2022/ 9 /18

我孫子サイエンスカフェ＠Zoom

量子コンピュータ

９月１８日（日）

我孫子に住む
理論物理学者
細谷　暁夫

自己紹介はブログ
akiobongo
の「私とっての科学」にあります

量子コンピュータ

量子計算機についての
５つの疑問

（１）そもそも計算とは何だろう？
（２）量子とは？
（３）量子計算機とは？
（４）量子計算機が有効な例
（５）研究はどこまで進んでいるか？

1.計算とは何だろうか？

問題　３＋１＝?

原始人のやり方

(いっしょにする)

１ ２ ３ ４　(左から数えて最後の４を答とする)

計算は物理的操作である！

２進法

１と０だけで数をあらわす
（２まで行くと、くりあがる）

例

１００１ → ８＋０＋０＋１＝９

011 → 010
（一番右の１を０に書き換える）

010 → 000
（左に一歩移動）（１を０に書き換える）

000 → 100
(左に一歩移動）（０を１に書き換える）

アルゴリズム

右からはじめて、１ならば０へ書き換えて左へ一歩進む。０ならば１へ書き換えてそこで停止して、結果を答えとする。

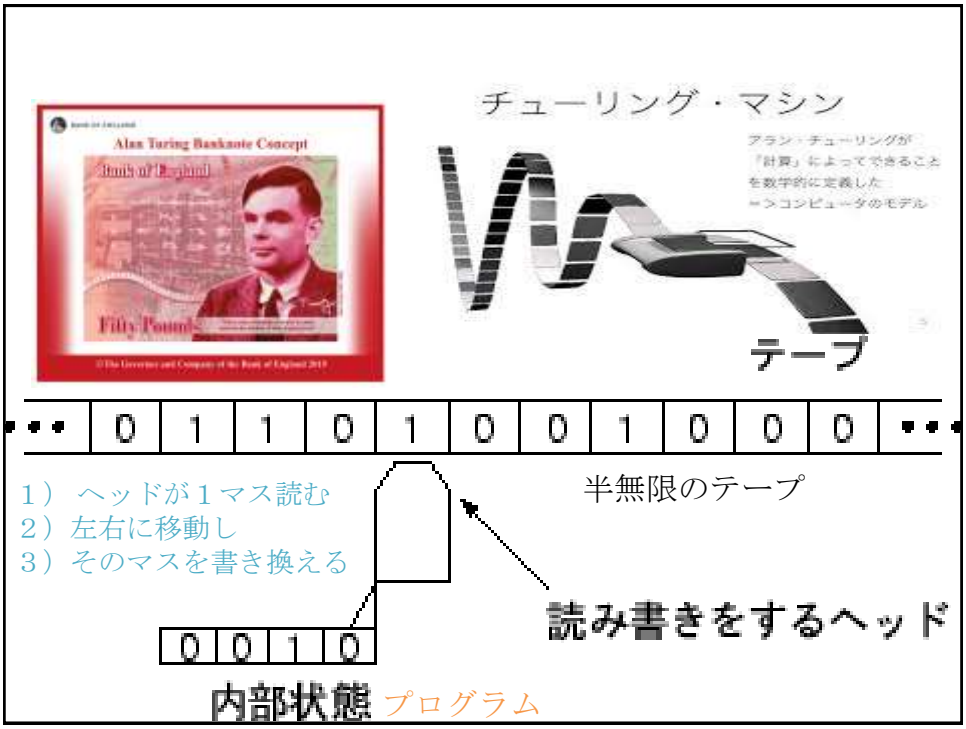
アルゴリズムを考えつくのは数学者です
物理屋には無理です

計算とは

計算とは、ある１と０の羅列を、一定のルールにしたがって、書きかえることである。

101010110101010001→110010101111010001

その数学的な意味はあとで解釈する。



解けない問題

- 近代論理学では、テューリングマシンがいつか仕事を終えて、停止するとき問題を解けたと言い、逆にいつまでも停止しないときに解けない問題という。

ゲーデルは、真であっても証明不可能な問題が存在することと、その例として公理系の中での無矛盾性を証明することが不可能であることを示した。

難しい問題

- 原理的には解けるけれども、テューリングマシンが動いている時間が長すぎれば、事実上実行できない。nビットの入力に対して、ｎのべき程度ならば実行可能で、exp[n]ならば実行できない

べきにならない代表的な例

素因数分解 と巡回セールスマン問題

ご質問をどうぞ

2. 量子とは何か？

- 量子状態であることをはっきりさせるために、

  ｜０＞、｜１＞

  のように書く。

例

電子は自転をあらわすスピンを持っていて、ｚ軸方向でみると上向き|⇑>か下向き|⇓>かである。

- 磁場をかけて、ｘ軸に向かせると、

$$|\Rightarrow\rangle = [|\Uparrow\rangle + |\Downarrow\rangle]/\sqrt{2}$$

と、⇑と⇓が重ね合わせられた状態になる。

重ね合わされた状態

- 量子的な世界では、状態として

｜０＞か｜１＞かではなくて、｜０＞も｜１＞も

という状態

$$\alpha|0\rangle + \beta|1\rangle$$

が可能（αとβは複素数）

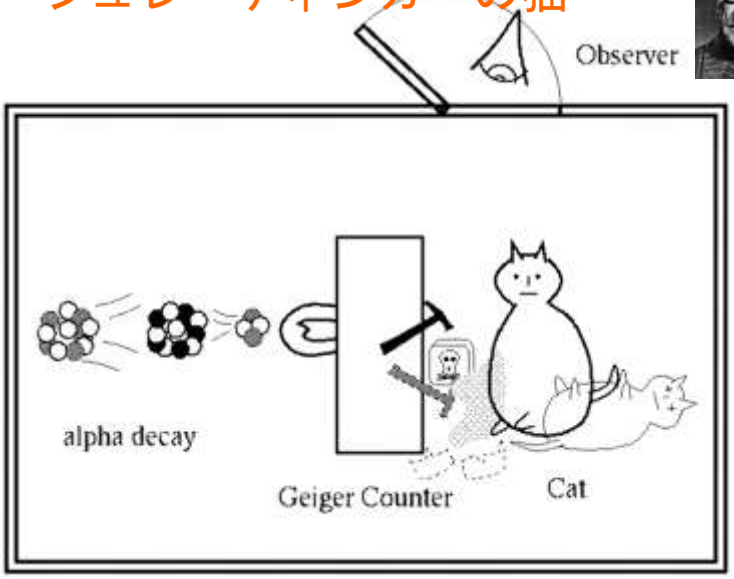
しかし、観測すると

- 状態は｜０＞か｜１＞かに定まる。

｜０＞を得る確率は、αの絶対値の２乗であり、
｜１＞を得る確率はβの絶対値の２乗である。
（その和は１に取っておく）

量子力学の摩訶不思議なところ
現代物理学は実験事実として受け入れている

シュレーディンガーの猫



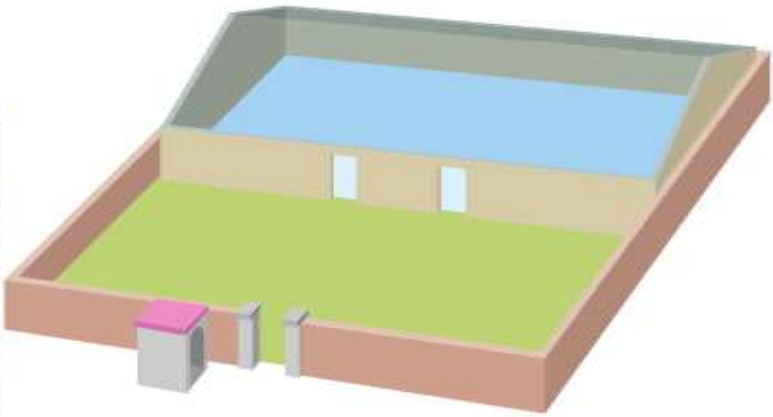
http://www.lassp.cornell.edu/ardlouis/dissipative/Schrcat.html

（1）

初版：1949年

しかし、光が
波でもあり粒子でもあるとは、
どういうことなのだろうか？

wiki

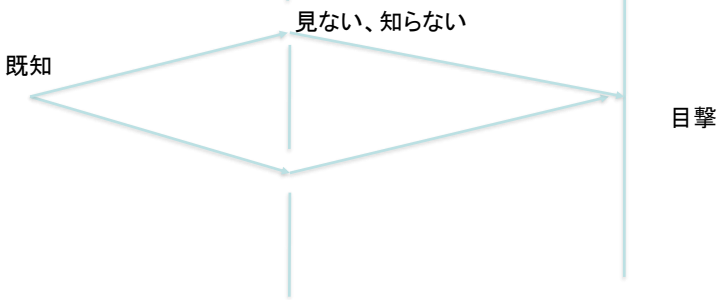


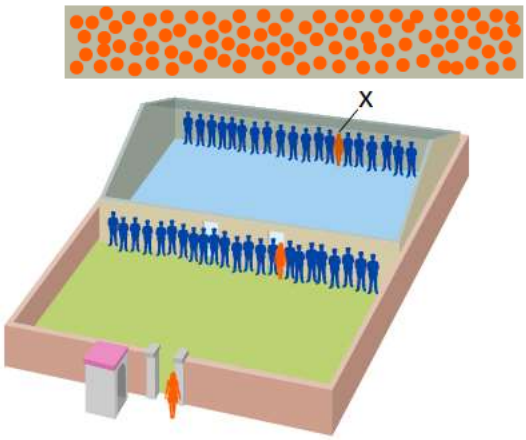
朝永振一郎「光子の裁判」／日経サイエンス

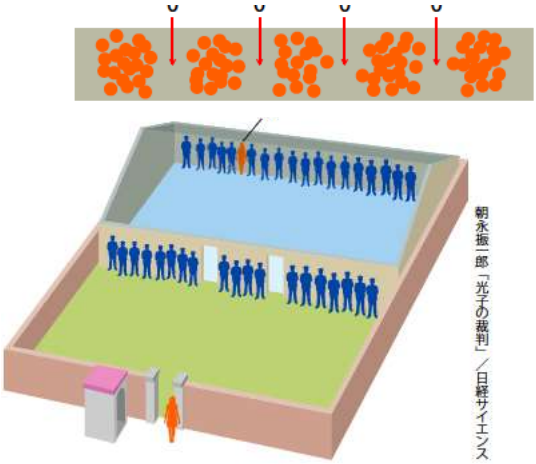
2つの窓　被告・波乃光子が侵入した家には窓が2つあった。果たしてどちらから入ったのか。

光子裁判

検事：「波乃光子はどちらの窓（スリット）を通ったのか？」
光子：「私は両方の窓を通りました」
検事：「怒！」
弁護士：「誰も目撃していなかったのだから、その質問自体が間違い」
判事：　？







光は量子ーまとめ

光は検出されるときは粒子として一個づつ検出される。検出する以前の光は波としてふるまう。検出を多数くり返すと、干渉縞があらわれ、波としての性質が示される。

光子の経路が分かるような実験だと、その縞は消える。

お奨め
浜松ホトニクス　https://www.youtube.com/watch?v=ImknFucHS_c
キャノン　サイエンスラボ　キッズ
https://global.canon/ja/technology/s_labo/light/001/11.html

「粒子でもあり波でもある」の誤った理解：

量子力学で「波」というときは、状態の重ね合わせのこと

測定したら粒子として測定されるが、測定前は
波＝重ね合わせ状態と理解される

粒子が多数あるとき

公理

スピンを持った粒子が多数あるときの状態は、積になる

例　５粒子

｜０＞｜１＞｜１＞｜０＞｜１＞

これは、２進法の数01101に対応させることができる

重ね合わせの公理と合わせよう

- ここで、各スピンをｘ軸方向に倒すと、

（|0>+|1>)（|0>+|1>)　（|0>+|1>)　（|0>+|1>)

= |0000>+|0001>+|0010>+|0011>
+|0100>+|0101> +|0110>+|0111>
+|1000>+|1001>+|1010>+|1011>
+|1100>+|1101>+ |1110>+ |1111>

２の４乗、すなわち１６通りの可能性が展開される。

- 一般にｎ粒子あれば、２のｎ乗の項が展開される。仮に、アボガドロ数（６ｘ１０の２３乗）だけあれば、天文学的な数の項が重ね合わされる。
- 　量子計算機の威力の原因の一つがここにある。

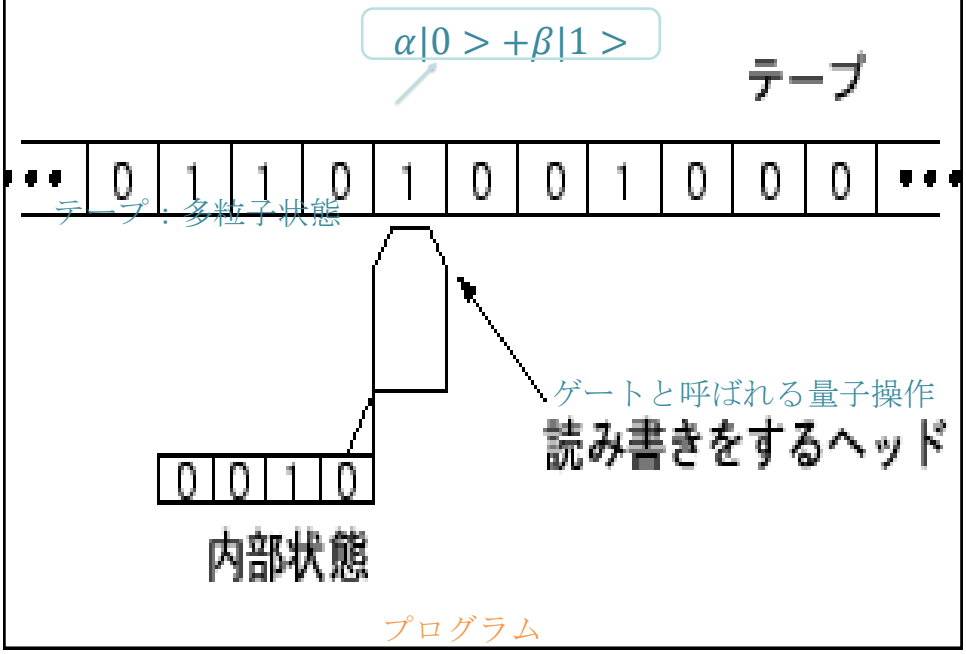
１０分ほど休憩

3.　量子計算とは何か？

D.ドイチ（１９８５）

多数の重ね合わせを用意して、それらを次の２種類の、物理操作による書きかえを組み合わせて実行すると、任意の状態を作ることができる。

量子チューリングマシン



古典計算機との比較

量子計算機で解ける（ない）問題は古典計算機でも解ける（ない）。

理由：量子計算は量子力学に従って（シュレーディンガー方程式のように）数式で記述されているので、それを古典的に実行すればよい。

違いは速さのみにある。

２つの基本的なゲート

・重ね合わせ状態を作る

｜０＞ ⇒ α｜０＞＋β｜１＞

・２ビットを相関させる(c-NOT)

|00> ⇒ |00>, |01> ⇒ |01> （第１ビットが０なら何もしない）

|10> ⇒ |11>, |11>. ⇒ |10> (第１ビットが1なら第２ビットにNOT

a+b mod 2

0+0=0, 0+1=1, 1+0=1, 1+1=2=0

を並列的実行しよう

まず、

(|00>+|01>+|10>+|11>)|0 >

を用意する。

|00> |0> +|01> |0> +|10> |0> +|11> |0>

cnot12 ⇒ (|00>|0>+|01>|0>+|11>|0>+|10>|0>

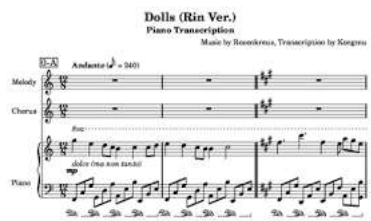
cnot23 ⇒ (| 0 0>|0>+| 0 1>|1>+| 1 1>|1>+|10>|0>

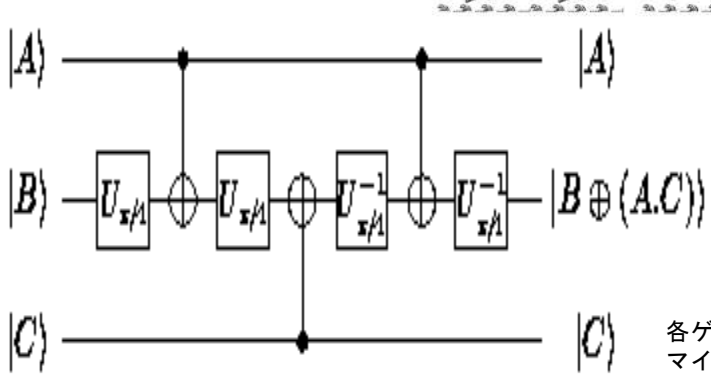
cnot12 ⇒ (|0 0 >|**0**>+|01> |**1**>+|10>|**1**>+|11>|**0**>

最後の行で、a+b mod 2の答えが、一番右に出ている。

問題と答が関連づいた重ね合わせとして出力される（エンタングルメント）

量子計算回路例





各ゲートはマイクロ波のパルス列

左から右に読む

解くのは難しいが、検算が簡単な問題

- 量子計算機は、確率的なので間違うこともある。（原発の管理には使えない）
- 量子計算機は解くのは難しいが、検算が簡単な問題（NP問題）に適している。

（何回かやって結果を検算して、正しいのがでるまでやればよい）

例　　素因数分解

４５７０７９＝３９１ｘ１１６９

4. 量子計算が有効な例

- P.Shor(1994)
- 入力ビット数の３乗程度のU1とCNOTの個数で、因数分解を行うアルゴリズムを発表した。
- ５００ビットくらいで通常の計算機の能力を超える。
- ➡ RSA公開鍵方式の暗号が破れる。

まとめ

- 量子計算機は、多数の状態の重ね合わせにより、たくさんの計算を同時並行して行うことにより、素因数分解のように計算が格段に速くなることがある。

- 確率的にしか正しい答えを出さないが、検算して間違いを排除することのできる問題に適している。

四則計算については従来型と能力は同じ

間違い：多くの近似解を出す。

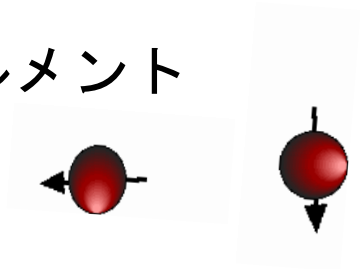
いさ進一財務政務官

現在は実験が先行して、研究が進んでいる。

最大の難関は、キュービットを増やすと雑音が増大して重ね合わせ状態が壊れることである。

エンタングルメント

(| 0 > -| 1 >)| 1 >



C-NOT

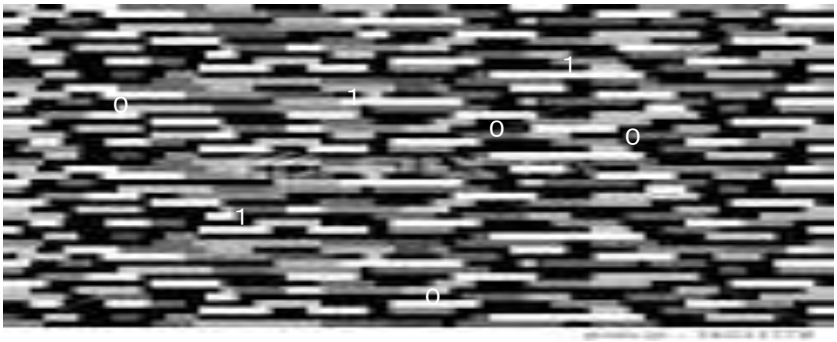
| 0 >| 1 > -| 1 >| 0> 絵に描けない

２つのスピンが強く相関している

EPR 状態

作るのが難しい理由

- 外界からのノイズで、重ね合わせ状態が壊れる。



「測定」と「雑音」は、同じものの別の顔なので

ノイズの少ない系では、測定に時間がかかる

クリーンな物理系

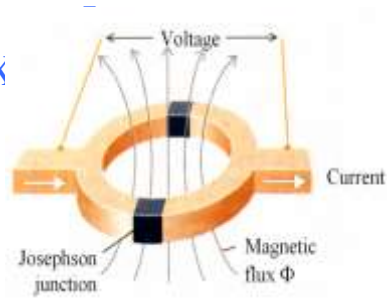
超伝導体、ダイヤモンド内部など

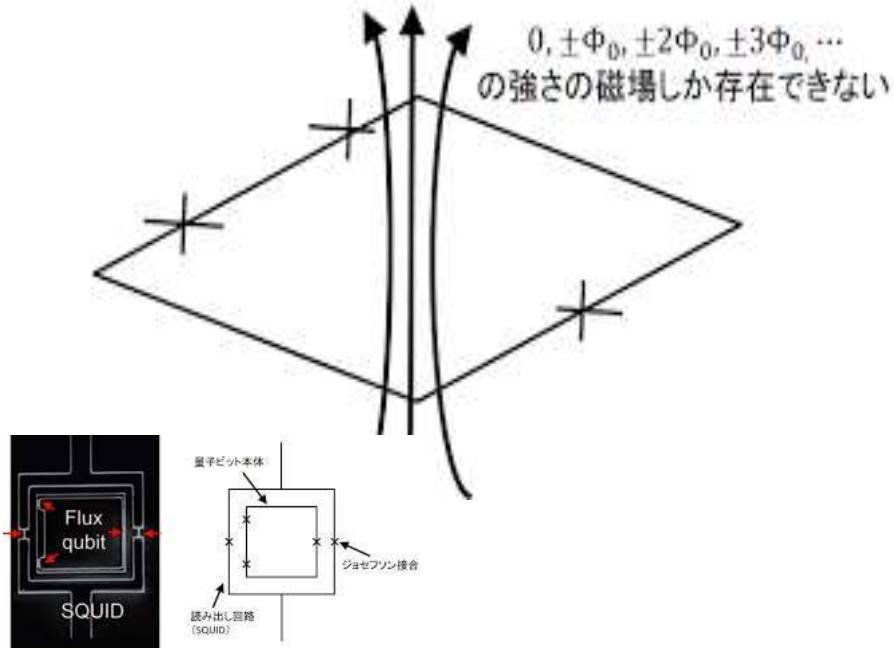
超電導量子ビット

- 磁束型が D-Waveで採用

超電導体の中で磁束が量子化される

h/2e=2.067…..X





$\Phi=0$ $|0>$

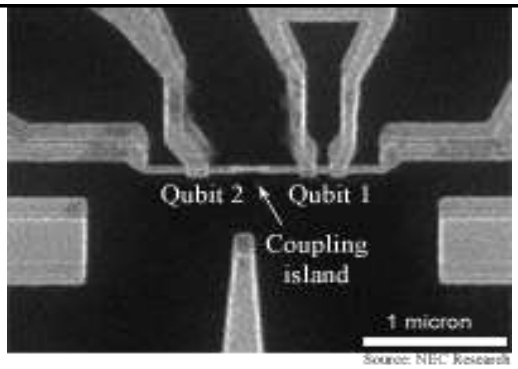
$\Phi=\Phi_0$ $|1>$

$\Phi=\Phi_0/2$ ならば重ね合わせ

$[|0>+|1>]/\sqrt{2}$

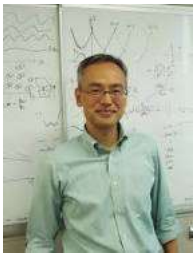
超電導電荷型キュービット（中村、蔡ら）
改良型（transmon）をGoogle, IBM, Intelなどが採用
超電導状態では２個の電子が対（クーパー対）になってぎっしり詰まってる。そのうちから０個あるいは１個取り出して箱に入れる。
箱の状態は |0>あるいは |１>になる。
適切な電圧をかけて1/2個にすると状態はかさねあわせ状態になる

[| ０>+| １>]/√2



The circuits in this image form a pair of quantum bits, or qubits, that can be entangled. Entanglement is a weird quantum property that gives quantum computers the potential to be extraordinarily fast. The circuits are a precursor to quantum computer chips.

Nakamura, Tsai et al
NEC group



それでもノイズは残る

　今後の課題は、「誤り訂正」を組み込んだ
次世代型の量子コンピュータが必要とされる。

理論的に可能であることは知られている。
誤り訂正のためのキュービットを増やさなくてはいけない。

クラウド量子コンピュータ

IBM は 2016年5月4日に世界で初めて、量子コンピューターをクラウドで公開し、誰でも使えるようにしました。2017年11月には50 量子ビットの試作機の製作と稼働に成功、12月には20 量子ビットの提供を始めた
Google, Intel なども同様のサービスを提供

量子超越性　quantum supremacy

Goolgeのチームは、２０１９年にとある量子回路を

Q: 超電導デバイスを使って計算
C: 同じ回路を普通の計算機でシミュレート

Qにかかる時間：３分２０秒
C :天文学的時間(IBMから異議)
　公平な比較か？

「量子情報科学の国家戦略概要」
アメリカ　「国家量子イニシアティブ法」成立（2018.12）
1,400億円/5年
「国家量子イニシアティブプログラム」
DOE：140億円/年 量子情報研究センター（最大数5）
NSF：56億円/年 量子研究・教育センター（最大数5）
NIST：89億円/年 量子情報研究・計量標準、ワークショップ
中国
「科学技術イノベーション第13次5ヶ年計画」（2016-20）
1,200億円/5年
「国家重点研究計画」「量子情報科学国家実験室」（合肥市）建設中。
2020年完成予定（～1兆円）
EU
「Quantum Manifesto」
（2016.5）
>1,250億円/10年
「Quantum Technology Flagship」20課題が採択（2019-28）

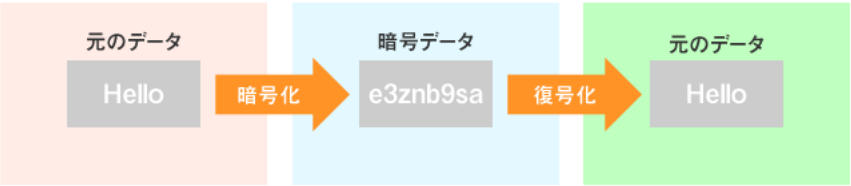
ご質問をどうぞ

1．はじめに

インターネット社会

便利だけれども
安全性は確保さ
れているの？

暗号化して通信



RSA公開鍵暗号

広くインターネットのセキュリティーに使われている

◎大きな数の素因数分解が困難であることに基づいている

発案者　Rivest Shamir　Adleman　の頭文字で呼ばれる暗号方式

RSA公開鍵暗号の考え方

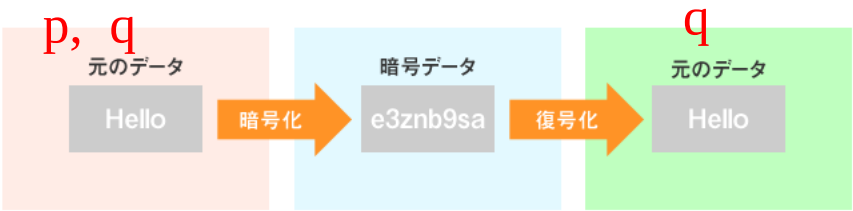
（１）Aさんは元の文章（平文）を素数pとqを使って暗号化し、暗号鍵　m=pxqをBさんに通常回線で知らせる（公開）

（２）Bさんは素数qをあらかじめ知っているので、送られてきたmをqで割って、pを求めることができる

（３）Bさんは素数pとqを使って暗号を平文に戻す

盗聴者は整数mを知ることができるが、素因数分解が難しいので、素数pとqを別々に知ることは宇宙時間かかってもできない

素数p, q で暗号化して通信



m
=
p
x

公開した通信路を使って、掛け算の結果mだけを送る

盗聴者が素数pとqを別々に取得することは困難

カシオの計算ウェブサイト

「指定した整数を素因数に分解します」

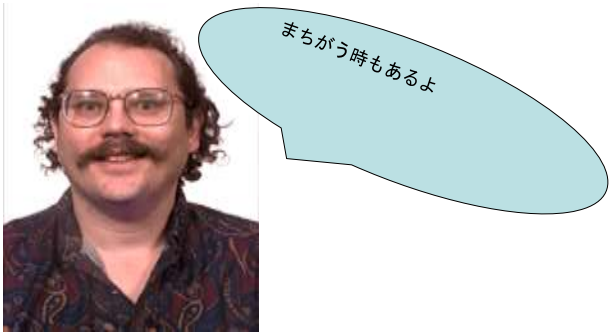
で、２０１９を分解させる
答

２０１９＝３x６７３

しかし、下の方に警告：

整数は最大50桁です。大きな素数を含む整数の素因数分解は、タイムアウトにより計算できないことがあります。

量子計算機が実装されると、素因数分解が短時間に、高い確率で、できるようになる。



その時、RSA公開鍵暗号方式は全面崩壊し、インターネット社会のセキュリティーシステムが危機に瀕する

ご質問をどうぞ

量子計算機の効能

得意な計算（NP問題）

解くことには面倒で時間がかかるけれども、検算は簡単なので間違いをすぐに排除できる

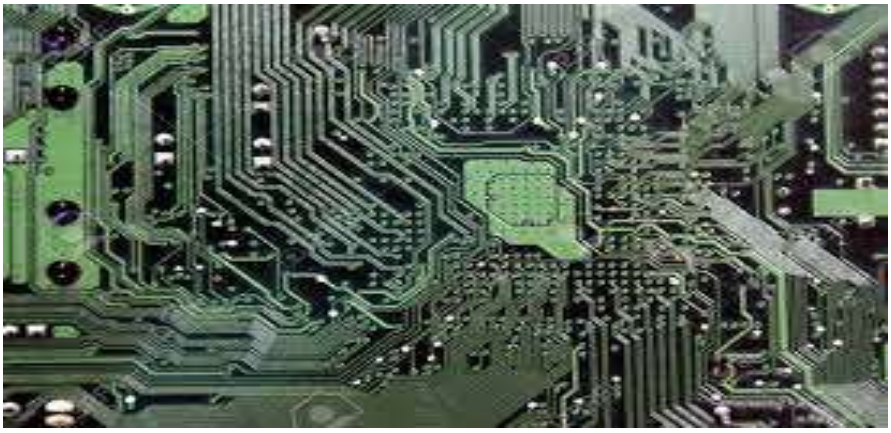
例１：素因数分解
例２：巡回セールスマン問題

５０の空港を全部回る出張命令を受けたセールスマン
与えられた出張旅費１０００万円以内で可能か？

量子計算で解けると期待される

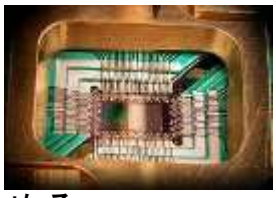
巡廻セールスマン問題の経済効果

例　　コンピュータ素子（チップ）の制作費は大幅ダウン



最近の話題

超伝導キュービット



- D-Wave（民間会社の名前）

量子系の最低エネルギ−状態を速く求める専用計算機　(事業はgoogleに引き継がれる)

原理は東工大の西森秀稔さんの「量子アニーング」

Goolgleの53qbit マシン

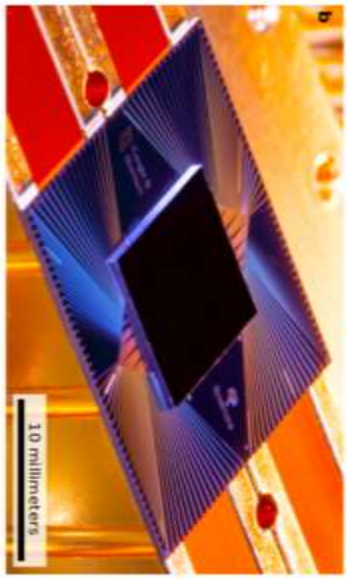
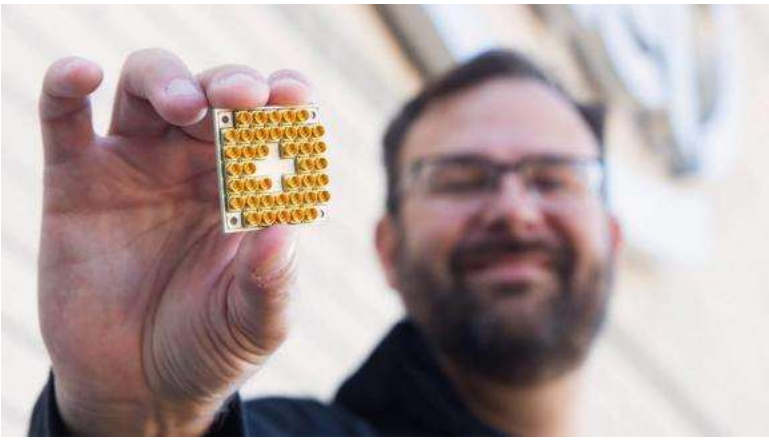


FIG. 1. **The Sycamore processor. a,** Layout of processor showing a rectangular array of 54 qubits (gray), each connected to its four nearest neighbors with couplers (blue). Inoperable qubit is outlined. **b,** Optical image of the Sycamore chip.

手に取ると

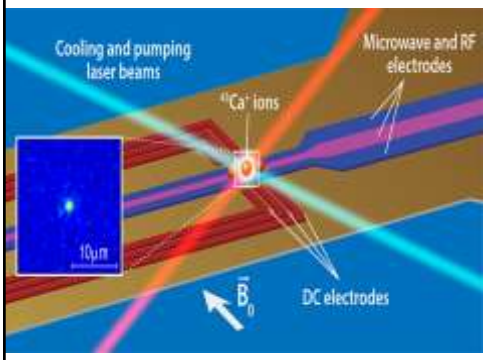


Intel

Google Machine

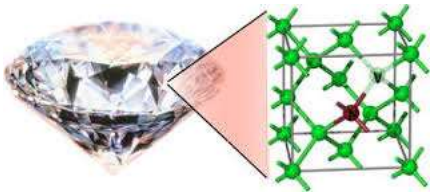
これが極低温に置かれる

イオントラップ(NIST,Sussex,Innsbrook)

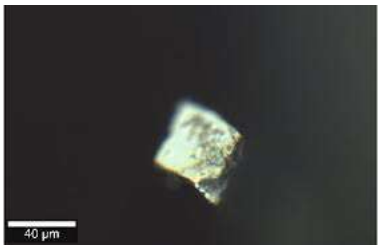


最大１４個のイオン

ダイヤモンドのNVセンター



単１スピン
常温



ダイヤモンドが好き

- 量子最速降下曲線に関する１１年前の理論的な論文　PRL 96,060503
  の内容が昨年、ダイヤモンドNV中心を使って実証された。

ご清聴をありがとうございました