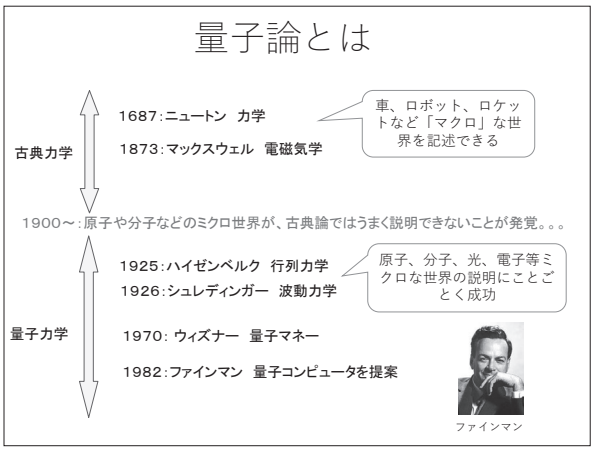
講演 1

量子計算と量子暗号

森前　智行（基礎物理学研究所　准教授）

こんにちは。それでは、お話を始めたいと思います。京都大学基礎物理学研究所の森前です。今回のお話の内容というのは、量子計算と、それから量子暗号ということで、お話をしたいと思います。内容ですけれども、まずは量子論とはどういうものか、ということについて説明します。次に今回のテーマであります、量子計算と量子暗号というものについてお話をする、という感じになります。

まず量子論とはどういうものか、ということですけれども、物理を勉強された方とかは、大学で聞いたことがあるかもしれませんけれども、ミクロな世界を説明する物理理論です。



ニュートンの力学とか、マックスウェルの電磁気学とか、そういうのは古典力学と呼ばれるものでして、高校生の人は皆さん、今、勉強していると思いますし、例えば大学で物理を習った人は、覚えていると思うんですけれども、こういう古典力学というのは、車とかロボットとか、そういう身の回りの大きなものをうまく説明することのできる、物理理論なんですね。

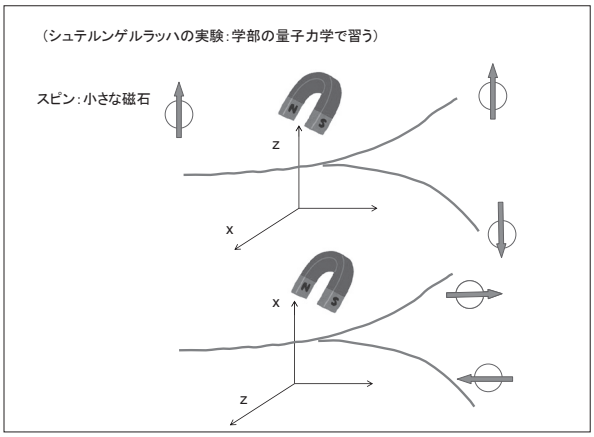
ところが、1900年ぐらいから原子とか分子とかいう、目に見えないミクロな世界にアクセスできるようになってくると、どうもこういう古典力学だとうまくミクロな世界が説明できない、というふうに気づいてしまったわけです。

なので、物理学者たちがそういうミクロな世界を説明できるような理論をつくろうということで、いろいろと研究をしてきまして、例えばハイゼンベルクという人が1925年に行列力学というものを提案したり、あと、1926年にシュレディンガーという人が波動力学というものを提案しました。これが量子力学とか量子論というものの始まりになります。

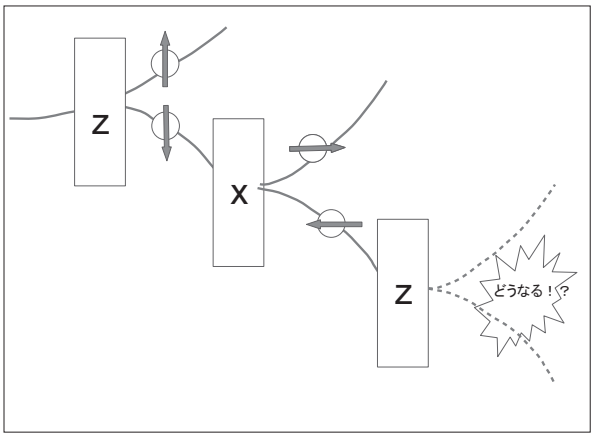
この量子論というのは、原子とか分子とか、光とか、そういうミクロな世界のものを、ことごとくうまく説明することができるという理論でして、今のところ正しいと信じられています。

今回、お話しする量子暗号や量子計算の歴史については、1970年に、イスラエルのウィズナー（Wiesner）という人が、量子マネーというアイデアを提案しました。これは量子を使って偽造できないお金をつくるというアイデアで、量子暗号の一番最初のアイデアになります。

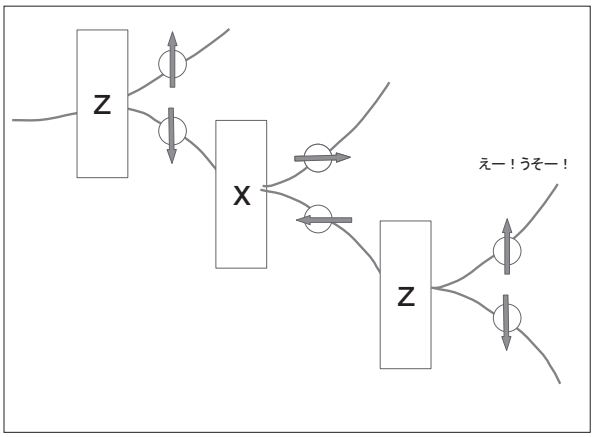
量子計算のほうは、1982年にアメリカの素粒子の物理学者のファインマンという人が、最初に提案したといわれています。彼は日本の朝永振一郎と一緒にノーベル賞を取った人ですけれども、素粒子だけではなくて、コンピューターにも興味があって、量子に基づいて動くコンピューターができたら面白いんじゃないか、ということを最初に言いだしたといわれています。



量子論というのは非常に不思議なものなんですけれども、それを理解するために、「シュテルン＝ゲルラッハの実験」というものを考えてみましょう。これは大学の学部の物理学科なんかに行くと、量子力学の授業で習うような内容です。



今、小さな粒子がいて、スピンという小さな磁石を持っています。このZ軸の方向に磁石を置くと、上向きのスピンは引き寄せられて、下向きのスピンは下に行ってしまうと。今後は逆にX軸の方向に磁石を置くと、右向きのスピンは引き寄せられて、左向きのスピンは下に行ってしまう。こういうことが起こるとしましょう。



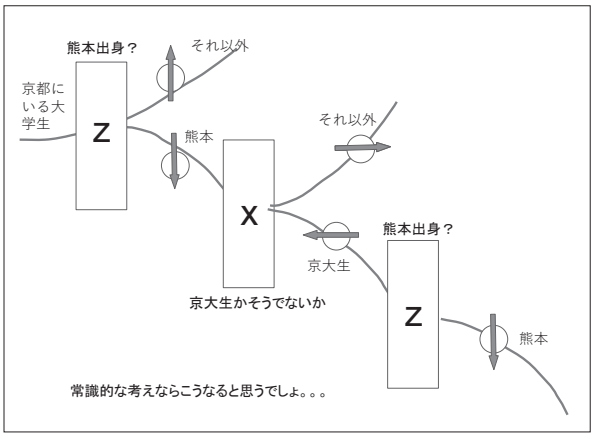
そのときに、じゃあこういう実験をしたら、どうなるでしょうと。まずZ軸の方向に磁石を置くと、上向きのスピンは上に飛んでいって、下向きのスピンは下に行くと。今後、下向きのものだけに対して、X軸の方向に磁石を置くと、右向きのスピンはこっちに行って、左向きのスピンはこっちに行くと。今度、左向きのものだけに対して、もう一度、Z軸の方向に磁石を置いたら、さあ何が出てくるでしょうと。

じゃあ上だけ出てくると思う人は？　下だけ。両方。何も出てこない。どうでしょうか。

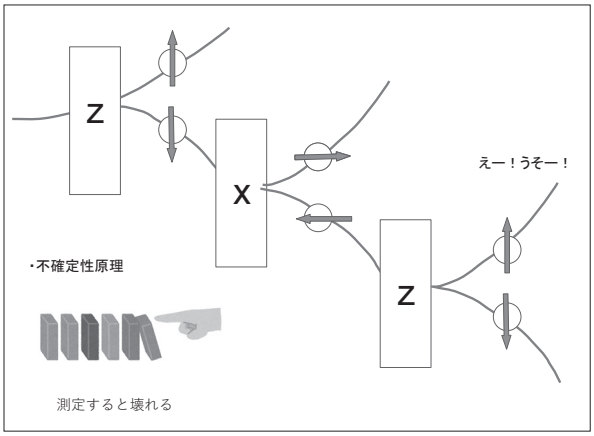
実は正解は、両方出てくるということですね。これはものすごく不思議なんですけれども、それはなぜかというと、もう上向きのものはここで排除しているわけですね。ですけど、また出てきているから、おかしいわけです。

これをミクロな粒子じゃなくて、京都にいる大学生で、今、考えてみましょう。京都に大

学生がいっぱいいますけれども、彼らに熊本出身かどうかをまず聞くわけです。熊本出身の人は下に行ってくださいと。それ以外の人は上に行ってくださいと。今後、熊本出身の人に対して、京大生かそうじゃないかというふうに聞きました。京大生はこっちに行ってください。そうじゃない人はこっちに行ってくださいと。

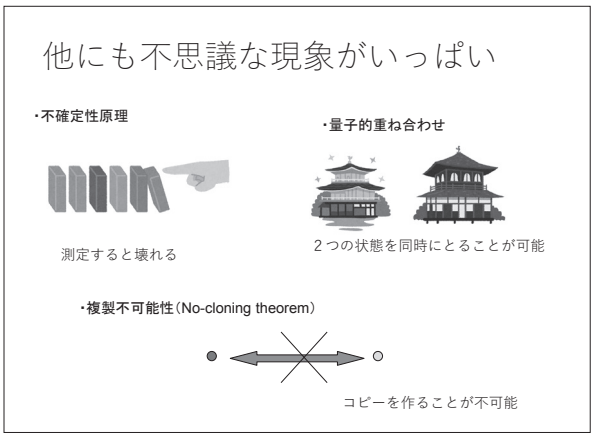


もう一度、ここで京大生に対して、熊本出身ですかと聞いたら、当たり前ですけど、熊本出身の人しか出てこないですよね。そうじゃない人はもうここでこっちに行っていますから、ここからまた出てくることはないですね。だから普通に考えたらそうなんですけど、なぜかミクロな粒子でやると、また熊本出身じゃない人が出てきちゃうという、不思議なことが起こる。



これは量子論が持つ、不確定性原理というものからきています。これは直感的にいうと、情報を得ようとして測定すると、違う情報が消えちゃう、壊されちゃうというものになります。ここで測定したから、もともとスピンは下向きに確定していたんですけど、ここで違う情報であるXというものを測定してしまったので、情報が壊れて、Zの情報がなくなって、またゼロに戻って二つ出てくる、ということになります。

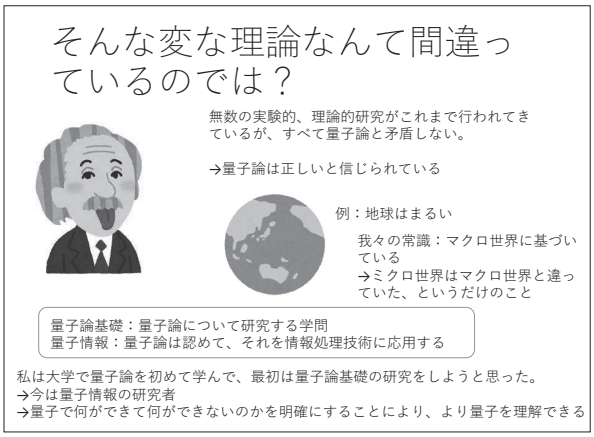
これは一つの事例なんですけれども、ほかにも不思議な現象がいっぱいありますということで、例えば通常ですと、金閣寺にいるか銀閣寺にいるかの、どちらかしかあり得ないんですけれども、二つの状態の量子的重ね合わせという、ある意味、同時に、ということが可能になります。あとは原理的にコピーをつくることができないという、No-cloningという性質も知られています。このコピーできないという性質を使って、偽造できないお金をつくろうというのが、量子マネーになります。



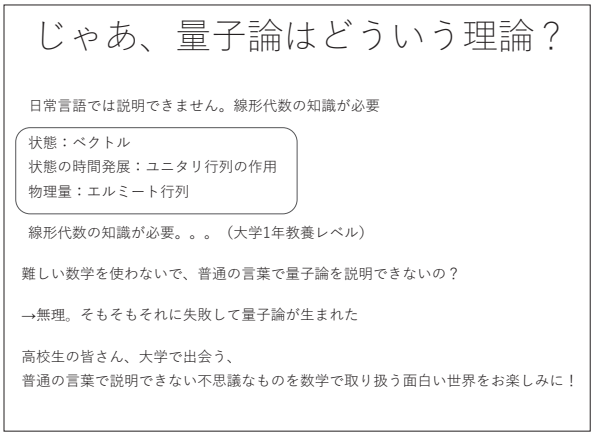
でも、こういう不思議な理論なので、間違っているんじゃないかというふうに思う人も多いわけで、有名な物理学者のアインシュタインも、最初は量子論を受け入れられなかったと

いう話があります。

そうなんですけれども、今のところは研究者たちがいろんな研究をしてきて、実験的、理論的研究をしてきて、これまで全く矛盾しなくて、量子論を支持しているわけですね。なので、科学だから受け入れざるを得ない。量子論は正しいというふうに認めざるを得ないということになります。それで今は、普通に高校とか大学で習うわけですね。教科書に書いてあるようなものになります。



これは、地球が丸いという例を考えてみると分かりやすいんですけれども、今、小学生でも地球が丸いと知っていますけれども、例えばタイムマシンに乗って過去にトラベルして、大昔の人に地球が丸いと言っても、信じてもらえないですね。こっち側の人は下に落ちちゃうだろうと、そういうことを言ってきますよね。それはでもある意味、自然で、普通に生活していたら、当然、平らだと思うほうが普通ですよね。ですけど、いろんな研究をした結果、どうも丸くないとおかしいということで、今はみんな、丸いと思っているわけです。



量子論もある意味、それと同じで、我々の常識というのは、マクロな世界の普段の生活からきているわけですね。だけど、ミクロな世界はたまたまそれと違っていたということにすぎなくて、間違っているとかじゃなくて、我々の常識というのが普段、マクロな世界からきているけど、ミクロな世界はそれと違っていましたというだけにすぎない、ということになります。

こういう非常に面白い量子論なので、量子論について研究したいという研究者がいっぱいいて、そういうのを研究する分野の量子論基礎というものがあります。今回、お話しする量子計算や量子暗号というのは、量子情報というものになります。これは量子論はもう正しいと認めて、それを情報処理技術に応用しましょうという研究になります。

今回は高校生の方が多いというふうに聞いていますので、個人的な話をしますと、私は大学に入って量子論を初めて勉強して、面白いと思ったわけですね。最初は量子論基礎の研究を志したんですけれども、今は量子情報の研究をしています。

それはなぜかというと、一つはもちろん役に立つからというのが大きいんですけれども、量子を使ってどういうことができて、何ができないか、ということを研究したほうが、より量

子が理解できると。単に量子だけ研究するよりも、量子を使ってどういうことができないとか、できるとか、そういうことをやったほうが、実はより量子を理解できるということに気づきまして、今ではこういう量子情報の研究をしています。

じゃあこういう量子論というのは、結局どういうものなんですか、ということなんですけれども、残念ながらこういう一般の講演でしゃべれるような、普通の言葉で説明することはできません。線形代数の知識が必要になってしまいます。

高校生の人は皆さん、大学に入ると１年で、教養の課程で線形代数というのを習うんです。行列とか、ベクトルですね。そういう言葉を使うと、量子状態はベクトルですとか、量子状態が時間的に動いていく様子はユニタリ行列という、ある特別な行列をベクトルに掛けて表されますと、そういうことを習うわけですね。それで理解できるわけです。

でも、そういう難しい数学を使わないで、普通の言葉で説明してよ、というふうに言われるんですけれども、ちょっとそれは無理と。それはなぜかというと、そもそもさっき歴史を説明しましたけど、もともとはこういう変なものじゃなくて、古典論でミクロな世界を説明したかったわけですね。

古典論はすごく直感的なわけです。ボールがぶつかって跳ね返りますとか、波が伝わりますとか、ものすごく分かりやすいんですね。最初はそういうもので、ミクロな世界を説明できるだろうと思ってやったけど、結局できなくて、こういうベクトルとかを使わざるを得ないものが生まれたということなので、そもそももし言葉で説明できるんだったら、量子論は生まれなかったわけですね。古典論でよかったわけです。なので、ちょっとなかなか納得はいかないんですけど、説明はできませんということになってしまいます。

でも、こういう普通の言葉では説明できないものも、数学を使うと、数学は抽象的なものを説明できる便利な言語なので、そういうものを使っていろいろと取り扱うことができるという、楽しい勉強が大学でできますので、高校生の皆さんは楽しみにしていてください。

ここまでのまとめをしますと、まず量子論というのは、ミクロな世界を説明する物理理論です。我々の直感に反する不思議なことが数多く起こります。それを説明とか、理解するために、線形代数という数学を使ってやります、というのが、ここまでのまとめになります。

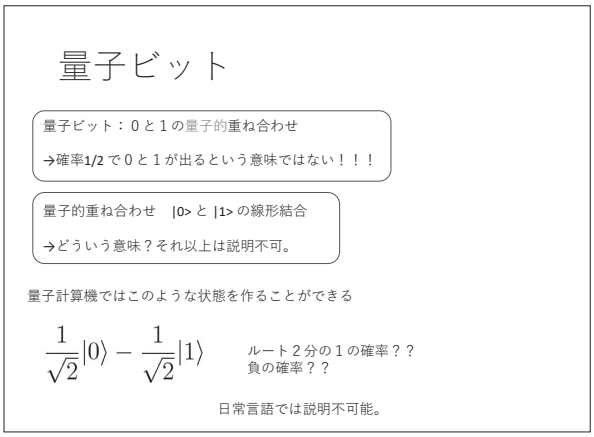
まとめ

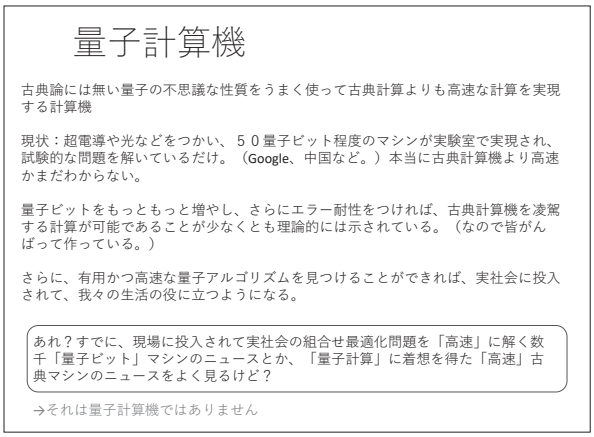
- 量子論はミクロな世界を説明する物理理論
- 我々の直感に反する不思議なことが数多く起こる
- それを説明・理解するためには線形代数をつかう

ここから量子計算の話に入りたいと思います。量子計算というのは、量子ビットというものを使って、計算を行います。この量子ビットというのは、０と１の量子的な重ね合わせも可能であるようなビットというものになりますが、これはよく誤解されるのは、確率が２分

の１で、０と１がランダムに出るというものではないわけですね。じゃあどういうものですかといったら、０を表すベクトルと１を表すベクトルの線形結合です、ということしかいえません。

そういうことじゃなくて、もっと普通の言葉で説明してよ、と言われるんですけど、それはまたさっき言ったように、残念ながら説明できないと。そういうふうに説明しようとして失敗して、結局こういうベクトルの線形結合という、抽象的な言葉でないと説明できない、ということになったのがそもそもの経緯なので、残念ながら直感的にどういう状態かというのを説明することは難しいです。





例えば量子計算機にはこういう状態が出てくるんですけれども、これは$\sqrt{2}$分の１の確率で０が出て、$\sqrt{2}$分の１の確率で１が出ると思うと、よく分からないわけですね。確率というのは足して１になりますけど、$\sqrt{2}$分の１と$\sqrt{2}$分の１を足しても、１にならないですよね。しかもこれはマイナスですから、確率がマイナスって、よく分からないですね。なので、そういうふうに分かりやすい言葉では説明できません。だけど実際、ミクロな世界ではこういうものが今、つくられているということになります。

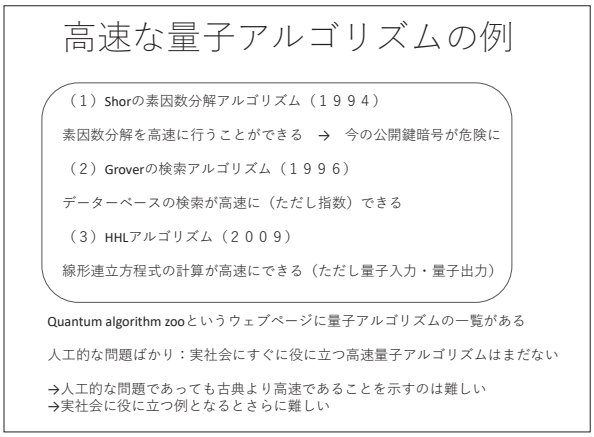
量子計算機というのはgeneralに言うと、古典論にはない量子、先ほど説明しましたが、いろんな不思議な重ね合わせとか、そういう不思議なものを使って、古典計算よりも高速な計算をしてくれる計算機のこといいます。

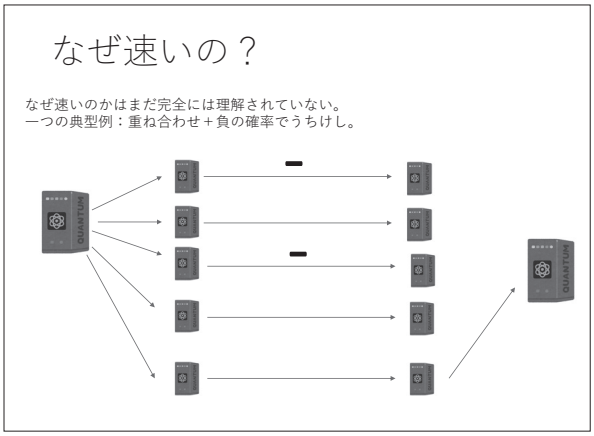
今、どのぐらいまでできているかといいますと、超伝導とか光とか、イオンとか、そういうものを使って、50個ぐらいの量子ビットが並んだようなマシンがつくられています。ただ、実験室でつくられていると。非常にコントロールされた、特殊な環境で実現できているという状況になっています。さらに、本当にそれが動いているかどうかをチェックするための、試験的な問題を解いているだけというレベルになっています。

ニュースなんかでGoogleの話とか、中国の話とか、目にされた方も多いと思うんですけれども、そういう人たちが今、50量子ビットぐらいのものをつくっているという状況になっています。ただそのレベルで、そのマシンが本当に古典より速いかは、まだちょっとよく分かっていない。まさに今、皆さんが研究をしているという状況になっています。

ですけれども、量子ビットを今後、もっともっと増やしていって、さらにエラー耐性を付

けることができれば、よいわけですね。エラー耐性というのは、量子コンピューターというのは、外からのノイズでデータが壊れてしまうわけです。パソコンも地面にたたきつけたら、データが消えちゃいますけど、量子コンピューターはもっと弱いノイズでも、すぐに壊れちゃうんですね。





そういうものを防ぐようなスキームがいろいろと提案されていて、そういうものを実装できて、なおかつQbit（quantum bit、量子ビット）がすごく増えれば、古典計算機、我々が使っている今のコンピューターとか、スパコンとか、そういうものを超える高速な計算ができるということが、少なくとも理論的には示されています。研究者たちが証明しています。なので今、世界中の研究者がみんな、頑張ってつくっていると。いろんな国の研究者が、しのぎを削っている状況になっています。

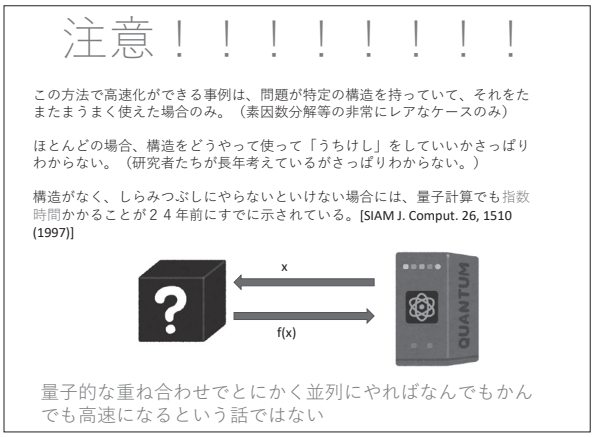
それに加えてさらに、後で説明しますけど、あまり有用なアルゴリズムがないんですね。実際に我々の社会に役に立つような有用な、高速な量子アルゴリズムが、もし今後、見つかれば、量子コンピューターが実際に実社会に投入されて、我々の社会に非常に役に立つということになります。

こういう話をよくすると、「あれ？　でも何か私がいろんなところで目にする話と違うな」ということを思う人もいると思うので、ちょっと補足をしておきますと、もう既に現場でいろんな問題を解いている量子コンピューターの話とか、あと、量子計算に着想を得た古典の高速マシンとか、日本のメーカーがよく出していますけど、そういう話が出てくるんですけど、それはちょっと違うものです。ということで、気を付けていただきたいと思います。

幾つかの問題については、高速に計算することができるということが知られていまして、例えば米国のショアー（Shor）という人が94年に提案した、素因数分解のアルゴリズムというのがあります。素因数分解というのは、例えば15を３×５にしましょうとか、素数の積に数を分けるわけですね。

そういうものは今の我々が使っているコンピューターとかスパコンでは、ものすごく難しいだろうと信じられていて、その難しさが実際に今、我々が使っている暗号の基礎になっています。インターネットとかで暗号を使っていますけど、そういうのの基礎になっています。ですから、もしこのショアーのアルゴリズムが本当に実現できると、暗号が破られてしまう

という話があります。



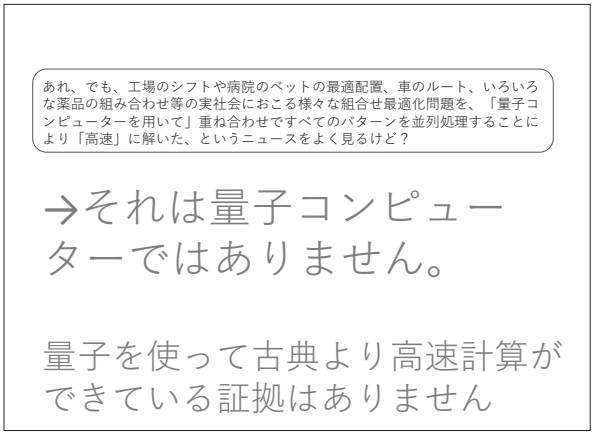
あとは米国のグローバー（Grover）という人が発見した、グローバーの検索アルゴリズムというのがあって、96年に提案しています。これはデータベースの中からアイテムを高速に見つけてくれるような、検索のアルゴリズムになります。高速になる。ただ、指数時間から指数時間なんですけど、ちょっとだけ高速になるという結果が知られています。

あとは2009年に提案された、HHLアルゴリズムというのがあって、これは発見した３人の頭文字を取っています。これは線形連立方程式の計算が高速にできるということで、線形連立方程式は身の回りに大量にありますから、ものすごく役に立つだろうと思うんですけれども、ちょっと注意していただきたいのは、入力と出力が量子的な状態でないと駄目なんですね。

そこの量子的な状態を、我々が分かるような古典のデータに置き換えるところで、ものすごく時間がかかってしまって、一般にはあんまり速くならない。だから何でもかんでもこれが速くなるというわけではないので、そこも注意していただきたいと思います。

いろんなアルゴリズムが提案されていまして、Quantum algorithm zooというウェブページがあります。検索していただくと出ますけれども、そのウェブページを見ていただくと、量子アルゴリズムの一覧が載っています。それを見ると気づくんですけれども、人工的な問題が多いんですね。実社会にすぐに役に立つ、いきなりスマホが速くなりますとか、そういうすぐに役立つような高速の量子アルゴリズムは、まだないという状況になります。

それはなぜかといいますと、そもそも人工的な設定で問題を考えても、古典計算より高速であることを示すのは、ものすごく難しいんですね。それに加えて、さらに実社会に役に立つ例でやってくださいとなると、もう全然できないということで、長年、研究者がみんな研究していますけれども、なかなか難しいという状況になっています。



じゃあなんで量子コンピューターは速いのか、ということなんですけれども、これもまさに今、みんなが研究している最中で、完全な理解はまだ得られていません。ですけれども、一つのよくある典型例というのは、重ね合わせをつくって、負の確率で打ち消す、というものになります。

これはつまり先ほど説明したような、量子的な重ね合わせをまずつくって、負の確率の

話をしましたね。なので、あるものは負の確率が出る。そうすると、この負とこの正で打ち消して、キャンセルして消えてしまうと。こういうふうにして間違ったものを消していって、正解だけ取り出す、ということをしているのが典型的です。

ただ、この説明は非常に注意して聞いていただかないといけないんですけれども、こういう方法で打ち消して高速になるのは、非常にレアなケースです。問題が何かうまいかたちを持っていて、構造を持っていて、たまたまそれをうまく使えたから打ち消しができた、という場面しかないです。多くの場合は、問題の構造を使ってどうやって打ち消していいか、さっぱり分からない。もう40年ぐらい、研究者がずっと考えていますけれども、さっぱり分からないという状況になっています。

さらに、構造がありませんと、しらみつぶしにやるしかありません。これはどういうことかというと、つまり問題が、よく分からないブラックボックスなかたちで与えられていて、入力を入れたら出力を返してくれる。だけど問題のかたちはよく分からない。こういうブラックボックスの状況で解かなければいけない場合は、たとえ量子コンピューターを使っても、指数時間がかかる。指数時間って、ものすごい時間ですよね。ものすごく長い時間がかかるということが、もう既に24年前に証明されています。

なので、量子的な重ね合わせをつくって、とにかく並列でやれば何でもかんでも速くなります、という話ではないというところは、非常に注意していただきたいと思います。

そうするとまた「何か聞いた話と違うな」ということを思う方もいるかもしれないので、一応、ちょっと補足をしておくと、よく現実に、いろんな組み合わせの問題というのは多いんですね。いろんな薬品を組み合わせて、何かいいものをつくろうとか。そういう組み合わせの数というのは、恐ろしく数が増えてきて、それを全部やるのは不可能になるんです。

そういう組み合わせの中で最もいいものを見つける問題というのは、実社会のありとあらゆるところにあるんですけれども、それをじゃあ量子コンピューターを使って、並列で全てのパターンを全部やればいいじゃないか、という話がよくあるんですけれども、残念ながらそれはまだ全然できないわけですね。量子を使って本当に速くなるかどうかは全然分からないと。

それはさっきも言ったように、本当に打ち消しでうまくいくというのは、非常にレアなケースなんですね。なので、ちょっとそのへんは、皆さん気を付けて、いろんな情報を見ていただきたいと思います。

ここまでのまとめをしますと、量子計算というのは、量子の不思議な性質を使って、高速計算をするようなものになります。だけど、なぜ速くなるかとか、いつ速くなるかとかい

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

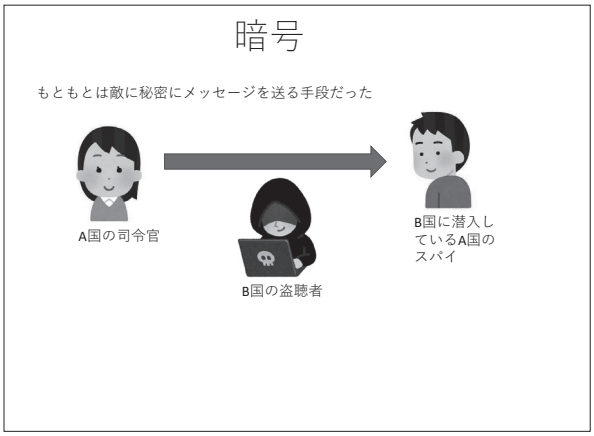
うのは、まだ完全に解明されていなくて、まさに今、みんなが研究しているものです。ですけれども、典型的には重ね合わせと打ち消しを使って、間違った解を消す、というのが典型的な方法になります。

ですけれども、重ね合わせとか打ち消しを使って速くできるのは、非常に限られた人工的な場合しかないと。多くの場合については、それでは全然うまくいかないという状況になっています。特に、もう既に実社会のいろんな組み合わせの問題に対して適用しています、みたいな話がありますけれども、それはちょっと皆さん、注意して聞いていただきたいと思います。

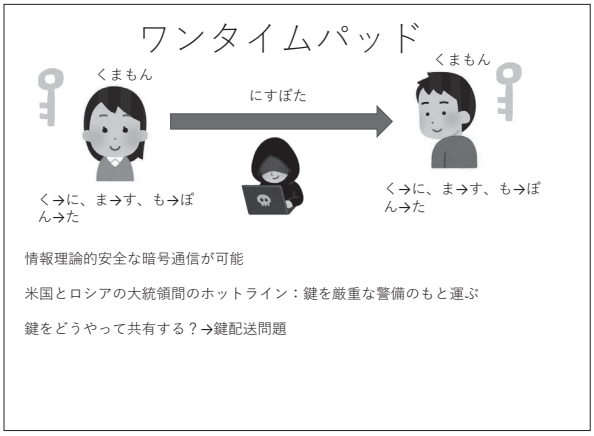
最後のテーマの量子暗号に入りたいと思います。暗号というのは、もともとは敵に秘密にメッセージを送る手段でした。例えばA国の司令官がB国に潜入しているスパイに、何か秘密の指令を送りたいんですね。だけどもちろんそのまま送っちゃったら、盗聴されるから駄目なわけです。だから秘密にメッセージを送りたいというのが暗号で、古代ローマの時代からやられていたといわれています。

実は絶対に安全な暗号というのは、既に知られています。これはワンタイムパッドと呼ばれる方式で、どういうものかというと、今、例えばこの人が秘密のメッセージ、「くまもん」というものを送りたいとしましょう。もちろんそのまま「くまもん」と送っては駄目ですね、盗聴されちゃうので。

どうするかといいますと、例えばこの文字を違う、ランダムな言葉に置き換えるルールが書かれた紙を、この人は持っています。「く」は「に」にしましょうとか、「ま」は「す」にしましょうとか、ランダムに換えるんですね。そうすると「くまもん」が「にすぽた」というランダムな文字に置き換わります。



そうすると、この人はこれを見ても何が書いてあるか、分からないわけですね、もちろん。ですけど、受け手の人は文字のルールの紙を持っているので、これを逆変換して「くまもん」を出すことができる。このようにして絶対に盗聴されない暗号ができます。これは情報理論的安全というんですけれども、要するにこの人がどんなに強力なコンピューターを持っていても絶対に破られないという、強力な暗号になります。



これは本当か分からないんですけど、米国

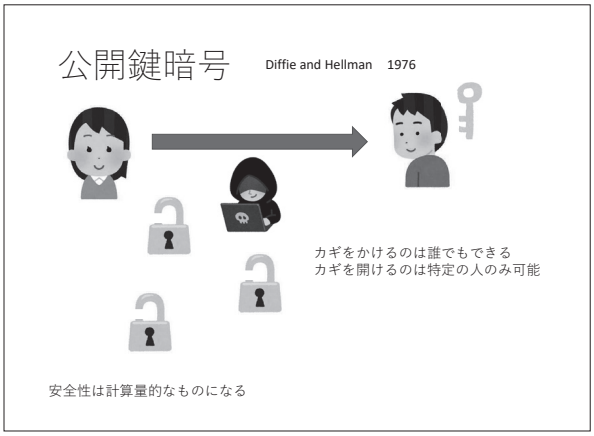
とロシアの大統領の間のホットラインでは、この暗号が使われているという話があるそうです。大統領間のホットラインのレベルになると、厳重な警備の下で、専用の飛行機でこの紙を運べばいいんですけど、普通の人がこういう暗号を使おうとすると、非常に面倒くさいわけですね。

例えばこの人にこの紙を渡さなきゃいけないから、会いに行かなきゃいけないと。だけど会うんだったら、その場でべつに伝えればいいわけですよね。もしくは、じゃあ郵便で送ろうと。だけど郵便で送って、これが盗まれちゃうかもしれないわけですね。なので、非常に使いづらい。もう絶対に安全であることは保証されているけど、ものすごく使いづらいというものになります。

これを解決する一つの方法に、公開鍵暗号というものがあって、これは皆さん、今はもう身の回りで普通に使っているやつですね。これは1976年に提案されたものになります。

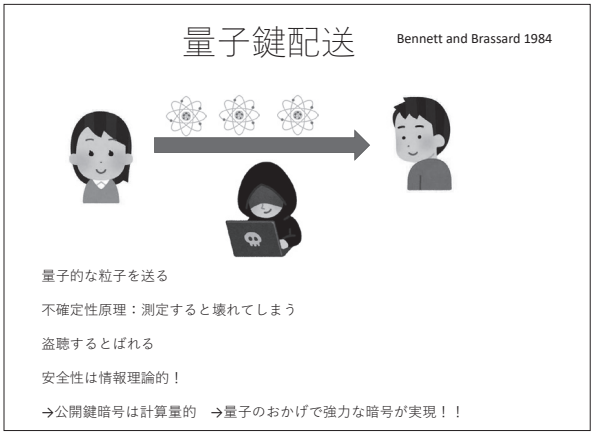
これを直感的に説明するとどういうものかというと、この人が鍵の開いた南京錠を道端にばらまいておきます。この人はメッセージを送りたくなったら、箱にメッセージを入れて、これをガチャンと閉めて、郵便で送ります。そうすると、この人は鍵を持っていないから、開けられないから、メッセージは秘密になるということになります。この人は鍵を持っているから、開けて、中を見ることができるということで、めでたく秘密にメッセージを送ることができました、ということになります。

これの素晴らしいところは、あらかじめ二人が鍵を共有していなくてもいいわけですね。さっきのワンタイムパッドと違って、あらかじめ会う必要はないと。つまり全く一度も会ったことのない人たちの間で、秘密のメッセージのやりとりができているということになります。



皆さんもインターネットとかで、ちょっとプライバシーのあるメッセージを送るとき、いちいちあらかじめ会ったりしないですよね。だけど、全く一度も会ったことのない人同士の間でも秘密のメッセージがやりとりできるという、素晴らしいアイデアなんですけれども、欠点は安全性がちょっと弱くなってしまうと。

計算量的というんですけれども、これはこの人が強力なコンピューターを持っていたら、破られてしまうと。例えば量子コンピューターがあったら、破られてしまうと。そうい



うもので、さっきとはちょっと弱くなるわけです。さっきのワンタイムパッドは、どんなにコンピューターが強力でも破られない、情報理論的なものだったんですけど、今回はちょっと弱まってしまうわけです。

それに対して、実は量子を使うと解決できるということが、84年に示されました。これはどういうことかというと、量子の粒子を送ります。この人が盗聴すると、状態が変わっちゃうわけです。最初のほうで説明した、不確定性原理ですね。状態が変わっちゃうんです。なので、そうすると盗聴がばれてしまって、この人はそういう盗聴された危ないものは使うのをやめようと、盗聴されていないものだけを使うということで、めでたく二人が鍵を共有できる、というアイデアになります。

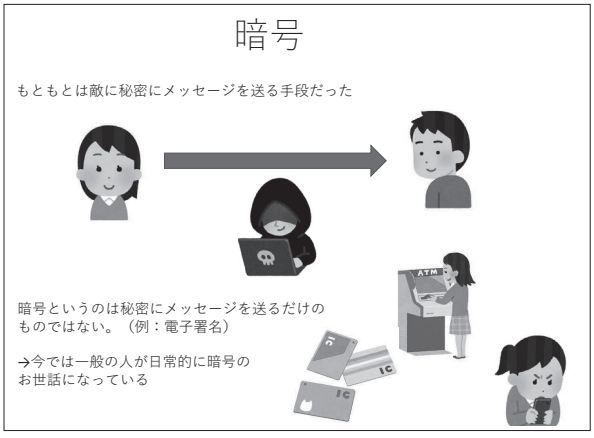
この不確定性原理というのは、べつにこの人のコンピューターの能力とは何の関係もない話なので、情報理論的安全性、つまりこの人がどんなに強力な計算機を持っていても、絶対に安全なものができるということになります。しかもこれもあらかじめ会う必要がないわけですね。

先ほど説明した公開鍵暗号は、安全性が計算量的なものになるけど、今回、この量子を使うことによって、強力な暗号が実現できたということで、量子を使うとすごいことができるという、最初の有名な例になっています。最初は量子マネーなんですけど、最もメジャーな、最初の例になっています。

このように暗号というのは、秘密にメッセージを送るというところから始まったんですけど、でも今は、べつに暗号というのはそれだけではないわけですね。例えば署名を考えてみますと、これは私が書いた書類ですと、サインをしたり、はんこを押したりしますよね。紙ならそれでいいんですけど、電子的に送る場合は、じゃあどうしましょうということになるわけです。

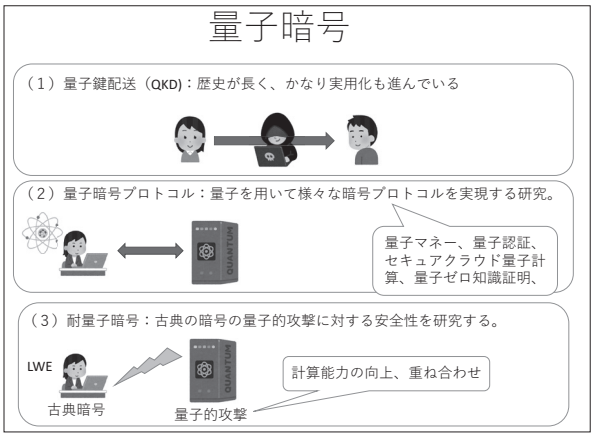
実際に電子的に送る場合にも、こういう署名ができる技術があるんですけれども、それはメッセージはべつに秘密になっていないですね。誰でも読めます、メッセージは。署名が偽造できないというだけで、メッセージは読めるので、べつにメッセージを秘密にしているわけではないですね。

なので、暗号というのは、べつに秘密にメッセージを送るだけではないと。ほかにいろんなことがあるわけです。そういういろんなものが最近、日常生活で我々がお世話になっているという状況になっています。



今回のテーマの量子暗号ですけれども、量子暗号というのは、量子と暗号に関係するものが量子暗号になります。特に大きく三つに分けることができまして、まずは先ほど説明

しました、秘密の通信ができるという、量子鍵配送というものがあります。

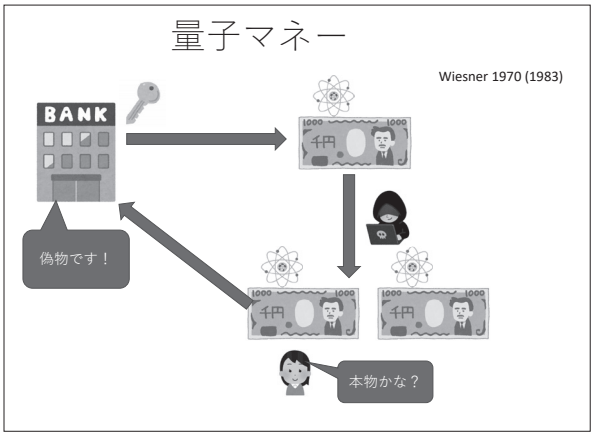


もう一つは、さっきも言いましたように、実は暗号というのはメッセージを秘密に送るだけではない。いろんなことができます。そういういろんなものを量子を使ってやりましょうという、量子暗号プロトコルという研究があります。

あともう一つ、ちょっと似ていて紛らわしいんですけど、耐量子暗号という研究もあって、これは暗号自体は普通の、我々が使っている古典のコンピューターと、今、使っているインターネット上で動く暗号を使います。ですけど、それが量子的な攻撃に対してどう安全化か、ということを調べるような研究になります。

つまり量子コンピューターを使うと計算能力が向上しますので、例えば素因数分解が解けるから、素因数分解とは違う、難しい問題を考えなきゃいけないとか、あるいはデータベースに量子的な重ね合わせでアクセスしてくるから、そういう攻撃に対しても安全かどうかを調べなきゃいけないと、そういうことの研究をしています。

でも、私は主に２番のほうを研究してきまして、２番の分野における例を最後に紹介して、終わりたいと思います。

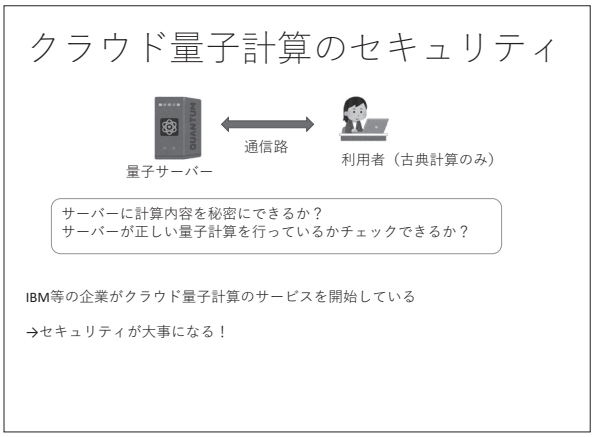


一つ目の最もメジャーな例が、量子マネーですね。これはイスラエルのウィズナーという人によって、1970年に提案されました。ですけど、1970年はそもそも量子コンピューターのアイデアが出ていない時代で、ものすごく革新的すぎて、みんなに受け入れられなくて、論文が公開されたのは、その13年後だそうです。

この量子マネーはどういうものかというと、量子状態はクローンをつくれないという、No-cloningがありますよね。なので、お札に量子状態を埋め込んで、そうすると悪い人が偽造して二つ、つくったとしても、偽物であるということが絶対にばれてしまうと。だから偽造できませんというのが、この量子マネーというアイデアになります。

もう一つは、クラウド量子計算のセキュリティーということで、量子コンピューターは今、いろいろとつくられつつありますけれども、非常に高価で巨大なんですね。何億もするんです。なので、一家に一台というよりかは、クラウド的に使われると。センターに大きな量子

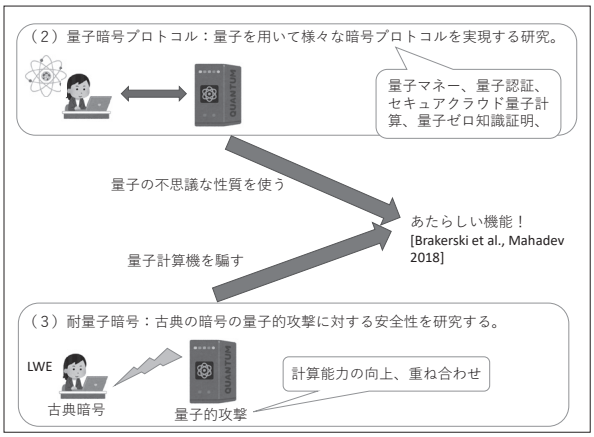
コンピューターがあって、使う人は自宅からインターネットでリモートにアクセスして、ここで量子計算する。そういうクラウド的に使うわけですね。



そういうときに、セキュリティーが気になる。サーバーに計算内容を秘密にできるかとか、あるいは正しい計算をしているかどうかをチェックしたい、そういうセキュリティーが気になってくるわけですね。そういうものについていろいろと研究するというのが、この分野になります。

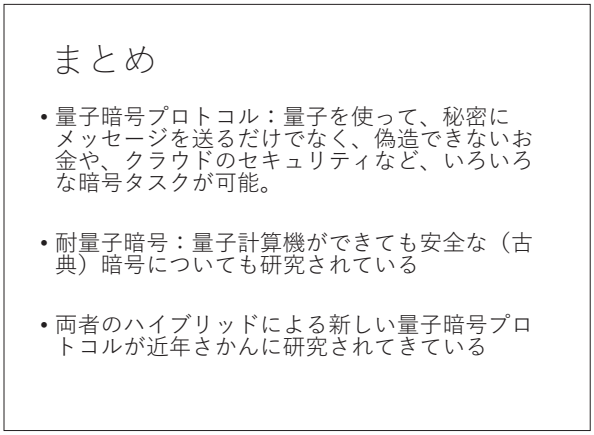
実際にクラウド量子計算のサービスというのは、今はもうありまして、米国のIBMとか、いろんな企業がそういうサービスをやっていて、研究者が実際にそれを使っているというレベルになっています。

最後になりますけれども、今、まさに最先端の研究の一つなんですけれども、これまではそういう量子暗号、量子を使っていろんな暗号をやろうという、量子暗号プロトコルの研究と、あとは量子から暗号を守ろうという研究は、別々に行われてきたんですね。ですけども最近、量子の不思議な性質を使って、いろんなことをやろうと。さらに、これは量子コンピューターから守るだけではなくて、積極的に量子コンピューターをだましに行こうと。



つまりこの暗号というのは、量子コンピューターで破られないようなものであるから、それをうまく使うと、量子コンピューターをだますことができるんですね。そういうことをして、ここだけやっていては、量子だけ使っていてはできなかったような、新しい機能を持つような暗号をつくろうという研究が、まさに今、行われているという状況になっています。

最後に、量子暗号のまとめですけれども、量子暗号プロトコルというのは、量子を使って秘密にメッセージを送りましょうとか、あるいは偽造できないようなお金とか、クラウドのセキュリティーとか、そういういろんな身の回りの暗号タスクを量子でやりましょう、という研究です。

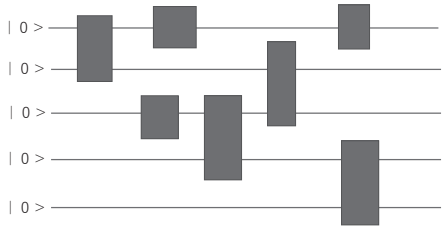


あと、耐量子暗号というのは、量子計算機ができても、安全な暗号をつくろうと。今、我々のコンピューター上で動くような古典の、安全な暗号をつくろうという研究になります。

最近では両者のハイブリッドによって、新しい量子暗号プロトコルをつくる研究なんかも盛んに行われている、というのが最近の状況になっています。

ということで、30分がたちましたので、以上になります。どうもありがとうございました。

量子回路、量子ゲート



1量子ビットゲート：1つの量子ビットを回す
2量子ビットゲート：2つの量子ビットの間にエンタングルメントをつくる

量子計算とは

古典計算機：古典論に基づく計算機。要するに今我々が使っているもの。

量子計算機：量子論の不思議な現象をうまく使って古典計算より高性能な計算を行うコンピューターのこと

高性能の意味

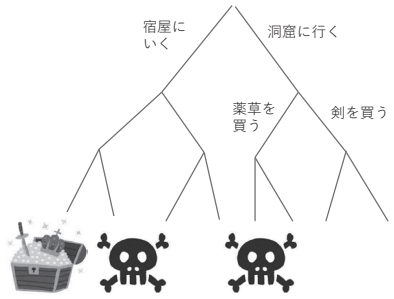
古典計算より高速
古典計算より省メモリ
古典計算にない機能がつく

量子計算に関する誤解

量子計算は重ね合わせにより、爆発的な組み合わせのすべてを並列に処理できる

これにより、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、等において高速に解を見つけてくれる

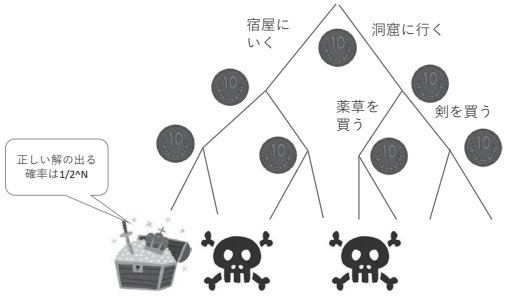
まちがい！



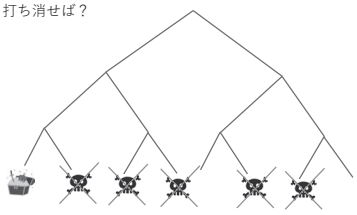
選択肢の数がN個あると、全てのパターンは２のN乗個になる。。。

量子的重ね合わせを使えば一発で並列処理できるのでは！？

重ね合わせを作って測定するだけなら古典の確率的計算（各分岐でコインを振る）と同じ



量子的干渉効果を使い、打ち消せば？



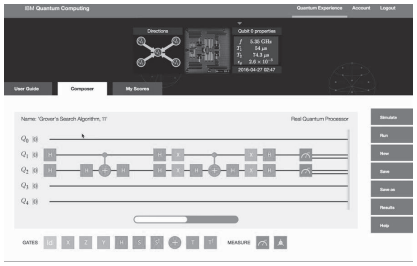
→しかし、打ち消してうまくいくのは特定のうまい構造がある場合のみしか知られていない。（素因数分解とか）。一般にはどうやって打ち消していいか分からない。

→まったく構造を使えない場合（＝しらみつぶし）は、量子計算機でも指数時間必要であることが数学的に証明されている！

[Bernstein et al. 1997]　ショアーのアルゴリズムは１９９４年！

つまり、研究者の間では、量子計算のかなり初期のころから知られている常識。

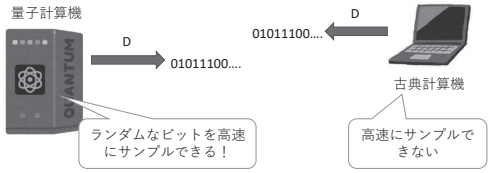
クラウド量子計算　（IBM）



今は研究者が使用。今後一般に普及するためにはセキュリティが大切に

量子スプレマシー

2019 Google　超電導量子計算機
2020 中国　光量子計算機



理論的に強力な基盤のもとで量子の高速性を証明することができる
比較的簡単な量子計算機で実現できる

人工的な問題であり、応用が無い

最近の発展

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、

これまでに無い新しい機能を持つ量子暗号プロトコルが作れる！

理論的にも面白い！（量子計算、計算量理論、暗号理論を駆使！）

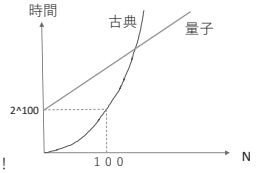
耐量子暗号：古典の暗号の量子的攻撃に対する安全性を研究する。

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！

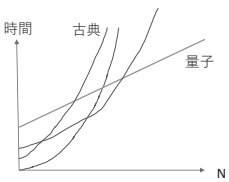
十分大きな量子ビットでは量子が勝つようになる

チャーチチューリングのテーゼ

どんな古典計算機も漸近的には同じ速度

→メーカー等が出しているいろいろな「量子コンピューターの原理にインスパイアーされて作った量子コンピューターより速い古典マシン」はあくまで古典マシンなのですべて漸近的には普通の古典計算機と等価。

→今後どんな古典マシンがでてきてもそれは漸近的には全て等価。



つまり、実測値でみるのか漸近でみるのかを区別しないといけない

意味があるのは

（1）量子的性質を使うことにより全ての古典マシンより漸近的に速いことが理論的に示されている

→量子計算機はこれ。

（2）量子か古典かとか高速証明とかおいといて、なぜかわからないけど使ってみるととにかくやたら実測値で爆速

→それはそれであり。ただし、（2）が達成できていないから（1）であるかのように錯覚させてごまかすのは詐欺。

なぜ量子計算機は速いの？

答え：負の「確率」のおかげ

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

負の確率以外古典計算機と同じなので。

古典計算機：マルコフ連鎖
量子計算機：負の確率を使ったマルコフ連鎖

ただし、「じゃあ負の確率をどう使って高速化を実現しているの？」と聞かれたら、答えは「まだわかりません」。

→現在研究中の最先端の研究テーマ

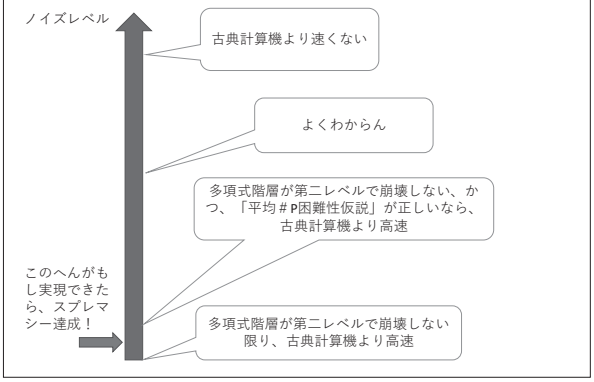
量子計算機は常に古典より高速というわけではない

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

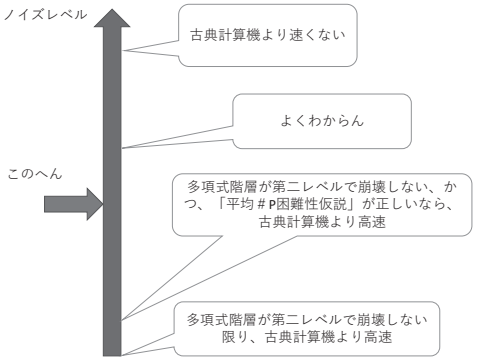
（1）の場合、（2）の場合ともに事例が知られている。

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

もっと正確には、ノイズレベルに応じて状況が変わる（実際のマシンにはノイズがある）



残念ながら、Googleマシンはノイズが大きすぎて、量子超越性理論は使えない。。。



なぜ量子計算は速いの？

量子的重ね合わせと、問題の構造をうまく利用した干渉による打消し。。。だろう

→完全にはよくわかっていない。

速くなる具体例、速くならない具体例が知られているのみ。

今まさに研究中のテーマ

えっじゃあ「古典計算機では１万年かかる」の根拠は？

→彼らが考えた「ベスト」の古典アルゴリズムで、１万年かかるというだけ。

→量子スプレマシー理論のように、「多項式階層が崩壊しない」とかで保証されたものではない。

実際、直後に

IBM：実際はもっとメモリ使えるから2.5日でできるよ。

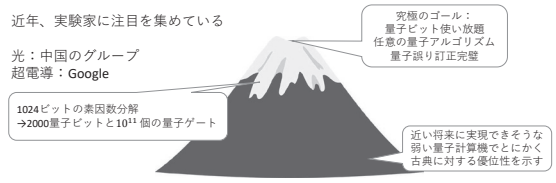
アリババ：テンソルネットワーク使うと20日でできるよ。

Barak：もっと直接的な高速アルゴリズムあるよ。（確率分布完全に計算しなくても、クロスエントロピーベンチマークを破れるような古典シミレーションを直接的につくれるよ。）

「弱い」マシンでもOK

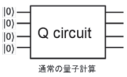
近年、実験家に注目を集めている

光：中国のグループ
超電導：Google



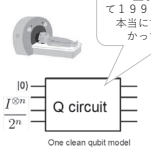
メジャーな「弱い」モデル

深さ４回路：Terhal-DiVincenzo 2004
IQP：Bremner-Montanaro-Shepherd 2016
ボソンサンプリング：Aaronson-Arkhipov 2011
One-clean qubit: Morimae 2017
ランダム回路：Fefferman-Bouland-Nirkhe-Vazirani 2018



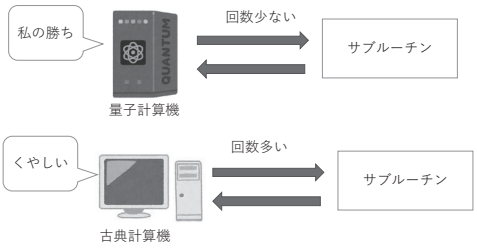
通常の量子計算

NMR量子計算のモデルとして１９９８年に提案される。本当に古典より速いか分かっていなかった。



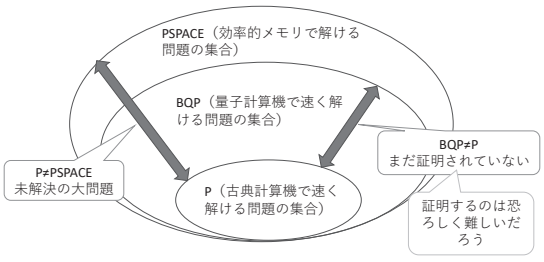
One clean qubit model

根拠１：グローバータイプ



サブルーチンを呼ぶ回数だけ見ている。
→計算量理論、アルゴリズムにおけるスタンダードなアプローチ（query complexity）
→古典の下限の証明がしやすい。（多くの結果が得られている。）
→実時間でどうなるか不明。

量子計算は古典計算より速いのか？
→計算量理論の標準的な意味ではまだ証明されていない



計算量理論の標準的な意味で「量子が古典より速い」を示すのは恐ろしく難しいだろう・・・

そうはいっても皆、量子計算は古典計算より速いだろうと信じている

根拠２：ショアータイプ

こちらは実時間を見る(time complexity)
量子アルゴリズムが古典のベストより高速であることを示す

素因数分解：古典では遅いが量子では速い

→古典では遅いという数学的証明があるわけではない

将来古典の高速アルゴリズムが見つかるかも！

例：recommendation system
客の購買データーからおすすめ商品を見つける量子機械学習アルゴリズム

→米国の１８歳の学部生が高速古典アルゴリズムを見つけてしまった！
[Tang, STOC2019]

古典のベストはアップデートされる可能性がある