量子計算と量子暗号

極限宇宙　市民講演会

森前智行（京都大学基礎物理学研究所）

（６０分）

内容（６０分）

- 量子論とは（１０分）
- 量子計算（２５分）
- 量子暗号（２５分）

量子論とは

量子論とは

古典力学

1687：ニュートン　力学

1873：マックスウェル　電磁気学

車、ロボット、ロケットなど「マクロ」な世界を記述できる

1900～：原子や分子などのミクロ世界が、古典論ではうまく説明できないことが発覚。。。

量子力学

1925：ハイゼンベルク　行列力学

1926：シュレディンガー　波動力学

原子、分子、光、電子等ミクロな世界の説明にことごとく成功

量子情報

1970：ウィズナー　量子マネー

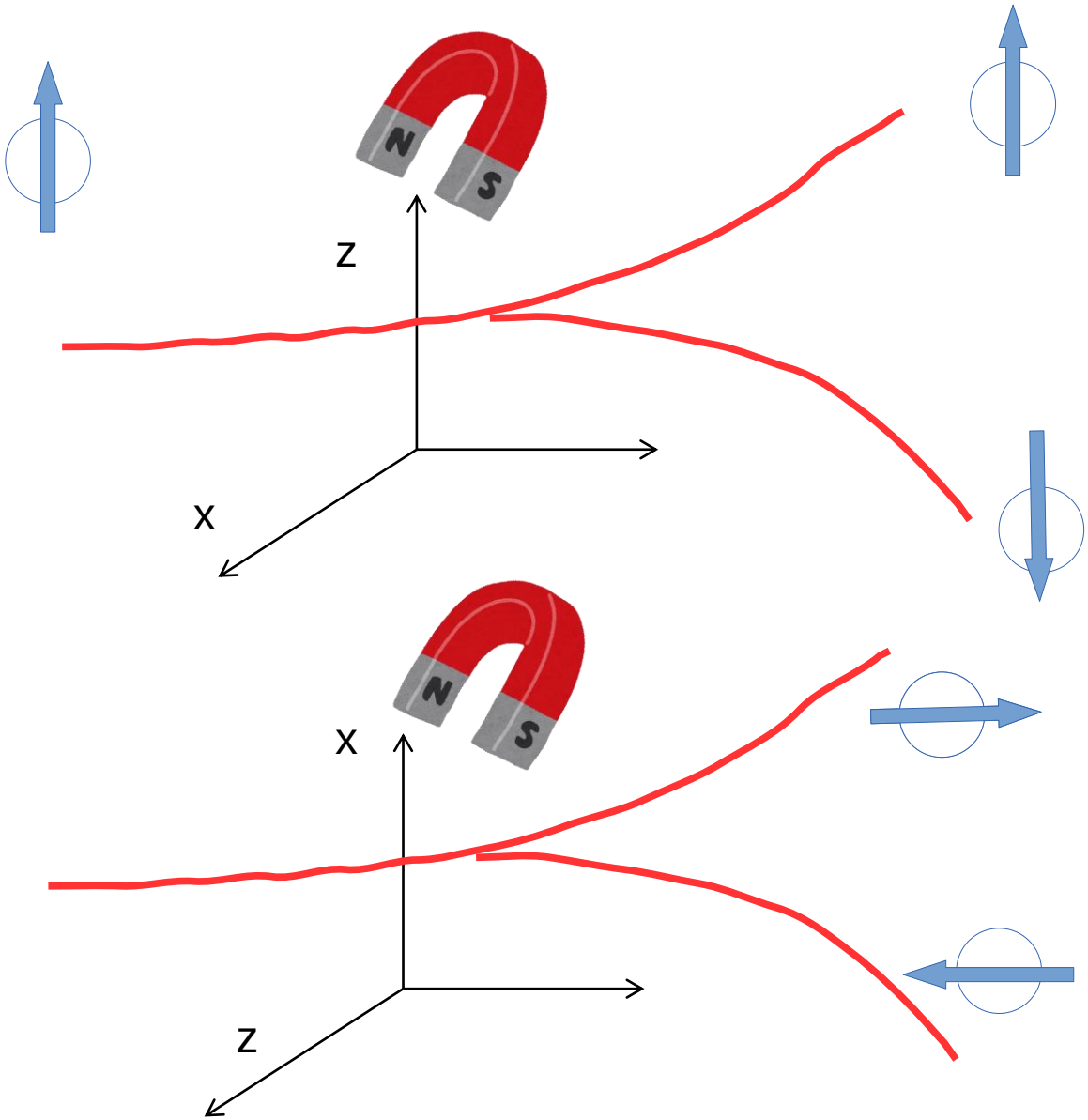
1982：ファインマン　量子コンピュータを提案

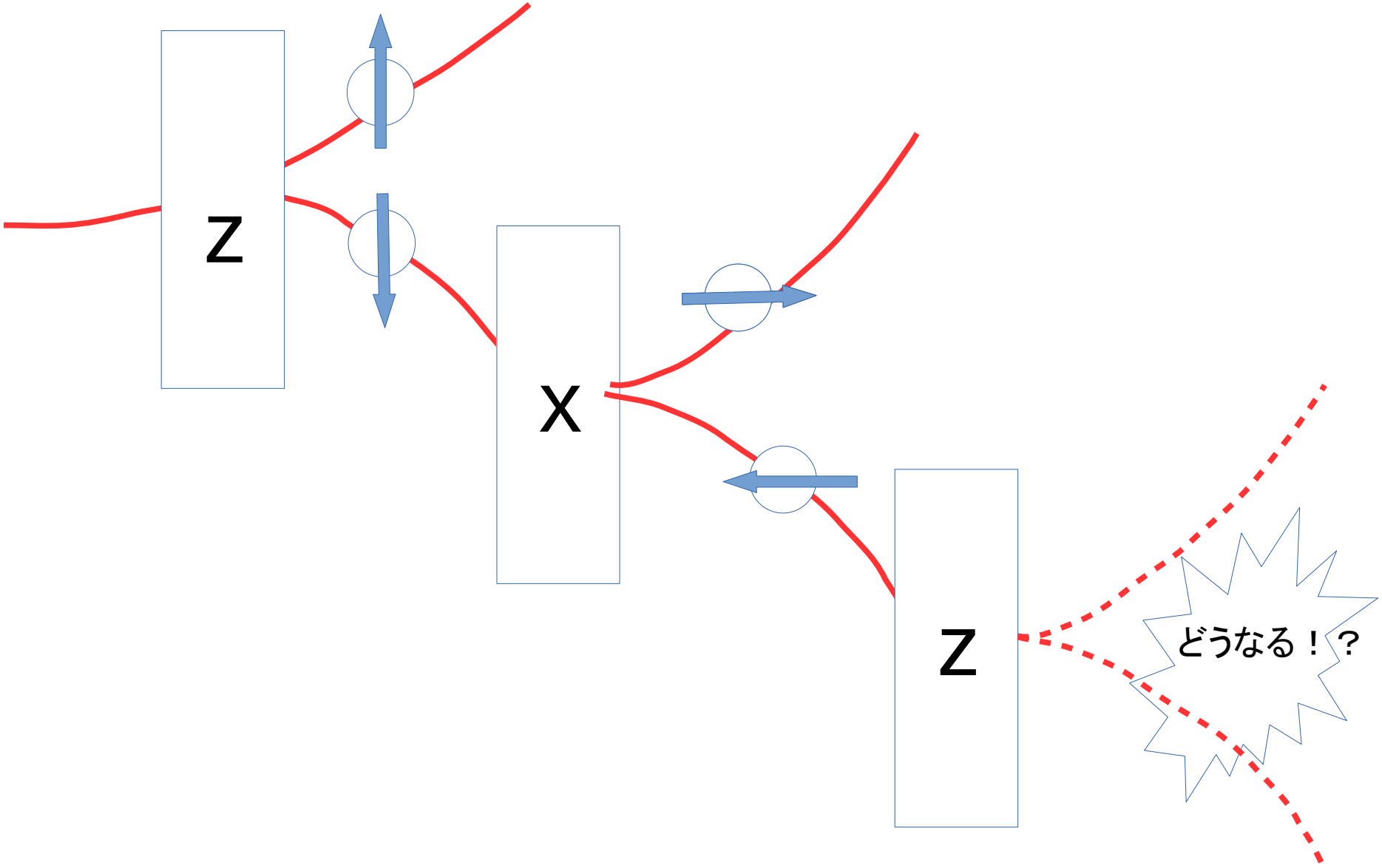
ファインマン
(from wikipedia)

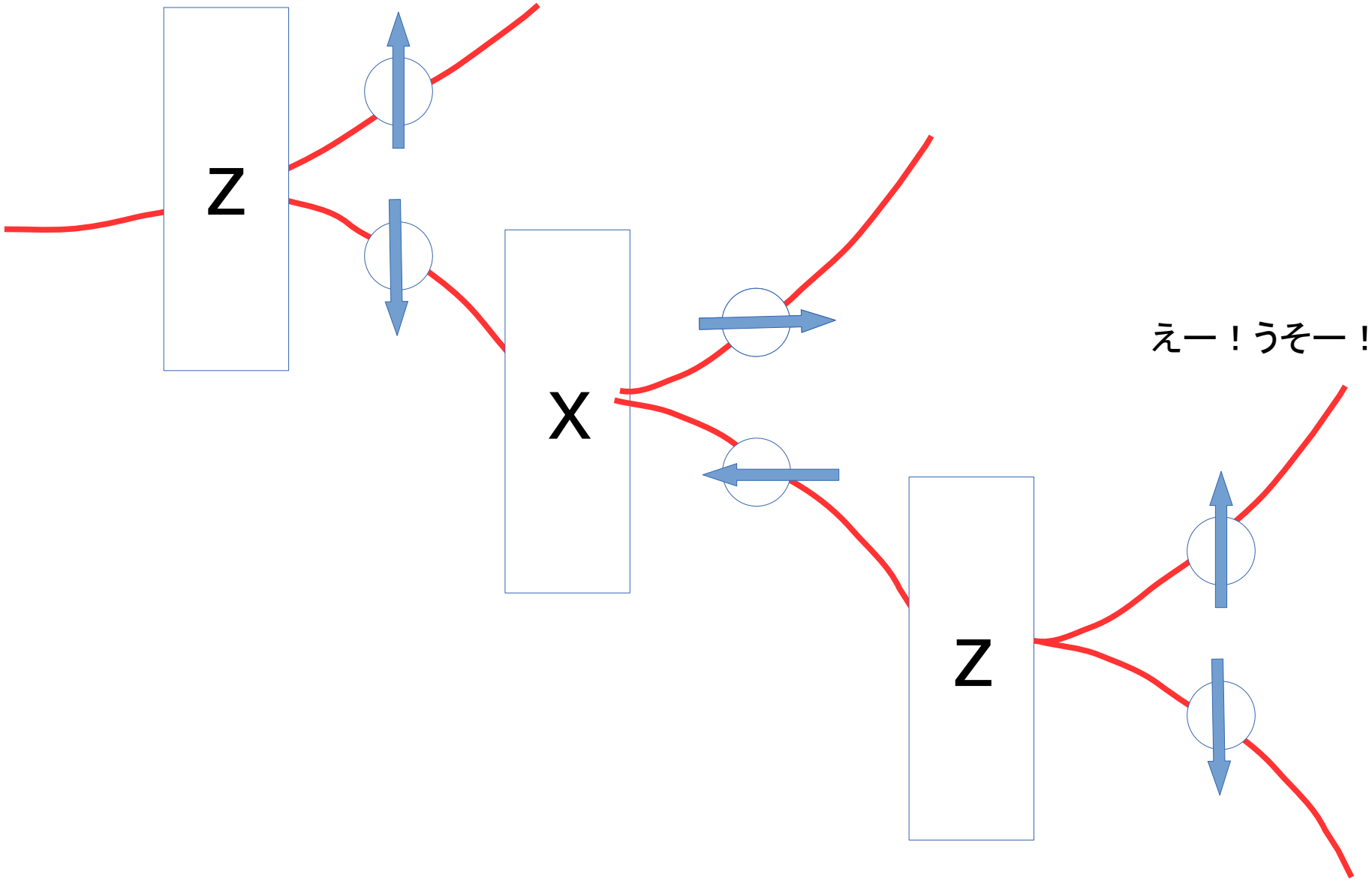
量子論はとっても変な理論

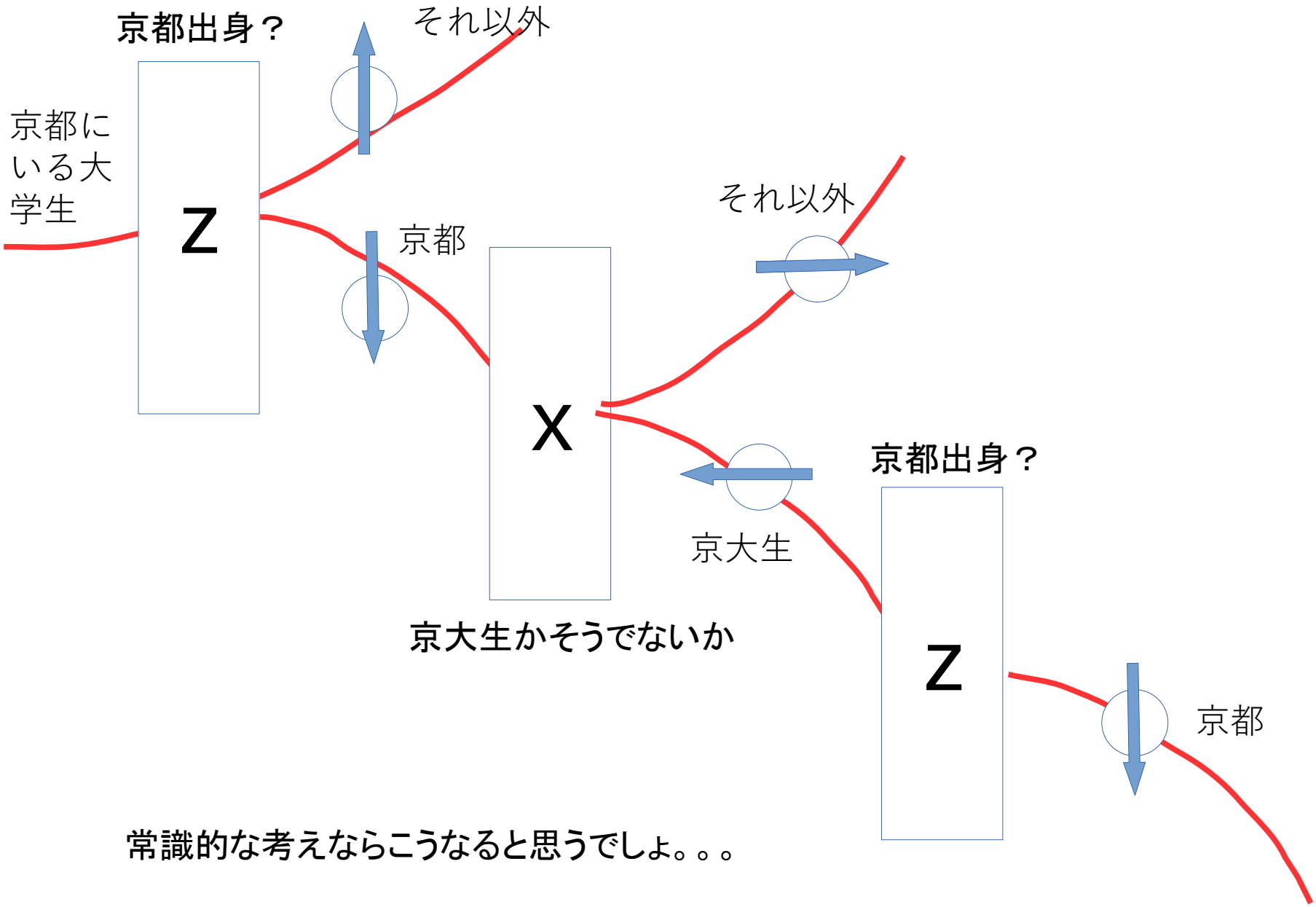
（シュテルンゲルラッハの実験：学部の量子力学で習う）

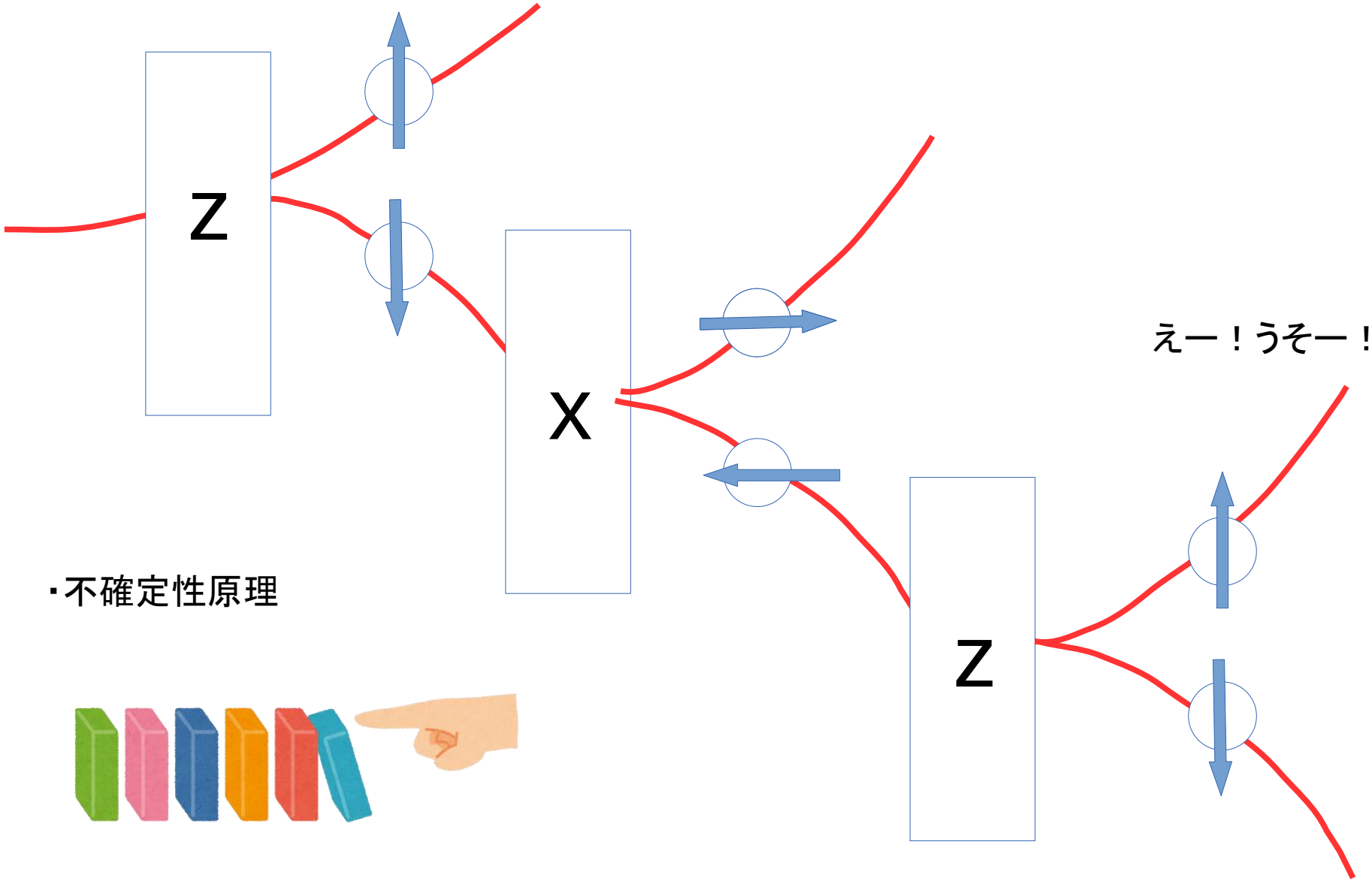
スピン：小さな磁石




Z
X
Z
どうなる！？


Z
X
Z
えー！うそー！


京都出身？
それ以外
京都にいる大学生
Z
京都
それ以外
X
京都出身？
京大生
京大生かそうでないか
Z
京都
常識的な考えならこうなると思うでしょ。。。



・不確定性原理

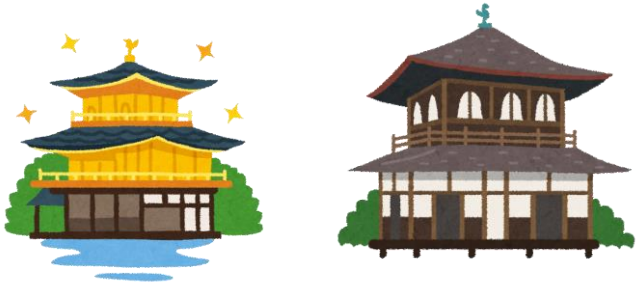
測定すると壊れる

他にも不思議な現象がいっぱい

・量子もつれ（エンタングルメント）

古典論ではありえない強力な相関

・量子的重ね合わせ

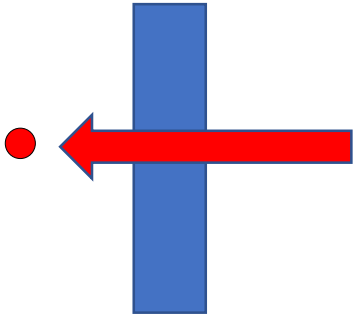


２つの状態を同時にとることが可能

・複製不可能性（No-cloning theorem）

コピーを作ることが不可能

・トンネル効果



そんな変な理論なんて間違っているのでは？

無数の実験的、理論的研究がこれまで行われてきているが、すべて量子論と矛盾しない。

→量子論は正しいと信じられている

例：地球はまるい

我々の常識：マクロ世界に基づいている
→ミクロ世界はマクロ世界と違っていた、というだけのこと

量子論基礎：量子論について研究する学問
量子情報：量子論は認めて、それを情報処理技術に応用する

じゃあ、量子論はどういう理論？

日常言語では説明できません。線形代数の知識が必要

状態：ベクトル
状態の時間発展：ユニタリ行列の作用
物理量：エルミート行列

線形代数の知識が必要。。。（大学1年教養レベル）

難しい数学を使わないで、普通の言葉で量子論を説明できないの？

→無理。そもそもそれに失敗して量子論が生まれた

日常言語では説明のできない不思議な世界を数学を駆使して理解していくという学問である量子物理を大学で勉強するのをおたのしみに！

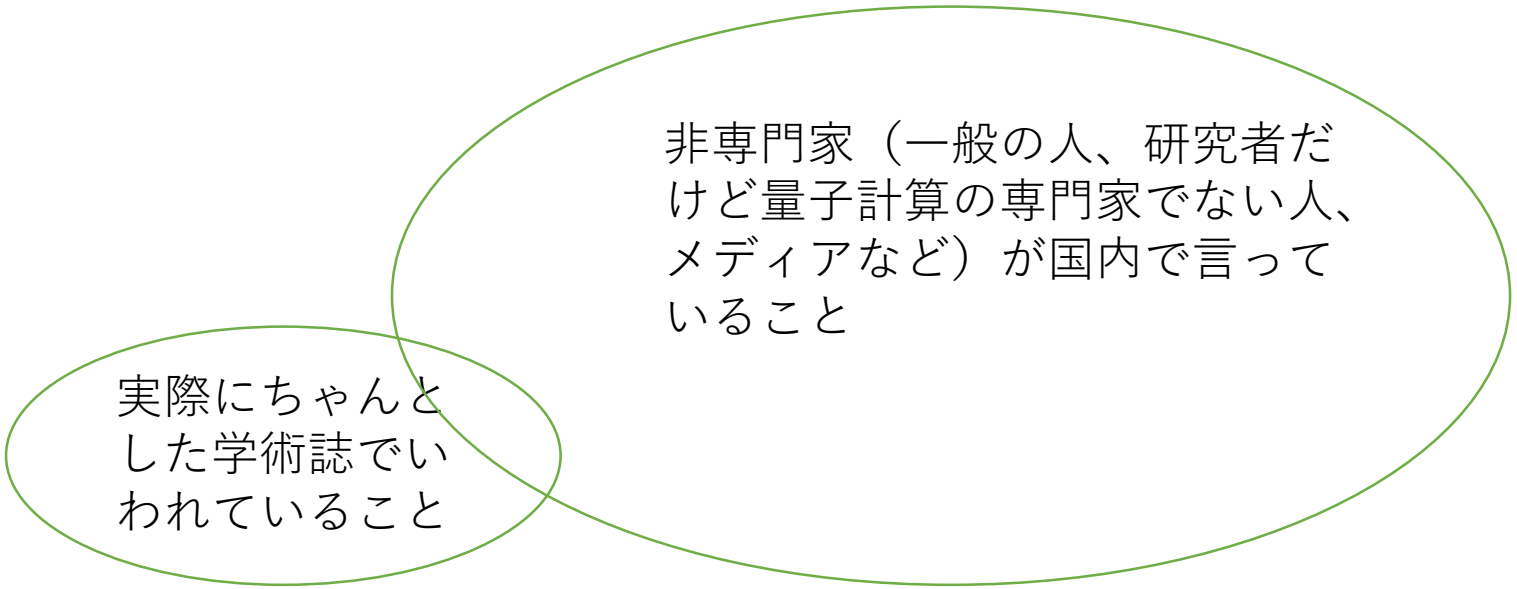
量子情報処理の主な応用

古典論には無い量子論特有の不思議な現象を情報処理に応用する

- 量子計算（量子コンピュータ）
- 量子暗号
- 量子センシング

量子計算

量子計算の一般向けの講演は非常にやりにくい。。。



間違った情報は巧みに正しいことも織り交ぜているので、
正しいことだけ話すと、それら間違ったことのお墨付きを与えてしまう。

間違った情報は派手な夢物語を言っているので、
正しいことだけ話すと、聞いた話とちがうじゃないか、とがっかりされる。

きをつけて！！

（1）数千「量子ビット」の「量子コンピューター実機」を実社会の組合せ最適化問題（配送ルートの最適化、薬の組合せ、ベットの配置等）に適用しました！という話は量子コンピューターとは関係ない！

→量子の性質を使ってそれらが古典のベストのアルゴリズムより高速に解けているという科学的証拠はないにもかかわらず、高速性の保証された量子コンピューターであるかのように錯覚させている

（2）量子コンピューターを「疑似的に」模した「疑似量子コンピューター」は量子コンピューターとは関係ない！

→（1）で述べた、量子コンピューターとは関係ないしろものを疑似したものなので、量子コンピューターとは全く関係ない

量子計算のおおざっぱな歴史

ファインマン
(from wikipedia)

量子多体系をコンピューターでシミレートするのは大変だなあ。
量子系でやっちゃえばいいのでは！？

１９８２年

ドイチュ
(from his HP)

量子計算だとすごくマニアックな問題が高速にとけるよ

１９８５年

ショアー
(from his HP)

量子計算だと素因数分解が高速にとけるよ

１９９４年

量子ビット

量子ビット：０と１の量子的重ね合わせ

→確率1/2 で０と１が出るという意味ではない！！！

量子的重ね合わせ　|0> と |1> の線形結合

→どういう意味？それ以上は説明不可。

量子計算機ではこのような状態を作ることができる

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

ルート２分の１の確率？？
負の確率？？

日常言語では説明不可能。

高速な量子アルゴリズムの例

（１）Shorの素因数分解アルゴリズム（１９９４）

素因数分解を高速に行うことができる　→　今の公開鍵暗号が危険に

（２）Groverの検索アルゴリズム（１９９６）

データーベースの検索が高速に（ただし指数）できる

（３）HHLアルゴリズム（２００９）

線形連立方程式の計算が高速にできる（ただし量子入力・量子出力）

高速な量子アルゴリズムがばんばん生み出され、実社会ですでにいろいろな問題を高速に解いている！スマホが速くなる！

→間違い！　人工的な設定で理論的な高速性が示されているだけに過ぎない

素因数分解アルゴリズム

素数の掛け算を計算するのはかんたん

３×５×５×７×２３×１９×…×９７＝？

素数の掛け算に分解するのはむつかしい

139585769998574=?

一方向性関数

$$x \to f(x): easy$$

$$f(x) \to x: hard$$

暗号に応用されている！

Shorのアルゴリズムを使うと量子計算機で解けてしまう
→量子計算機でも解けないような暗号が研究されている（格子など）

検索アルゴリズム

Nページの電話帳から山田太郎さんの電話番号を検索したい

→あいうえお順なので簡単

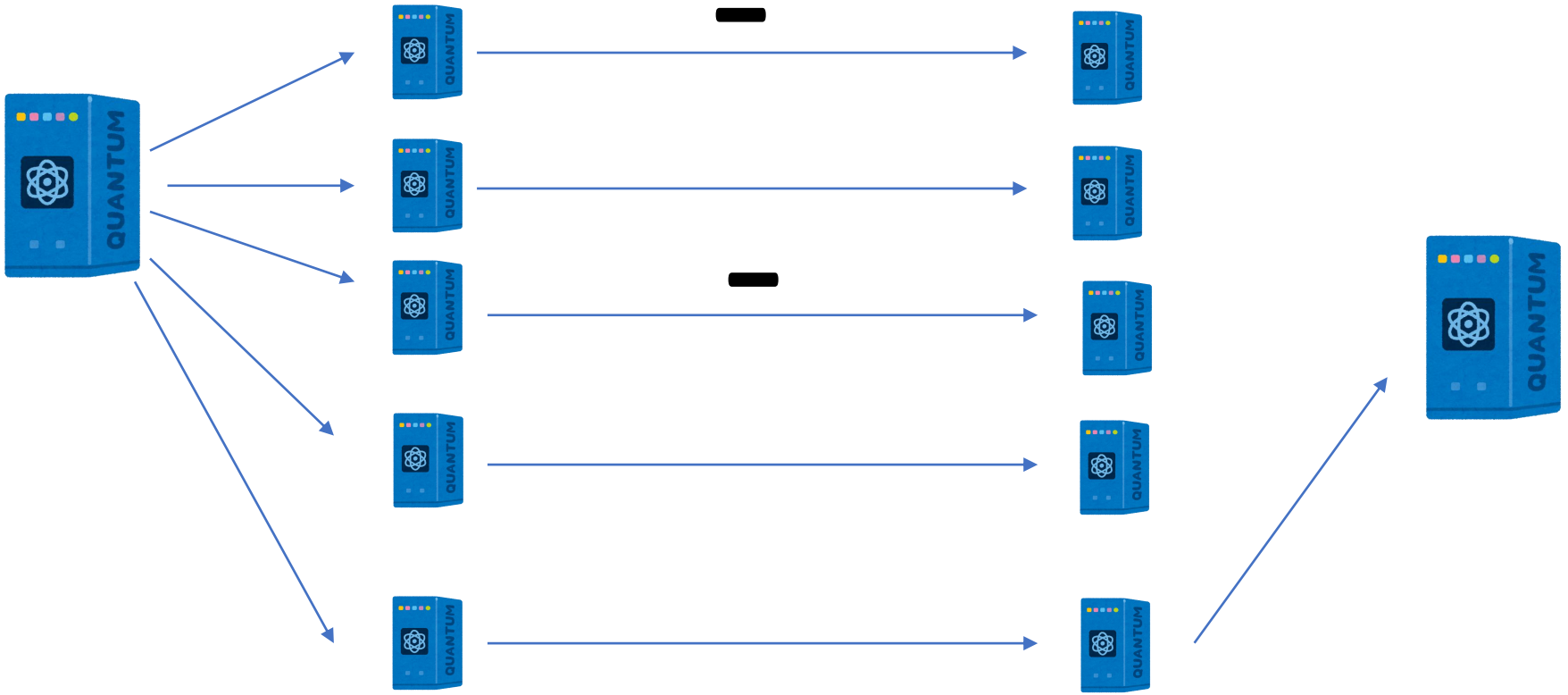
→もしランダムに並んでいたら？

古典計算機だとN時間かかる。

Groverのアルゴリズムを使うと$\sqrt{N}$時間になる！

なぜ速いの？

なぜ速いのかはまだ完全には理解されていない。
一つの典型例：重ね合わせ＋負の確率でうちけし。

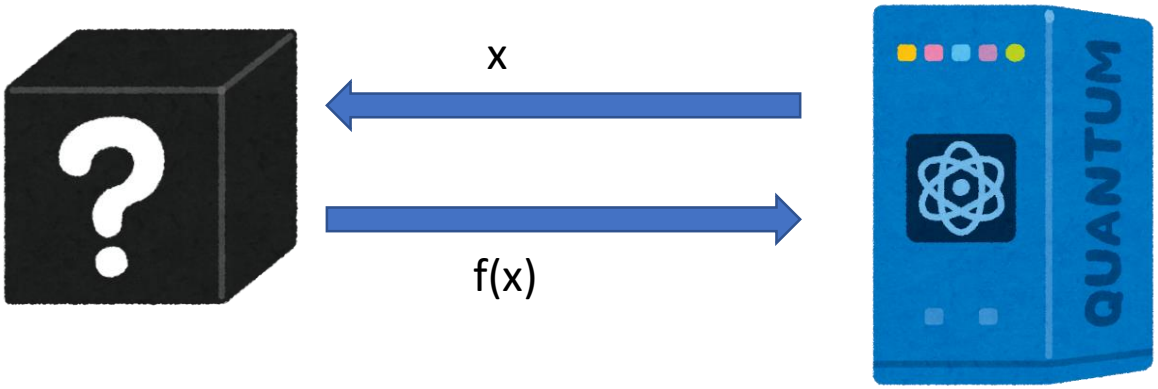


注意！！！！！！！！

この方法で高速化ができる事例は、問題が特定の構造を持っていて、それをたまたまうまく使えた場合のみ。（素因数分解等の非常にレアなケースのみ）

ほとんどの場合、構造をどうやって使って「うちけし」をしていいかさっぱりわからない。（研究者たちが長年考えているがさっぱりわからない。）

構造がなく、しらみつぶしにやらないといけない場合には、量子計算でも指数時間かかることが２４年前にすでに示されている。[SIAM J. Comput. 26, 1510 (1997)]



量子的な重ね合わせでとにかく並列にやればなんでもかんでも高速になるという話ではない

あれ、でも、工場のシフトや病院のベットの最適配置、車のルート、いろいろな薬品の組み合わせ等の実社会におこる様々な組合せ最適化問題を、「量子コンピューターを用いて」重ね合わせですべてのパターンを並列処理することにより「高速」に解いた、というニュースをよく見るけど？

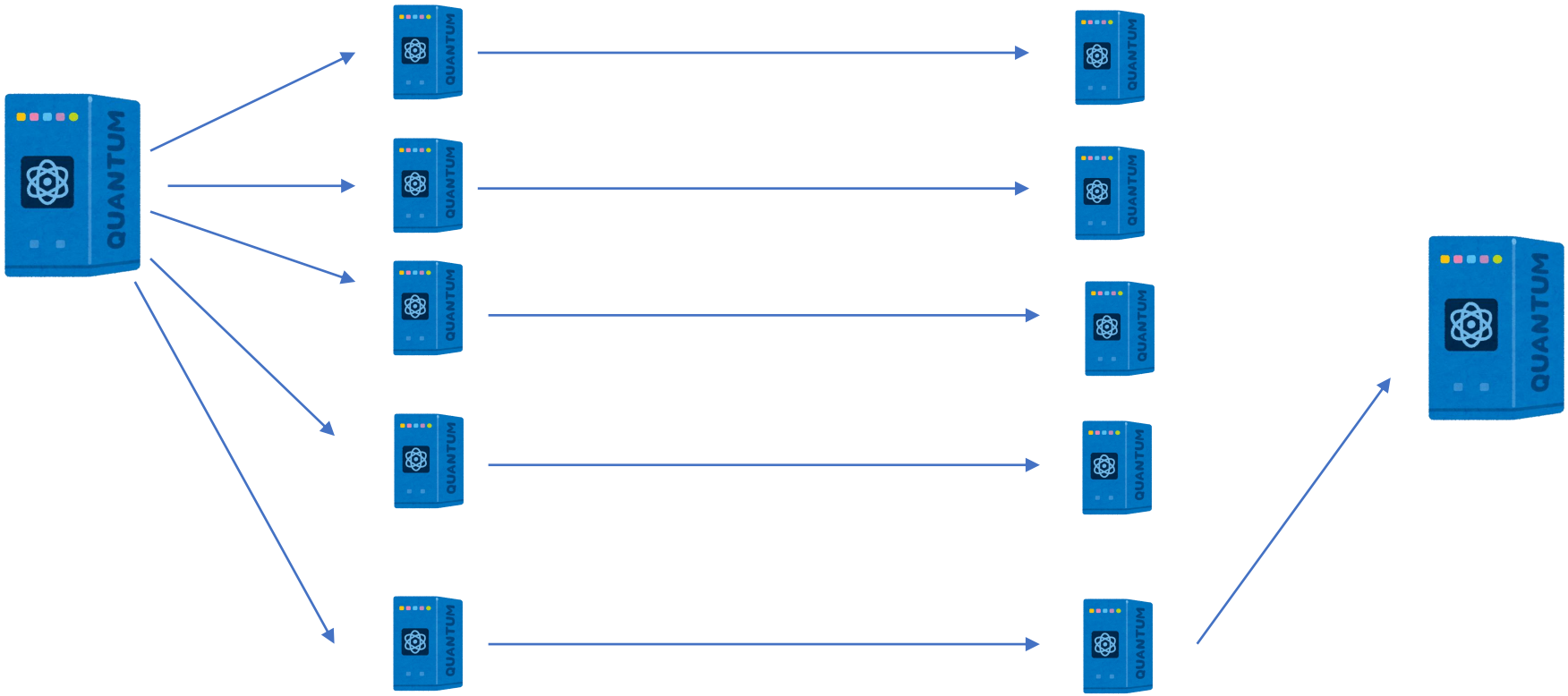
→それは量子コンピューターではありません。

量子を使って古典より高速計算ができている証拠はありません

時間さえかければ古典でも代用可

量子計算機はすごいといっても、なんでもできるわけではない。

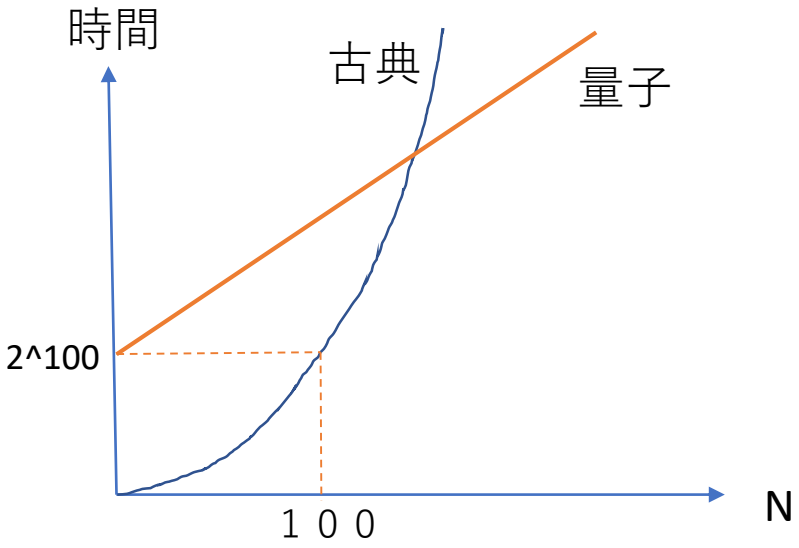
量子計算機は、指数時間かけてよいなら古典計算機でシミレート可能。
→古典計算機で指数時間かけても解けない問題は量子計算機でも解けない



量子計算が速いの意味

漸近的な意味であることに注意！

例：
古典計算だと2^N時間かかる
量子計算だとN+2^100時間で解ける



100量子ビット以下だと古典のほうが速い

→量子が古典に負けていることを意味しない！

十分大きな量子ビットでは量子が勝つようになる

何量子ビットまでできたら量子超越性が達成できるんですか？
という問いは意味を持たない

量子性があるなら速いとは限らない

計算機が量子系なら常に自動的に速くなるというわけではない。

例：クリフォード回路

→エンタングル状態を作るけど、古典でシミレート可能

「量子性がでている」だけでは駄目で、「量子性が高速化にきいている」ことを示さないといけない！

そろばんにレーザーポインターくっつけたら量子コンピューターになるんか

量子計算機は常に古典より高速というわけではない

量子計算機は古典計算機の上位互換なので
（1）量子計算機＞古典計算機
（2）量子計算機＝古典計算機
のどちらか

（1）の場合、（2）の場合ともに事例が知られている。

どういう時に（1）になり、どういう時に（2）になるのかという一般的な理解はまだ全然できていない
→まさに最先端の研究テーマ

まとめ

- 量子の不思議な性質を使って高速計算をするのが量子計算機
- 素因数分解、検索、連立方程式の計算等で高速になる例が知られている
- なぜ、いつ、速くなるかはまだ完全に解明されていないが、重ね合わせ＋うちけしを使うのが典型的
- 重ね合わせ＋うちけしで高速化できるのは非常に限られた人工的な場合のみしか知られていない。なんでもかんでも量子的並列処理で速くなるわけではない。
- 実際の現場の組合せ最適化問題に投入されている「実機」は量子コンピューターではない。要注意！！

量子暗号

暗号

もともとは敵に秘密にメッセージを送る手段だった

A国の司令官

B国の盗聴者

B国に潜入しているA国のスパイ

ワンタイムパッド

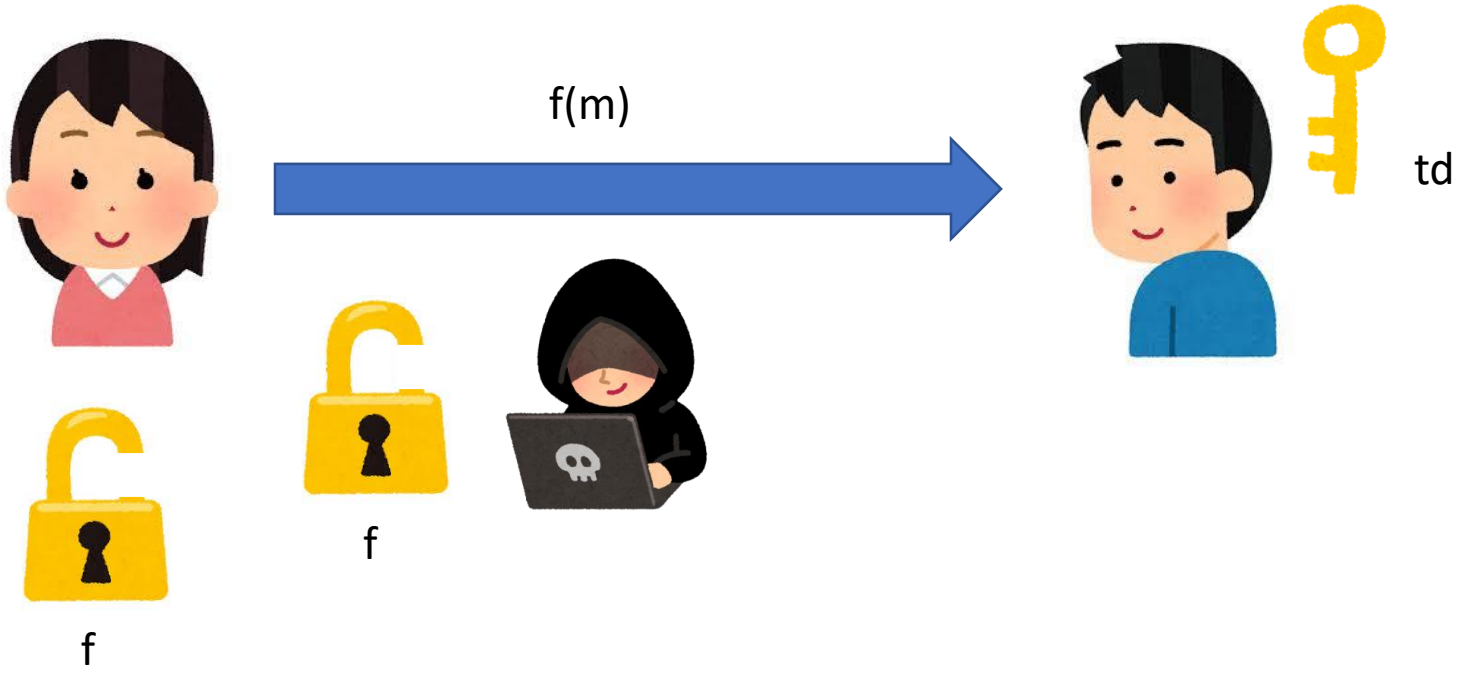
情報理論的安全な暗号通信が可能

米国とロシアの大統領間のホットライン：鍵を厳重な警備のもと運ぶ

鍵をどうやって共有する？→鍵配送問題

公開鍵暗号

Diffie and Hellman　1976



カギをかけるのは誰でもできる
カギを開けるのは特定の人のみ可能

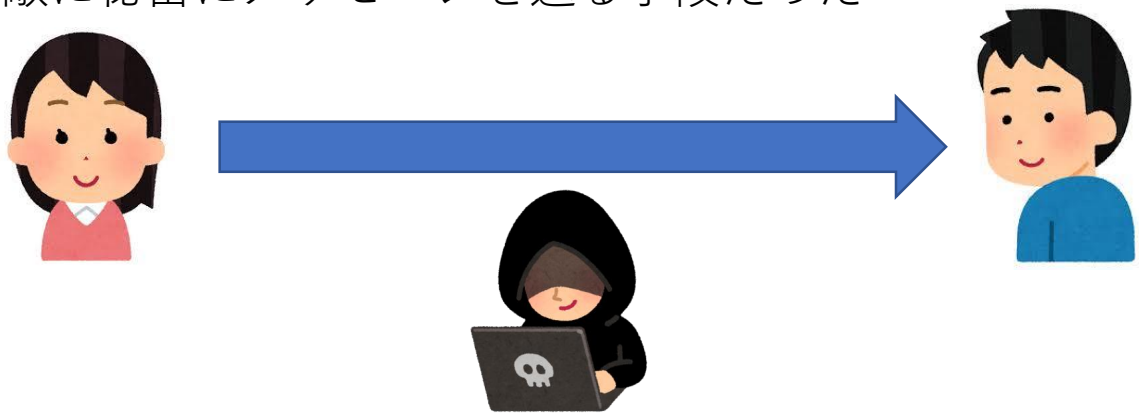
m→f(m)は簡単
f(m)→mは難しい。しかし、tdがあれば簡単

トラップドア関数を使用：安全性は計算量的なものになる

注：本当の作り方はもう少し複雑

暗号

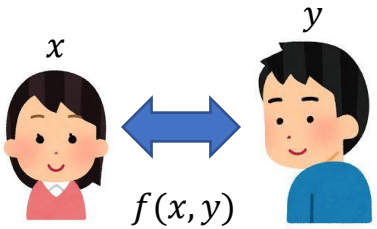
もともとは敵に秘密にメッセージを送る手段だった



暗号というのは秘密にメッセージを送るだけのものではない。

電子署名

コミットメント



多者間計算

→今では一般の人が日常的に暗号の
お世話になっている

ここまでのまとめ

（１）暗号の安全性には2種類ある

情報理論的安全性：絶対に安全。例：ワンタイムパッド

→安全性は高いが機能が少ない

計算量的安全性：ある問題（素因数分解など）が難しいなら安全。例：公開鍵暗号

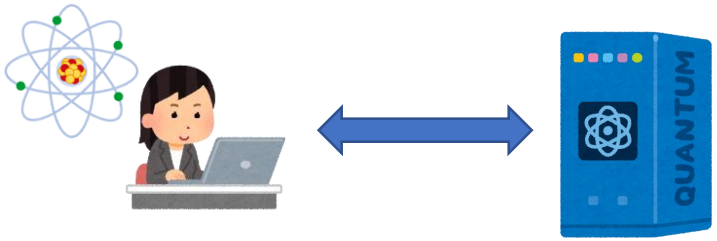
→安全性は低いが機能が多い

（２）暗号というのは秘密にメッセージをおくるだけではなく、いろいろな有益な機能がある。

量子暗号

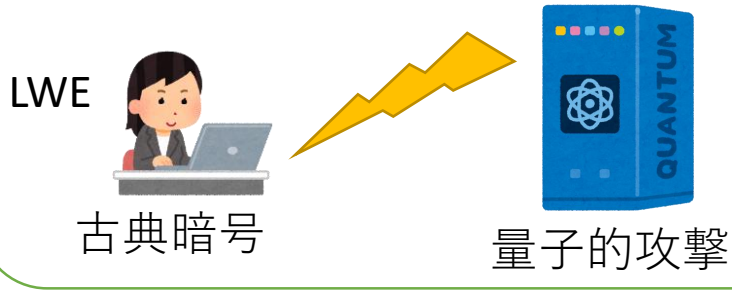
量子暗号の研究は2種類に分類することができる。

（1）量子暗号プロトコル：量子を用いて様々な暗号タスクを実現する研究。



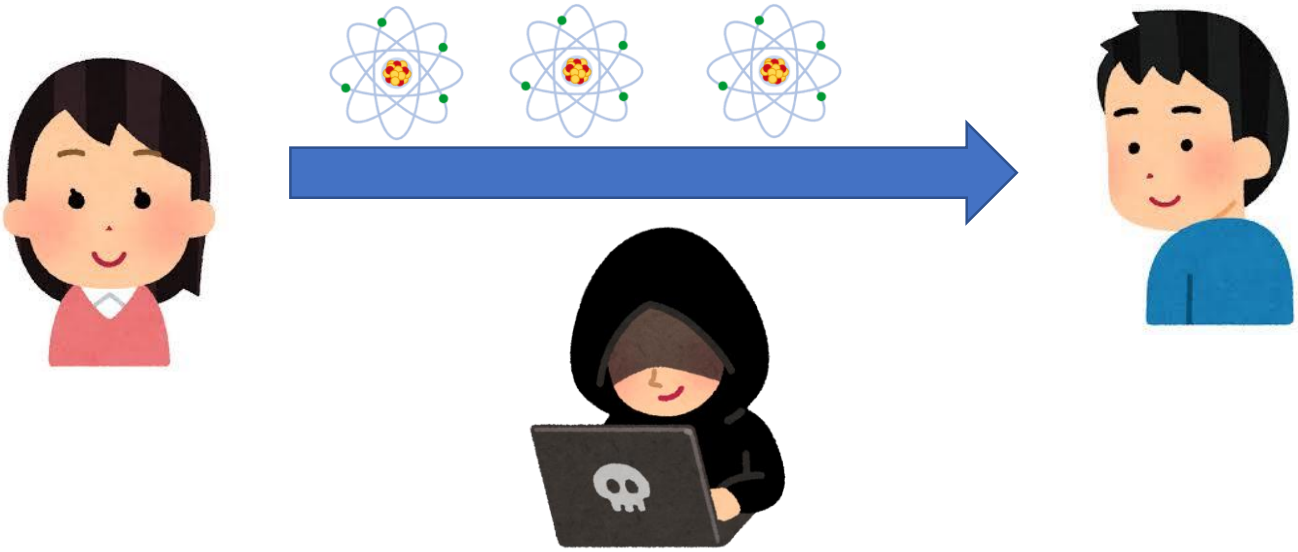
量子の性質（No-cloning等）に基づくため、情報理論的安全なものが多い

（2）耐量子暗号：古典の暗号の量子的攻撃に対する安全性を研究する。



量子鍵配送

Bennett and Brassard 1984



量子的な粒子を送る

不確定性原理：測定すると壊れてしまう

盗聴するとばれる

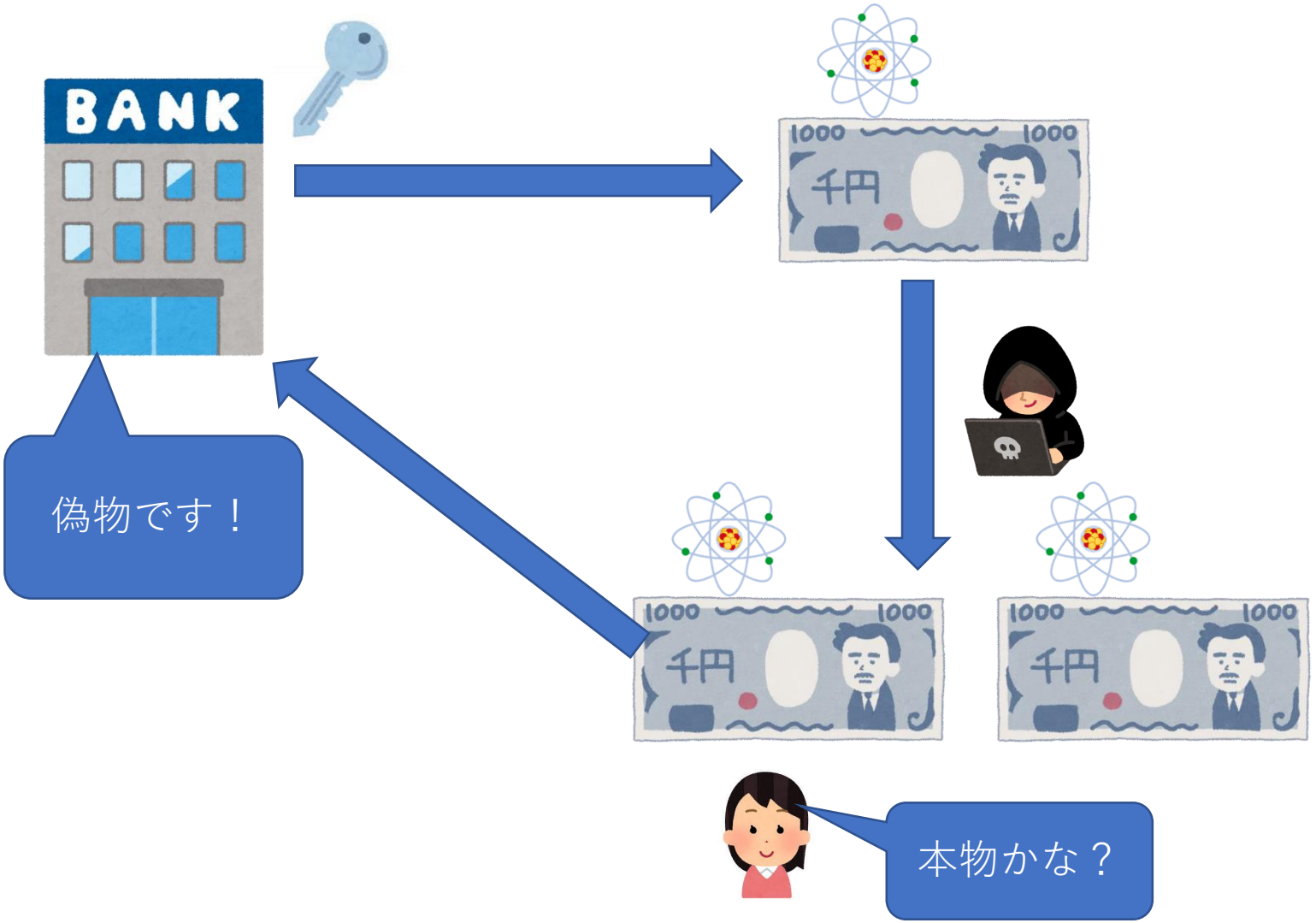
安全性は情報理論的！

→公開鍵暗号は計算量的　→量子のおかげで強力な暗号が実現！！

量子マネー

No-cloningを使って偽造できないお金を作る！

Wiesner 1970 (1983)



クラウド量子計算のセキュリティ

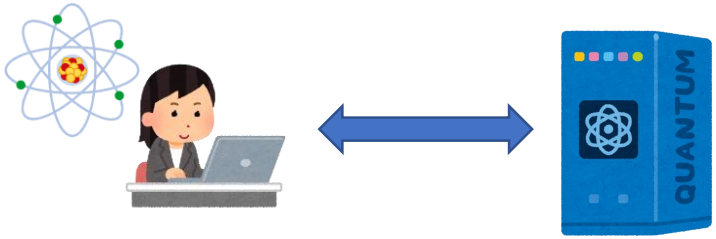
量子サーバー

通信路

利用者（古典計算のみ）

サーバーに計算内容を秘密にできるか？
サーバーが正しい量子計算を行っているかチェックできるか？

量子暗号プロトコル：量子を用いて様々な暗号プロトコルを実現する研究。



主に情報理論的安全なものが多い

量子の不思議な性質を使う

量子計算機を騙す

あたらしい機能！
[Brakerski et al., Mahadev 2018]

耐量子暗号：古典の暗号の量子的攻撃に対する安全性を研究する。

Quantamagazine | Physics | Mathematics | Biology | Computer Science | All Articles

QUANTUM COMPUTING

Graduate Student Solves Quantum Verification Problem

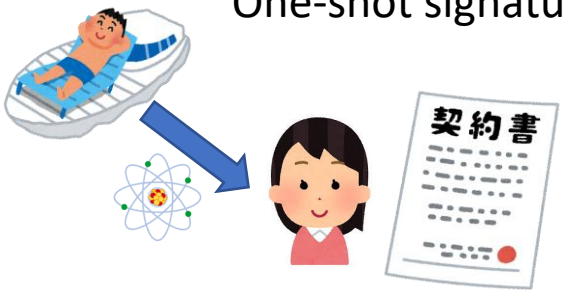
72

Urmila Mahadev spent eight years in graduate school solving one of the most basic questions in quantum computation: How do you know whether a quantum computer has done anything quantum at all?

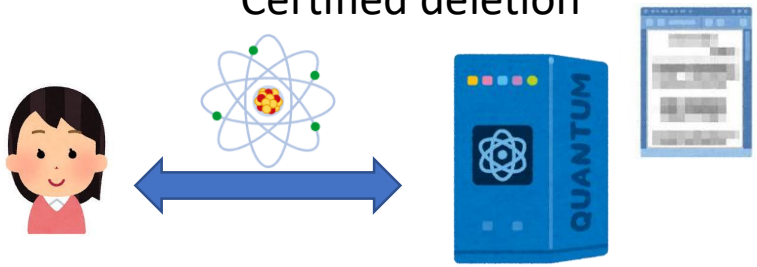
耐量子暗号を組み合わせることにより、古典通信でもセキュアクラウド量子計算が可能！ [Mahadev, FOCS2018]

新しい機能の例

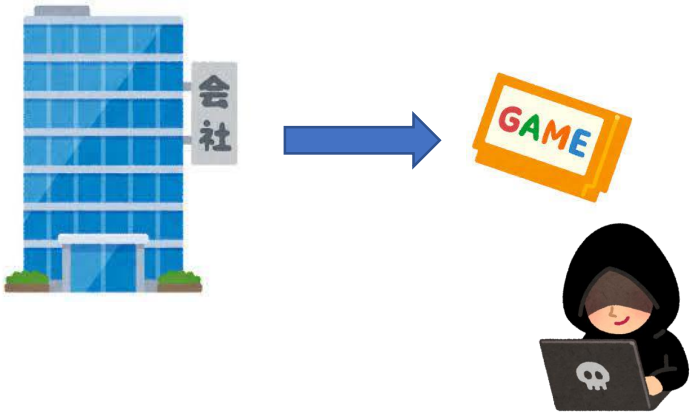
One-shot signature



Certified deletion

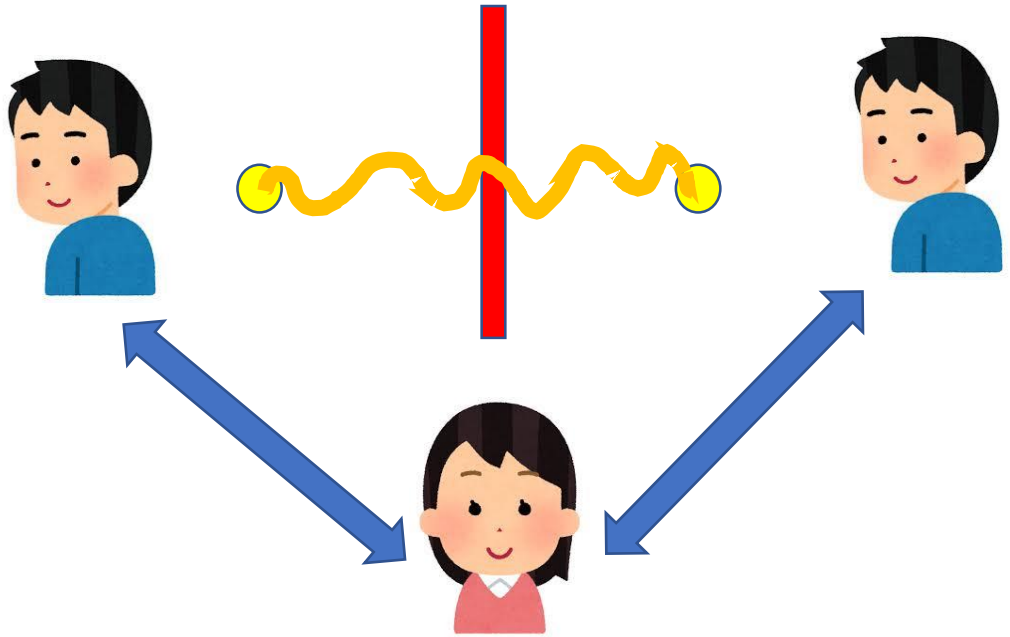


Quantum copy protection



ベルの不等式

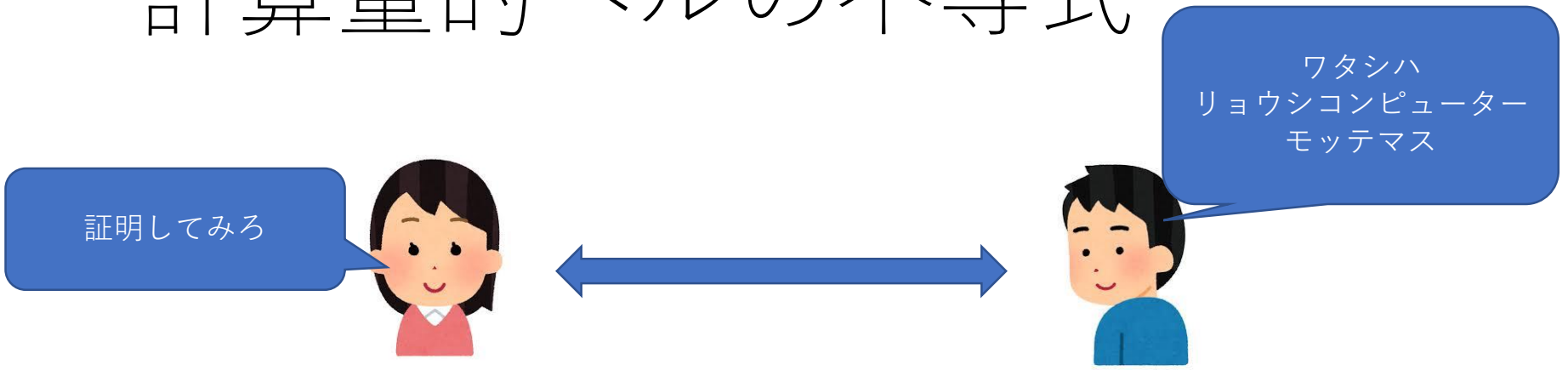
２０２２物理賞



（１）ボブたちがエンタングルメントを共有しているとアリスは受理
（２）ボブたちがエンタングルメントを共有していないとアリスは受理しない

Unconditionalにproof of quantumnessが達成できる！　ただし、二人のボブが通信できないという仮定が必要

計算量的ベルの不等式



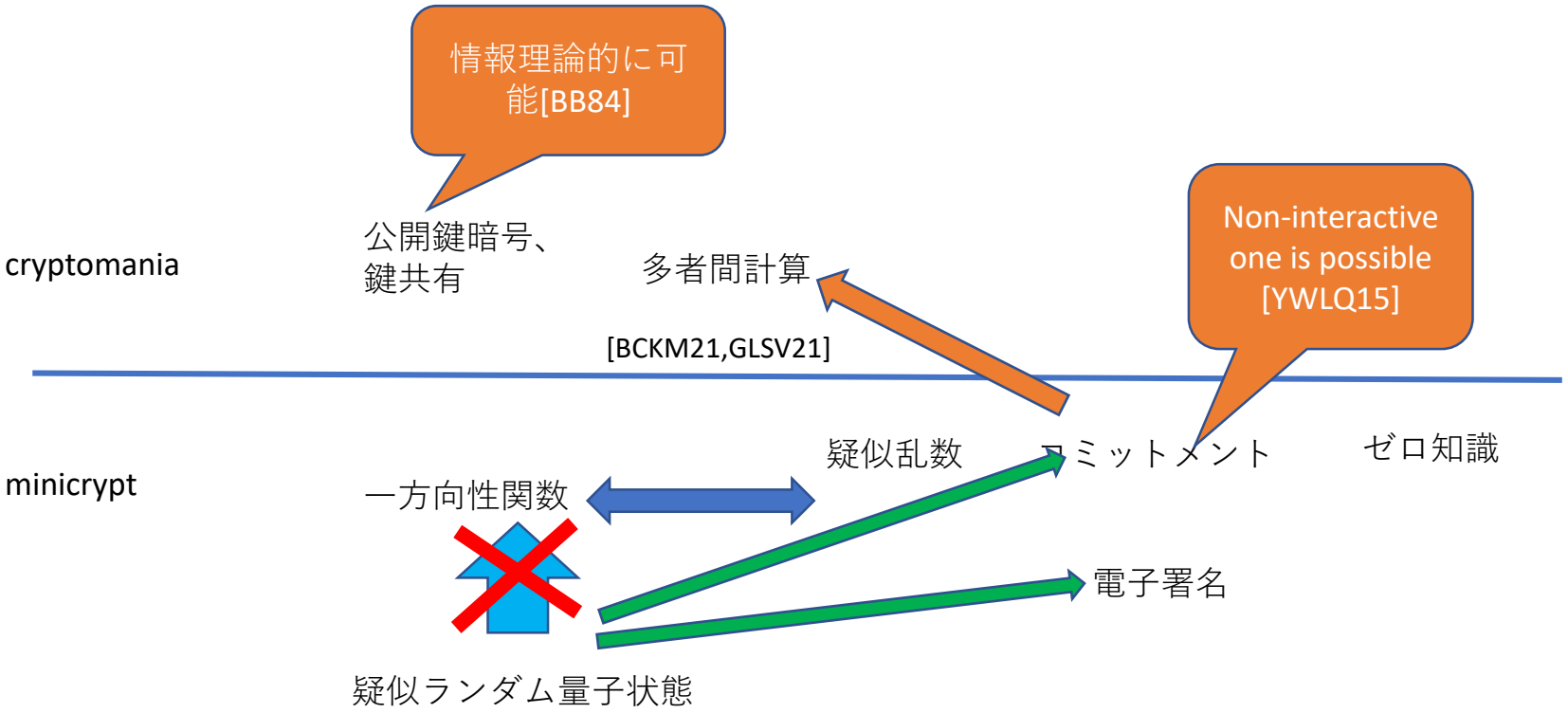
BQP⊆PSPACEなのでボブが一人だと計算量的仮定が必要になる

これまでの「計算量的ベルの不等式」はCollision resistanceを仮定：
Brakerski-Christiano-Mahadev-Vazirani-Vidick FOCS 2018
Brakerski-Koppoula-Vazirani-Vidick TQC2020
Kahanamoku-Meyer-Choi-Vazirani-Yao Nature Phys. 2022

Collision resistance:
$f(x) = f(x')$なるx, x'を見つけるのは計算量的に困難（例えばLWEを仮定）

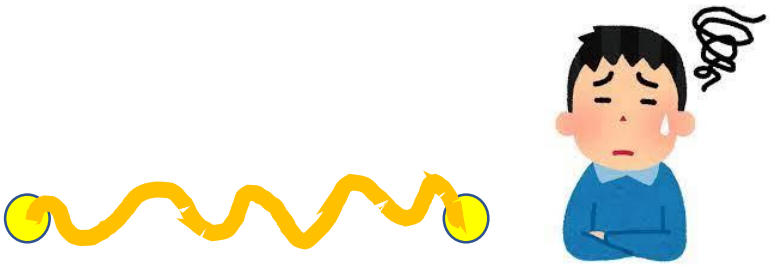
新しい結果：
Trapdoor
permutationで
できた！

$$f: \{0,1\}^n \to \{0,1\}^n$$
$$x \to f(x): easy$$
$$f(x) \to x: hard$$
$$(easy\ with\ trapdoor)$$



量子暗号における最も基礎的な仮定はなにか！？

量子暗号→ブラックホール！？



ブラックホールのパラドックスを説明するためには
「原理的には取り出せるけど、取り出すのが非常に難しい、隠れたエンタングルメント」が必要

量子暗号において、「実際は異なるけど、区別するのが非常に難しい量子状態のペア」が重要な働きをする

→これをつかうと、上記のような隠れたエンタングルメントが作れる！

Brakerski, arXiv: 2211.05491

まとめ

- 量子暗号プロトコル：量子を使って、秘密にメッセージを送るだけでなく、偽造できないお金や、電子署名、クラウドのセキュリティなど、いろいろな暗号タスクが可能。

- 耐量子暗号：量子計算機ができても安全な（古典）暗号についても研究されている

- 両者のハイブリッドによる新しい量子暗号プロトコルが近年さかんに研究されてきている

END