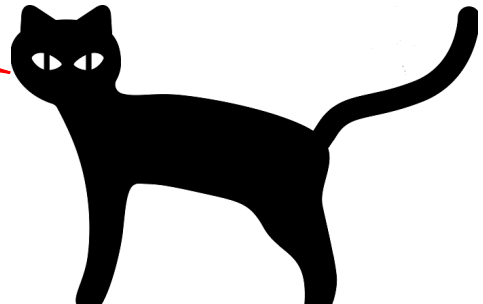
# 重なり合う量子の世界

## 「存在とはなにか」～
## 量子コンピューターまで

量子力学は「存在とはなにか」という当たり前のような認識を
一変させる

静岡大学理学部　　冨田　誠（量子光学）

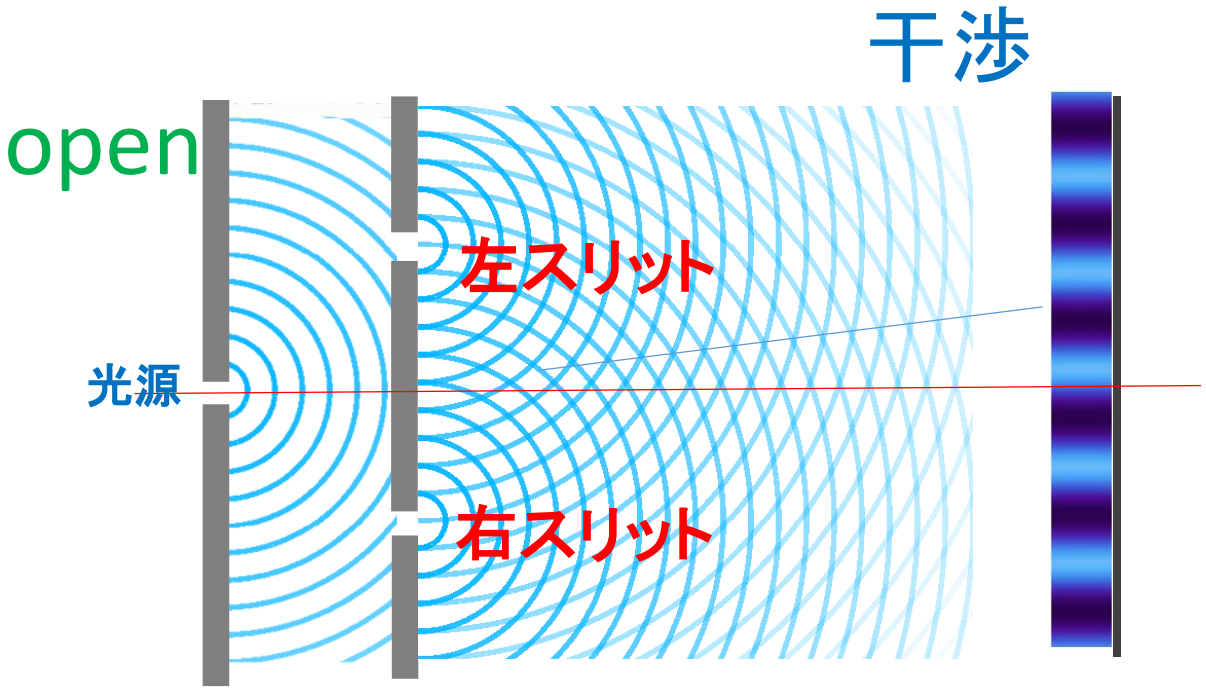
・基礎科学は世界観をかたちつくる。
・基礎科学は先端技術を切り開く



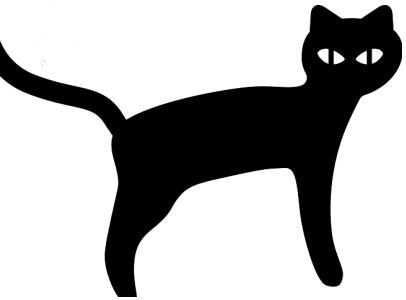
# 二重スリットの実験

光源から出射した波は、
右のスリットと左のスリット
に分かれて通過し、
スクリーン上で
　強めあったり
　弱めあったりする

干渉

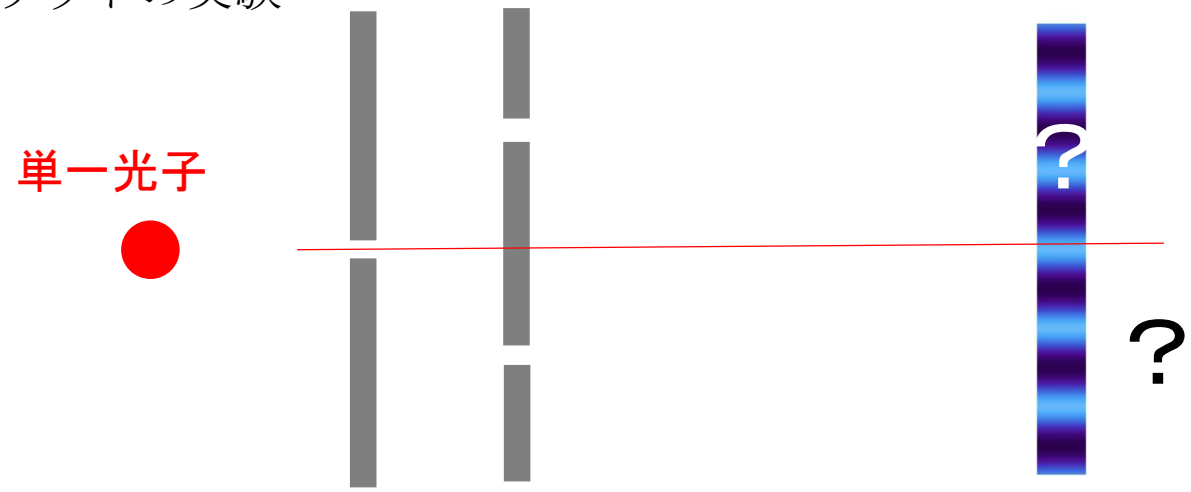



干渉縞が観測されるということは、波が2つの経路を通過した結果である。



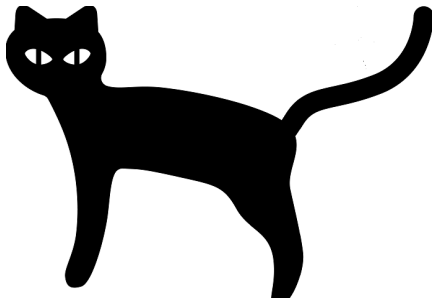
# 単一光子を用いた二重スリットの実験

１つの光子をもちいて２重スリットの実験を行うとどうなるか？

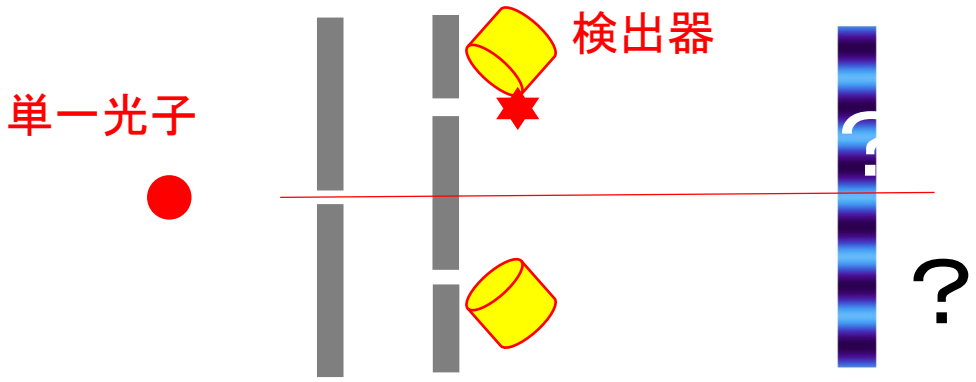



光子は分割できない。
　　上のスリットを通るか
　　下のスリットを通るか
どちらかでしょう。

　干渉縞は、２つの光路の重ねあいの結果なので、干渉縞は出ないのではないか



# Which path experiments




・1つの光子で干渉が現れる

→1つの光子が2つの経路を重なり合って通過していると考えざるを得ない

→では、どちらを通過したか観測する。両方のスリットで観測されるか

→否。(観測はできるが)どちらかでしか観測されない

→　確率的に現れるが観測してみないとわからない

# 電子も干渉する！

**波動性と粒子性はあらゆる物質に普遍的な性質電子**

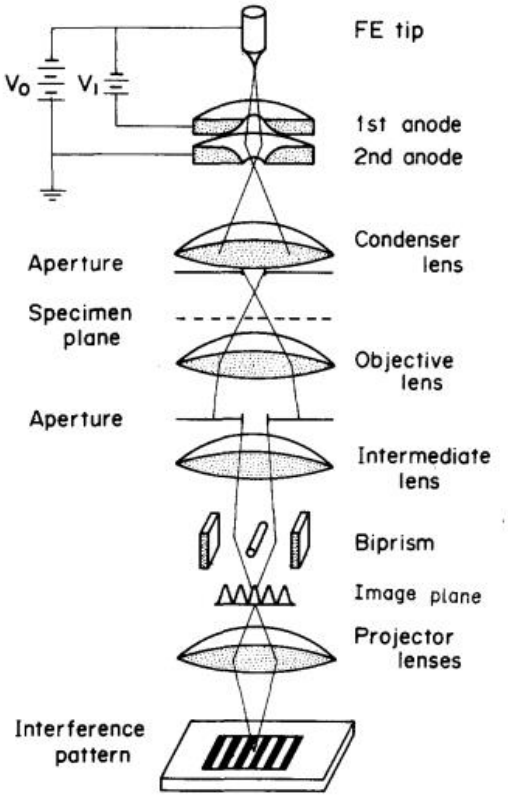
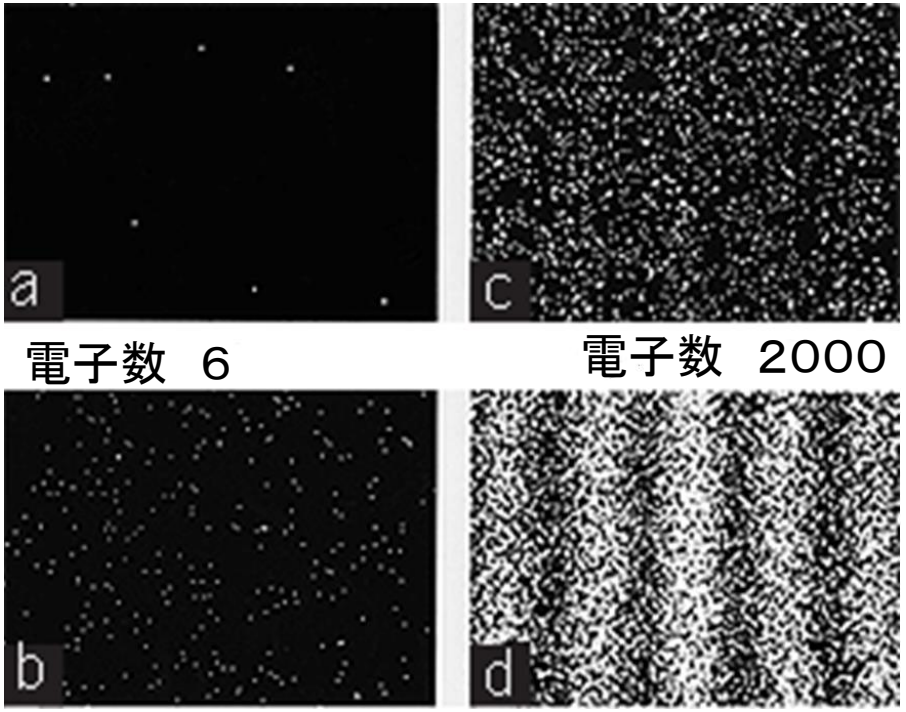



Fig. 3. Electron-optical diagram of the interference experiment.




電子数　6　　電子数　2000

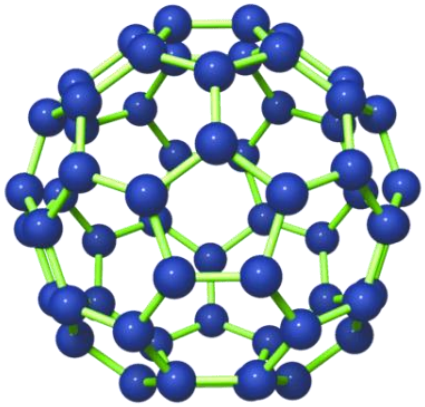
電子数　270　　電子数　60000

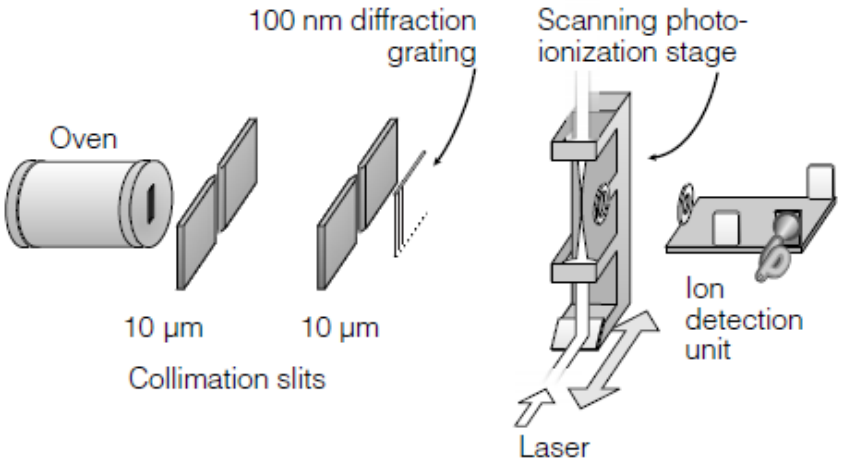
電子の二重スリット実験による干渉

：American Journal of Physics 57, 117 (1989); doi: 10.1119/1.16104

# $C_{60}$も干渉する！

NATURE | VOL 401 | 14 OCTOBER 1999 |






## Wave–particle duality of $C_{60}$ molecules

NATURE | VOL 401 | 14 OCTOBER 1999 n Vos-Andreae, Claudia Keller, Gerbrand van der Zouw & Anton Zeilinger

*Institut für Experimentalphysik, Universität Wien, Boltzmanngasse 5, A-1090*

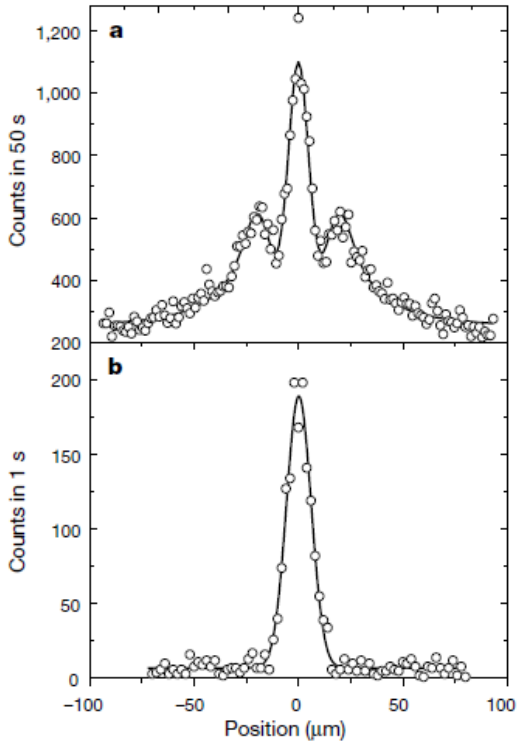



**Figure 2** Interference pattern produced by $C_{60}$ molecules. **a**, Experimental recording (open circles) and fit using Kirchhoff diffraction theory (continuous line). The expected zeroth and first-order maxima can be clearly seen. Details of the theory are discussed in the text. **b**, The molecular beam profile without the grating in the path of the molecules.

# 生体分子も干渉する！

VOLUME 91, NUMBER 9 PHYSICAL REVIEW LETTERS week ending 29 AUGUST 2003

## Wave Nature of Biomolecules and Fluorofullerenes

Lucia Hackermüller, Stefan Uttenthaler, Klaus Hornberger, Elisabeth Reiger, Björn Brezger,*
Anton Zeilinger, and Markus Arndt
*Institut für Experimentalphysik, Universität Wien, Boltzmanngasse 5, A-1090 Wien, Austria*†

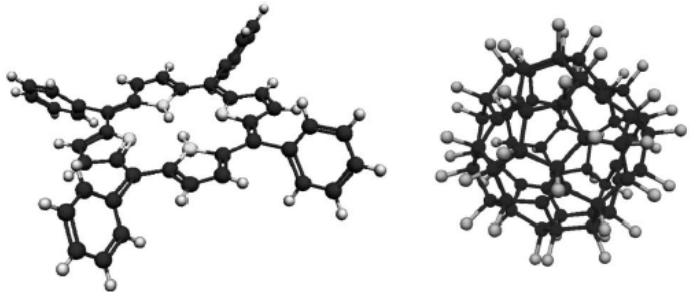


FIG. 1. 3D structure of tetraphenylporphyrin (TPP) $C_{44}H_{30}N_4$ (left) and the fluorofullerene $C_{60}F_{48}$ (right) [10]. TPP ($m = 614$ amu) is composed of four tilted phenyl rings attached to a planar porphyrin structure. The fluorofullerene ($m = 1632$ amu) is a deformed $C_{60}$ cage surrounded by a shell of 48 fluorine atoms. Only an isomer with $D_3$ symmetry is drawn here.

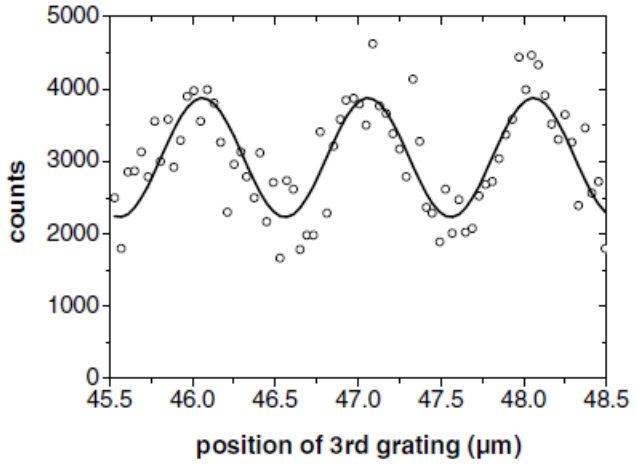



FIG. 4. Quantum interference fringes of $C_{60}F_{48}$. The beam has a mean velocity of $v_m = 105$ m/s and a velocity spread (FWHM) of $\Delta v/v_m = 20\%$. To obtain this pattern, 14 scans with the lowest noise were selected and summed after subtracting the individually measured background (see text). The observed interference contrast of 27% lies significantly above the value of 12% expected by a classical model.

# 哲学の世界：実在とは

・歴史は、本当に存在したのだろうか？
・私が見ているこの人は、本当に存在するのだろうか？

何もかも疑わしい。。。。

『我思う、ゆえに我あり』



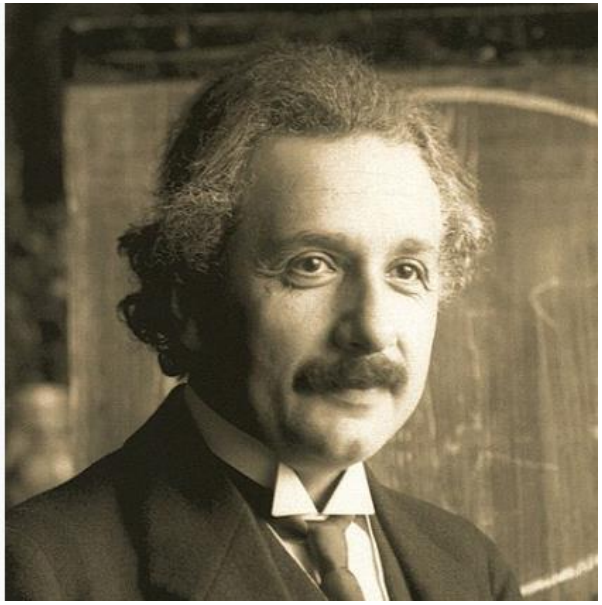



**ルネ・デカルト(Rene Descartes, 1596-1650)**
あらゆる外的事物の実在を疑ったデカルトは、思考する起点としての**『自我意識の実在』**だけは疑えないとした。

**唯物論**
主観（主体）に先行する客観（客体）の実在性を重視する立場

**唯心論**
客観（客体）が主観（主体）の認識作用によって構成されるという立場。世界は心の作り出す表象

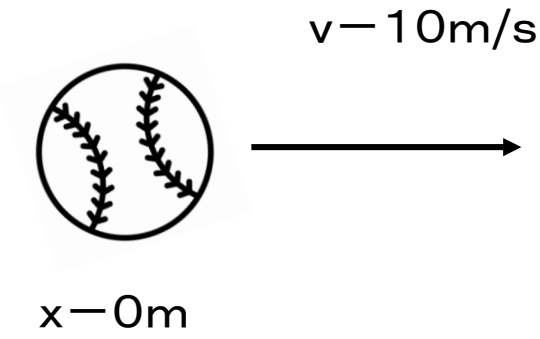
# 物理の世界：実在とは



CC Wikipedia
Creative Commons license

物理学の世界での「実在」の基準

その物理量を有する系の状態を乱すことなしに、その物理量を確実に予言することが可能であること（byアインシュタイン）



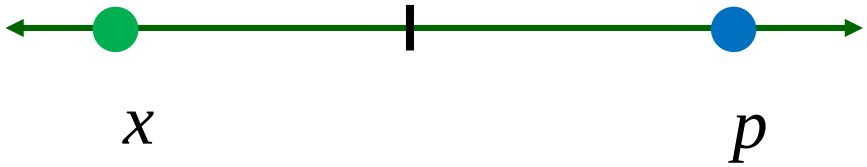

ボールの速さは確定している
ボールの位置は確定している

ボールは実在している

# 素朴実在論　Vs　量子論

## EPRパラドクス　Einstein–Podolsky–Rosen paradox1935年

非局所性を前提に、相関を持った2粒子の運動を考えると1つの粒子の位置と運動量が同時に実在することになる（確定する）。量子力学では共役な物理量の間には不確定性関係が存在し、同時に正確に確定することはできない。即ち、波動関数による実在の記述は完全ではない。

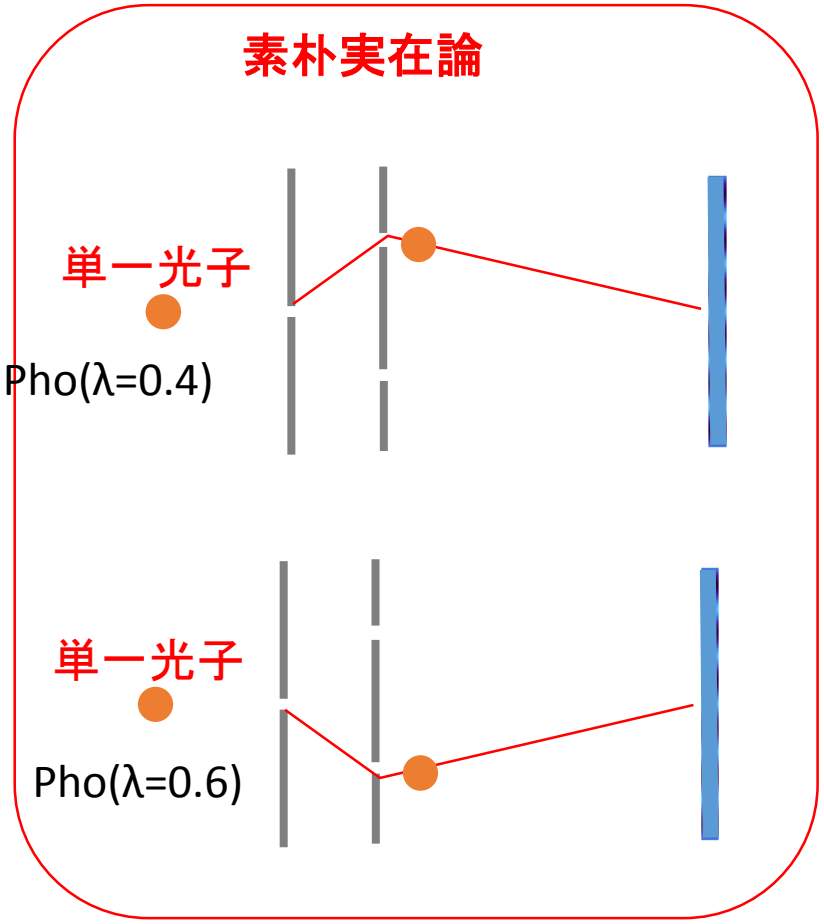



$$[\hat{x}, \hat{p}] = i\hbar$$

## 隠された変数理論

量子力学に特徴的な確率的な性質を、実験者が観測できない変数を導入して説明する理論である。アインシュタインの言葉に、「神はサイコロを振らない」というものがある。これはアインシュタインの、完全な物理学理論は決定論的であるべきとの信念の表れである。

# 隠された変数理論で考えてみる




光子は分割されない粒

→我々がまだ知らない隠された変数
　λがある

→例えば
　・λ >0.5 なら右スリット
　・λ <0.5 なら左スリット
を通過する。

光子は、
（かなり不自然な仮定であるが、例えば）
通過するときに隣のスリットの
位置を確認して、
　・自分が向かってよい場所（明の干渉）
　・自分が向かってはいけない場所（暗の干渉）

を感じ取ってスクリーンに進む。

、

、

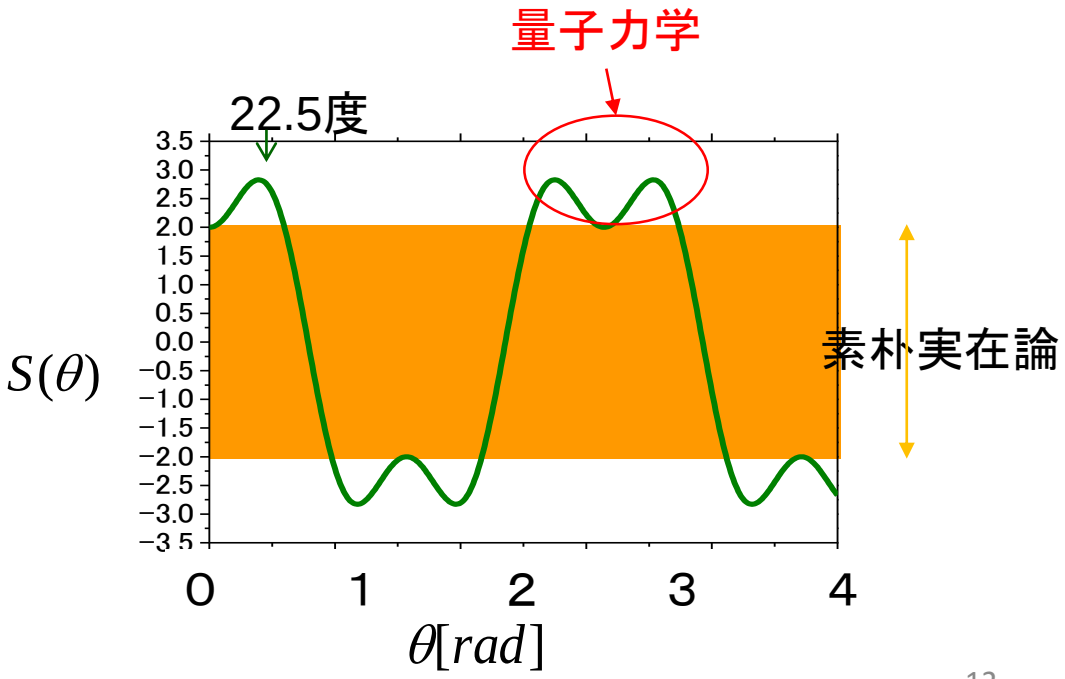
素朴な実在論！

# Bellの不等式 (隠された変数理論が満たすべき)

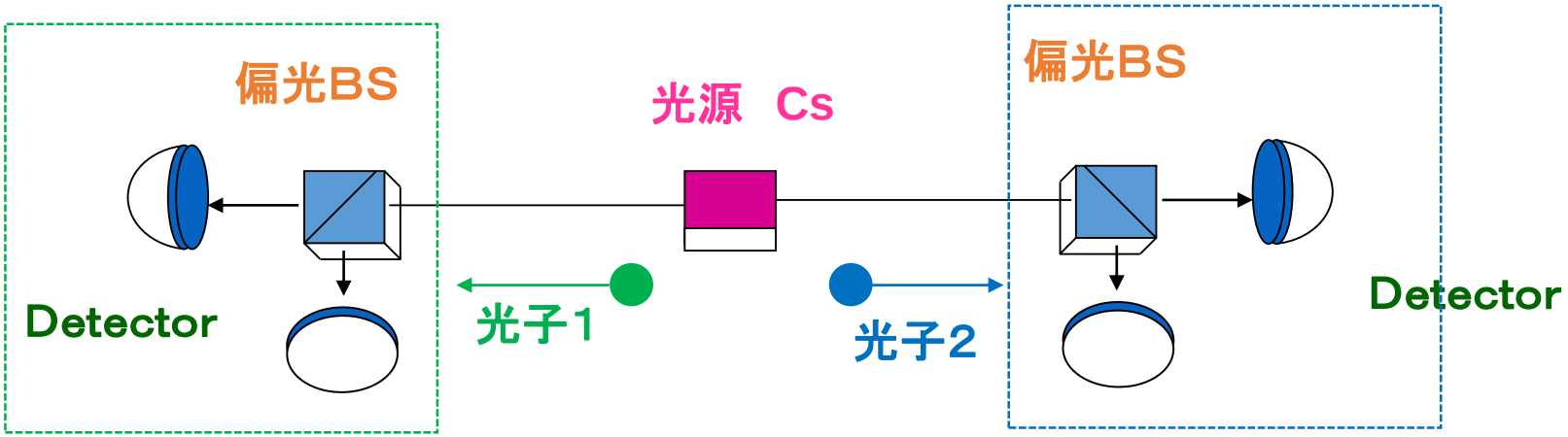
ジョン・スチュアート・ベル（John Stewart Bell, 1928年6月28日 - 1990年10月1日）は物理学者である。

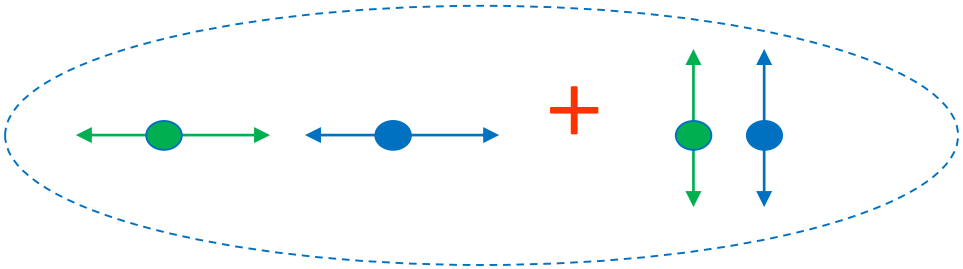


ベルの不等式とは、局所的な隠れた変数理論が満たすべき相関の上限を与える式である。量子力学ではこの上限を破ることができ、実験的に、量子論と局所的な隠れた変数理論を区別することができる。



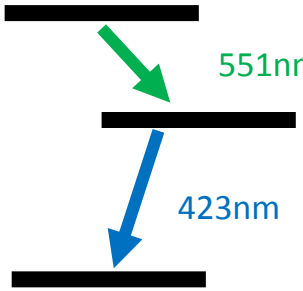
# (Bellの不等式の実験検証）双子の光子



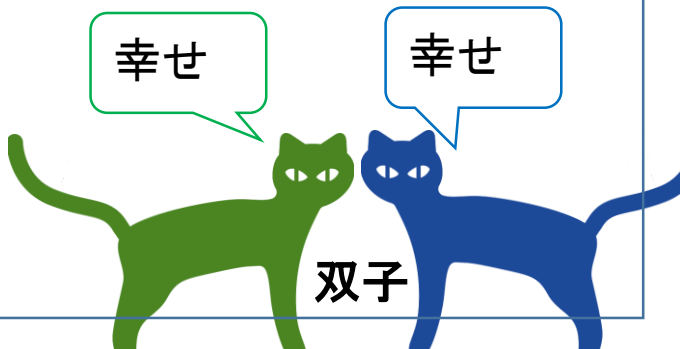



$$|\Psi>_{12}=\frac{1}{\sqrt{2}}(|H>_1|H>_2+|V>_1|V>_2)$$

Cs原子の
カスケード放射




・相関をもった2つの光子対を発生させ
・反対方向に伝播させる
・2つの光子が充分離れたとき観測する



# Aspectの実験

VOLUME 49, NUMBER 2 PHYSICAL REVIEW LETTERS

**Experimental Realization of Einstein-Podolsky-Rosen-Bohm *Gedankenexperiment*: A New Violation of Bell's Inequalities**

Alain Aspect, Philippe Grangier, and Gérard Roger
*Institut d'Optique Théorique et Appliquée, Laboratoire associé au Centre National de la Recherche Scientifique, Université Paris-Sud, F-91406 Orsay, France*
(Received 30 December 1981)

The linear-polarization correlation of pairs of photons emitted in a radiative cascade of calcium has been measured. The new experimental scheme, using two-channel polarizers (i.e., optical analogs of Stern-Gerlach filters), is a straightforward transposition of Einstein-Podolsky-Rosen-Bohm *gedankenexperiment*. The present results, in excellent agreement with the quantum mechanical predictions, lead to the greatest violation of generalized Bell's inequalities ever achieved.

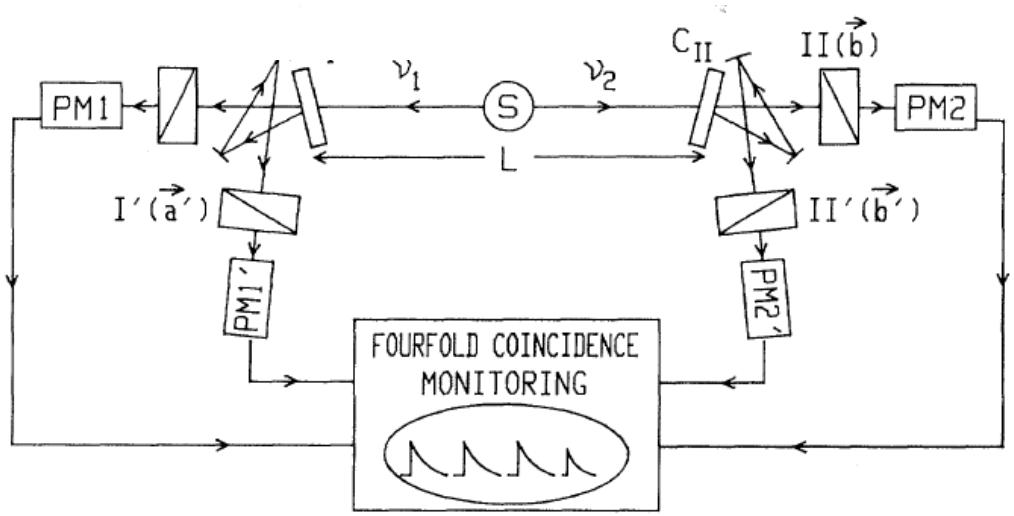
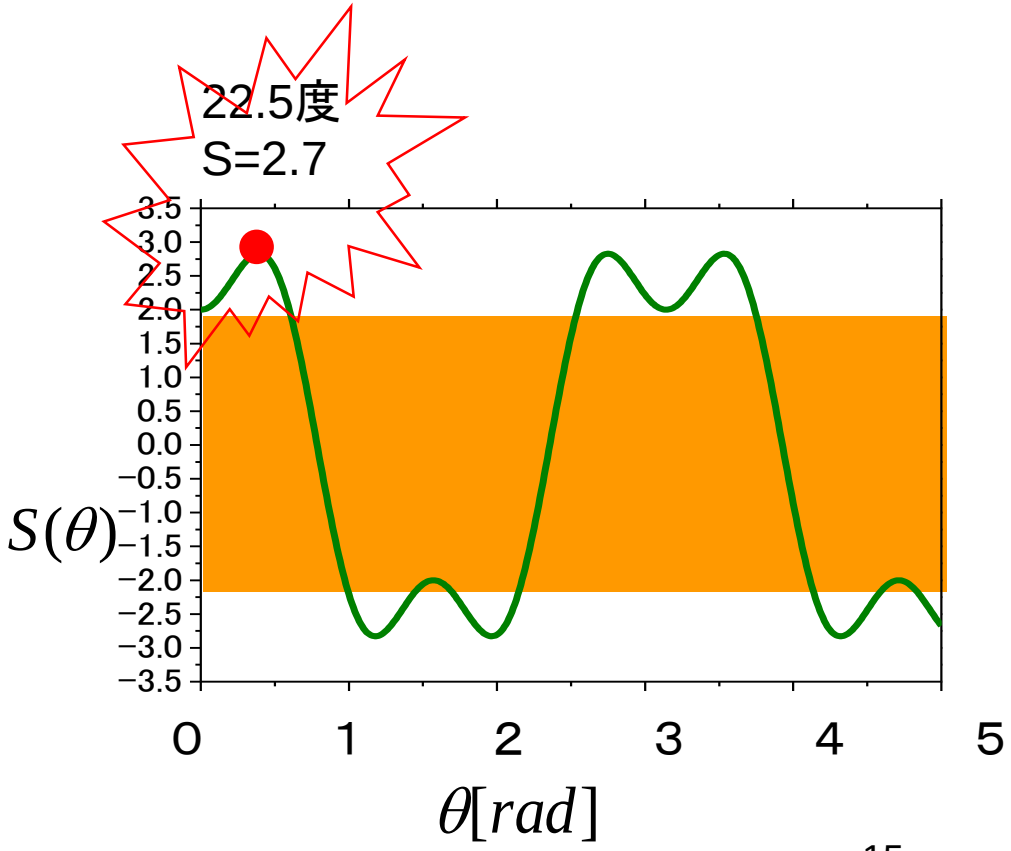



FIG. 2. Timing experiment with optical switches. Each switching device ($C_I$, $C_{II}$) is followed by two polarizers in two different orientations. Each combination is equivalent to a polarizer switched fast between two orientations.

# A.Aspectの実験

Bellの不等式は実験的に成立しない。我々の世界は**素朴な意味では実存していない。**




アラン・アスペ（Alain Aspect, 1947年6月15日 - ）は、フランス出身の物理学者である。アスペは、1980年代初期にベルの不等式を検証する実験を行った。

# われわれの住んでいる世界は、

× 隠された変数理論
＝素朴実在論

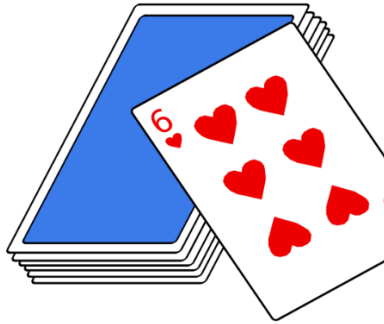
vs

○ 量子論
＝非実在論

・この2つは区別がつかないのではないか？

→ 両者はBellの不等式によって実験的に区別がつく

・われわれの住む世界は、素朴に実在しない（非実在性）



・区別することに意味があるのか？役に立つのか？

・ 古典論世界観 （決定論的世界観）

vs

量子的世界観 （神はさいころを振る。重なり合った世界。

・例えば、量子暗号鍵配布の安全性には、非実在性が根底にある

# 量子暗号鍵配布と量子コンピュター

古典暗号

1．共通鍵暗号

2．公開鍵暗号　RSA

量子暗号

3．BB84プロトコル

C.H. Bennett, G. Brassard,

# 共通鍵暗号（古典暗号その1）

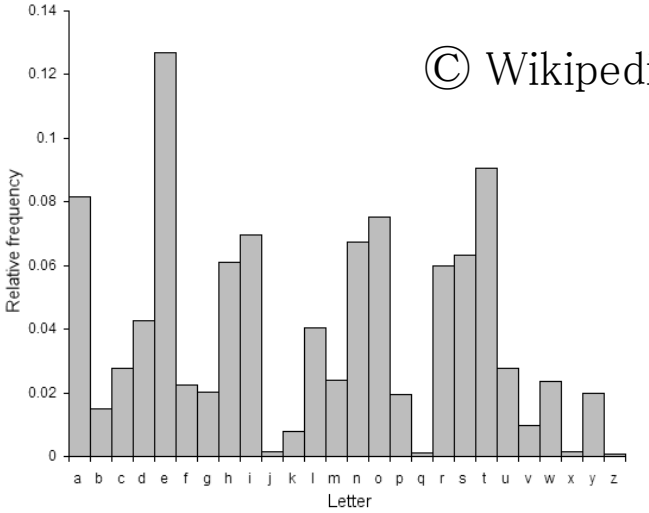

特徴
・暗号化と復号化に同じ鍵を使う
・ワンタイムパッド方式は安全な暗号方式
・量子コンピュターでも解読不能

十分な長さの共通鍵を事前に用意する必要がある
繰り返し使用すると解読される危険性が高い

# 共通鍵暗号（古典暗号その1）

## 共通暗号鍵への攻撃

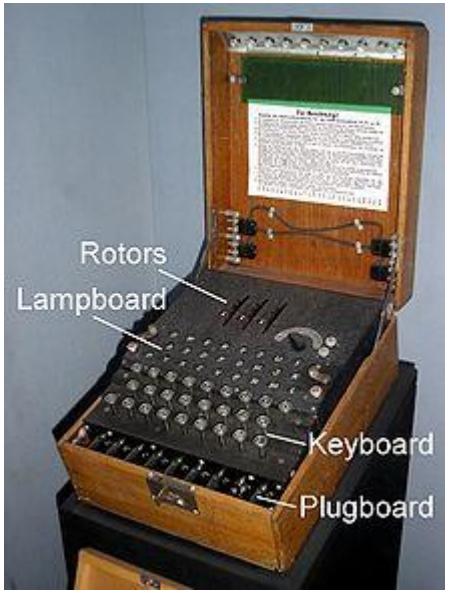
頻度分布
　同様に2文字（連接文字）の場合、t-h, h-e, i-n, e-r, ... 、3文字の場合には、t-h-e, a-n-d, i-n-g, i-o-n, ... などの順で出現頻度が高いことが知られている。



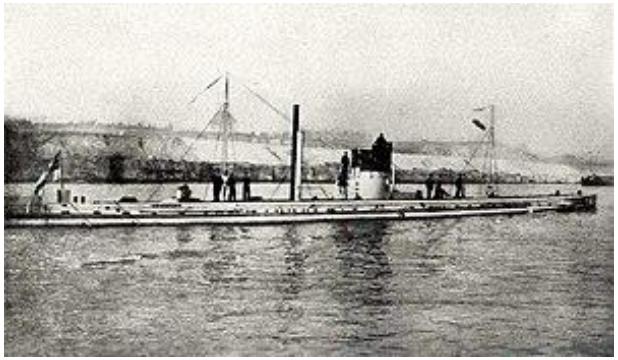


# 共通鍵暗号（古典暗号その1）

エニグマ(Enigma)
第二次世界大戦でナチス･ドイツが用いたローター式暗号機である。換字式の暗号方式。暗号文を同じ鍵で再暗号化すると平文が得られる。
　大戦中にイギリスはエニグマの解読に成功したが、その事実は徹底して秘密にされ、ドイツ軍は終戦までエニグマを使用し続けた



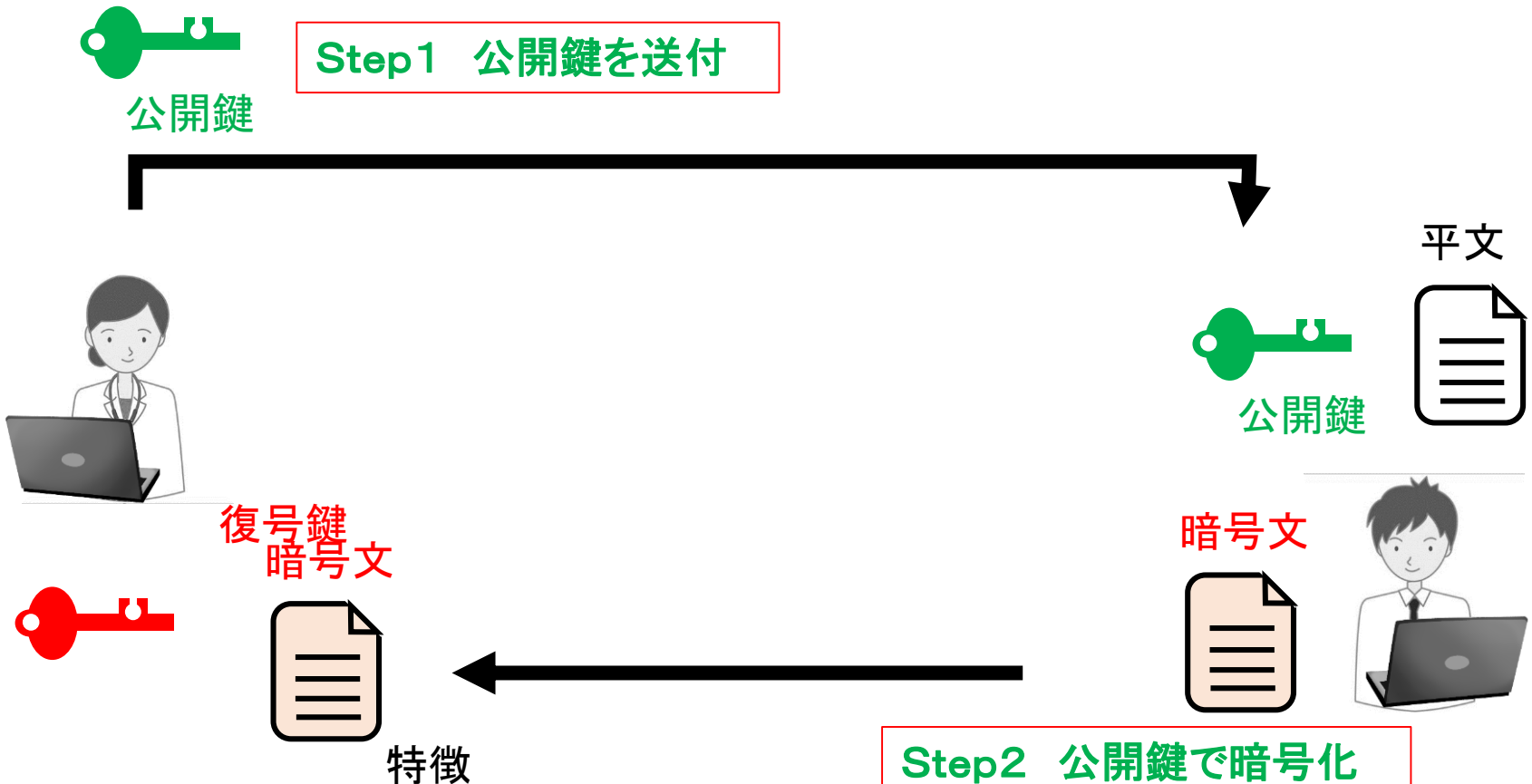




2019年5月29日 by Devin Coldewey

# 公開暗号鍵（古典暗号その2）




特徴
・鍵をあらかじめ共有している必要がない
・複数の相手との鍵の共有が可能
・計算の困難さを安全性の根拠とする

限界
・RSA暗号などは量子コンピュターが開発されると解読される

# 公開暗号鍵（古典暗号その2）

・計算の困難さを安全性の根拠とする

**素数**（そすう、英: prime number）とは、2 以上の自然数で、正の約数が 1 と自分自身のみであるもののことである。

素因数分解

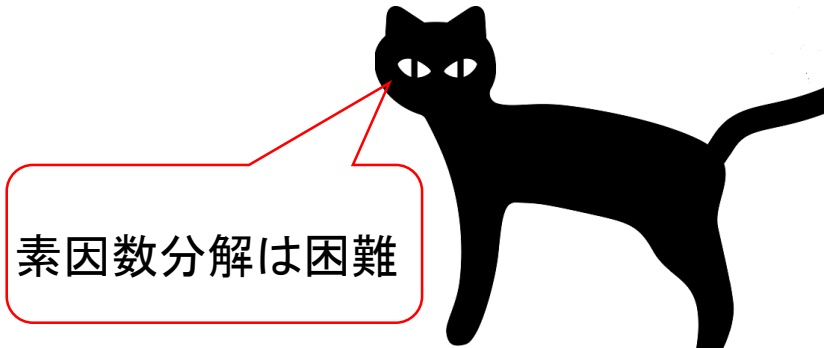
$$n = 15 = 3 \times 5$$

$$n = 481 = \square$$

$$n = 19235397083296222649360741129429957966009$$

$$= \square$$

「素数として確認された最大の数」は $2^{82,589,933} - 1$



# 公開暗号鍵への攻撃

共通の素数を使った2つの公開鍵から秘密鍵が容易に生成される

公開鍵1

$p = 375882326621802029434230962 3$

$q_1 = 91238371784768816724423920 81$

$q_2 = 31190614638779435799298807 07$

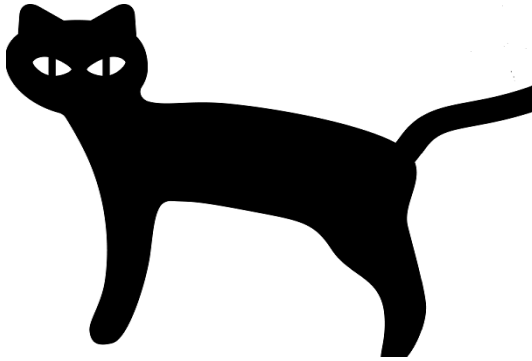
公開鍵

$n_1 = 342948914636438789406882918780638636450722565364652954 63$

$n_1 = 117240007991884516109021906433017411379861356892481434 61$

$n_1$と$n_2$の最大公約数

$p = 375882326621802029434230962 3$



公開鍵が偶然同じ複素数を
使っていると、最大公約数として素数がわかってしまう。
最大公約数は間単に計算できる。

# 量子暗号鍵配布

古典暗号
1. 共通鍵暗号
2. 公開鍵暗号　RSA

量子暗号
3. BB84プロトコル

C.H. Bennett, G. Brassard,

# 量子暗号BB84

## 量子暗号鍵配布

"Quantum Cryptography: Public Key Distribution and Coin Tossing",
Proceedings of IEEE International Conference on Computers Systems
and Signal Processing, Bangalore India, pp 175-179, December 1984.

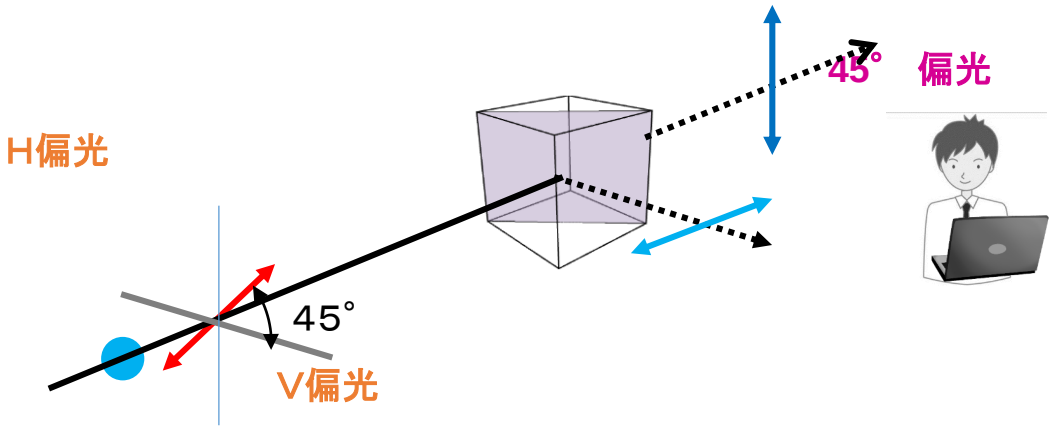
C.H. Bennett, G. Brassard,



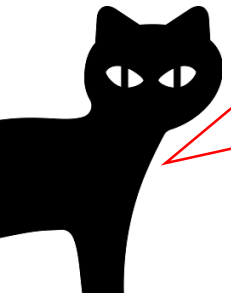
古典暗号の安全性
- 計算の困難さを安全性の根拠とする
- 量子コンピュターが開発されると解読される（RSA暗号）
- データハーベスト

量子暗号の安全性
- 物理的な原理を根拠とする

# 単一光子の偏光の観測基底




| アリスの基底 | ボブの基底 | | bit 結果 |
|---|---|---|---|
| ✢ | ✢ | ○ | 必ず一致 |
| ✕ | ✕ | ▲ | 一致するとは限らない |
| ✕ | ✢ | ▲ | 一致するとは限らない |
| ✢ | ✕ | ○ | 必ず一致 |

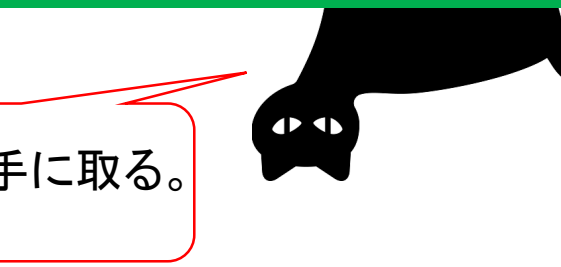


観測基底が一致しないときは結果が一致しない場合がある。

# 量子暗号BB84

基底の取り方

| | ✢ | ✕ |
|---|---|---|
| 0 | ↕ | ⤢ |
| 1 | ↔ | ⤡ |



基底は勝手に取る。
後で確認

| アリスの送信 bit | 0 | 1 |
|---|---|---|
| アリス基底 | ✕ | ✢ |
| アリス送信偏光 | ⤢ | ↔ |

←情報
←自由に選択
←送信信号

古典通信

量子通信

| ボブ基底 | ✢ | ✢ |
|---|---|---|
| ボブ観測偏光 | ↕ | ↔ |
| ボブの受信 bit | 0 | 1 |

←試しに選択
←観測
←復号結果

アリスの基底と
ボブの基底が同じ

ボブの観測結果は
アリスの情報と同じ

**Bobの通信後の作業**

| 基底の確認 | — | ○ |
|---|---|---|
| 結果 | | 1 |

アリスの基底と
ボブの基底が異なる

ボブの観測結果はアリス
の情報と同じとは限らない

# 量子暗号BB84

基底の取り方

| | ＋ | × |
|---|---|---|
| 0 | ↕ | ⤢ |
| 1 | ↔ | ⤡ |

アリスの基底と
ボブの基底が異なるにも「関わらず

偶然、ボブの観測結果は
アリスの情報と同じになる場合もある

古典通信

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| アリスの送信 bit | 0 | 1 | 1 | 0 | 0 | 1 | 0 | 0 | 0 | 1 | 0 | 1 | 1 | 0 | 1 |
| アリス基底 | × | ＋ | × | ＋ | ＋ | × | × | × | ＋ | × | × | ＋ | ＋ | × | × |
| アリス送信偏光 | ⤢ | ↔ | ⤡ | ↕ | ↕ | ⤡ | ⤢ | ⤢ | ↕ | ⤡ | ⤢ | ↔ | ↔ | ⤢ | ⤡ |

←情報
←自由に選択
←送信信号

量子通信

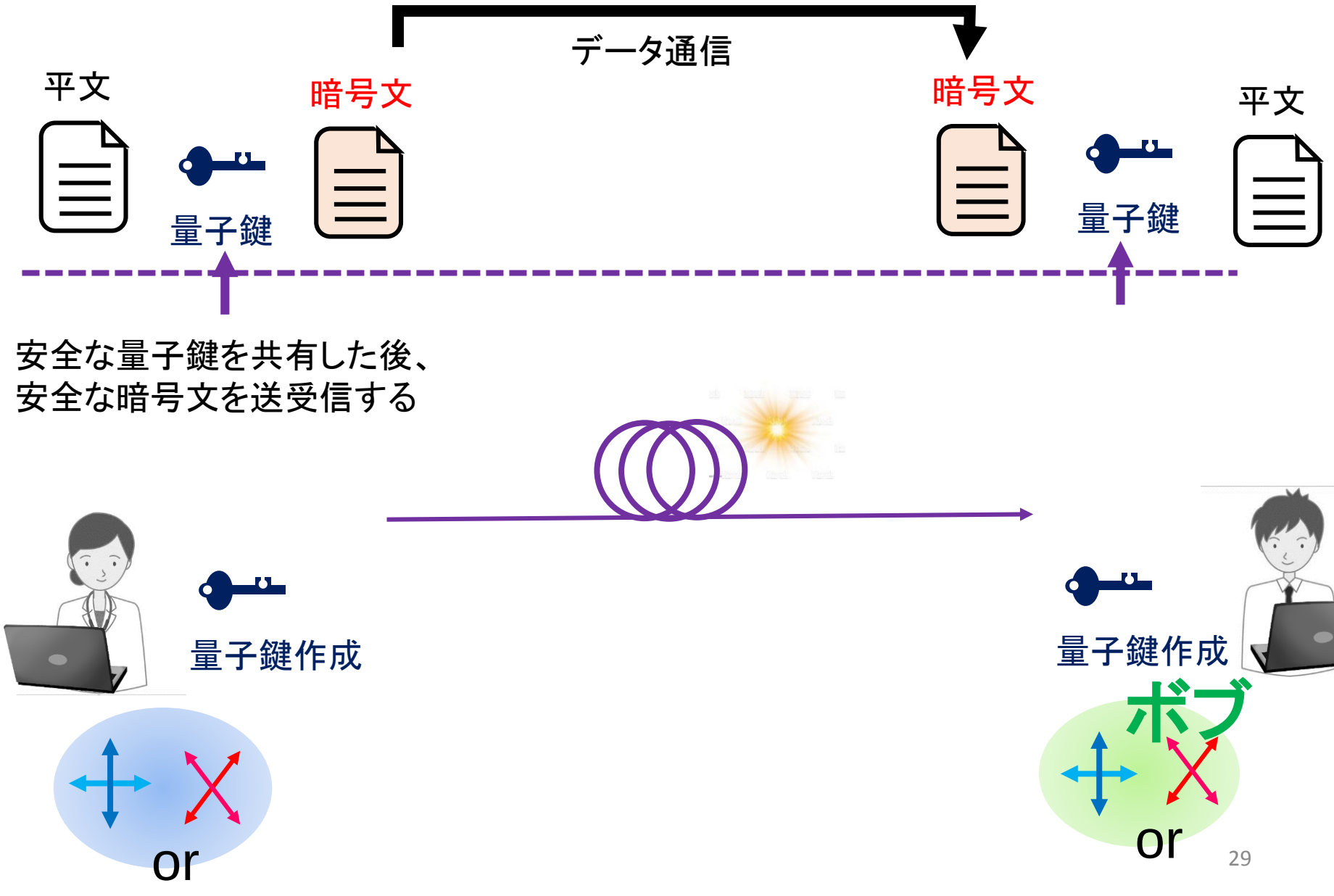
| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| ボブ基底 | ＋ | ＋ | ＋ | × | ＋ | × | × | ＋ | × | × | ＋ | × | ＋ | ＋ | × |
| ボブ観測偏光 | ↕ | ↔ | ↔ | ⤡ | ↕ | ⤡ | ⤢ | ↔ | ⤢ | ⤡ | ↕ | ⤡ | ↔ | ↔ | ⤡ |
| ボブの受信 bit | 0 | 1 | 1 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 1 | 1 | 1 |

←試しに選択
←観測
←復号結果

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 基底の確認 | — | ○ | — | — | ○ | ○ | ○ | — | — | ○ | — | — | ○ | — | ○ |
| | | 1 | | | 0 | 1 | 0 | | | 1 | | | 1 | | 1 |

暗号鍵の完成！

# 量子暗号BB84

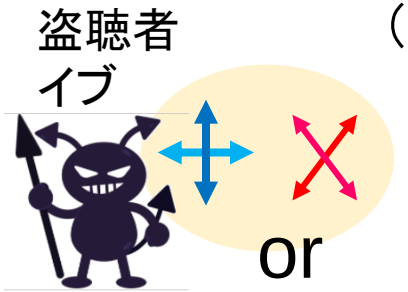

データ通信
平文
暗号文
暗号文
平文
量子鍵
量子鍵
安全な量子鍵を共有した後、
安全な暗号文を送受信する
量子鍵作成
量子鍵作成
ボブ
or
or

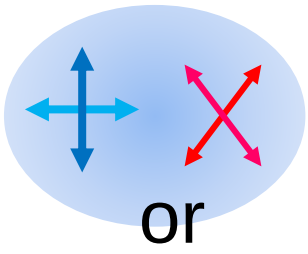
# 量子暗号BB84

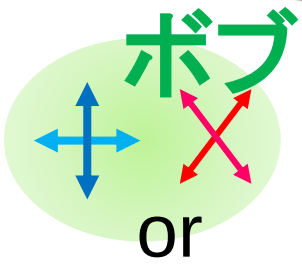
量子暗号、どこがいいの？？

盗聴者の存在が判定できる！！

・光子は分割できない！
・光子はコピーできない！
（非クローン定理）

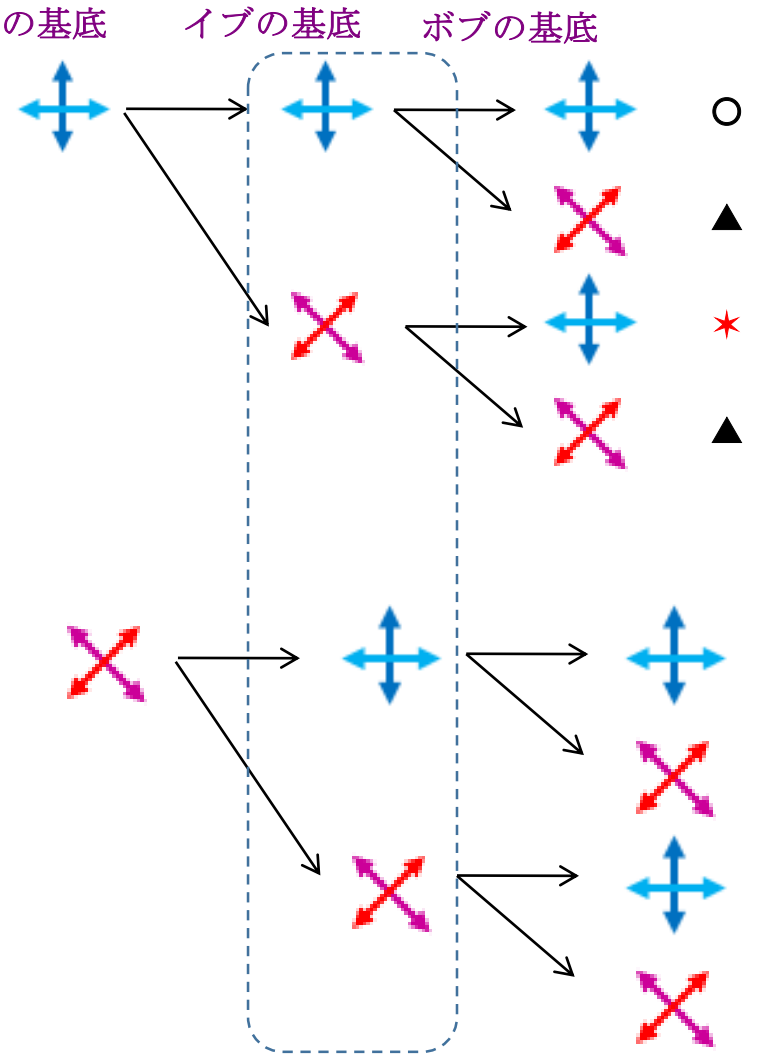


# 量子暗号BB84

アリスとイブとボブの基底の取り方による、送信bitの一致、不一致




bit 結果

○ 必ず一致

▲ 一致するとは限らない

✶ アリスとボブの基底が一致しているにもかかわらず、bit は一致するとは限らない

▲ 一致するとは限らない

▲ 一致するとは限らない

✶ アリスとボブの基底が一致しているにもかかわらず、bit は一致するとは限らない

▲ 一致するとは限らない

○ 必ず一致

盗聴者

# 盗聴者のいる場合

| | + | × |
|---|---|---|
| 0 | ↕ | ↗ |
| 1 | ↔ | ↘ |

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| アリスの送信 | 0 | 1 | 1 | 0 | 0 | 1 | 0 | 0 | 0 | 1 | 0 | 1 | 1 | 0 | 1 |
| アリス基底 | × | + | × | + | + | × | × | × | + | × | × | + | + | × | × |
| アリス偏光 | ↗ | ↔ | ↘ | ↕ | ↕ | ↘ | ↗ | ↗ | ↕ | ↘ | ↗ | ↔ | ↔ | ↗ | ↘ |

←情報
←自由に選択
←送信信号

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| イブの検出 | + | × | × | + | × | × | + | + | + | + | × | + | × | + | × |
| イブの結果 | ↕ | ↘ | ↘ | ↕ | ↗ | ↘ | ↔ | ↔ | ↕ | ↕ | ↗ | ↔ | ↘ | ↕ | ↘ |
| イブの基底 | + | × | × | + | × | × | + | + | + | + | × | + | × | + | × |
| イブの送信 | ↕ | ↘ | ↘ | ↕ | ↗ | ↘ | ↔ | ↔ | ↕ | ↕ | ↗ | ↔ | ↘ | ↕ | ↘ |

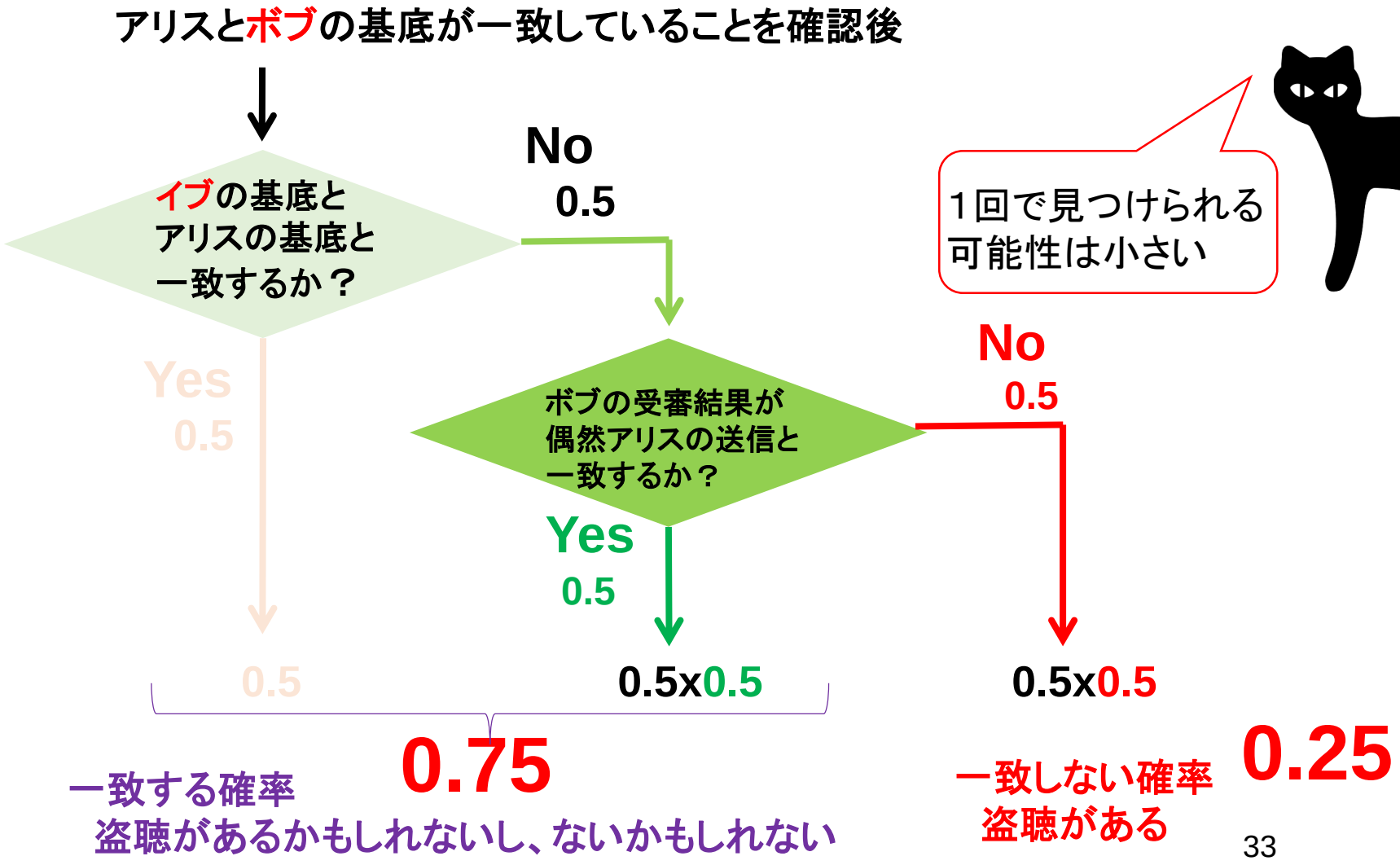
| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| ボブ基底 | + | + | + | × | + | × | × | + | + | × | + | × | + | + | × |
| ボブ観測偏光 | ↕ | ↕ | ↔ | ↘ | ↔ | ↘ | ↗ | ↔ | ↕ | ↘ | ↔ | ↘ | ↕ | ↕ | ↘ |
| ボブの受信bit | 0 | 0 | 1 | 1 | 1 | 1 | 0 | 1 | 0 | 1 | 1 | 1 | 0 | 0 | 1 |

←試しに選択
←観測
←復号結果

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 基底の確認 | — | ○ | — | — | ○ | ○ | ○ | — | — | ○ | — | — | ○ | — | ○ |
| | | 0 | | | 1 | 1 | 0 | | | 1 | | | 0 | | 1 |
| 盗聴の確認 | | ✔ | | | | ✔ | | | | ✔ | | | | | ✔ |
| | | No | | | No | Ok | Ok | | | Ok | | | No | | Ok |

# 盗聴が発見できる確率

アリスとボッブの基底が一致している場合に、
盗聴者がいるとき、1つのビットの照合が一致する確率　0．75

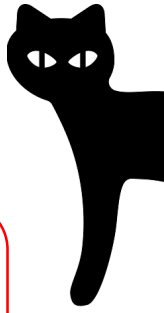


# 安全な量子暗号鍵

盗聴者がいるとき、1つのビットの照合が一致する確率　0．75
盗聴者がいるとき、2つのビットの照合が一致する確率　$(0.75)^2$

⋮

盗聴者がいるとき、n個の照合が一致する確率　$(0.75)^n$



盗聴を1回で見つけられる可能性は小さいけど繰り返せは大丈夫

盗聴が発見できる確率

$P(n)= 1-(0.75)^n \rightarrow 1$

例　n=52　P(52)=0.9999999

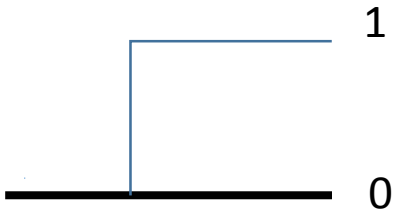
単一光子の偏光基底を操作することで、盗聴される可能性が限りなくゼロに近い状態で、暗号鍵の共有が可能となる。

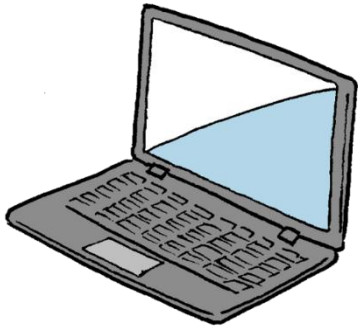
盗聴されない量子暗号鍵の完成

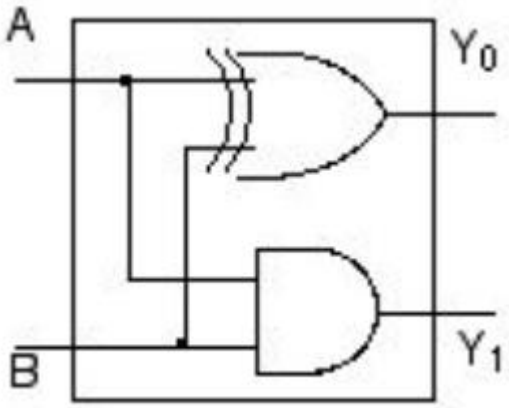
# 古典コンピュター　古典ビット

0+0=00
0+1=01
1+0=01
1+1=10

A　B　Y1 Y0






論理和

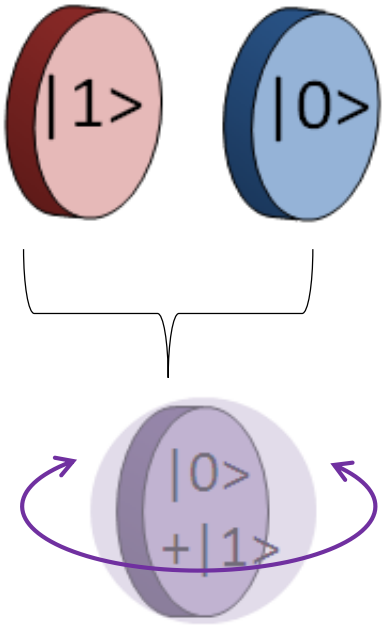

| A | B | Y |
|---|---|---|
| 0 | 0 | 0 |
| 0 | 1 | 0 |
| 1 | 0 | 0 |
| 1 | 1 | 1 |

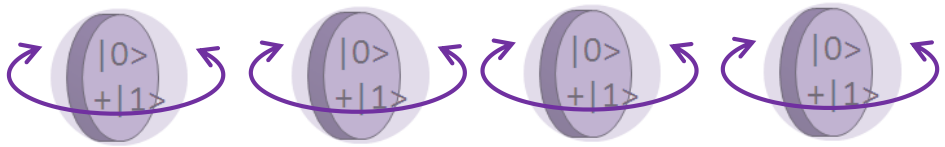
排他的論理和


| A | B | Y |
|---|---|---|
| 0 | 0 | 0 |
| 0 | 1 | 1 |
| 1 | 0 | 1 |
| 1 | 1 | 0 |

# 量子コンピュター　Ｑビット

superposition




1　　2=2
2　　2×2=4
3　　2×2×2=8
4　　2×2×2×2=16

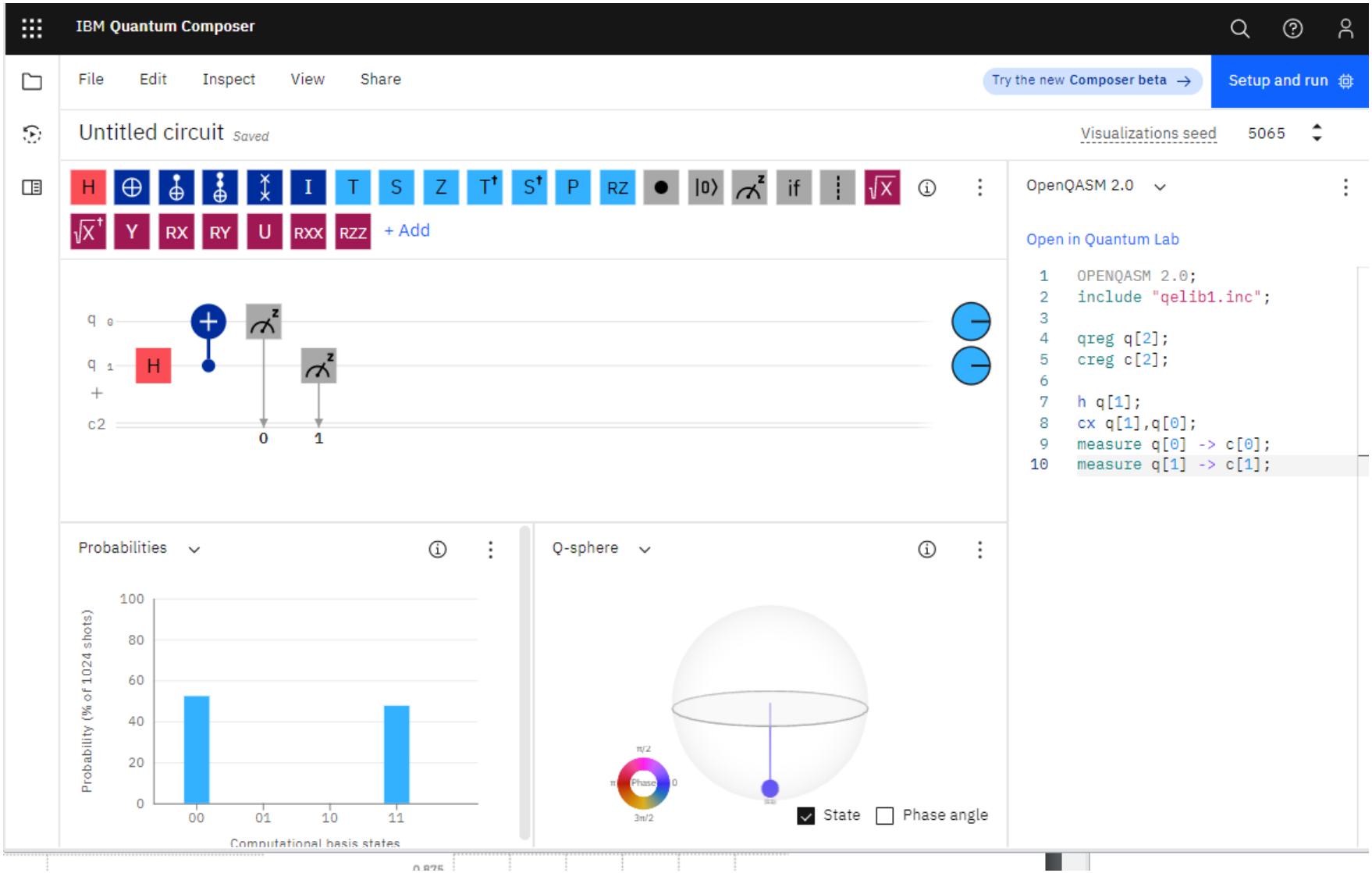
10　　$2^{10}$=1024
30　　$2^{30}$=1073741824
100　$2^{100}$=1267650600228229401496703205376

宇宙の原子の数　　$10^{80}$~$2^{256}$

$10^{100}$をあらわすgoogol

# IBM Q

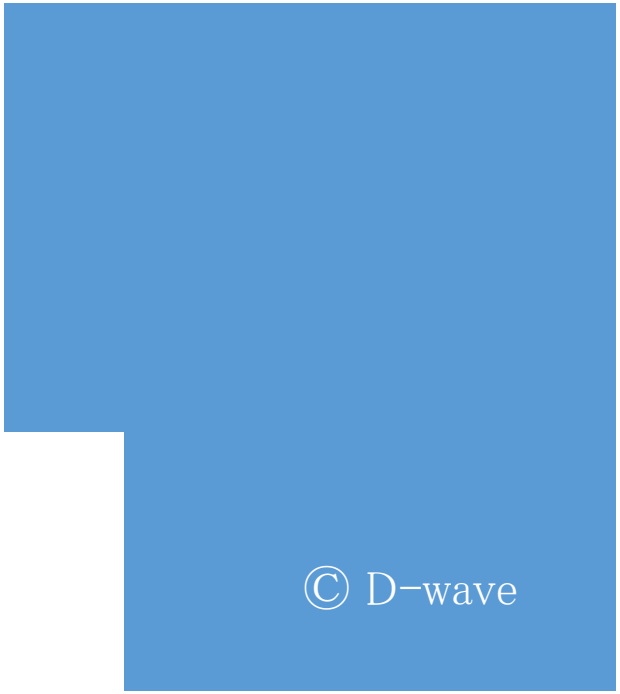
https://quantum-computing.ibm.com/composer/files/cdcebf3ef466e[redacted]267db6795157



# 量子コンピューターは市販されていた(2011年)

歴史

| | |
|---|---|
| 1980年代 | 量子コンピューターのアイデア(情報と物理) |
| ・ | |
| ・ | （マニアックな理論家） |
| ・ | |
| 1994 | ショアのアルゴリズム（素因数分解） |
| 2001 | 15=3x5 の素因素分解 |
| ・ | |
| ・ | （実現は？？の時代） |
| ・ | |
| 2011 | D-wave 128qbit (量子annealing) |
| 2012 | IBM 12qbit (量子gate) |
| 2019 | Google 量子超越 |
| 2021 | D-wave 5640qbit |




Geordie Rose
ブラジル柔道 世界チャンピョン ブリティッシュコロンビア大学Ph.D

# 量子コンピュターD－waveの歴史

発表

2007年2月13日　D-Wave発表
2011年5月11日　D-Wave One発売「世界初の商用量子コンピュータ」
2011年5月25日　ロッキード・マーティン購入

論争

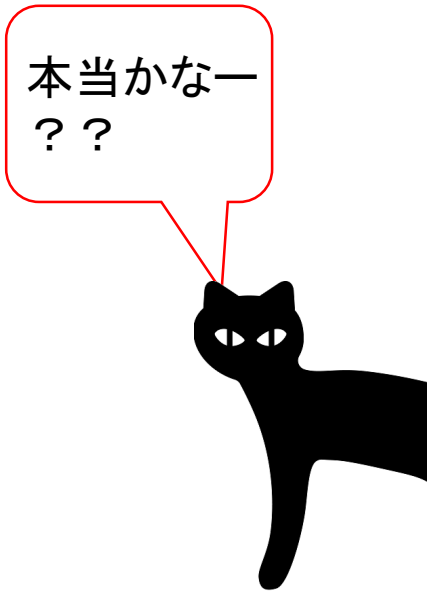
2007年　U Vazirani（カリフォルニア大学：量子計算量理論の創始者）
“古典的コンピュータより高速になることはない”

2007年　S Aaronson（MIT）自称「主任D-Wave懐疑論者」
“コンピュータの働きに関して何も証明していない”

2008年　Wim van Dam（カリフォルニア大学）
“D-Waveが量子コンピュータかをいうことは不可能”

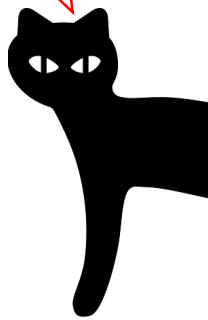
発展

2011年5月　Aaronson「主任D-Wave懐疑論者を退く」
2013年3月　D-Wave　量子もつれの証拠
2015年9月28日　Google、NASA、USRA　D-Wave購入



# 重なり合う量子の世界

・基礎科学は世界観をかたちつくる。
・基礎科学は先端技術を切り開く



## 「存在とはなにか」～
## 量子コンピュターまで

内容

１．重なり合う量子（which path experiment）
２．実在とは？
　　隠された変数理論とベルの不等式

３．暗号：古典暗号と量子暗号
４．量子コンピュター

まとめ

**ご清聴ありがとうございました**