
量子情報とエントロピー
21/09/04 マルレク

What is information? The question has received many answers in different fields. Unsurprisingly, several surveys do not even converge on a single, unified definition of information.

Information is notoriously a polymorphic phenomenon and a polysemantic concept ….

--- Stanford Encyclopedia of Philosophy

The word 'information' has been given different meanings by various writers in the general field of information theory.

It is hardly to be expected that a single concept of information would satisfactorily account for the numerous possible applications of this general field.

--- Shannon 1993

In seeking tales and Informations
Against this man, whose honesty the devil at

--- Shakespeare Henry VIII

I propose to consider the question, "Can machines think?"

....

The original question, "Can machines think?" I believe to be too meaningless to deserve discussion. Nevertheless I believe that at the end of the century the use of words and general educated opinion will have altered so much that one will be able to speak of machines thinking without expecting to be contradicted.

-- Alan Turing

はじめに

「物質の世界」と「情報の世界」

はじめに
「物質の世界」と「情報の世界」

はじめに

私たちは、日常的に「情報」という言葉を使っています。

英語の”information” という言葉は古いものですが、その翻訳としての「情報」という言葉が日本に生まれ、現在のような意味で使われ始めたのは、1954年以降だといいますので、日本語としては、とても新しい言葉です。

「情報」という言葉が日常語になったのは、いうまでもなく、情報技術が、我々の生活の至る所に浸透したからです。技術が日常の生活を変え、日常の言葉遣いを変えました。

はじめに

一方で、少なくない哲学者や情報理論の創始者のシャノンでさえも、「情報」に、ユニークな定義を与えることは難しいと考えているようです。

それは、情報概念の「古さ＝普遍性」と情報技術の「新しさ＝多様性」の反映なのかもしれません。

ただ、哲学的にしろ情報理論的にしろ、情報の世界それのみを単独の対象として捉えるのではなく、情報の世界と物質の世界の両者の関係を考えて見たほうがいいと筆者は考えています。

はじめに

「情報の世界と物質の世界」という一見すると対立する二項を立てることで、関連する問題領域は大きく広がります。

「物質の世界と情報の世界」の問題群

セミナー冒頭で、情報に対する「哲学的」アプローチに、少し疑問を示したのですが、「物質の世界と情報の世界」の関係という視点で振り返ると、少なくない「哲学的」問題が、この視点の射程に入ることに気づきます。

ただ、もっとも、真剣に考えるべきことはそうした「哲学的」問題ではありません。重要なことは、現代の科学と技術が生み出した様々な問題の理解に、こうした構造の存在の認識が、極めて有効だということです。以下、いくつかの例をあげたいと思います。


イデア
質量と形相
ヒューレーとエイドス
身体と心
「物質の世界」と「情報の世界」の
哲学バージョン
プラトン
アリストテレス
デカルト

「物質の世界と情報の世界」の問題群

質量と形相
ヒューレーとエイドス
MatterとForm

身体と心
BodyとMind

物質の世界と情報の世界

人工知能
機械と思考

量子コンピュータ
自然とそのシミレーション

生命現象
代謝過程と情報過程

計算可能性
物質過程と情報過程

自然科学と数学

二時間のセミナーで取り上げるのは、
すこし、トピックスが広すぎます。

このセミナーでは、
情報の世界は物質の世界とが
密接に繋がっていることを示すもの
として、エントロピーと量子情報に
注目しています。

なぜ、「エントロピー」が重要なのか

20世紀は、科学・技術が飛躍的に発展した時代でした。特筆すべきは、20世紀前半の量子論・相対論の成立を画期とした科学的自然認識の拡大と、20世紀後半のコンピュータ・通信技術の成立・発展による、技術的情報世界の拡大です。

自然科学が対象とする「物質の世界」と、IT技術が対象にする「情報の世界」は、異なる世界のように見えます。ただ、21世紀の科学・技術は、この二つの世界の交差するところで発展するだろうと、丸山は考えています。

物質の世界と情報の世界という二つの世界を結びつける、重要な概念が「エントロピー」です。

なぜ、「量子情報」なのか

今回のセミナーで伝えたかったことの一つは、「量子の世界」に飛び込んだ時、「物質の世界」と「情報の世界」のつながりが、より一層明確に見え始めるということです。

こうした現象は、20世紀後半から21世紀初頭にかけて、科学・技術の非常に広い分野で確認できることです。

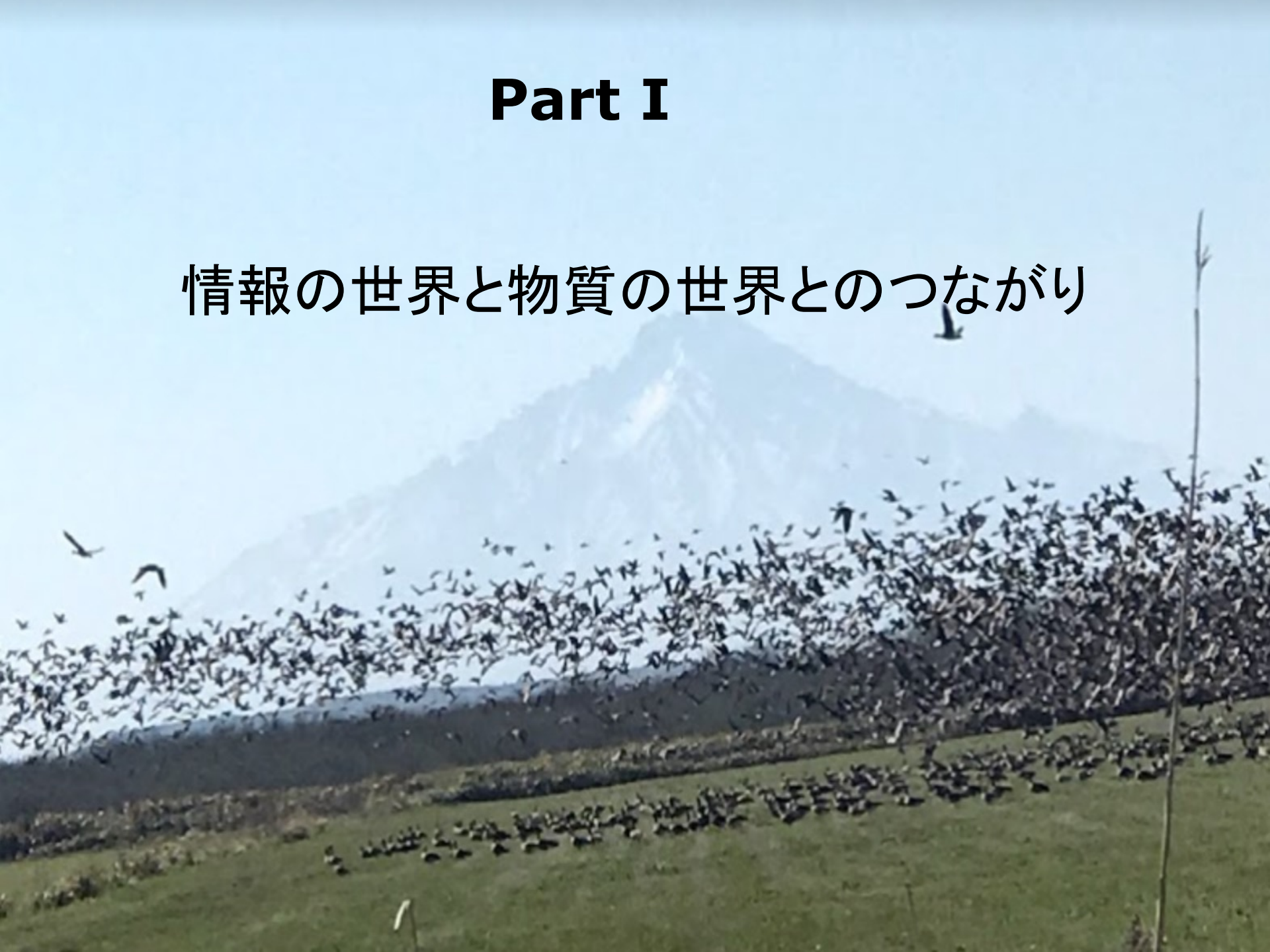
このセミナーの第一部では、
20世紀の後半に明らかになった
情報の世界は物質の世界とが
密接に繋がっていることを示す
次のようなエピソード達を
紹介しようと思います。

情報の世界は物質の世界と
密接に繋がっていることを示すエピソード達

- エントロピーの再発見
  1950年代-- シャノンの情報理論
- なぜ、コンピュータは電力を消費し、熱くなるのか
  1960年代-- ランダウアーの原理
- エントロピー概念の三つ目の起源
  1970年代--エントロピーとコルモゴロフ複雑性との接点
- 情報過程は物質過程である
  1980年代-- Church-Turing-Deutsch Principle

Part I

情報の世界と物質の世界とのつながり



Agenda　量子情報とエントロピー

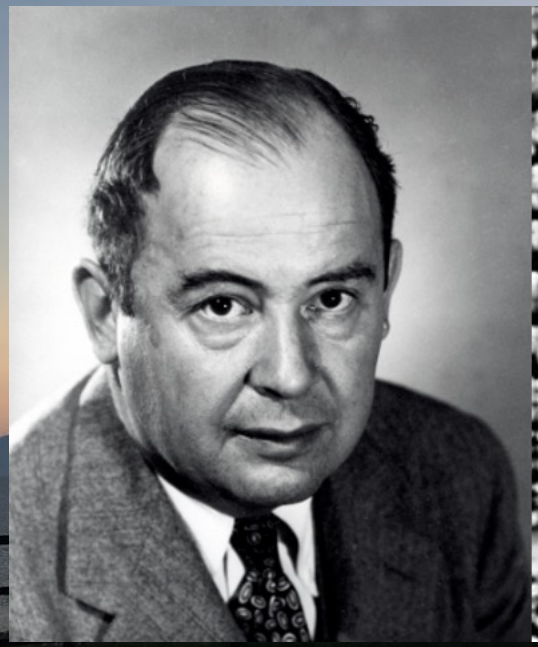
はじめに

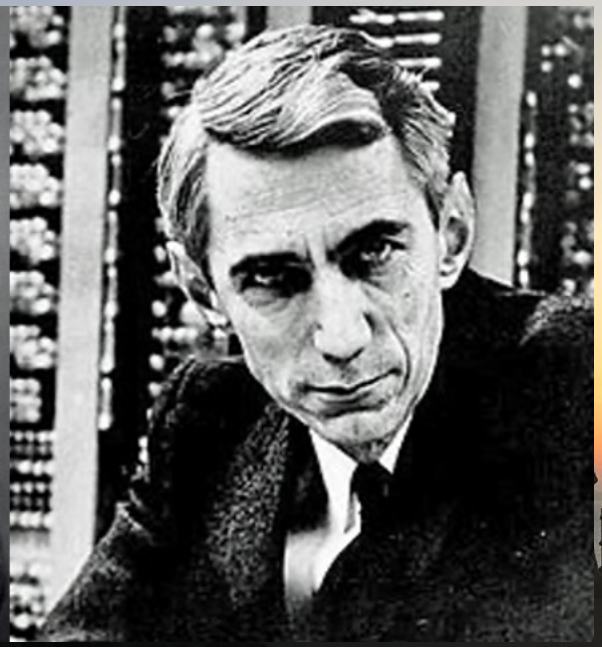
- 「物質の世界」と「情報の世界」
- なぜエントロピーと量子情報が重要なのか

第一部　情報の世界と物質の世界とのつながり

- エントロピーの再発見
  1950年代-- シャノンの情報理論
- なぜ、コンピュータは電力を消費し、熱くなるのか
  1960年代-- ランダウアーの原理
- エントロピー概念の三つ目の起源
  1970年代--エントロピーとコルモゴロフ複雑性との接点
- 情報過程は物質過程である
  1980年代-- Church-Turing-Deutsch Principle

エントロピーの再発見
-- シャノンの情報理論 --





1930年代

1950年代

エントロピーの理論史

熱力学的エントロピー
- カルノー
- クラシウス

統計力学的エントロピー
- ボルツマン
- ギブス

情報理論的エントロピー
- フォン・ノイマン
- シャノン

量子情報理論のエントロピー

エントロピーの理論史

熱力学的エントロピー

- カルノー
- クラシウス

統計力学的エントロピー

- ボルツマン
- ギブス

情報理論的エントロピー

- フォン・ノイマン
- シャノン

量子情報理論のエントロピー

統計力学的エントロピーから
情報理論的エントロピーへ

エントロピーの理論史

熱力学的エントロピー

カルノー

クラシウス

統計力学的エントロピー

ボルツマン

ギブス

情報理論的エントロピー

フォン・ノイマン

シャノン

量子情報理論のエントロピー

統計力学的エントロピーから
情報理論的エントロピーへ

エントロピーの再発見

エントロピー概念の二つの起源

エントロピーという概念は熱力学の中で発見され、ボルツマン、ギブスらの研究の中で、熱力学的・統計力学的概念として理論的に定式化された。

こうした研究の系譜とは全く独立に、シャノンは、自ら作り上げた情報理論の中で、エントロピー概念を再発見する。（シャノンに「エントロピー」という言葉を使うように勧めたのは、フォン・ノイマンだと言われている。）

エントロピー概念には、歴史的には、熱力学と情報理論の二つの起源がある。

ボルツマンとシャノンのエントロピーの比較

$$\frac{N!}{(p_1N)!(p_2N)!\cdots(p_\ell N)!}$$

ボルツマン

- ガス
- 異なるミクロな状態を数え上げる
- N:ミクロな粒子の数
- $\{n_1,\cdots,n_l\}$:l-cellへの分布
- $\{p_1,\cdots,p_l\}$:cell上の確率分布
- $p_i=n_i/N$=ミクロな状態がcellにある確率
- p_iN: cell内のミクロ状態の数

シャノン

- メッセージ
- 異なるメッセージを数え上げる
- N:メッセージの文字数
- $\{a_1,\cdots,a_l\}$:l文字のアルファベット
- $\{p_1,\cdots,p_l\}$:文字の確率分布
- $p_i=n_i/N$: a_iがメッセージにある確率
- p_iN: メッセージ内のa_iの数

$$S_B(\Gamma_{D_i}) = -Nk\sum_{j=1}^{\ell} p_j \ln p_j$$

$$H(X) = -\sum_{j=1}^{\ell} p_j \log_2 p_j$$

エントロピーの「再発見」の意味すること

情報理論の「情報」は、
物理的な熱力学の「エントロピー」と
同じ数学的形式を持つ。

情報は、物理的なエントロピーと共通な構造を持つ

フォン・ノイマンによるエントロピーの定式化

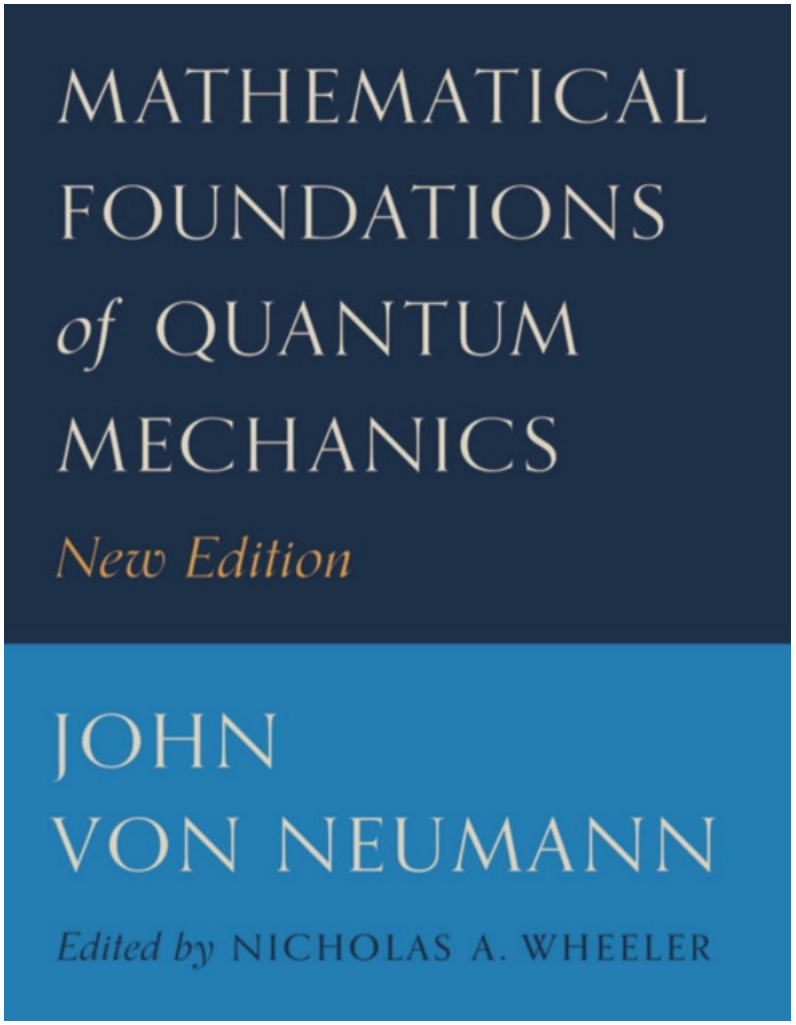
エントロピーの量子論的定式化を行ったのは、フォン・ノイマンである。もちろん、シャノンの登場のはるか以前である。驚くほどの慧眼である。

すでに、1932年の「量子力学の数学的基礎」の中で、次のようなエントロピーの定式化を与えている。

$$S = - Tr (\rho \log \rho)$$

ここで、ρ は密度行列、Trは行列のTrace（対角要素の和をとったもの）である。この式の説明は、別の機会にゆずるが、ギブスの与えた密度関数 ρ を用いたエントロピーの式と、基本的には同じ形をしている。（ΣもTrも、和をとる演算である）

$$S = - \Sigma (\rho \log \rho)$$



CONTENTS

フォン・ノイマンのもう一つの「貢献」

エントロピーの歴史の中で、フォン・ノイマンは、エントロピーの量子化だけでなく、もう一つの重要な「貢献」をしている。

1940年、それまでの熱力学的エントロピー概念の系譜とは全く独立にシャノンが発見した「不確実さの関数」＝「情報量」の概念に、「エントロピー」という名前をつけることを勧めたのは、フォン・ノイマンだと言われている。
http://www.eoht.info/page/Neumann-Shannon%20anecdote

Wikipedia の “Talk:History of entropy” にも、詳しい記事がある。
https://en.wikipedia.org/wiki/Talk%3AHistory_of_entropy

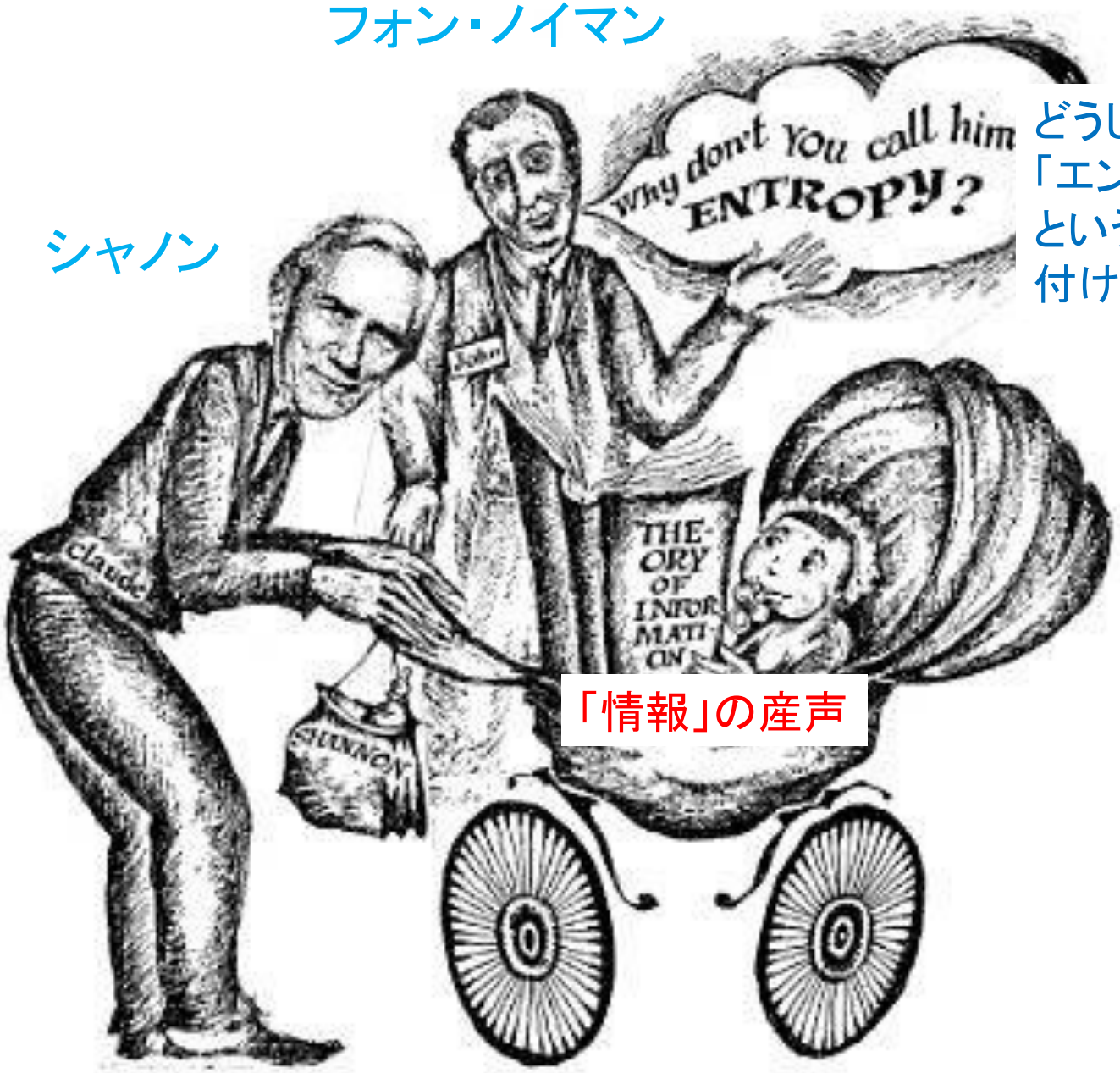
フォン・ノイマンのもう一つの「貢献」

“You should call it ‘entropy’ for two reasons:
First, the function is already used
in thermodynamics under that name;

second, and more importantly, most people don’t know what entropy really is, and if you use the word ‘entropy’ in an argument you will win ever time.”

“nobody really knows what entropy is anyway.”
「どうせ誰もエントロピーがどんなものかわかっていないんだから」

フォン・ノイマン



シャノン

どうして彼に「エントロピー」という名前を付けないんだ？

「情報」の産声

フォン・ノイマン

どうせ誰も「エントロピー」がどんなものかわかっていないんだから

シャノン

フォン・ノイマン

「エントロピー」という
言葉を使えば、いつだって
議論に勝てるだろう。

シャノン

なぜ、コンピュータは
電力を消費し、熱くなるのか？
ランダウアーの原理

Pioneering Efficiency

1 bitの情報を消去するには、エネルギーが必要である

コンピュータが情報の 1bitを消去すると、最低でも

$$k_B T \ln 2$$

のエネルギーを環境に放出する。

ここで、k_Bはボルツマン定数、Tは環境の温度である。

これを、「ランダウアーの原理」と呼ぶ。

「ランダウアーの原理」を
エントロピーの言葉で語る

コンピュータが情報の 1bitを消去すると、
環境のエントロピーは、最低でも
$k_B T \ln 2$ 増大する

「ランダウアーの原理」が意味すること

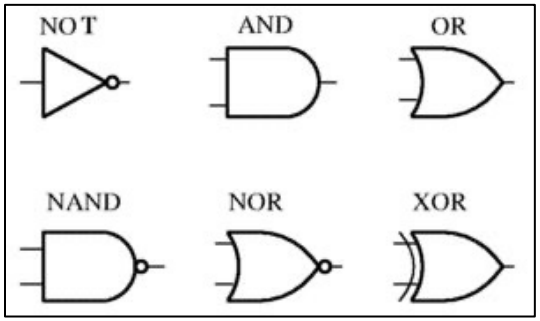
コンピュータの「情報」は、「物理的」な法則に従う。

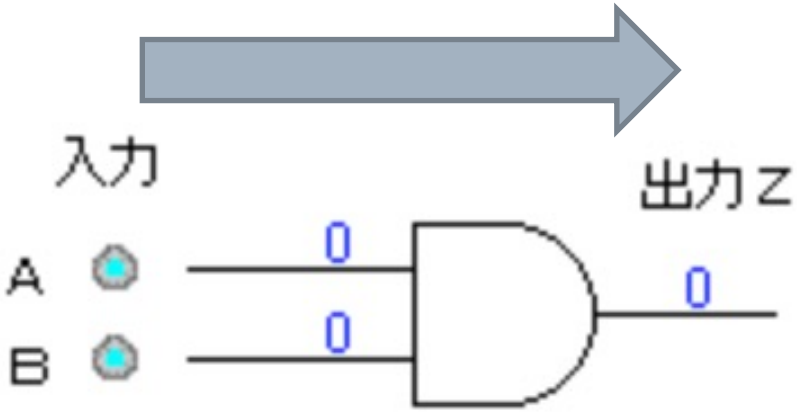
情報は、物理的である。

「1bitの情報の消失」？
演算の「非可逆性」

コンピューターを構成する、基本的な論理ゲートでは、時間に関して「非可逆」な演算が行われ、演算のステップごとに、情報の消失が起きている。

基本的な論理ゲート

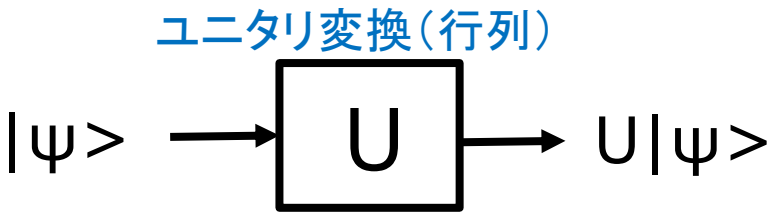




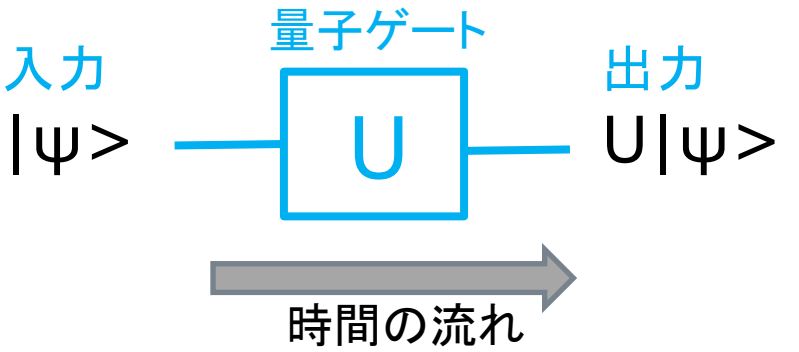
入力 A,B から出力Z を決定することはできるが、
出力Z から入力A,B を求めることはできない。
A またはBの情報は、失われている。

量子ゲートは「可逆的」である

- 量子の状態 $|\psi\rangle$は、ユニタリ変換U（ユニタリ行列）の作用を受けて、状態 $U|\psi\rangle$ に変化する。
- この変化 $|\psi\rangle \rightarrow U|\psi\rangle$を、次のように表そう。



- この時、Uを、$|\psi\rangle$ を入力、$U|\psi\rangle$ を出力とする回路と考えることができる。これを、「量子ゲート」と呼ぶ。

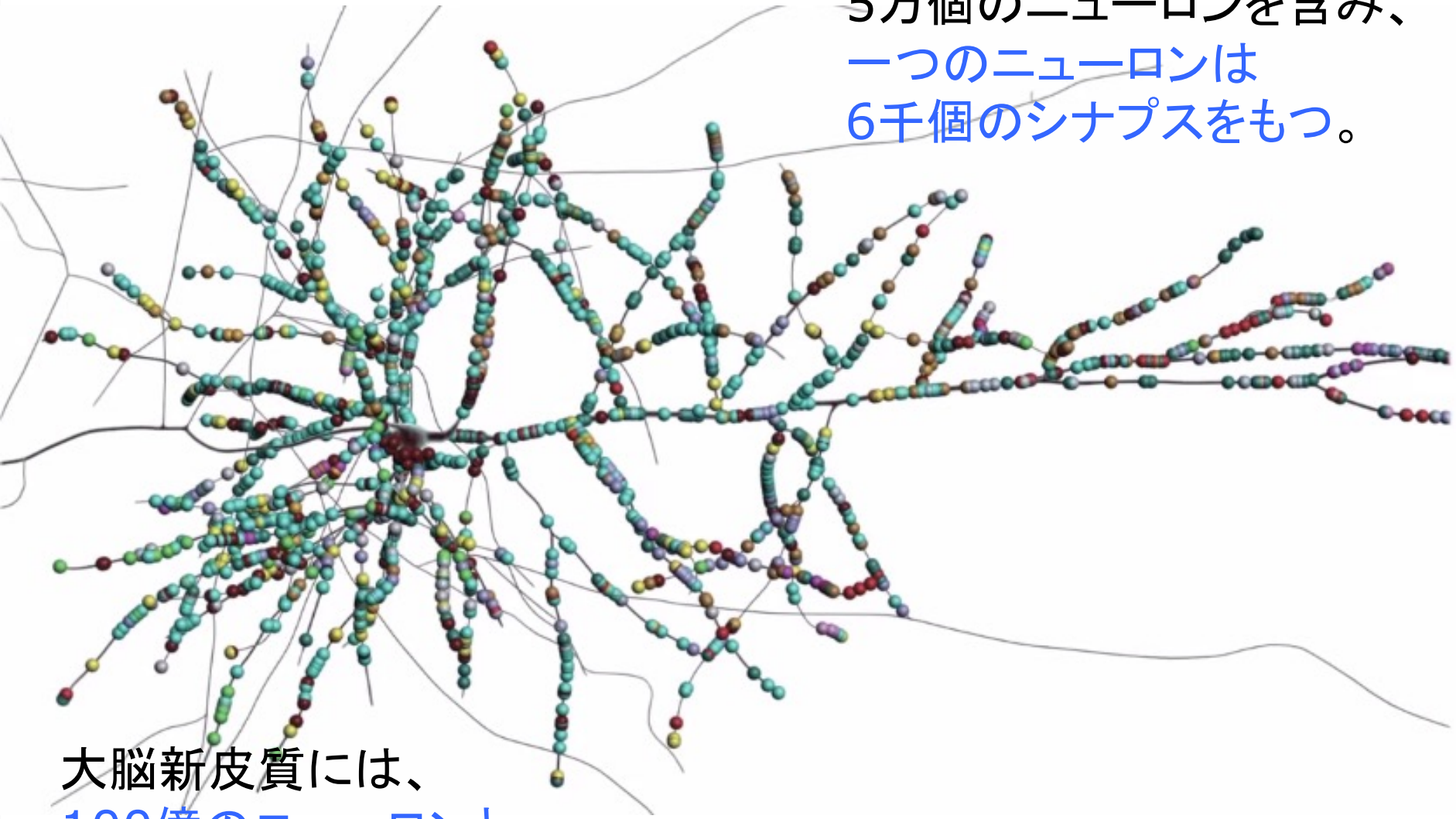


量子ゲートは
ユニタリ行列と
一対一に対応する

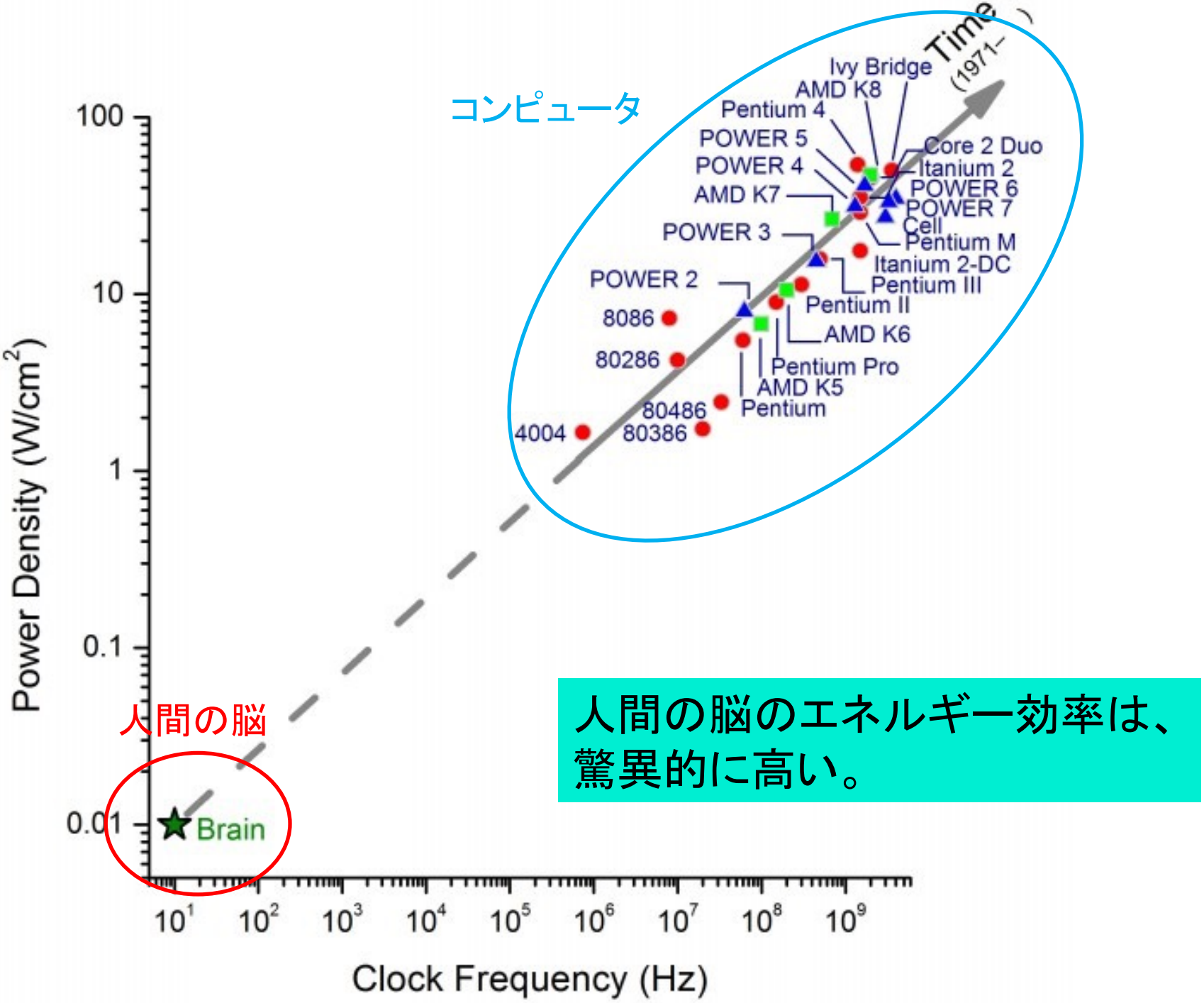
量子ゲートは
可逆的である

補足

脳は、1mm立方に
5万個のニューロンを含み、
一つのニューロンは
6千個のシナプスをもつ。



大脳新皮質には、
100億のニューロンと
60兆個のシナプスがある！



人間の脳のエネルギー効率は、驚異的に高い。

エントロピー概念の三つ目の起源
エントロピーとコルモゴロフ複雑性との接点

1970年代

Andrey Kolmogorov

Gregory Chaitin

コルモゴロフの複雑性

ある対象の「コルモゴロフの複雑性」と言うのは、その対象を出力する「最も短いプログラム」の「大きさ」のことである。

ある対象を出力する、同じ機能を持つ多数のプログラムがあったとしても、そのプログラム・サイズからなる自然数の全体の集まりを考えれば、その中に、最小の自然数が、一つは存在するはずである。

重要なことは、具体的にその数字を示すことができなくとも、また具体的にそのプログラムを示すことができなくとも、最小のプログラム・サイズが存在するのは確かであると言うことである。

チャイティンの不完全性定理

「コルモゴロフの複雑性」が奇妙な性質を持つことを、驚くような形でまとめたのは、チャイティン(G. J. Chaitin)である。

「どのような特定のビット列をとっても、そのコルモゴロフの複雑性が L 以上であることを証明できないような数 L が存在する。」

これを「チャイティンの不完全性定理」という。

チャイティンは、こういう言い方もしている。

「あるプログラムを、それより小さいサイズのプログラムが同じ出力を行うことがない時、"エレガント"と呼ぶことにしよう。

あるプログラムが "エレガント" であることを、我々は証明できない。」

シャノンの情報理論と
コルモゴロフの複雑性理論

シャノンの情報理論

シャノンの理論は、複数のオブジェクトの集まりをどのようにエンコードし、そうしたオブジェクトのシークエンスを如何に効率的に送るかについて関心を持っている。

例えば、アルファベットの集まりXがある確率分布に従う時、そのエントロピーH(X)を用いて、N文字のメッセージを。NH(X)ビットに情報圧縮できることを示せる。

コルモゴロフの複雑性理論

コルモゴロフの複雑性理論は、一つのオブジェクトを、最も効率的にエンコードすることを考える。

「ランダムさ」を定義する

あるオブジェクトが、それより短い記述を持たない時、そのオブジェクトを「圧縮不可能」という。

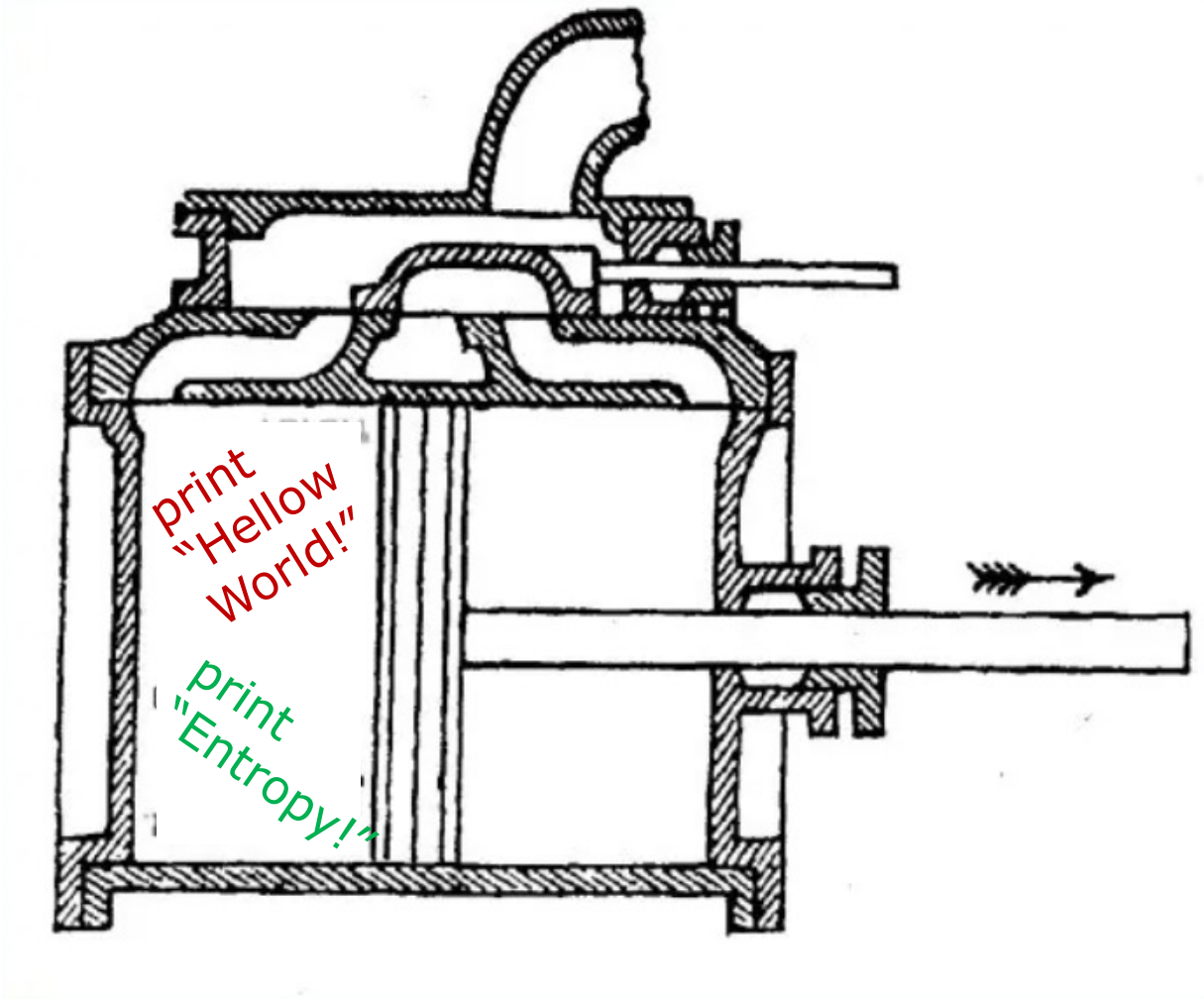
あるビット列が「ランダム」だと判断されるのは、それが「圧縮不可能」な時である。

Per Martin-Lof　1966年
“The Definition of Random Sequences”

Charles Bennet 1979年

“On Random and Hard-to-Describe Numbers”

バエズの「アルゴリズム論的熱力学」



熱力学とプログラムとの対応の例

熱力学	アルゴリズム論的熱力学
E:容器中のガスのエネルギー	プログラムの実行時間の対数の期待値
V:容器の体積	プログラムの長さの期待値
N:容器中のガスの分子の数	プログラムの出力の期待値

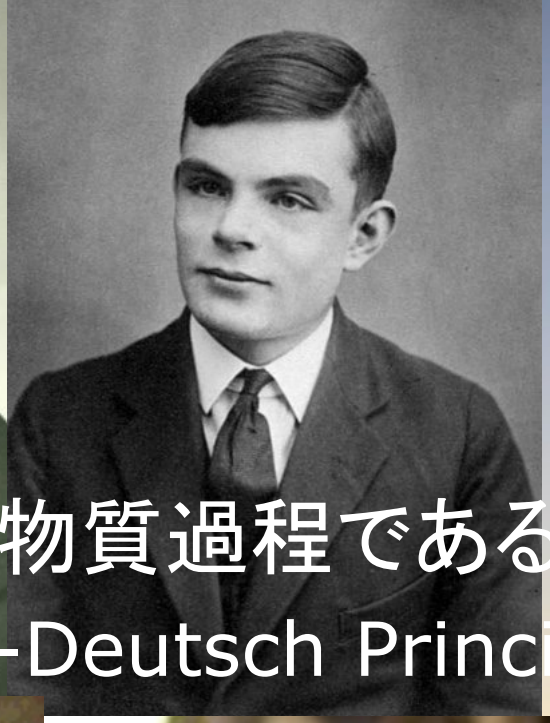
「ランダムさ」の認識
アルゴリズム論的熱力学

計算不可能性は、

「ランダムさ」と結びついている

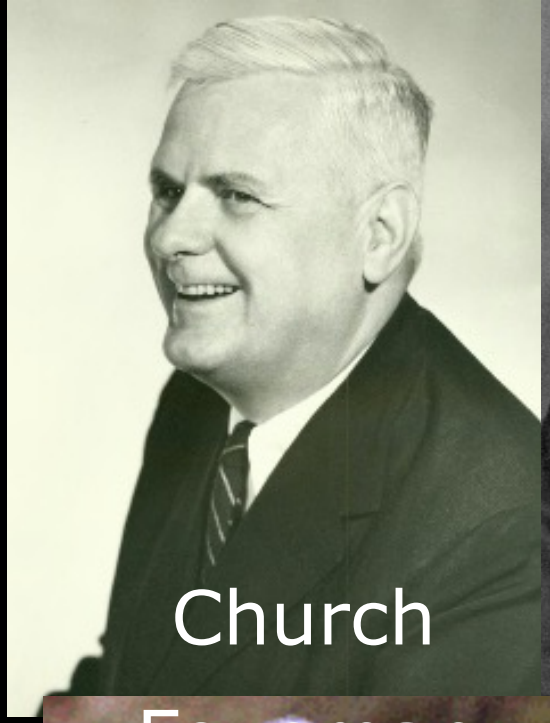
-- チャイティンのΩ --

熱力学とプログラムは対応している

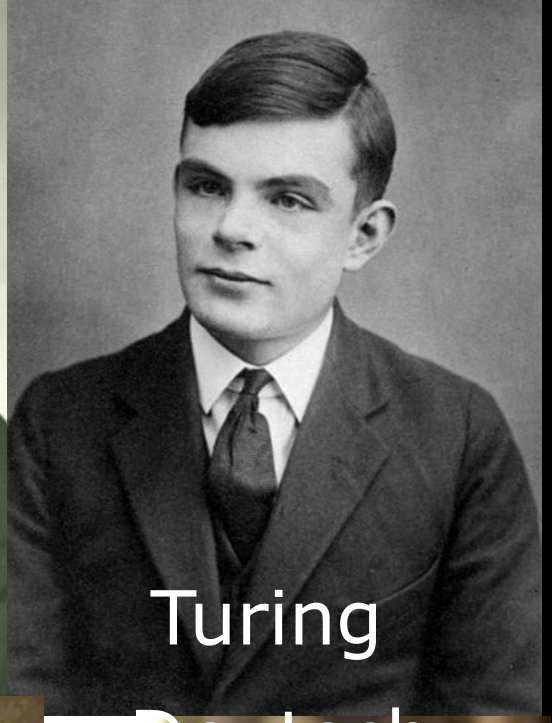



情報過程は物質過程である
Church-Turing-Deutsch Principle


1980年代

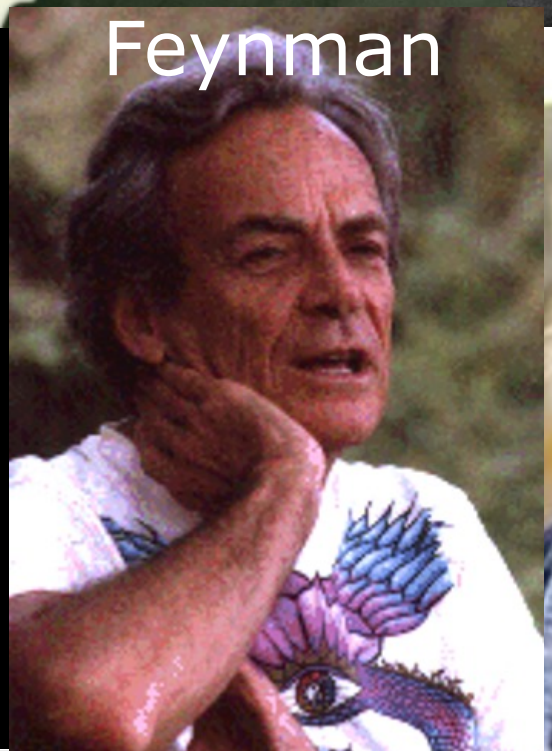


Church



Turing

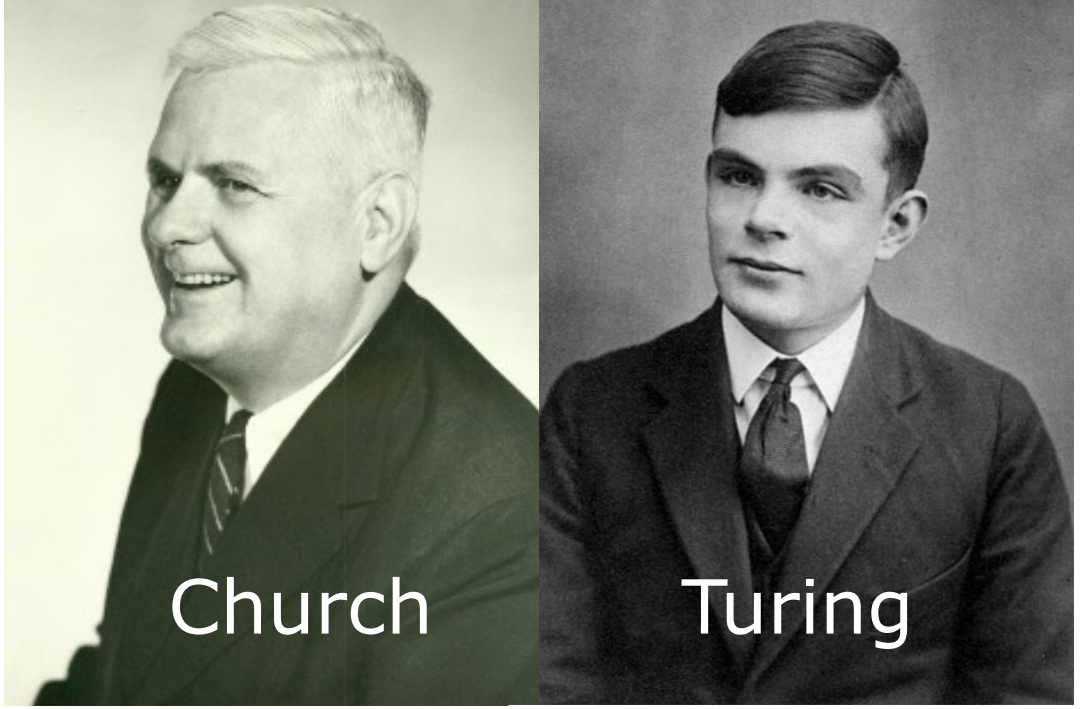
1940年代



Feynman

Deutsch

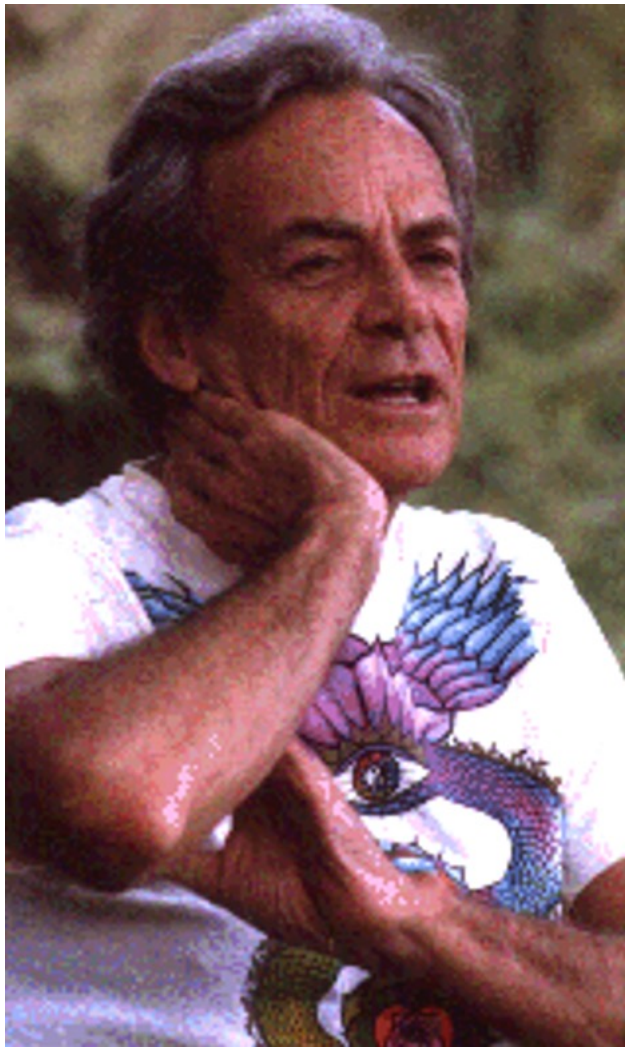
1980年代



Church-Turingのテーゼ

「計算可能と自然に見なされる関数は、全て、万能テューリング・マシンで計算可能である。」

量子コンピュータ
自然をシミレートするコンピュータ



量子論的なシステムは、古典的な万能計算機で、確率論的にシミュレートされるだろうか？

答えは明らかにノーである。

それは、新しいタイプのコンピューター、量子コンピューターで可能になるだろう。

それはチューリング・マシンではない。別のタイプのマシンである。

万能量子チューリングマシン
Church-Turing-Deutsch Principle

Church-Turingの仮説の基礎には、暗黙の物理学的主張があるとドイッチェは考える。彼は、チューリングマシンの量子版を構成し、次のようにChurch-Turingのテーゼを書き換える。

「有限な方法で実現可能な物理システムは、有限な手段によって操作される万能計算機械のモデルで完全にシミュレート可能である。」

万能量子チューリングマシン
Church-Turing-Deutsch Principle

この万能量子Turingマシンによって実行できない計算は、物理的システムでは実行できない

ということになるのだが、この命題は物理的な法則の限界として計算可能性について語っている。

量子Turingマシンによって実行できない計算は物理法則を破らない限り実行できない

「計算過程」＝「物理過程」＝「情報過程」

形式的・数学的で抽象的な「計算可能性」の原理だった「チャーチ＝チューリングのテーゼ」は、ここに「チャーチ＝チューリング＝ドイッチェのテーゼ」として、実在的な過程としての「計算」の原理として「物理化」されることになる。

「計算可能性」の原理の「物理化」は、関連する諸科学に、一つのインパクトをもたらすことになる。なぜなら、それは、それまで別々の学問の対象だった「計算過程」「物理過程」「情報過程」（それぞれ、数学・物理学・コンピュータ科学が扱っていた）に対して、「計算過程」＝「物理過程」＝「情報過程」という、強力な三位一体の図式が、しかも、物理学の優位の元に生まれたことを意味することになるからである。

Church-Turing-Deutsch Principleの意味するところ

数学　　物理学　　情報科学

「計算過程」＝「物理過程」＝「情報過程」

Part II

量子情報技術の応用の展望

セミナー後半の問題意識

謎に満ちたエントロピーの探究は、現在も活発に続けられています。

21/03/27 マルレク 「エンタングルする自然」

21/04/10 マルゼミ 「エンタングルする認識」

ただ、日常の意識に深く広い影響を与えるのは、科学ではなく技術かもしれません。そうした観点から、小論の第二部は、量子技術の応用の展望のオーバービューを与えたいと思います。小論の第三部では、量子技術の重要な応用として、「量子暗号」技術を、すこし具体的に紹介します。

Agenda　量子情報とエントロピー

第二部　量子情報技術の応用の展望

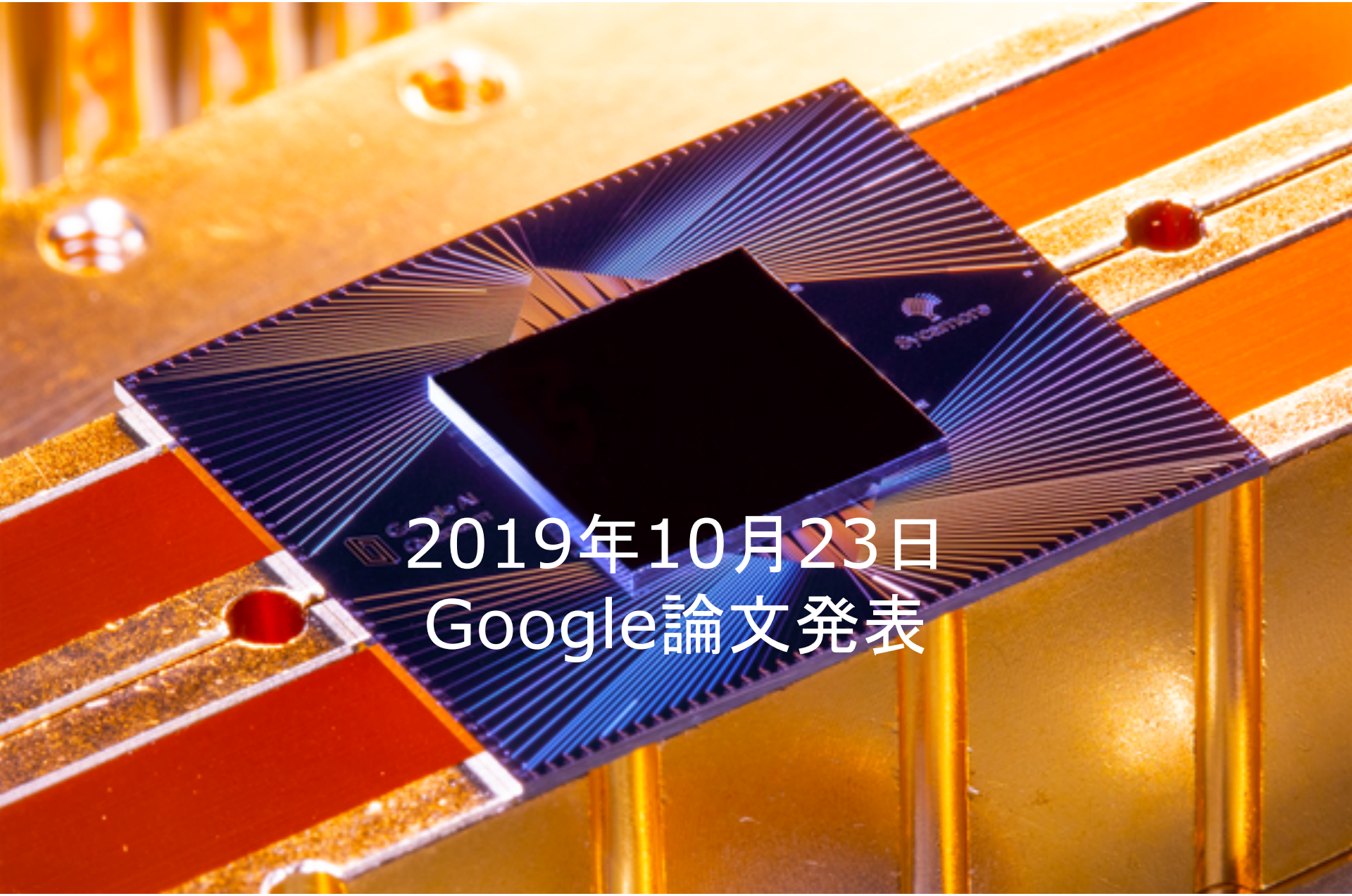
- 量子コンピュータの到達点 – 量子優越性の実証
- 量子コンピュータと量子通信
- 量子通信の世界

第三部　たとえ話で理解する「量子暗号」

- コイントスで量子暗号をシミレートする
- 共有キーの構成
- コインからqubitへ

量子コンピュータの到達点

-- 量子優越性のマイルストーンの達成 --


2019年10月23日
Google論文発表

Article | Published: 23 October 2019

Quantum supremacy using a programmable superconducting processor

Frank Arute, Kunal Arya, [...] John M. Martinis

Nature **574**, 505–510(2019) | Cite this article

Abstract

The promise of quantum computers is that certain computational tasks might be executed exponentially faster on a quantum processor than on a classical processor[1]. A fundamental challenge is to build a high-fidelity processor capable of running quantum algorithms in an exponentially large computational space. Here we report the use of a processor with programmable superconducting qubits[2,3,4,5,6,7] to create quantum states on 53 qubits, corresponding to a computational state-space of

2019年10月23日
Natureに論文発表

circuit a million times—our benchmarks currently indicate that the equivalent task for a state-of-the-art classical supercomputer would take approximately 10,000 years. This dramatic increase in speed compared to all known classical algorithms is an experimental realization of quantum supremacy[8,9,10,11,12,13,14] for this specific computational task, heralding a much-anticipated computing paradigm.

ビットコイン価格が10月23日夜、急落し、1BTCあたり80万円に迫った。このところ80万円後半で推移していたが、一気に10%ほど下落した。これは、5カ月前の5月に80万円を割り込んだ時以来だ。

過去1日の円建てビットコイン価格の推移（=bitFlyer）

このあたりの議論は、以前のマルレク「暗号技術の現在 ― ポスト量子暗号への移行と量子暗号」を参照されたい。
https://www.marulabo.net/docs/cipher/

NISQ 時代の課題

2018年　プレスキル

Quantum Computing in the NISQ era and beyond

John Preskill 2018/01/27

https://arxiv.org/abs/1801.00862v2

現代を「NISQ 時代」と名付け、その課題を整理したのは、プレスキルの論文 “Quantum Computing in the NISQ era and beyond” だった。

彼は、「50～100qubitの量子コンピュータは、今日の古典的なデジタルコンピュータの能力を上回るタスクを実行する可能性を持つ」ことを指摘し、「量子複雑性」と「量子誤り訂正」の二つを、この時代の課題として提示した。

Quantum Computing in the NISQ era and beyond

John Preskill 2018/01/27

https://arxiv.org/abs/1801.00862v2

論文概要

近い将来、ノイズの下での中規模程度の量子技術NISQ (Noisy Intermediate-Scale Quantum)が利用可能になるだろう。50～100qubitの量子コンピュータは、今日の古典的なデジタルコンピュータの能力を上回るタスクを実行する可能性を持つのだが、量子ゲートのノイズは、信頼性をもって実行できる量子回路のサイズを制限する。NISQデバイスは、多体量子物理学の研究の有用なツールとなるだろう。その他の有用な応用もあるのだが、100qubitの量子コンピュータは、すぐには世界を変えないだろう。我々は、それを、将来のより強力な量子技術に向けた重要なステップとみなすべきである。量子技術者は、完全にフォールト・トレラントな量子コンピューティングを結果的に可能とする、より正確な量子ゲートの実現に向けて努力しなければならない。

量子技術の商業的可能性について

量子コンピューティングの現在の状況と将来の可能性を評価するこの機会に参加できたことを、私は喜んでいる。量子コンピューティング技術は現在我々が使用している情報技術とは非常に異なるため、将来の応用を予想するのも、これらの応用が実現した際のプロジェクトを考えるのにも、我々は非常に限られた能力しか持っていない。この不確実性は楽観主義を助長するのだが、我々は、楽観主義を注意深く調整する必要がある。我々は、将来の数十年にわたって量子技術が社会に重要な影響を及ぼすと確信しているのだが、今後の5～10年という短期間での量子技術の商業的可能性については、あまり自信を持っているとは言えないのだ。それが、私がこの話で伝えたい主なメッセージである。私は、この会議を組織したようなすべての利害関係者間の活発な議論が、将来の進展に向けての道筋を照らすと確信している。

現在のコンピュータでは
自然のシミュレートはできない

私のような物理学者が、量子コンピューティングについて本当に興奮しているのは、量子コンピュータが自然界で起こる全てのプロセスを効率的にシミュレートできると信じる十分な理由があるからである。これは、古典的（すなわち非量子）デジタルコンピュータでは当てはまらないことだ。古典的コンピュータは、高度にもつれあった量子システムをシミュレートすることができないのだ。

量子コンピュータがあれば、きっと複雑な分子やエキゾチックな材料の特性をより深く探求することが可能になるだろう。それだけでなく、例えば、基本粒子の性質やブラックホールの量子的挙動やビッグバン直後の宇宙の進化をシミュレートすることで、新しいやり方で、基本的な物理学を切り開いていくだろう。

「量子複雑性」と「量子誤り訂正」という二つの原理

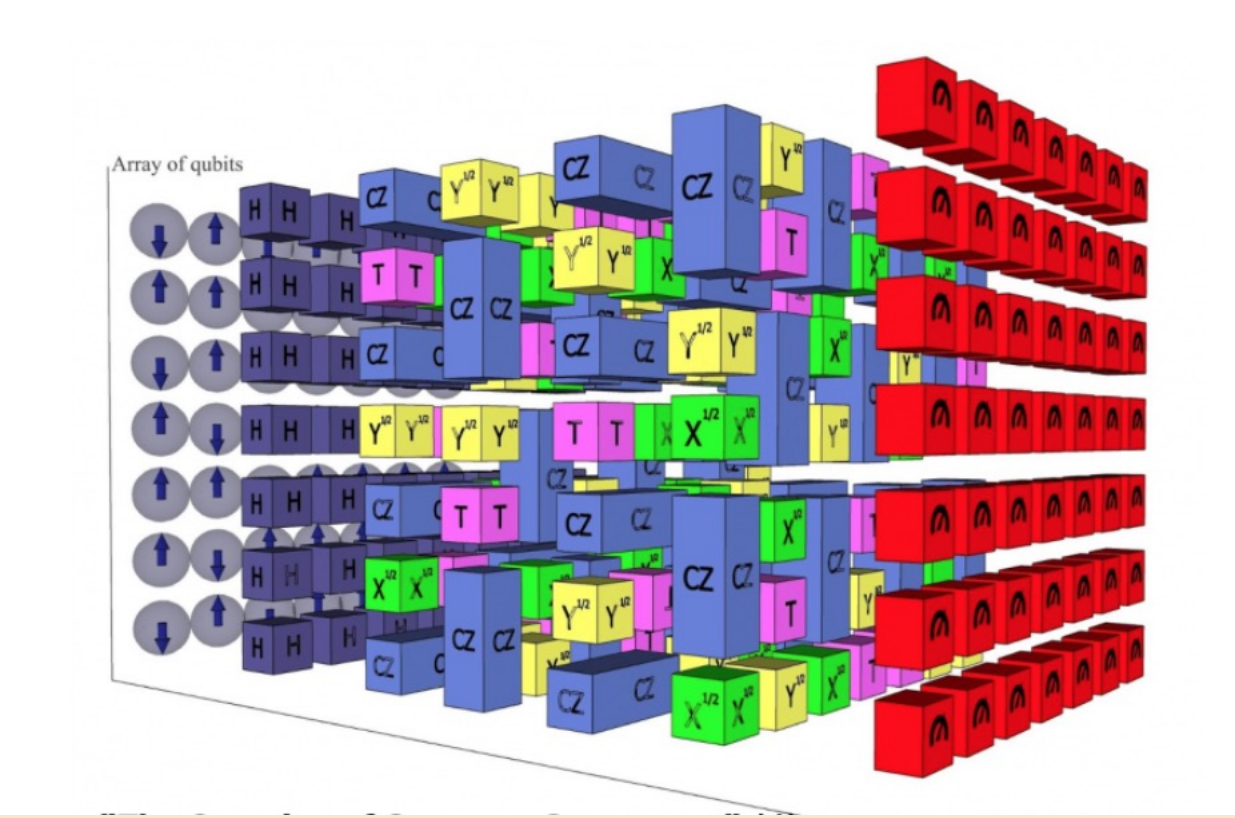
エンタングルメント（量子もつれ）の最前線の開拓が実り多いものであるという我々の確信は、次の二つの原理に基づいている。

(1) 量子複雑性（量子コンピューティングが強力であると考える我々の考えの基礎）

（2）量子誤り訂正（量子コンピュータは、難しい問題を解決する大規模なデバイスに拡張可能であると考える私たちの基礎）

これらの二つの原理の基礎となるのは、量子エンタングルメントの考え方である。エンタングルメントは、私たちが日常生活でであう相関とは全く異なる、量子システムの部分の間の特徴的な相関のために使用する言葉である。

詳しくは、次の資料を参照されたい



2020/02/17マルレク

「量子コンピュータの現在 ― 量子優越性のマイルストーンの達成 ―」

https://www.marulabo.net/docs/q-supremacy


量子コンピュータと量子通信

量子コンピュータと量子通信

量子論のIT技術への「応用」では、「量子コンピュータ」をイメージする人が、一番多いのではと思いますが、もう一つ重要な応用分野があります。

それが「量子通信」の分野です。

「量子コンピュータ」と並んで「量子通信」が重要であることは、現在のIT技術の中心が、大雑把に言って、コンピュータ技術とネットワーク技術の二つであることを考えればわかります。どちらか一つだけでは、現代のITの世界は成り立ちません。

なぜ、量子通信の理論が重要なのか
実用化の速度

第一に、量子コンピュータより量子通信の「実用化」が、早く進むだろうということです。

何をもって「実用化」というかは、いろいろ議論があると思います。ただ、現在のスマートフォンやクラウドが、「量子コンピュータ」に置き換わることを展望する必要はありません。それらの技術とその発展系は、今後も生き続けると考える方が現実的です。

それにもかかわらず、量子通信技術は、ネットワークの世界で現実的な応用課題を見出して、じわじわとその影響力を広げていくのは確実だと考えています。

なぜ、量子通信の理論が重要なのか
理論的基礎

第二に、量子通信の理論は、古典的ですが、しっかりとした理論的基礎をもっています。それは、シャノンが創設した「情報理論」です。情報理論は、通信の理論に他なりません。そこでの考察の中心は「情報量＝エントロピー」です。

もちろん「情報理論の量子化」の課題は、簡単なものではありません。それでも、多くの知見が得られています。

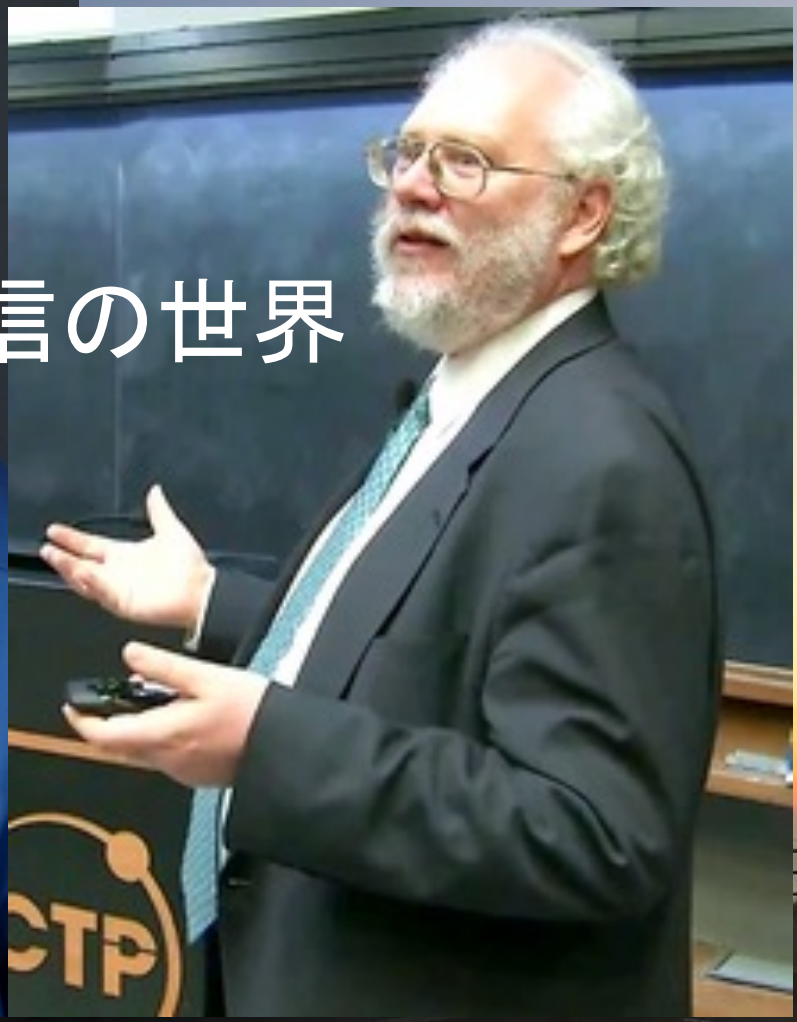
8月20日開催のMaruLabo片桐ゼミで取り上げる「量子通信路符号化定理 」も、その重要な成果のひとつです。
https://www.marulabo.net/docs/katagiri5/

なぜ、量子通信の理論が重要なのか
量子コンピュータ実用化の鍵

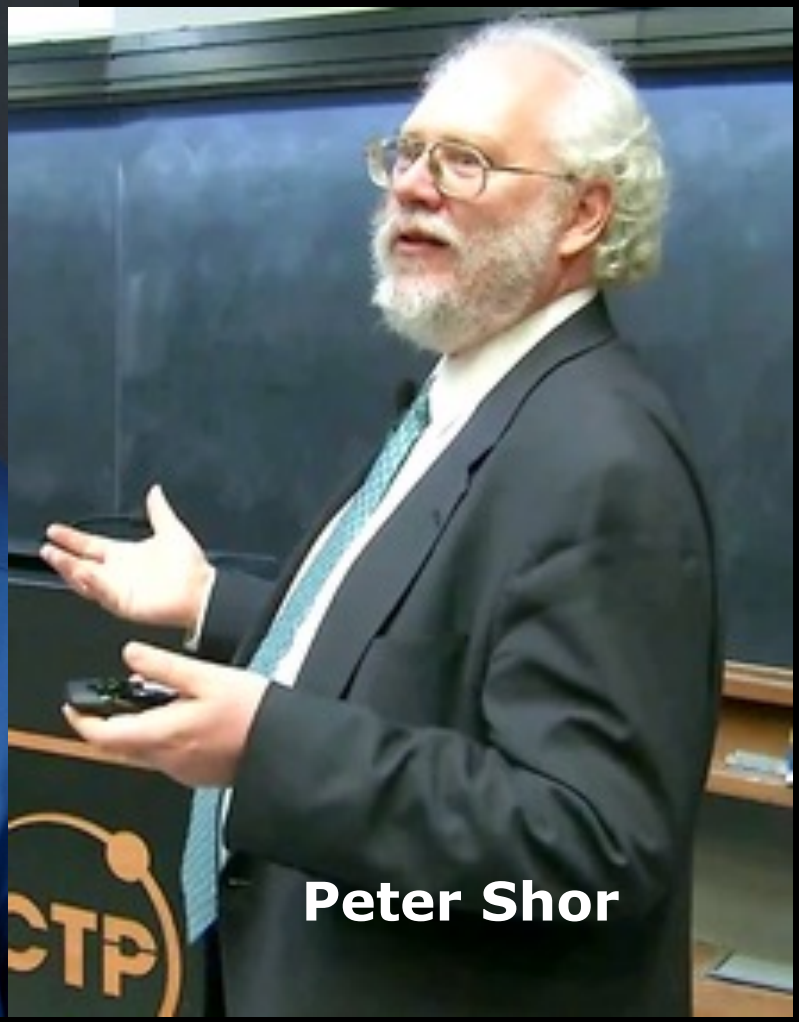
第三に、量子コンピュータの「実用化」の鍵を握っているのは、環境のノイズの影響を強く受け不安定な量子コンピュータを、安定的に動作させる「量子エラー訂正技術」です。ここでも、量子通信の理論が中心的な役割を果たします。

MaruLabo小又ゼミの「誤り訂正符号の初歩ー古典と量子 」というテーマも、こうした問題意識を掘り下げたようとしたものです。https://www.marulabo.net/docs/komata01

量子通信の世界

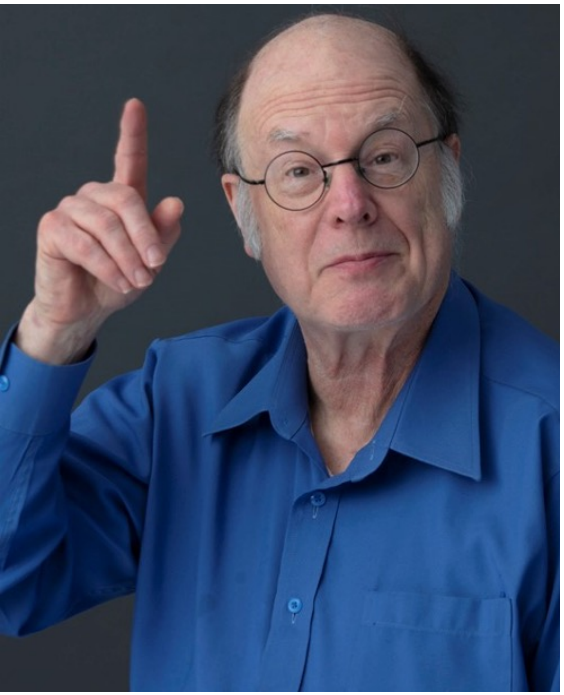


Charles H. Bennett



Peter Shor

量子暗号



RSA公開キー暗号の安全さは、公開キーが簡単には素因数分解されないことに依存している。

強力な計算パワーを持つマシンが登場すれば、公開キーが破られる可能性はある。

ただ、量子の性質を利用すれば、どんな計算パワーでも破れない、公開キーの構成が可能だ。

しかも、悪意のある第三者が、公開キーの構成を「盗聴」して、それを再構成しようとしても、それは現実的には不可能であることが保証される。

基底 |0>, |1> と基底 |+>, |−>を利用する

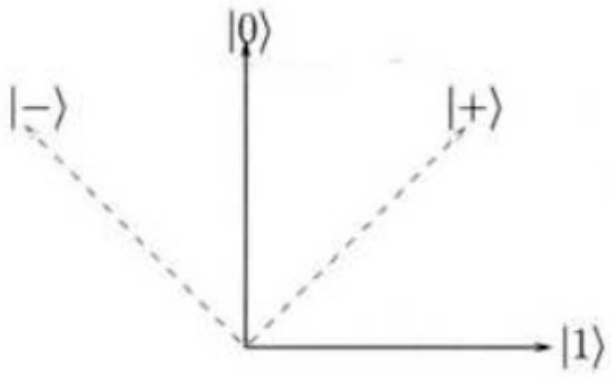
基底 |0>, |1> と基底 |+>, |−>の間には、つぎのような関係がある。

1. $|0\rangle = \frac{1}{\sqrt{2}}|+\rangle + \frac{1}{\sqrt{2}}|-\rangle$

   $|1\rangle = \frac{1}{\sqrt{2}}|+\rangle - \frac{1}{\sqrt{2}}|-\rangle$

2. $|+\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$

   $|-\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$



基底 |0>, |1>を「標準基底」、
基底 |+>, |−>を「アダマール基底」と呼ぶ。

詳しくは、次の資料を参照されたい

2019/06/03 マルレク
「暗号技術の現在 ― ポスト量子暗号への移行と量子暗号」
https://www.marulabo.net/docs/cipher/

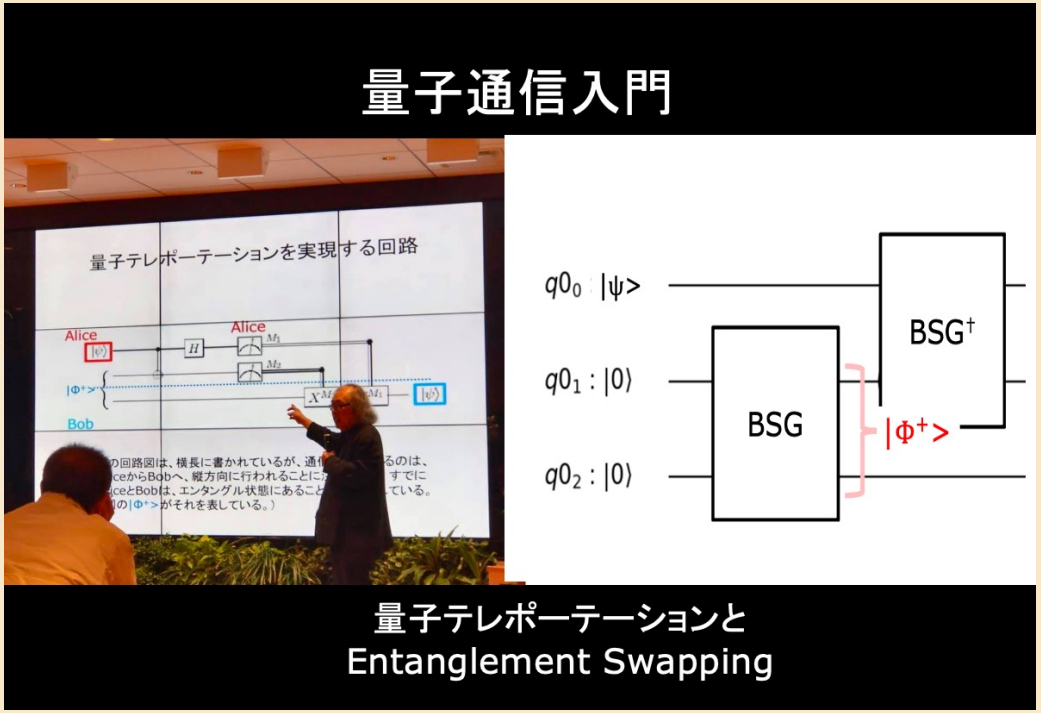
量子テレポーテーション

量子Aと量子Bがエンタングルメント状態にある時、量子Aの状態変化は、瞬時に量子Bに反映される。たとえAとBとが、どんなに離れていても。

このことを利用して、量子Xの状態を、遠く離れた場所に転送することが可能となる。

このことは、量子状態のコピーを禁じた量子情報論の「No Cloning定理」にも、光速を超えた情報伝達を禁じた相対論の原理とも矛盾しない。

詳しくは、次の資料を参照されたい



2020/08/28 マルゼミ

「量子通信入門 – 量子レレポーテーションと Entanglenent Swapping」

https://www.marulabo.net/docs/teleportation-2

量子エラー訂正

ハミング・コードは、冗長なbitを付加して転送されたbit の誤りを検出し訂正する。

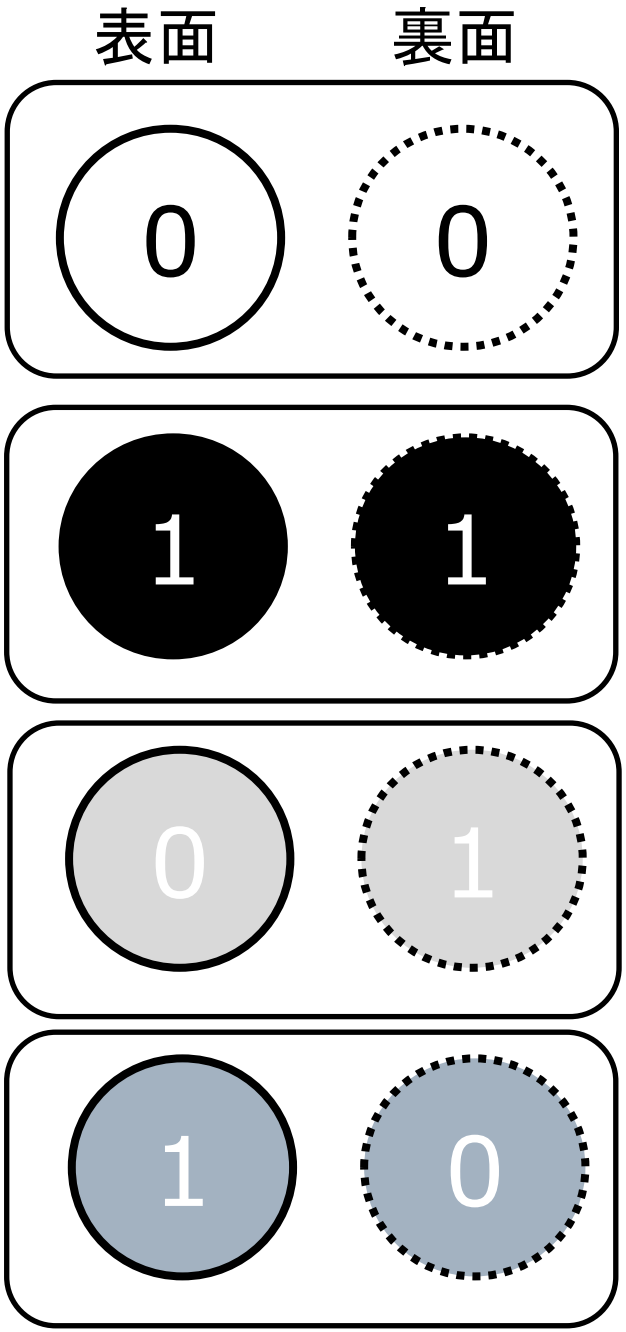
これは古典bitに対するものだが、同様なことが、量子bit=qubit に対しても可能である。

すなわち、qubitの誤りを検出し、それを訂正する量子回路を構成できる、

Part III

たとえ話で理解する「量子暗号」


たとえ話で理解する「量子暗号」１
コイントスで「量子暗号」をシミレートする



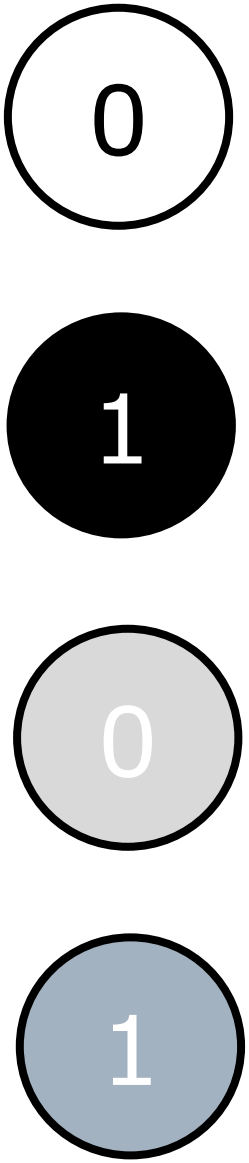
次のような4種類のコインがある。

コインには、表面と裏面の区別があって、それぞれの面に、0または1の文字が刻まれている。

例えば、上から三番目のコインは、表面に0が、裏面に1が、刻まれている。

上から四番目のコインは、表面に1が、裏面には0が、刻まれている。

表面



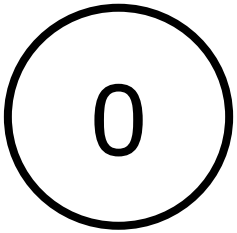
次のような4種類のコインがある。

コインには、白、黒、二つの灰色と色がある。

コインの色と、表面に刻まれた数字で、四つのコインの区別ができる。

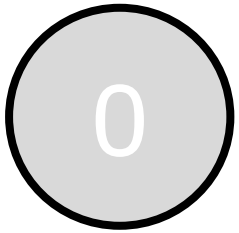
それぞれのコインの名前を、「白0」、「黒1」、「灰0」、「灰1」としよう。

表面



白0

黒1



灰0

灰1

次のような4種類のコインがある。

コインには、白、黒、二つの灰色と色がある。

コインの色と、表面に刻まれた数字で、四つのコインの区別ができる。

それぞれのコインの名前を、「白0」、「黒1」、「灰0」、「灰1」としよう。

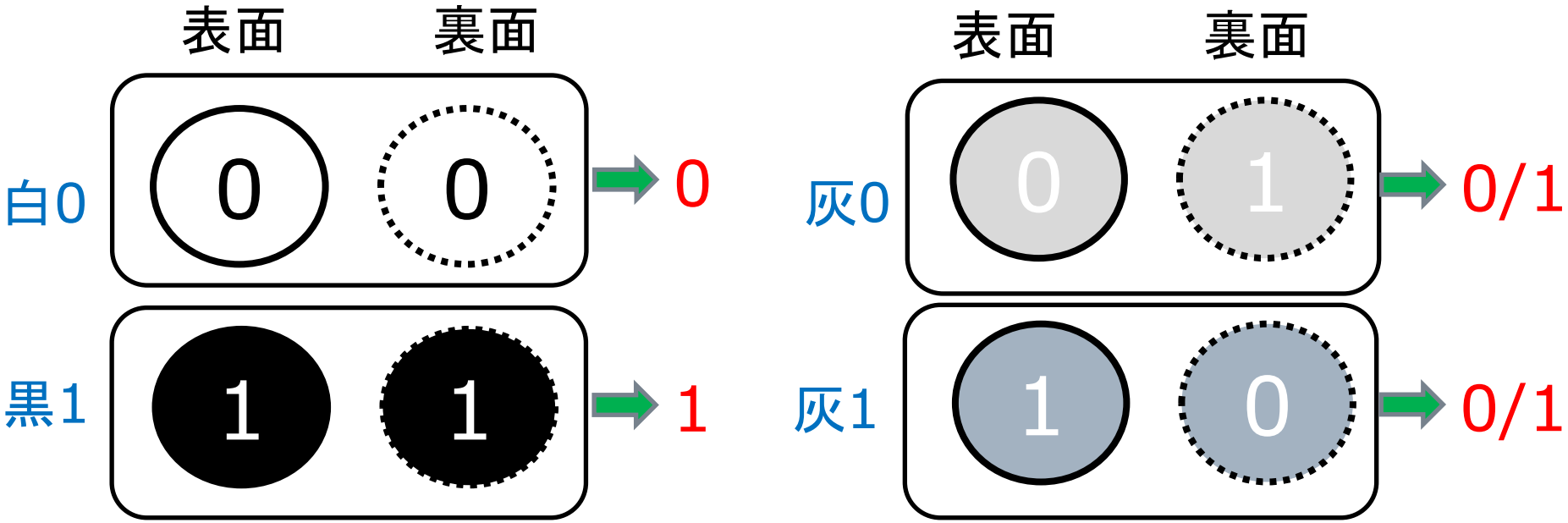
AliceとBobがコインを介して通信する

- Aliceが受け取った 入力1bitは、あるルールでコインにエンコードされ、そのコインがBobに送られる。あとで見るように、Aliceのエンコードには、二つのタイプがある。

- Bobにも二つのタイプのデコードの仕方がある。 Bobは、ある場合には、うけとったコインをそのまま、ある場合にはコインを他のコインに変えてからデコードする。コインは、1bitの出力にデコードされる。
- Bobは、最終的に与えられたコインをトスして、でた面の数字を出力とする。

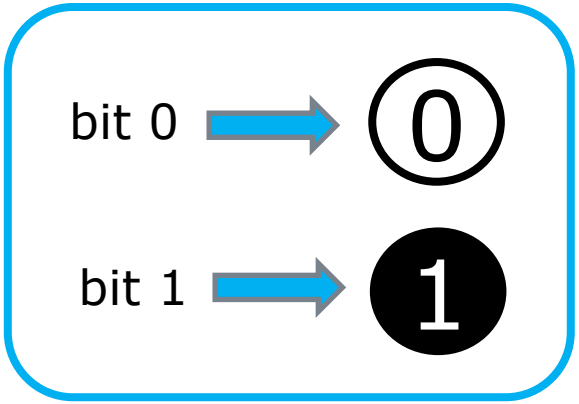
Bobの最後のデコードの例

- コイン「白0」の場合、両面が0なので、必ず0が出力される。
- コイン「黒1」の場合、両面が1なので、必ず1が出力される。
- コイン「灰0」の場合、1がでる確率は1/2、0が出る確率は1/2。
- コイン「灰1」の場合、1がでる確率は1/2、0が出る確率は1/2。

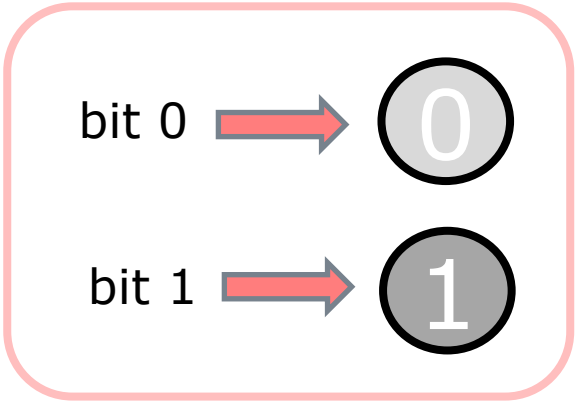


Aliceのエンコードの二つのタイプ

- Type I
  - bit 0をコイン「白0」にエンコードする
  - bit 1をコイン「黒1」にエンコードする



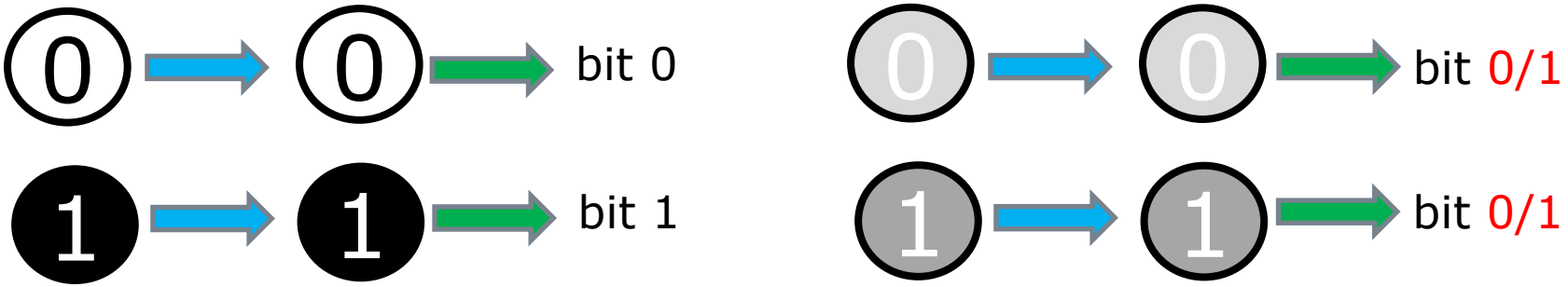
- Type II
  - bit 0をコイン「灰0」にエンコードする
  - bit 1をコイン「灰1」にエンコードする



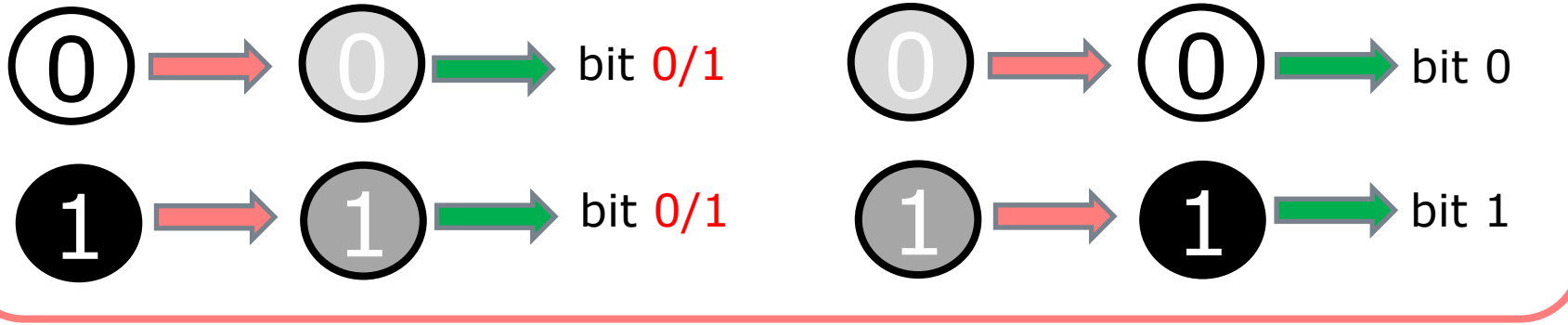
Type I をストレート、Type II をミクストと呼ぼう。

Bobのデコードの二つのタイプ

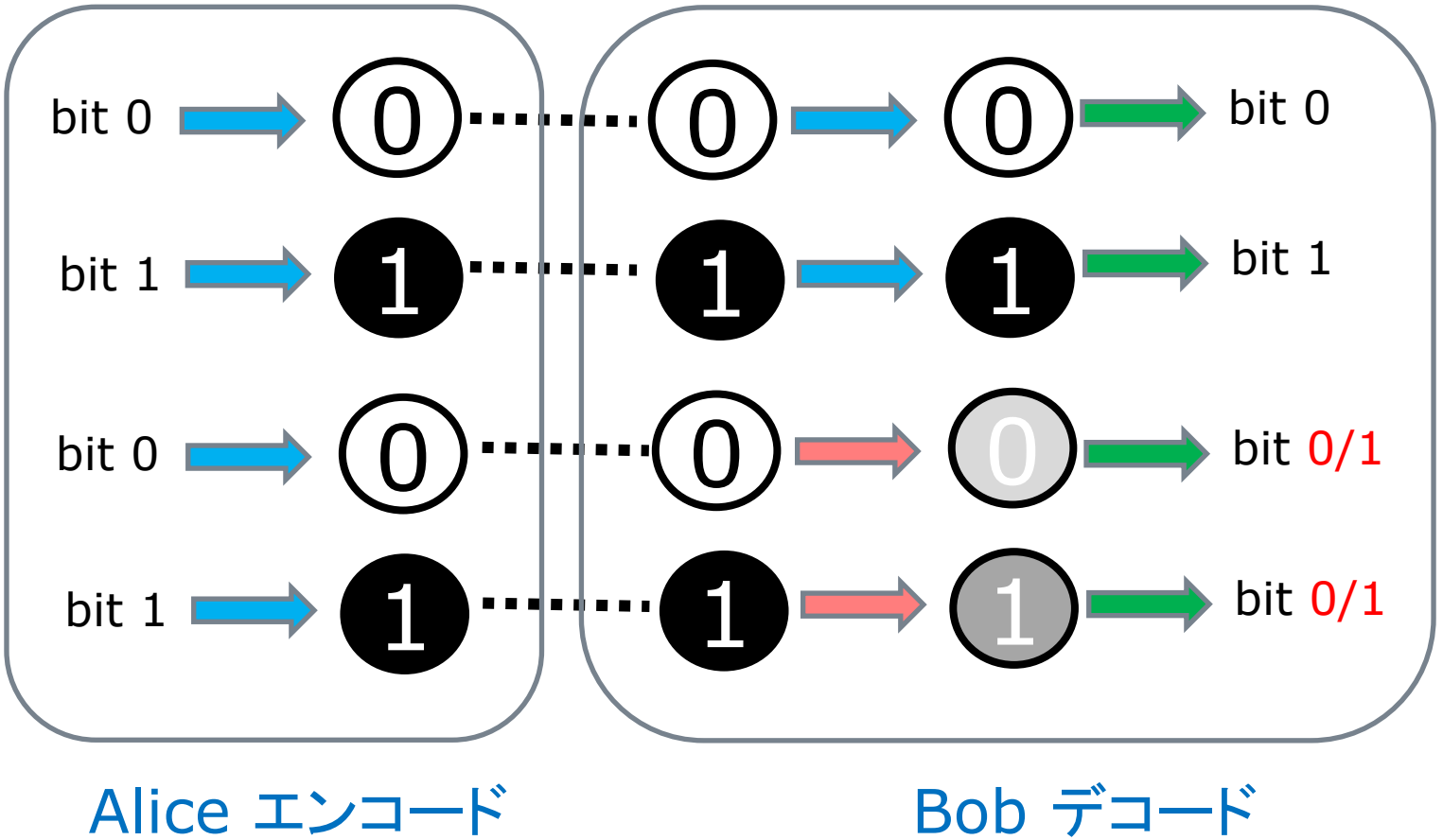
- Type I 素通り　これもストレートと呼ぼう。



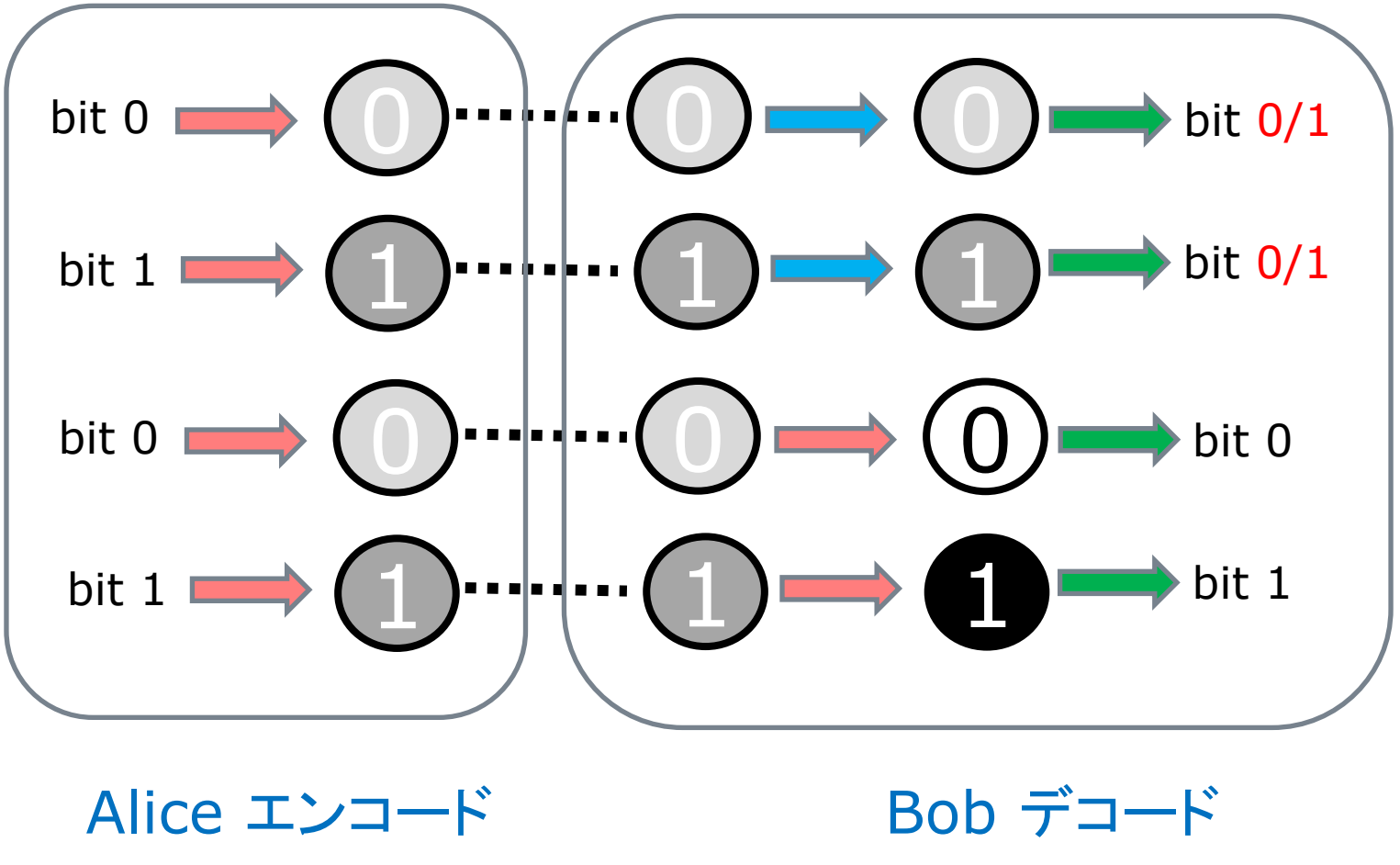
- Type II コイン交換　これもミクストと呼ぼう。



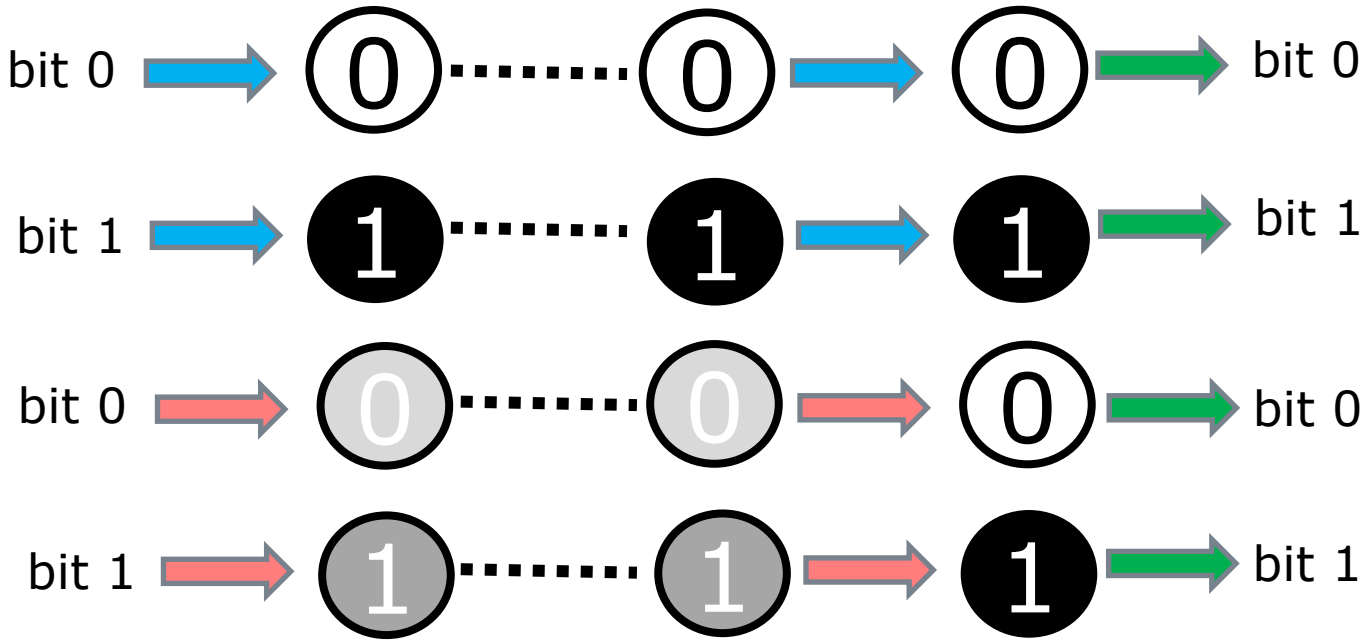
エンコードとデコードの例



エンコードとデコードの例



入力が正しく出力されるのは、次の場合である



エンコードもデコードもストレートか、あるいは、
エンコードもデコードもミクストの場合である。


たとえ話で理解する「量子暗号」２
共有キーの構成

共有キーの構成　Step 1

- Aliceは、ランダムなビット列を準備する。
- Aliceは、ランダムなビット列を、順番にコインにエンコードする。この時、エンコードの方式として、「ストレート」を選ぶか「ミクスト」を選ぶかはランダムに決める。
- Bobは、Aliceから受け取ったコインを、順番にビットにデコードする。この時、エンコードの方式として、「ストレート」を選ぶか、「ミクスト」を選ぶかはランダムに決める。
- エンコードの「ストレート」「ミクスト」を、'=','x' で表そう。
  デコードの「ストレート」「ミクスト」も、'=','x' で表そう。

共有キーの構成　Step 1
サンプル

- Aliceは、ランダムなビット列を準備する。
- Aliceは、ランダムなビット列を、順番にコインにエンコードする。この時、エンコードの方式として、「ストレート `=′」を選ぶか「ミクスト `x′」を選ぶかはランダムに決める。
- Bobは、Aliceから受け取ったコインを、順番にビットにデコードする。この時、エンコードの方式として、「ストレート `=′」を選ぶか、「ミクスト `x′」を選ぶかはランダムに決める。

Aliceの送信ビット	0	1	1	0	0	.....	0	1	0	1
Aliceのエンコード	=	x	x	=	=	.....	x	=	x	x
Bobのデコード	x	x	=	x	=	.....	=	x	=	x
Bobの受信ビット	0	1	0	0	0	.....	1	1	0	1

共有キーの構成　Step 1
お互い知らないこと

- Aliceが送ったビットを、Bobは知らない。

Aliceの送信ビット	0	1	1	0	0	.....	0	1	0	1
Aliceのエンコード	=	x	x	=	=	.....	x	=	x	x
Bobのデコード	x	x	=	x	=	.....	=	x	=	x
Bobの受信ビット	0	1	0	0	0	.....	1	1	0	1

共有キーの構成　Step 1
お互い知らないこと

- Aliceが送ったビットを、Bobは知らない。
- Aliceが使ったエンコード方法を、Bobは知らない。

Aliceの送信ビット	0	1	1	0	0	.....	0	1	0	1
Aliceのエンコード	=	x	x	=	=	.....	x	=	x	x
Bobのデコード	x	x	=	x	=	.....	=	x	=	x
Bobの受信ビット	0	1	0	0	0	.....	1	1	0	1

共有キーの構成　Step 1
お互い知らないこと

- Aliceが送ったビットを、Bobは知らない。
- Aliceが使ったエンコード方法を、Bobは知らない。
- Bobが使ったエンコード方法を、Aliceは知らない。

Aliceの送信ビット	0	1	1	0	0	.....	0	1	0	1
Aliceのエンコード	=	x	x	=	=	.....	x	=	x	x
Bobのデコード	x	x	=	x	=	.....	=	x	=	x
Bobの受信ビット	0	1	0	0	0	.....	1	1	0	1

共有キーの構成　Step 1
お互い知らないこと

- Aliceが送ったビットを、Bobは知らない。
- Aliceが使ったエンコード方法を、Bobは知らない。
- Bobが使ったデコード方法を、Aliceは知らない。
- Bobが受け取ったビットを、Aliceは知らない。

Aliceの送信ビット	0	1	1	0	0	.....	0	1	0	1
Aliceのエンコード	=	x	x	=	=	.....	x	=	x	x
Bobのデコード	x	x	=	x	=	.....	=	x	=	x
Bobの受信ビット	0	1	0	0	0	.....	1	1	0	1

共有キーの構成　Step 2
情報の共有

- Aliceが送ったビットを、Bobは知らない。
- Aliceは、使ったエンコード方法を、Bobに伝える。
- Bobは、使ったデコード方法を、Aliceに伝える。
- Bobが受け取ったビットを、Aliceは知らない。

Aliceの送信ビット	0	1	1	0	0	.....	0	1	0	1
Aliceのエンコード	=	x	x	=	=	.....	x	=	x	x
Bobのデコード	x	x	=	x	=	.....	=	x	=	x
Bobの受信ビット	0	1	0	0	0	.....	1	1	0	1

共有キーの構成　Step 2
情報の共有

- Aliceが送ったビットを、Bobは知らない。
- Aliceは、使ったエンコード方法を、Bobに伝える。
- Bobは、使ったデコード方法を、Aliceに伝える。
- Bobが受け取ったビットを、Aliceは知らない。

Aliceの送信ビット	0	1	1	0	0	.....	0	1	0	1
Aliceのエンコード	=	x	x	=	=	.....	x	=	x	x
Bobのデコード	x	x	=	x	=	.....	=	x	=	x
Bobの受信ビット	0	1	0	0	0	.....	1	1	0	1

共有キーの構成　Step 2
情報の共有

- Aliceが送ったビットを、Bobは知らない。
- Aliceは、使ったエンコード方法を、Bobに伝える。
- Bobは、使ったデコード方法を、Aliceに伝える。
- Bobが受け取ったビットを、Aliceは知らない。

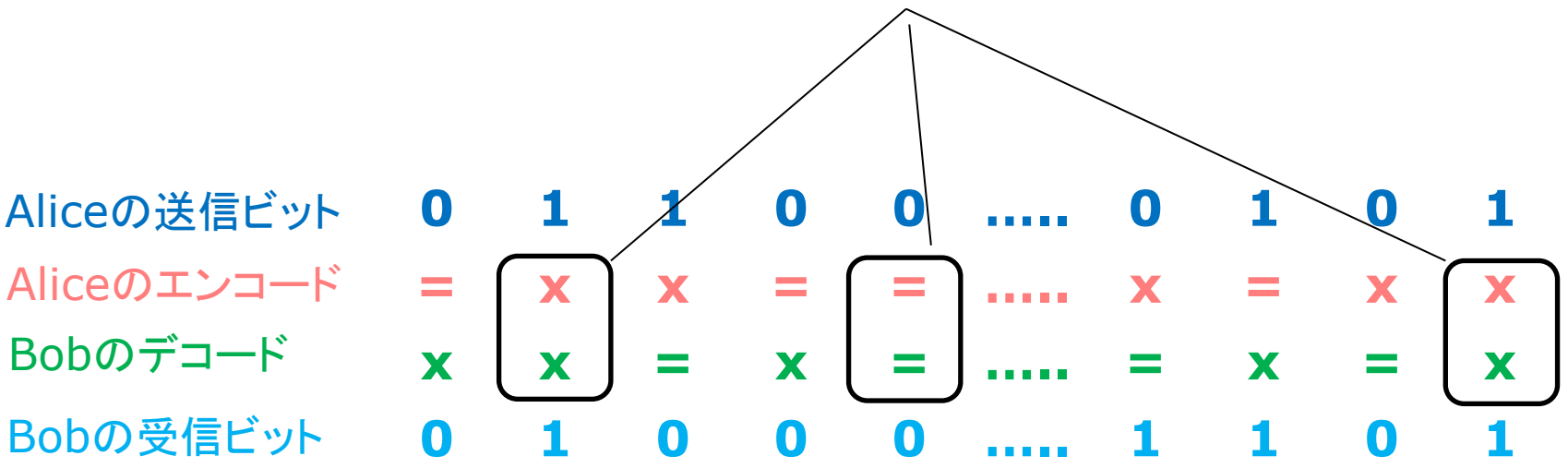
AliceとBobは、各ビットのエンコード方法と
デコード方法の情報を共有する。

Aliceの送信ビット	0	1	1	0	0	.....	0	1	0	1
Aliceのエンコード	=	x	x	=	=	.....	x	=	x	x
Bobのデコード	x	x	=	x	=	.....	=	x	=	x
Bobの受信ビット	0	1	0	0	0	.....	1	1	0	1

共有キーの構成　Step 3

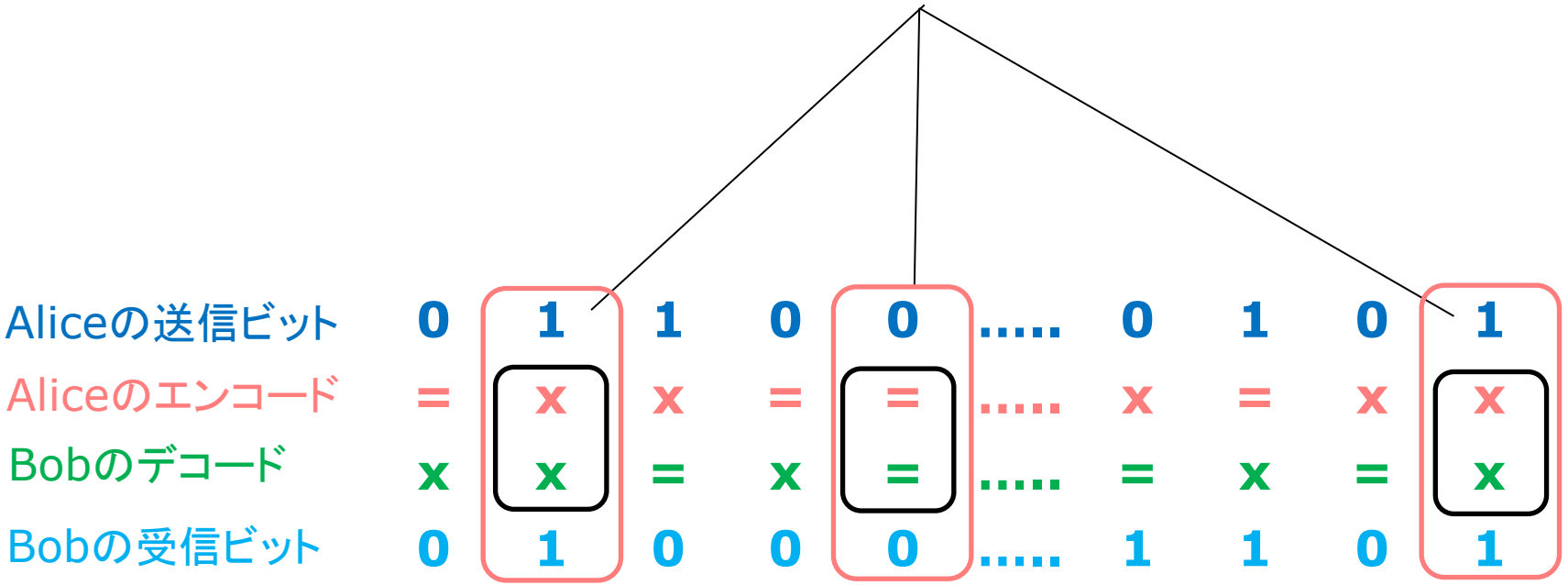
- AliceとBobが共有する、エンコード・デコードの情報で、エンコードのタイプとデコードのタイプが等しいものをピックアップする。

Aliceのエンコードの方法とBobのデコードの方法が等しいものをピックアップする。



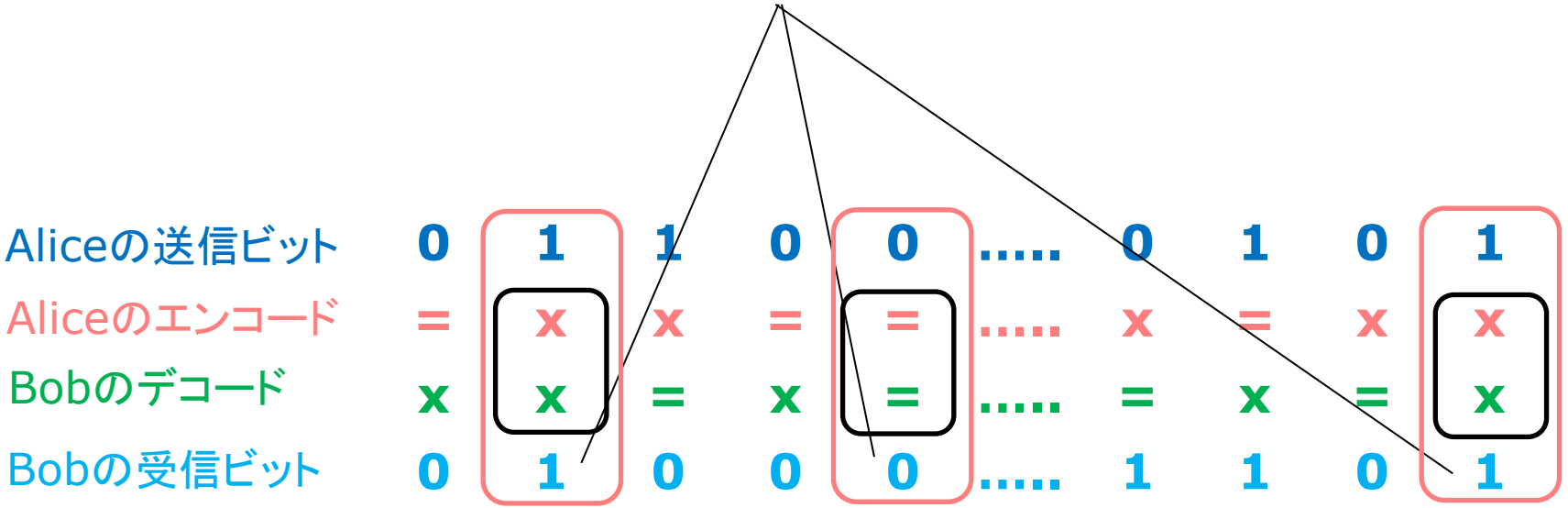
共有キーの構成　Step 3

- AliceとBobが共有する、エンコード・デコードの情報で、エンコードのタイプとデコードのタイプが等しいものをピックアップする。
- ピックアップしたコラムの、Aliceの送信ビットを見る。



共有キーの構成　Step 3

- AliceとBobが共有する、エンコード・デコードの情報で、エンコードのタイプとデコードのタイプが等しいものをピックアップする。
- ピックアップしたコラムの、Aliceの送信ビットを見る。
- それは、Bobの受信ビットと一致しているはずである。



共有キーの構成　Step 3

- AliceとBobは、二人が共有しているエンコード・デコードの情報を公開しても構わない。
- 第三者が、公開されたエンコード・デコードの情報から、共有キーを推測することはできない。Aliceがどのようなビットを入力したのかは、誰にもわからないから。
- Bobだけが、エンコード・デコードの情報から、Aliceの入力ビットがBobが受信したビットに等しいことを知る。
- それが、AliceとBobの共有キーになる。

Aliceの送信ビット	?	?	?	?	?	.....	?	?	?	?
Aliceのエンコード	=	x	x	=	=	.....	x	=	x	x
Bobのデコード	x	x	=	x	=	.....	=	x	=	x
Bobの受信ビット	?	?	?	?	?	.....	?	?	?	?

共有キーの構成は、安全に行われるか？

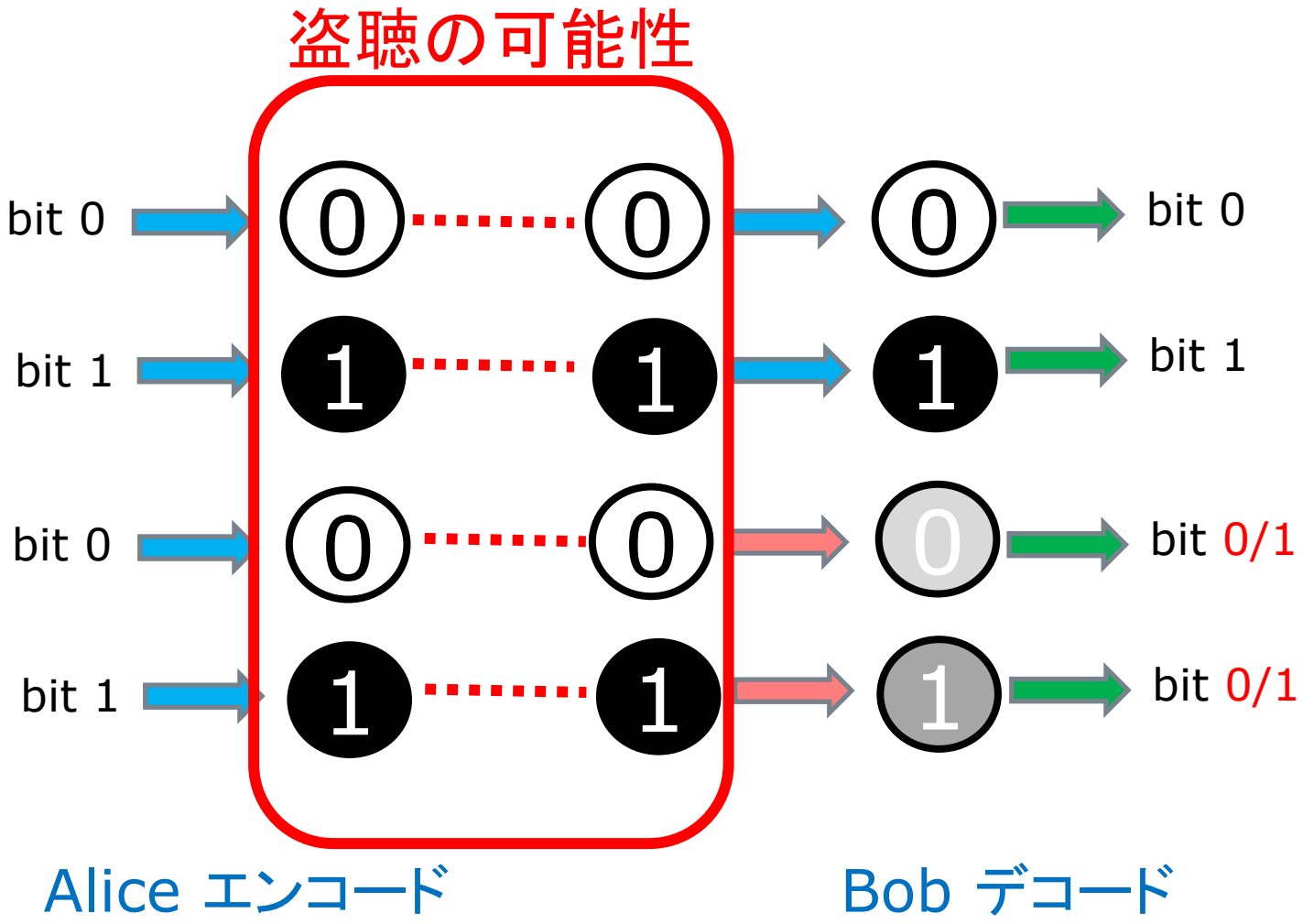
AliceとBobの間の、こうした共有キーの構成のプロトコルは、安全だろうか？

それについては、次に考察する。

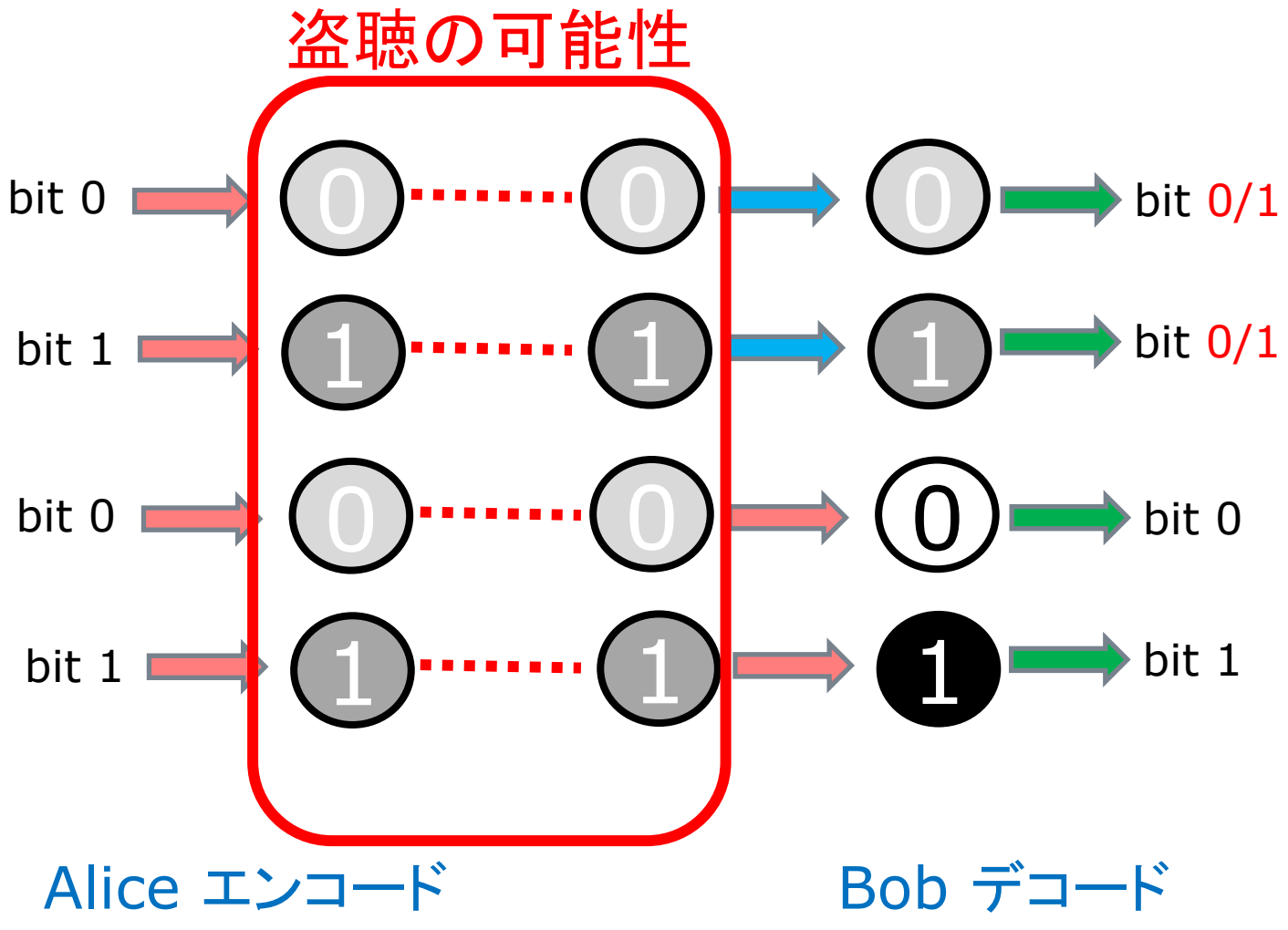
ちょっとした「どんでん返し」がある。


たとえ話で理解する「量子暗号」3
コインからqubitへ

コインでの通信には脆弱性がある



コインでの通信には脆弱性がある



中間者攻撃

- 中間攻撃者Eveは、AliceからBobに送られるコインをBobが受け取る前に密かに奪取して、コインの表の数字(Aliceの送信ビット)を記録し、同じコインを改めてBobに送る。Bobは情報が盗まれたことに気づかない。

盗聴されたデータ

Aliceの送信ビット	0	1	1	0	0	….	0	1	0	1
Aliceのエンコード	=	x	x	=	=	….	x	=	x	x
Bobのデコード	x	x	=	x	=	….	=	x	=	x
Bobの受信ビット	?	?	?	?	?	….	?	?	?	?

中間者攻撃

- 中間攻撃者Eveは、AliceからBobに送られるコインをBobが受け取る前に密かに奪取して、コインの表の数字(Aliceの送信ビット)を記録し、同じコインを改めてBobに送る。Bobは情報が盗まれたことに気づかない。

- 攻撃者は、公開されたエンコード・デコードの情報から、たやすく共有キーを知ることができる。

Aliceの送信ビット	0	1	1	0	0	.....	0	1	0	1
Aliceのエンコード	=	x	x	=	=	.....	x	=	x	x
Bobのデコード	x	x	=	x	=	.....	=	x	=	x
Bobの受信ビット	?	?	?	?	?	.....	?	?	?	?

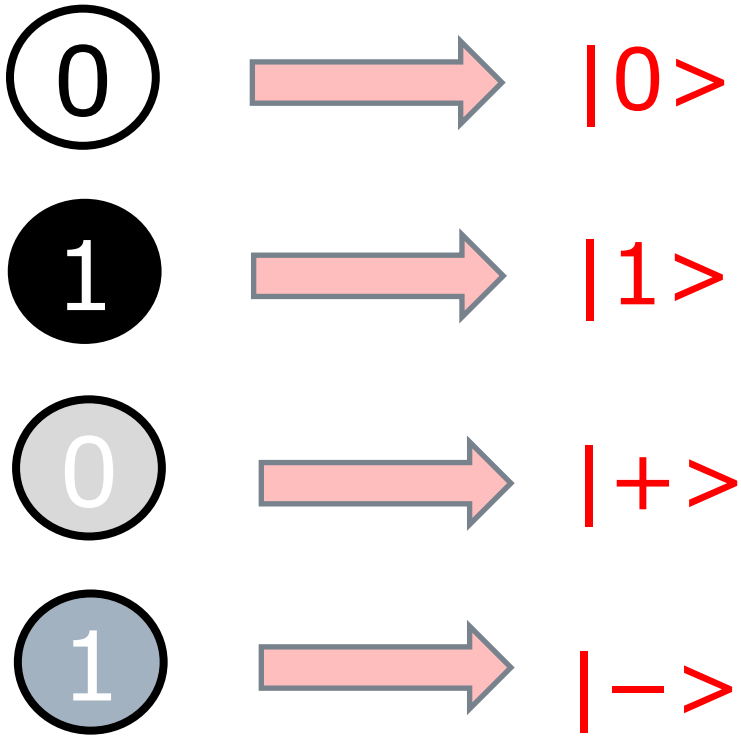
物理的コインによる
量子暗号のシミレーションは失敗する

- 量子暗号のエンコード・デコードのシミレーションは、物理的コインでも可能である。
- 量子暗号の共有キーの構成のシミレーションは、物理的コインでも可能である。
- ただ、AliceからBobに、物理的コインを渡すというスタイルでは、中間者攻撃により、共有キーの秘密は破られる。

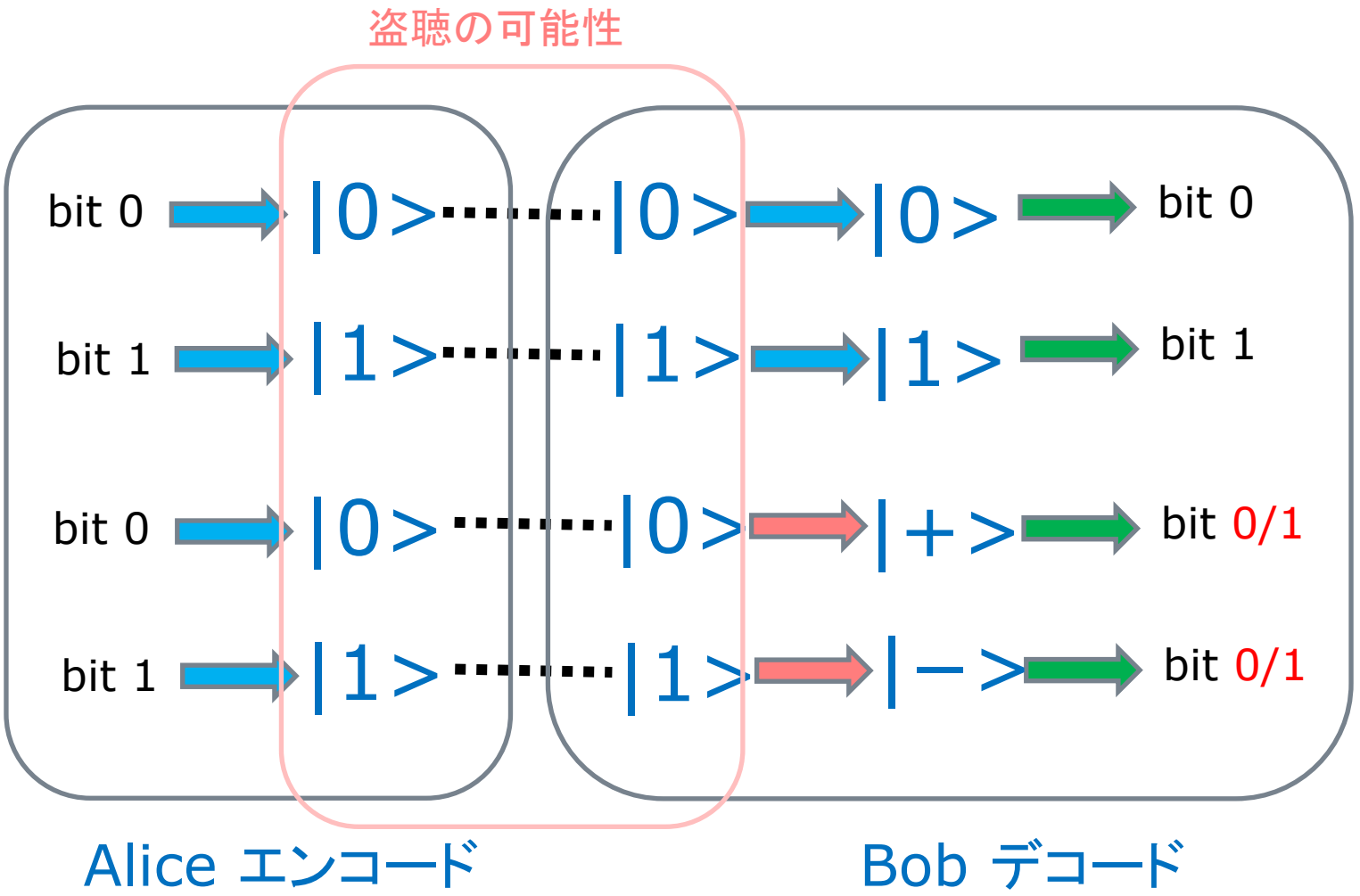
- それでは、この問題に、量子暗号はどう対処しているのであろうか？

コインからqubitへ

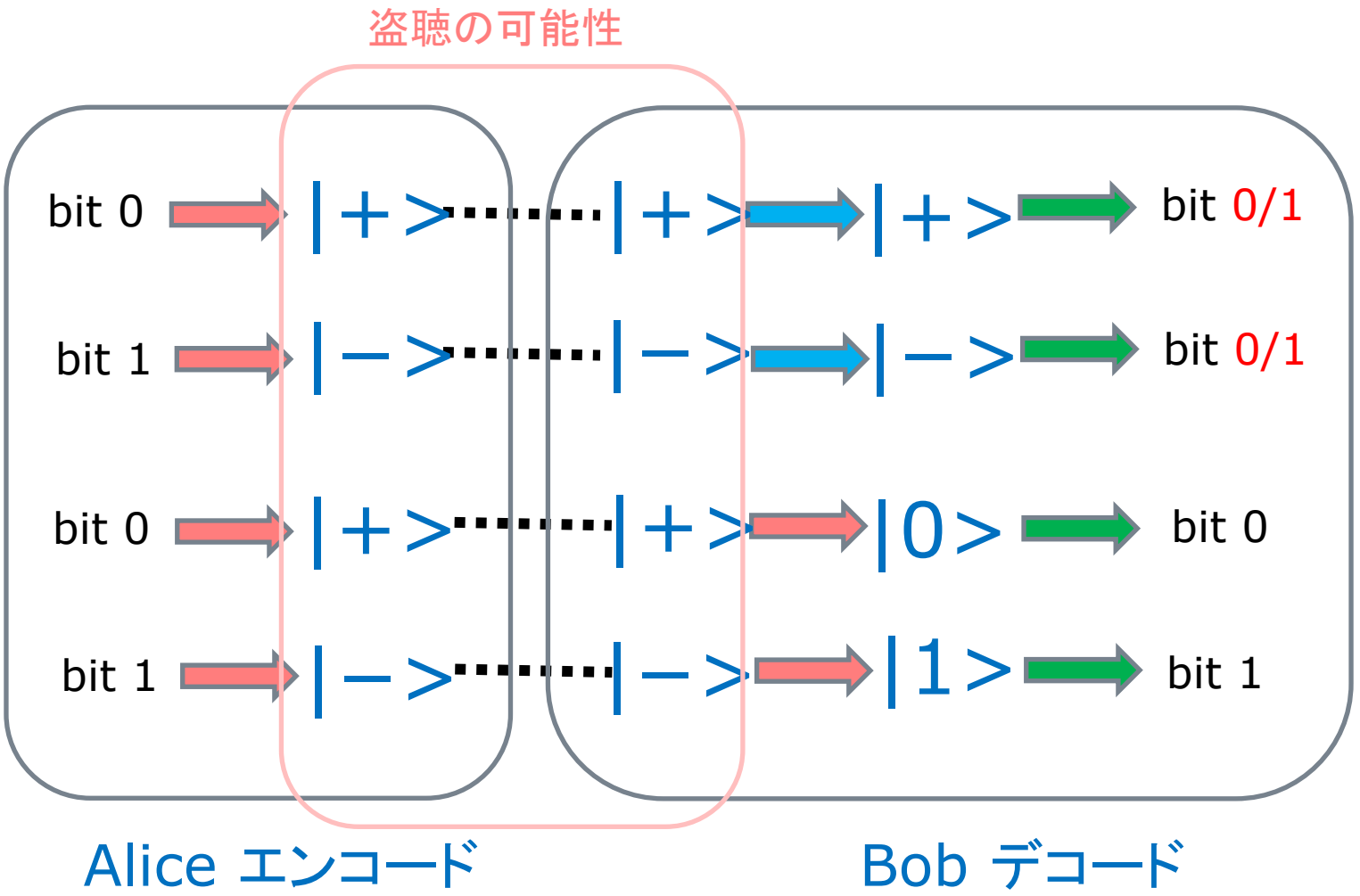
メッセージの担い手を、つぎのように、
コインからqubitに切り替える。



qubit バージョン


盗聴の可能性
bit 0
|0>
|0>
|0>
bit 0
bit 1
|1>
|1>
|1>
bit 1
bit 0
|0>
|0>
|+>
bit 0/1
bit 1
|1>
|1>
|−>
bit 0/1
Alice エンコード
Bob デコード

qubit バージョン


盗聴の可能性
bit 0
|+>
|+>
|+>
bit 0/1
bit 1
|−>
|−>
|−>
bit 0/1
bit 0
|+>
|+>
|0>
bit 0
bit 1
|−>
|−>
|1>
bit 1
Alice エンコード
Bob デコード

攻撃者Eveが行うべきこと

メッセージの担い手がコインなら、中間攻撃者Eveは、AliceからBobに送られるコインをBobが受け取る前に密かに奪取して、コインの表の数字（Aliceの送信ビット）を記録し、同じコインを改めてBobに送ればいい。

メッセージの担い手がコインからqubitに変わっても、Eveが行うべきことは、基本的には、Aliceから送られたqubit |X>から、Aliceの送信ビットの情報を盗んで、qubit |X>をBobに送ることである。

Eveは、盗聴した|X>から何を知ることができるか？

- Eve は、Aliceが送った|X>が何かを知り、|X>をBobに送るためには、まず |X>を観測しなければならない。
- 観測結果が 0 の場合、|X>は |0>,|+>,|−>の可能性があり、Aliceの送信ビットは、0,1 の可能性がある。
- 観測結果が 1 の場合、|X>は |1>,|+>,|−>の可能性があり、Aliceの送信ビットは、0,1 の可能性がある。
- Eveは、|X>から、Aliceのエンコードの形式も、Aliceの送信ビットも、正確には知り得ない。

Aliceの送信ビット	?	?	?	?	?	.....	?	?	?	?
Aliceのエンコード	=	x	x	=	=	.....	x	=	x	x
Bobのデコード	x	x	=	x	=	.....	=	x	=	x
Bobの受信ビット	?	?	?	?	?	.....	?	?	?	?

このプロトコルは、攻撃に対して安全である

- Aliceの送信ビットが、0か1かの Eveの推測が正しい確率は、1/2 である。
- Aliceの行ったエンコードの方式が分からないと、|X>の形は分からない。エンコードには、「ストレート」と「ミクスト」の二つがあるので、そのどちらかというEveの推測が正しい確率は 1/2 である。
- その両方の推測が正しい場合に、AliceとBobが共有するビットの正しい推測ができる。AliceとBobが共有する 1 ビットについて、盗聴によってEveが正しい推測を行う確率は、 1/2 x 1/2 = 1/4 である。
- AliceとBobが共有するビットの桁数が大きくなるにつれ、正しい情報が盗まれる可能性は、ゼロに近づく。

基底 |0>, |1> と基底 |+>, |−>の関係

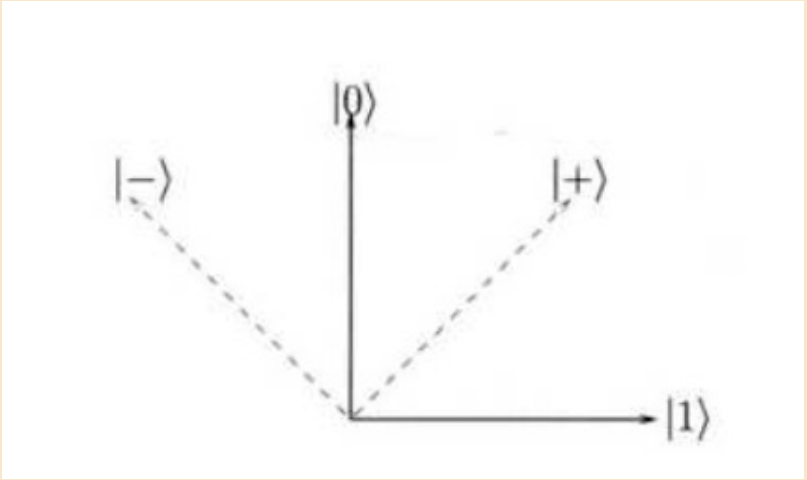
基底 |0>, |1> と基底 |+>, |−>の間には、つぎのような関係がある。

1. $|0\rangle=\frac{1}{\sqrt{2}}|+\rangle+\frac{1}{\sqrt{2}}|-\rangle$

   $|1\rangle=\frac{1}{\sqrt{2}}|+\rangle-\frac{1}{\sqrt{2}}|-\rangle$

2. $|+\rangle=\frac{1}{\sqrt{2}}|0\rangle+\frac{1}{\sqrt{2}}|1\rangle$

   $|-\rangle=\frac{1}{\sqrt{2}}|0\rangle-\frac{1}{\sqrt{2}}|1\rangle$



基底 |0>, |1>を「標準基底」、
基底 |+>, |−>を「アダマール基底」と呼ぶ。