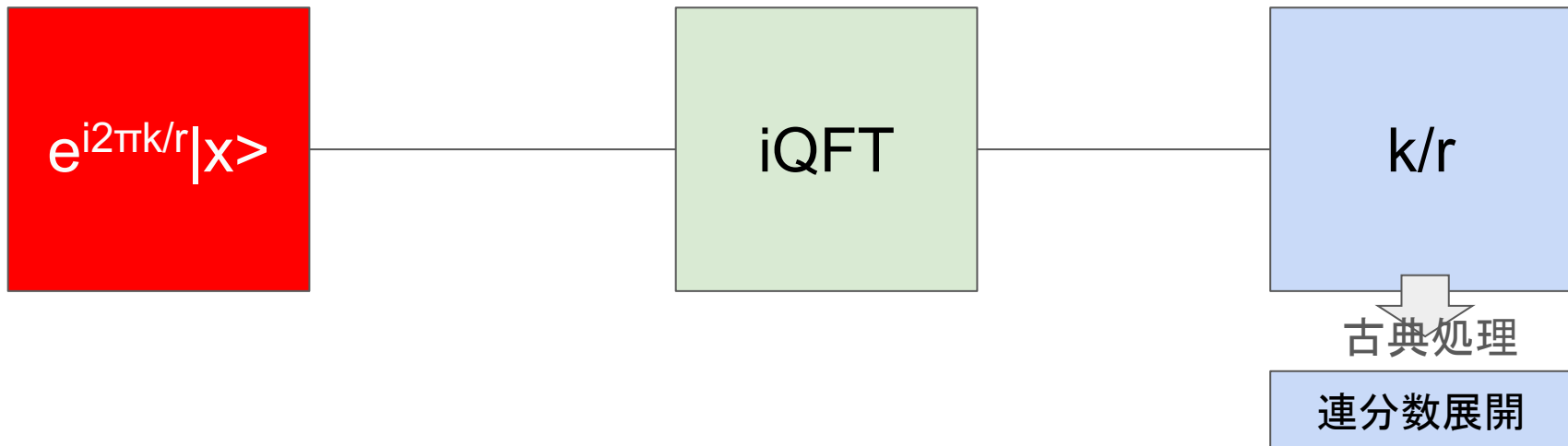
今のパーツを使って制御つきの累乗計算 $a^x \bmod N$ を実現する。

回路の左右逆にすると二番目の出力をなんでも0にリセットできる



[量子] 逆量子フーリエ変換

逆量子フーリエ変換を利用して、得られた量子状態から周期 r をビット列として取り出す操作。逆量子フーリエ変換は普通ならランダムになってしまう周期付きの情報をビットに直してくれる便利な量子回路。



[古典・後処理] 周期発見問題

やること

量子部分から得られた周期 r （例: 4）を使い、 $a^{r/2} \pm 1$ と N の最大公約数（ユークリッドの互除法）を計算します。

連分数展開必要

r の条件多少あり

狙い

超高速に求まる古典計算だけで、目的の素因数が手に入ります。

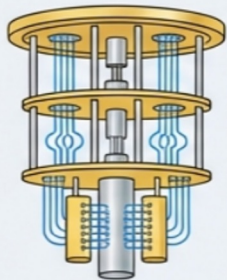
例

$$\gcd(7^{4/2} - 1, 15) = \gcd(48, 15) = 3 \quad (\text{因数解が得られた！})$$

ハードウェア最新動向

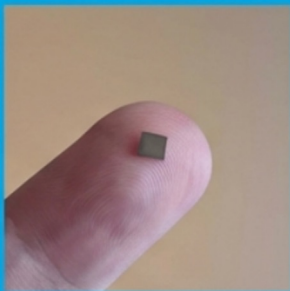
量子コンピュータの5大方式

世界で最も進んでいる5社の最新動向を紹介。



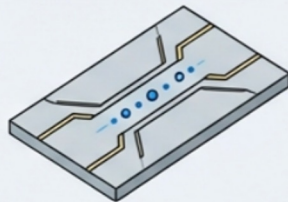
超伝導
(Superconducting)

IBM



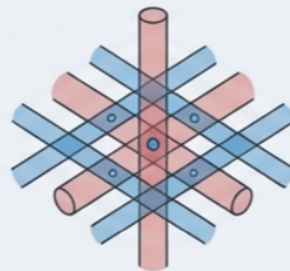
半導体
(Semiconductor)

Intel



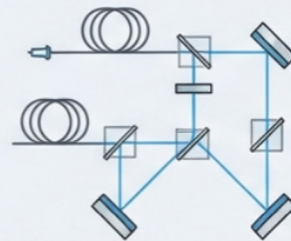
イオントラップ
(Ion Trap)

Quantinuum



中性原子
(Neutral Atom)

QuEra



光量子
(Optical)

PsiQuantum

誤り訂正技術との統合がトレンド

ハードウェア単体ではなく、エラーを減らすために誤り訂正を実装しやすいハードウェアの開発がトレンド。評価軸もより複雑に

量子ビット数

並び方・結合数

エラー率

動作周波数

コヒーレンス時間

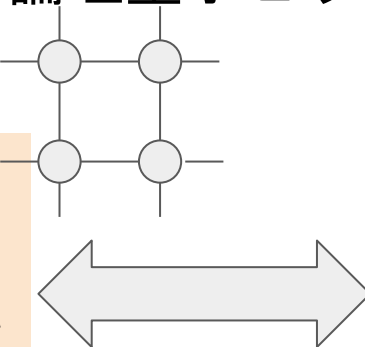
実行可能回路深度

誤り訂正の効率性

超伝導 / IBM社

IBM社は従来の六角形の接続方法を十字に変更し120量子ビットに固定したチップNighthawkを中心に将来の拡張性を考える。

120量子ビットx3(360量子ビット)やx9(1080量子ビット)を接続想定。また、qLDPC符号を意識した新アーキテクチャを実験的にリリース予定。29年に200論理量子ビット計画。33年に1000論理量子ビット計画。



120量子ビットの
Nighthawkチップを中心に
性能を高め、複数チップを
接続するプラン

qLDPC符号など接続を意識
した
実験的なチップ

イオントラップ / Quantinuum社

米国ハネウェルと英国CQCが合併したイオントラップの企業。
98量子ビット全結合のHeliosが最新。バリウムイオンを使って2次元配置が特徴。1量子ビットゲート99.9975%、2量子ビットゲート99.921%の高精度計算が特徴。接続性を活かした少ない量子ビットでの誤り訂正も特徴。29年に1000量子ビットの次世代機

98量子ビット（50論理量子ビット）の高精度量子ビット
Helios



29年には、1000量子ビット
の2D格子型の次世代機

中性原子 / QuEra社

ハーバード・MIT発ベンチャー。23年にブレイクスルー。260物理量子ビットのゲート型マシンGeminiをリリース。光ピンセットにより移動可能な量子ビットを利用した誤り訂正アルゴリズム。計算損失を抑える3,000原子連続供給システムや中性原子の移動自由度と並列処理性能を最適活用し、初期FTQCシミュレーションに必要な物理量子ビット数を半減させ、実行速度を最大250倍加速させるアーキテクチャを発表

260物理量子ビットGemini

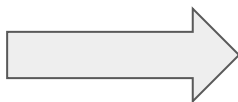


28/29年にはgigaquosという10億回の論理演算を実現するマシンを予定。1000論理量子ビット・20000以上の物理量子ビット

光量子 / PsiQuantum社

NISQを作らず、100万物理量子ビット規模のメガスケールFTQCシステムのための開発に特化したベンチャー。GlobalFoundriesの45nmSOIにてOmegaチップを開発。光量子は環境熱や磁気ノイズの影響を受けにくい反面、「光子の損失（Loss）」が主要なエラー原因となる。PsiQuantumはこれに対し、三次元誤り訂正の「フュージョンベース量子誤り訂正（FBQEC）」を採用。超伝導センサーを使うため4K冷却をブレード型サーバーに利用。

45nmOmegaチップ
FBQECシステム

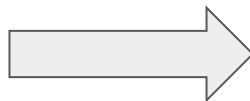


2027～2028年の商用実用機の稼働を
目指し、世界2箇所で大規模データ
センターの建設

半導体 / インテル社

沈黙を破り、26年春に学会で最新チップを予告。Intel18A（1.8ナノ相当）のプロセスを利用した最新チップで、26年に243量子ビット、27年に657量子ビット、28年に3300量子ビットを予告。積層配線とインターポザーで従来のCPUのように量子ビットを量産可能。Exchange Onlyと呼ばれる高周波を使わず、従来の半導体工学の延長で制御することで熱を抑えスケールを実現。2年で10倍ずつのスケールアップを予告。スケールに自信ありと。

26年に243量子ビット



28年に3300量子ビット

まとめ

Shorのアルゴリズムは現時点で実装可能。回路の効率化なども可能になっている。

一方それを実現するためのハードウェア開発が過熱しており、各社アーキテクチャを見越した開発を行っている。