量子計算と量子暗号

森前智行
京都大学基礎物理学研究所
（３０分）

内容（３０分）

- 量子論とは（１０分）
- 量子計算（１０分）
- 量子暗号（１０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

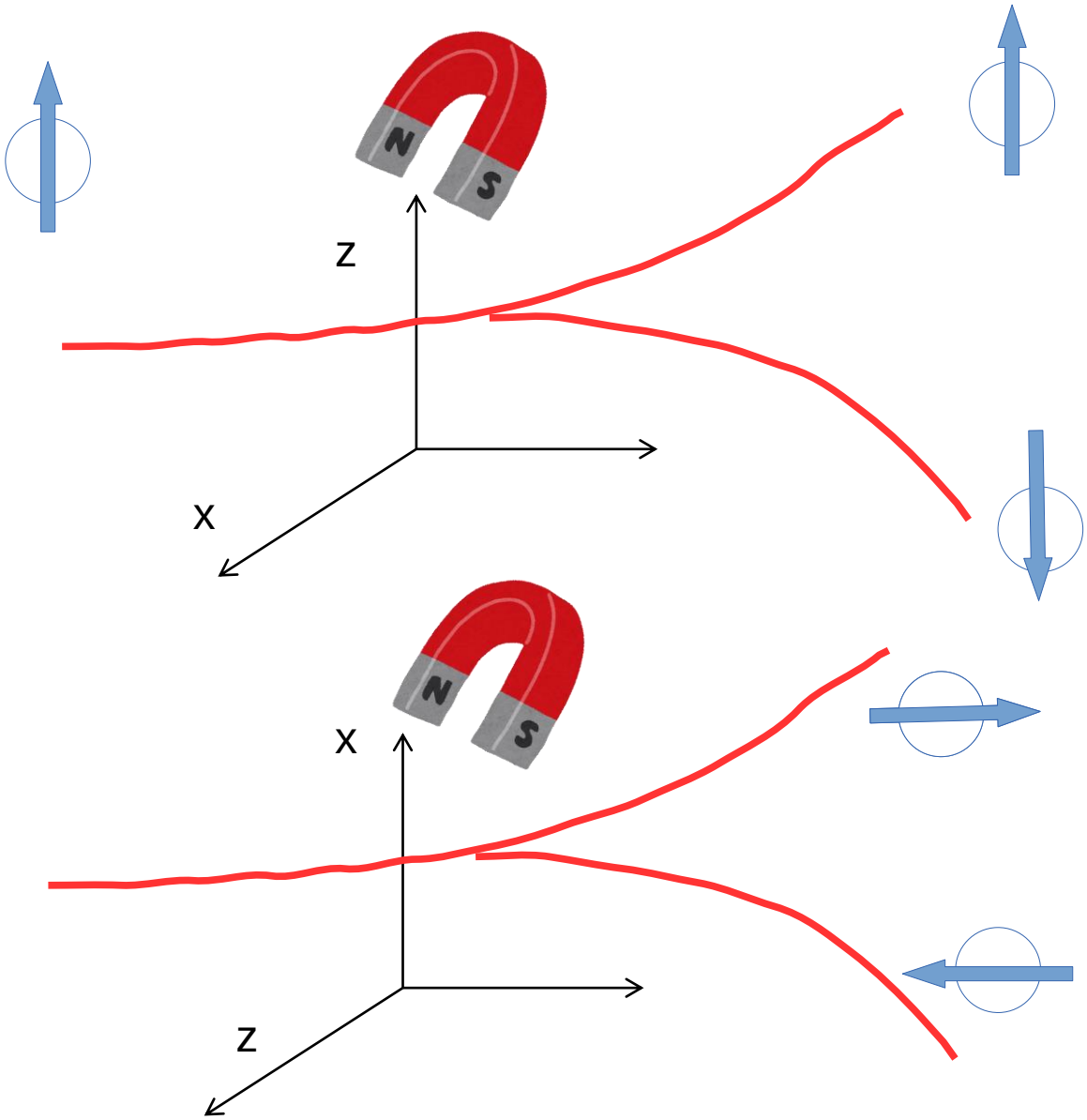
1970：ウィズナー　量子マネー

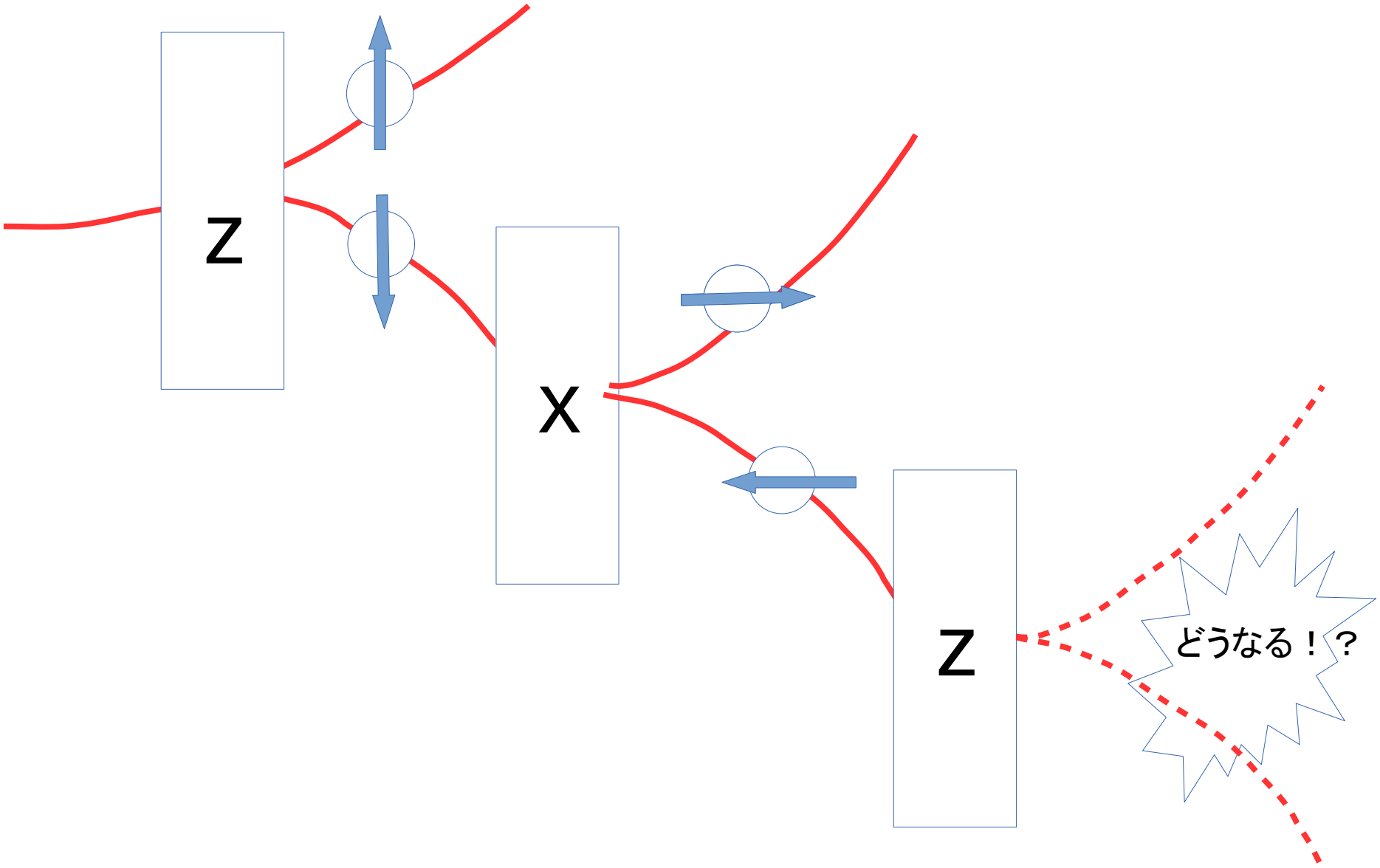
1982：ファインマン　量子コンピュータを提案

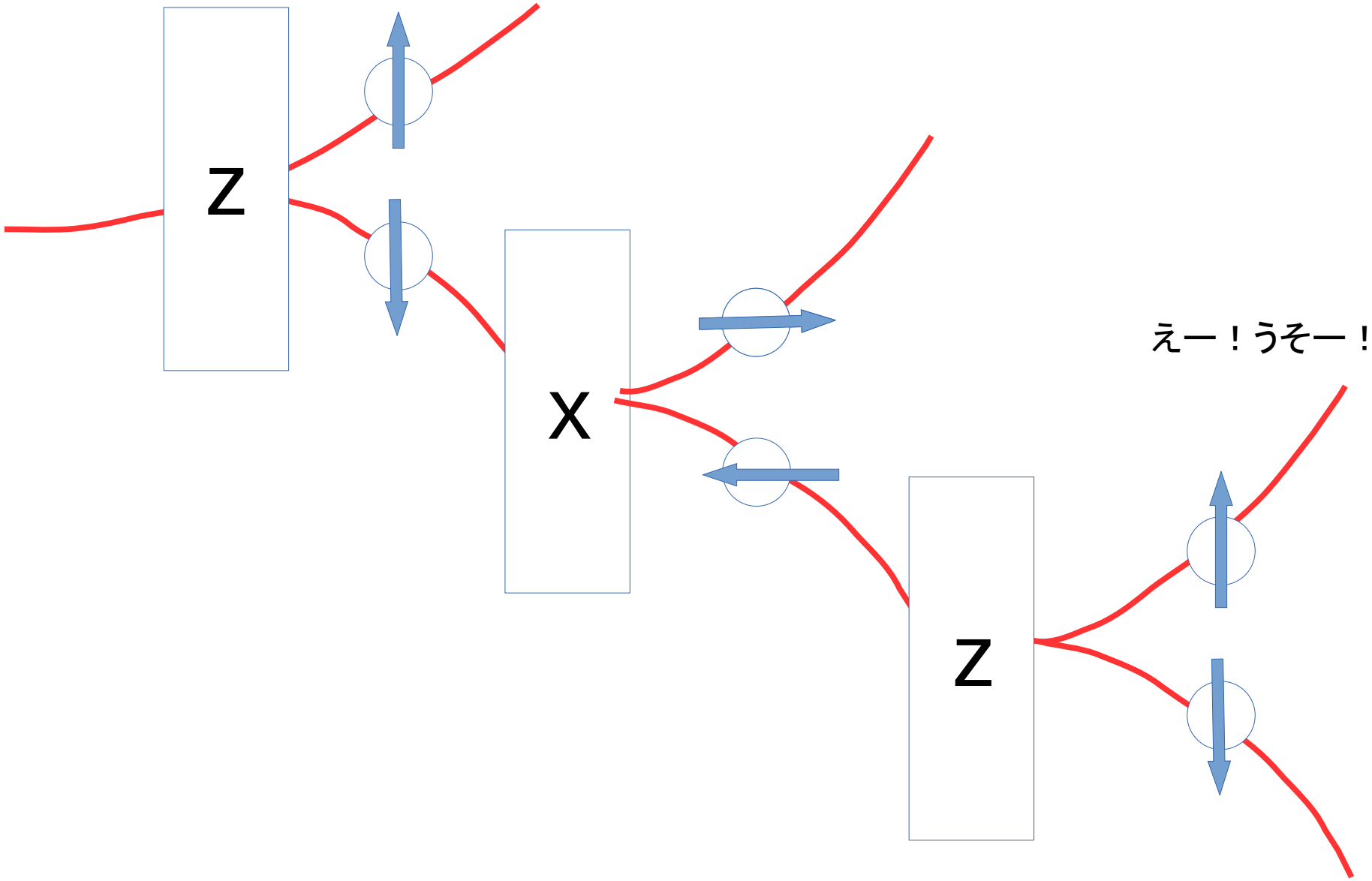
ファインマン

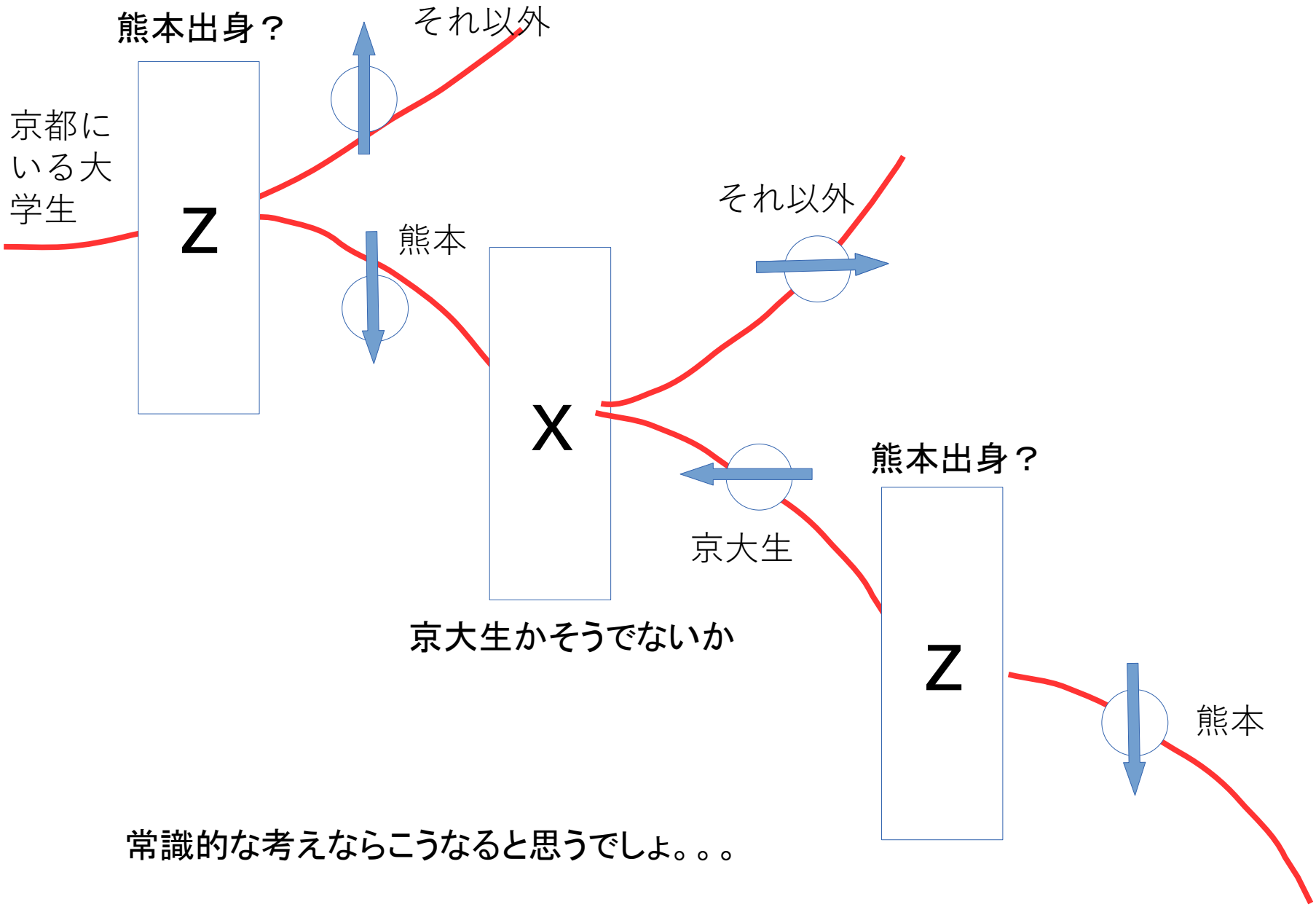
（シュテルンゲルラッハの実験：学部の量子力学で習う）

スピン：小さな磁石

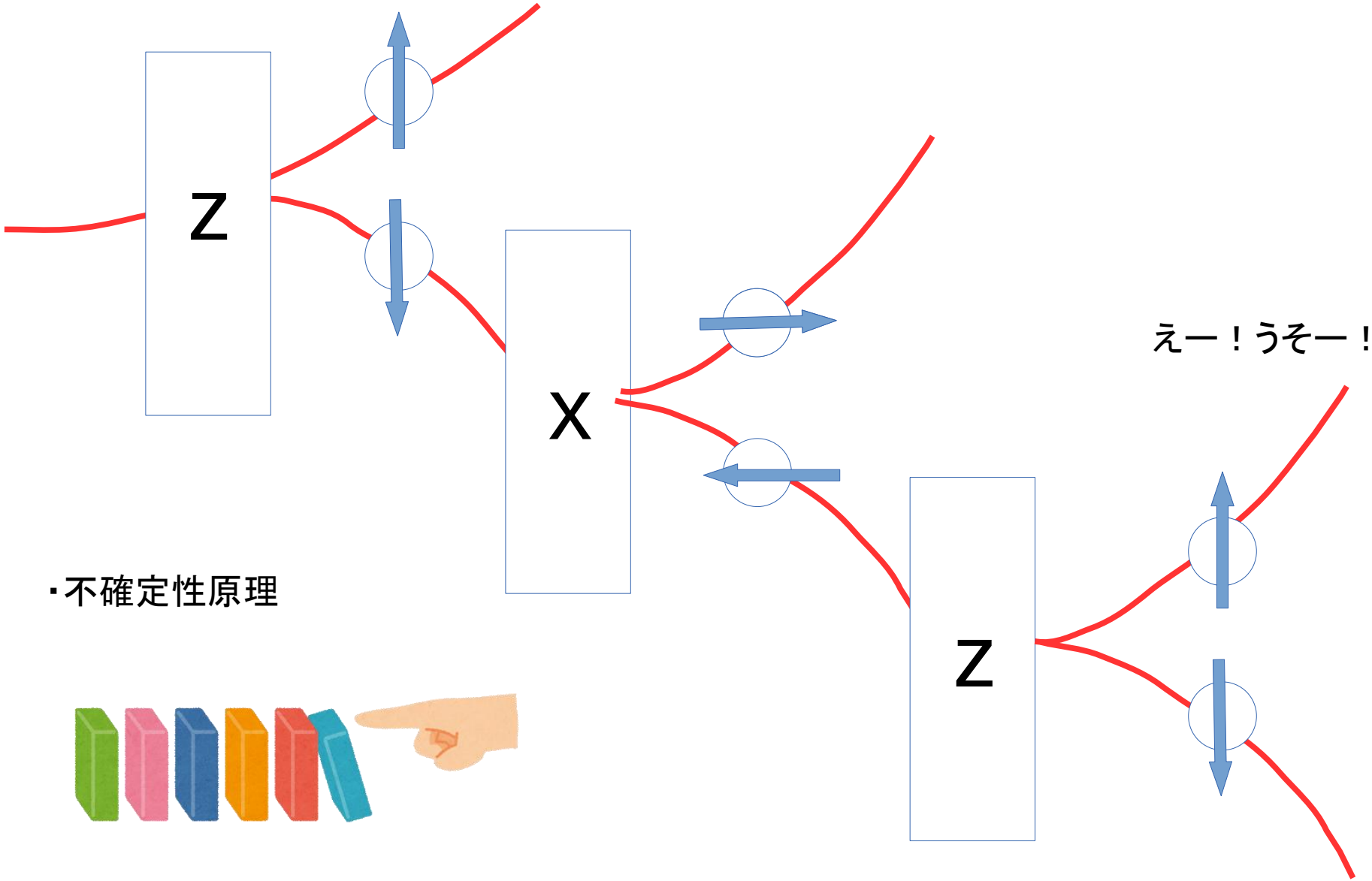



Z
X
Z
どうなる！？


Z
X
Z
えー！うそー！



常識的な考えならこうなると思うでしょ。。。



・不確定性原理

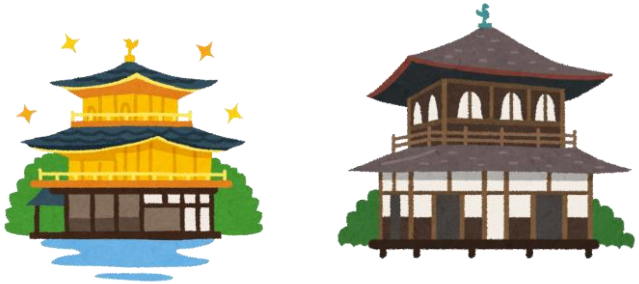
測定すると壊れる

他にも不思議な現象がいっぱい

・**不確定性原理**

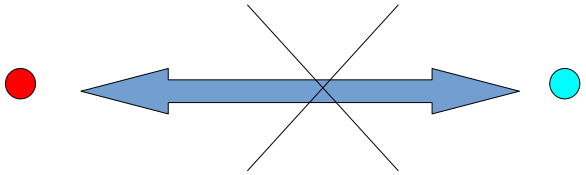
測定すると壊れる

・**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

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

私は大学で量子論を初めて学んで、最初は量子論基礎の研究をしようと思った。
→今は量子情報の研究者
→量子で何ができて何ができないのかを明確にすることにより、より量子を理解できる

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

高校生の皆さん、大学で出会う、
普通の言葉で説明できない不思議なものを数学で取り扱う面白い世界をお楽しみに！

まとめ

- 量子論はミクロな世界を説明する物理理論
- 我々の直感に反する不思議なことが数多く起こる
- それを説明・理解するためには線形代数をつかう

量子計算

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。

量子計算機

古典論には無い量子の不思議な性質をうまく使って古典計算よりも高速な計算を実現する計算機（超電導や光、イオンなどを使う。）

現状：５０量子ビット程度のマシンが実験室で実現され、試験的な問題を解いているだけ。（Google、中国など。）本当に古典計算機より高速かまだわからない。

量子ビットをもっともっと増やし、さらにエラー耐性をつければ、古典計算機を凌駕するものが実現することが少なくとも理論的には示されている。（なので皆がんばって作っている。）

さらに、有用かつ高速な量子アルゴリズムを見つけることができれば、実社会に投入されて、我々の生活の役に立つようになる。

あれ？すでに、現場に投入されて実社会の組合せ最適化問題を「高速」に解く数千「量子ビット」マシンのニュースとか、「量子計算」に着想を得た「高速」古典マシンのニュースをよく見るけど？

→それは量子計算機ではありません

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）

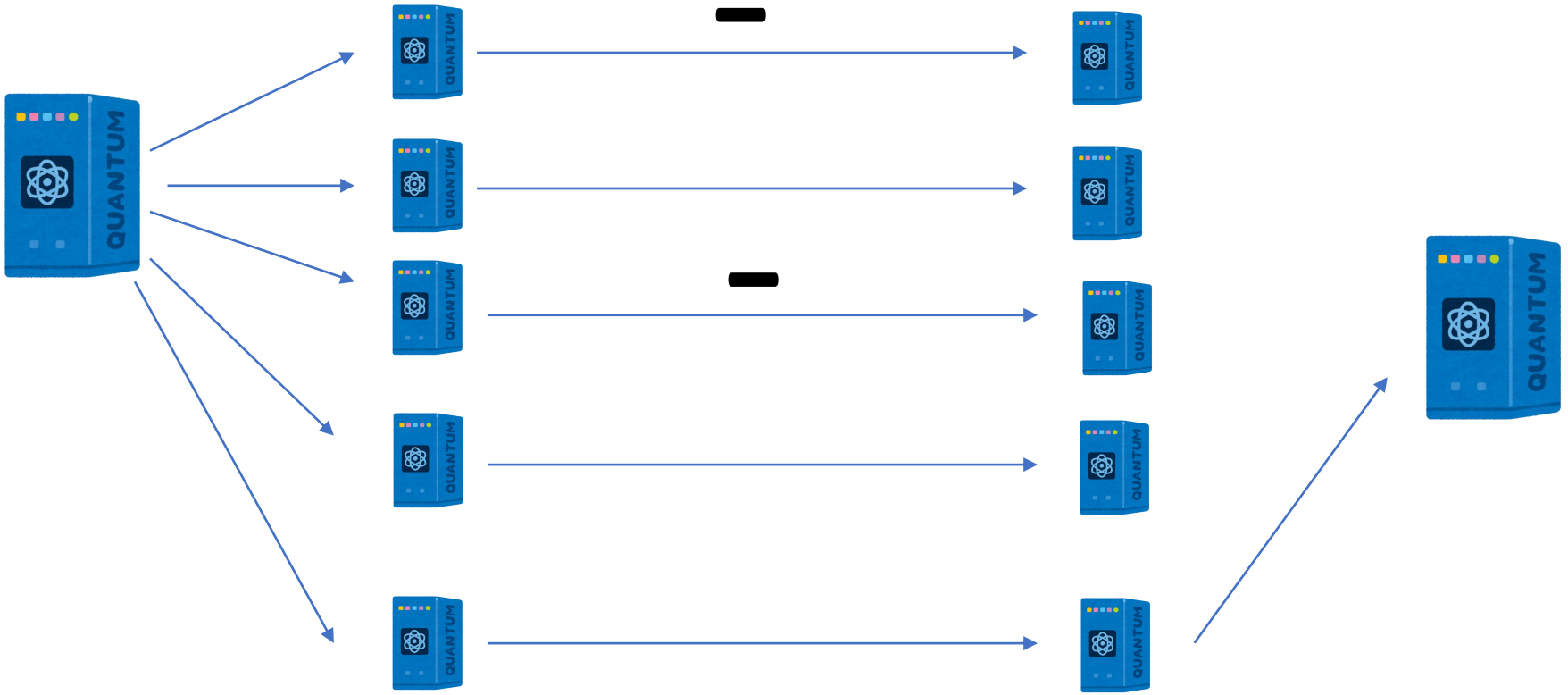
Quantum algorithm zooというウェブページに量子アルゴリズムの一覧がある

人工的な問題ばかり：実社会にすぐに役に立つ高速量子アルゴリズムはまだない

→人工的な問題であっても古典より高速であることを示すのは難しい
→実社会に役に立つ例となるとさらに難しい

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。

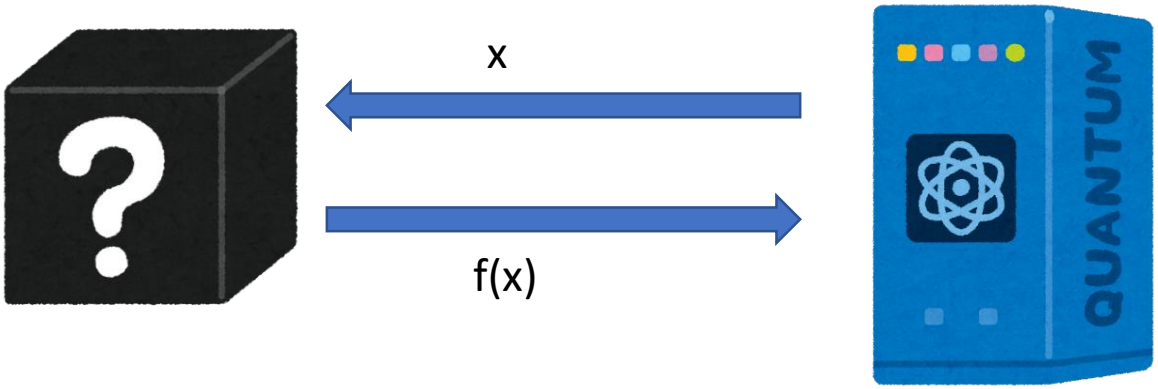


注意！！！！！！！！

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

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
- 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
- 実社会の組合せ最適化問題に適用している話は要注意

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

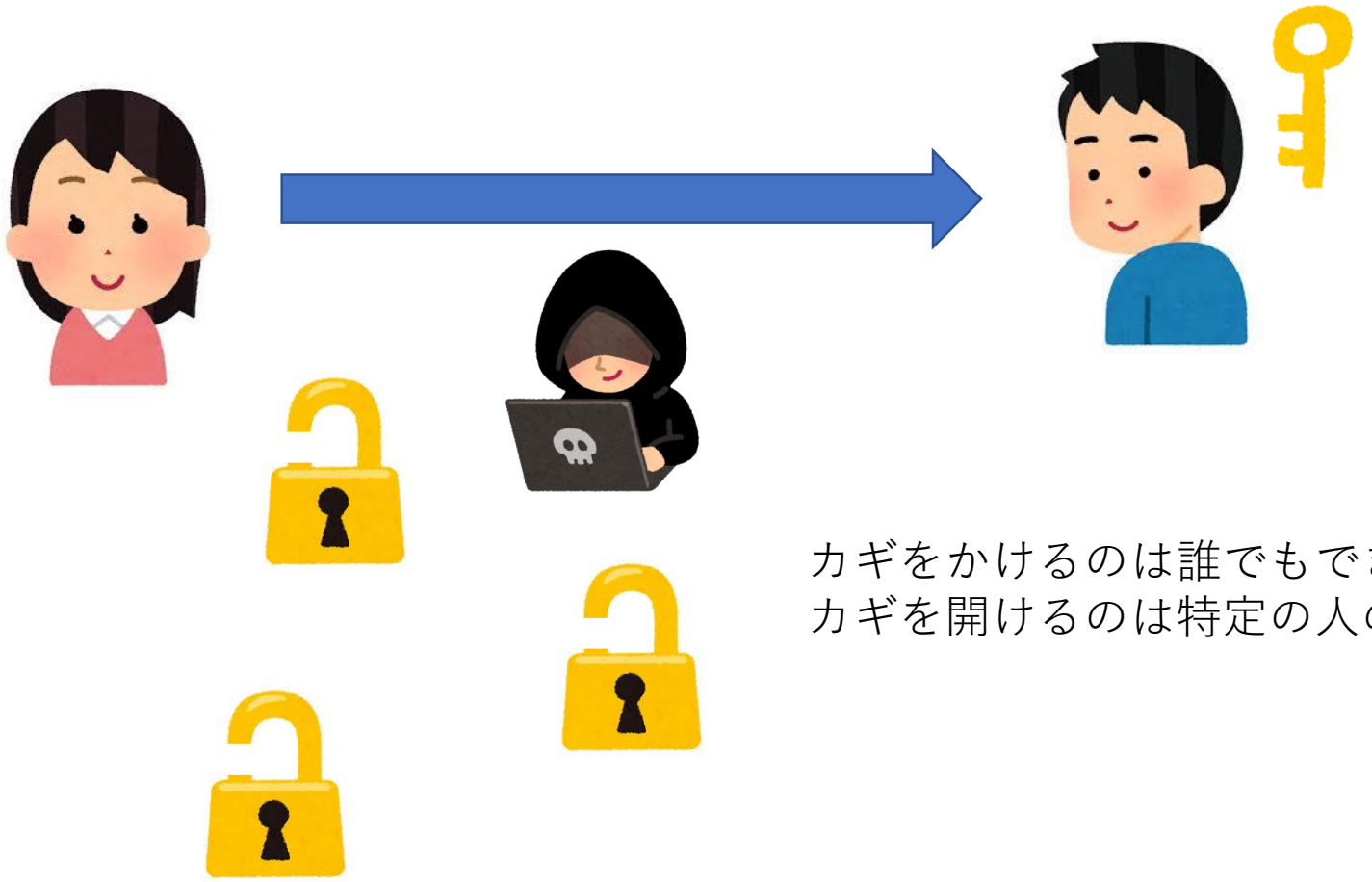
情報理論的安全な暗号通信が可能

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

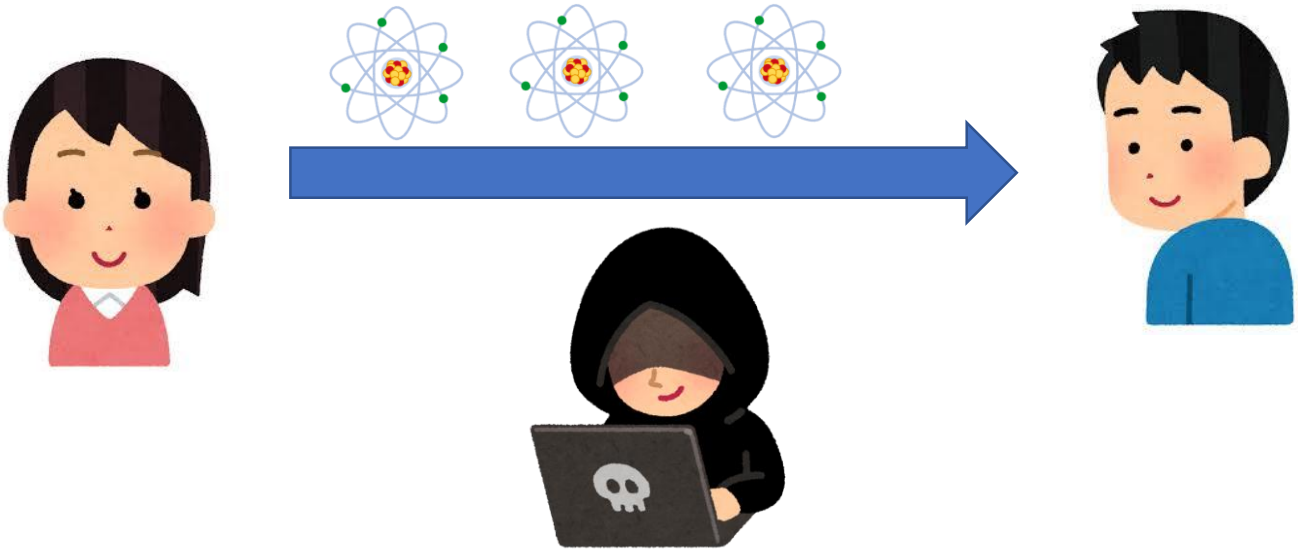


カギをかけるのは誰でもできる
カギを開けるのは特定の人のみ可能

安全性は計算量的なものになる

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！！

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

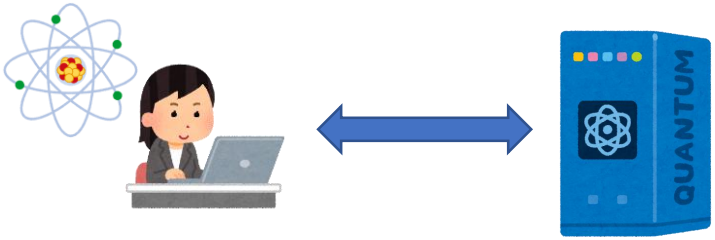
暗号というのは秘密にメッセージを送るだけの
ものではない。（例：電子署名）

→今では一般の人が日常的に暗号の
お世話になっている

量子暗号

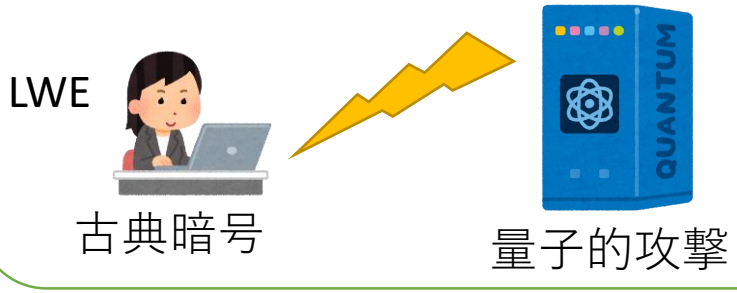
（1）量子鍵配送（QKD)：狭い意味で量子暗号といったらこれを指す。歴史が長く、かなり実用化されている

（2）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。



量子マネー、量子認証、セキュアクラウド量子計算、量子ゼロ知識証明、

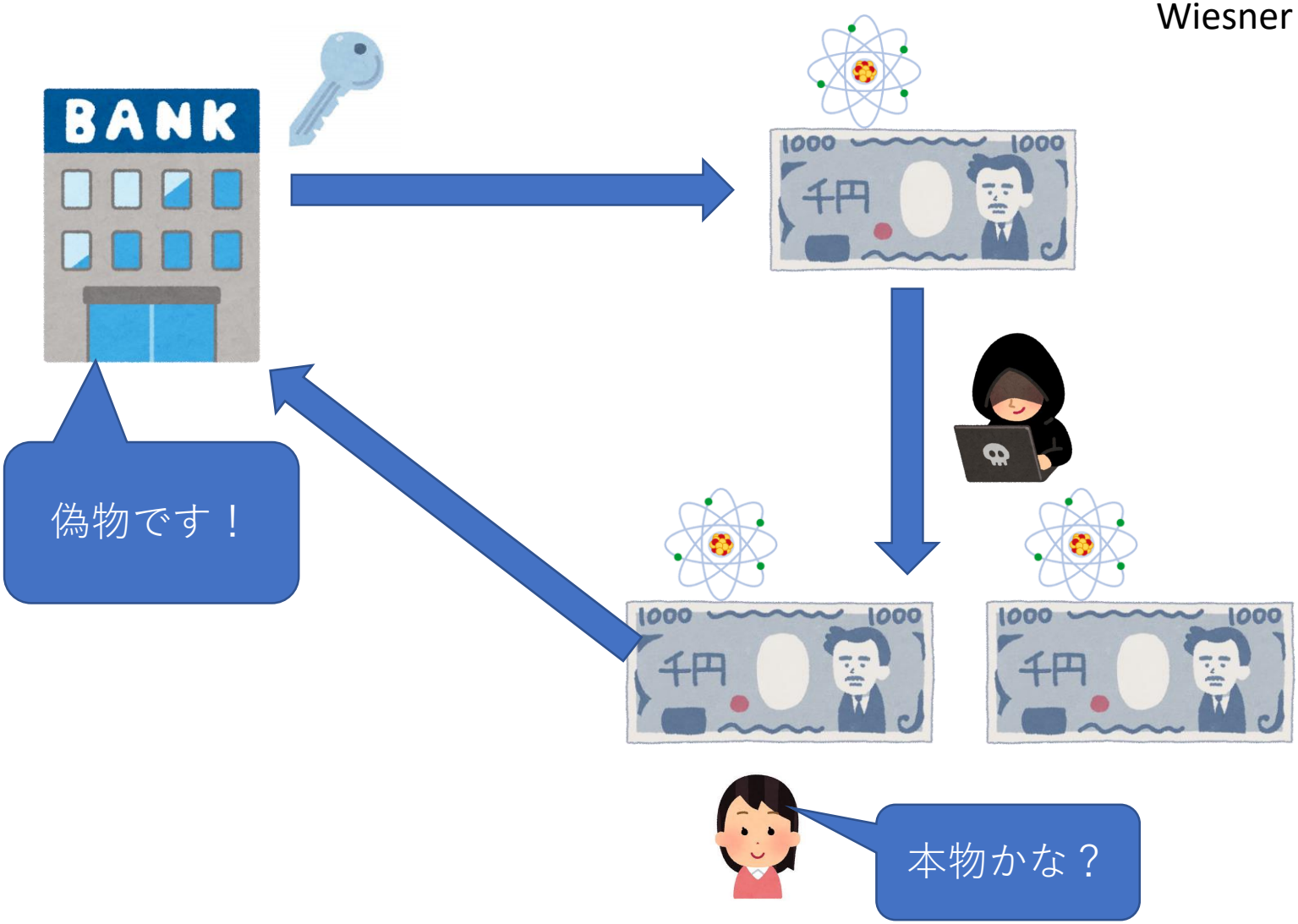
（3）耐量子暗号：古典の暗号の量子的攻撃に対する安全性を研究する。



計算能力の向上、重ね合わせ

量子マネー

Wiesner 1970 (1983)



クラウド量子計算のセキュリティ

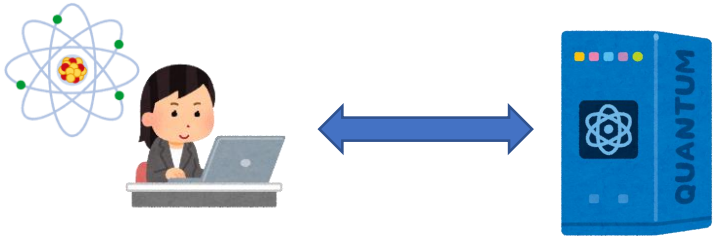
量子サーバー

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？

（2）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。



量子マネー、量子認証、セキュアクラウド量子計算、量子ゼロ知識証明、

量子の不思議な性質を使う

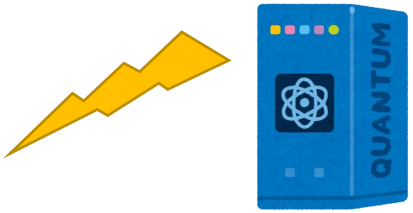
量子計算機を騙す

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

（3）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。

LWE

古典暗号



量子的攻撃

計算能力の向上、重ね合わせ

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、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