量子コンピュータとは

ナノテクノロジーを利用した革新的なコンピュータ

- **量子効果**を利用し超高速計算を実現
- 専用の**量子アルゴリズム**が高速性の鍵

（注：アルゴリズム＝計算手順）

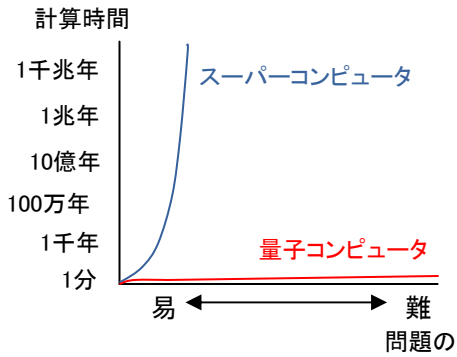
量子ビット

30%×  + 70%× 

観測すると，↑（0）が30%，↓（1）が70%の
確率で得られる重ね合わせ状態が存在する

計算速度比較例

例：
公開鍵暗号
(RSA)解読



研究の目的

新しい量子アルゴリズムの発見により
量子コンピュータ(ハードウェア)の
潜在的な超高速性能を引き出す

将来どのように役に立つか

- 巨大データベースの超高速検索
- 莫大なデータの超高速学習

などへの応用が期待されている

量子コンピュータ研究の現状と課題

ハードウェアもソフトウェアも新しく研究する必要がある

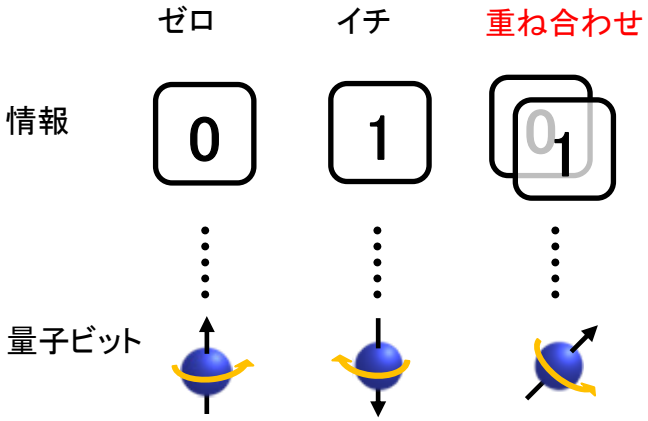
	現状	課題
ソフトウェア	• 因数分解，データ検索などの超高速量子アルゴリズムが見つかっている	• 量子通信プロトコル • 量子アルゴリズム • アルゴリズムの具体的実装方法 （当研究所の研究ターゲット）
ハードウェア	• 複数の方式が研究されている • 7量子ビットの計算が最大 • 量子アルゴリズムを使い，15=3×5の因数分解に成功	• 1000量子ビット以上の重ね合わせ状態の長時間制御

量子ビットと量子コンピュータ上の計算

量子ビットで情報を表現し，ユニタリ演算を作用させて計算を進める

量子ビット

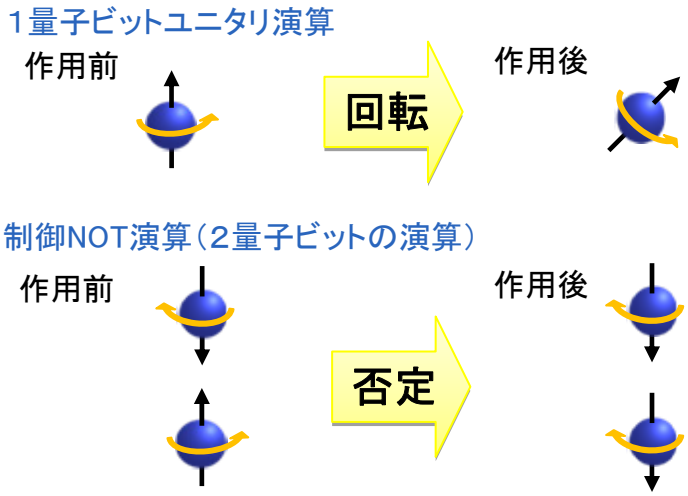
- 情報を表現する基本単位
- 0と1の重ね合わせを表現可能



量子コンピュータ上の計算

基本ユニタリ演算を量子ビットに作用させること

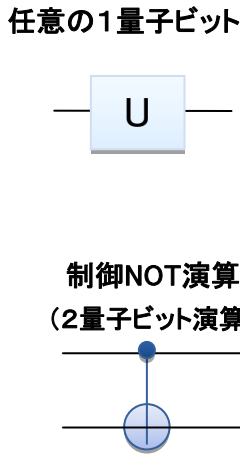
基本ユニタリ演算の例

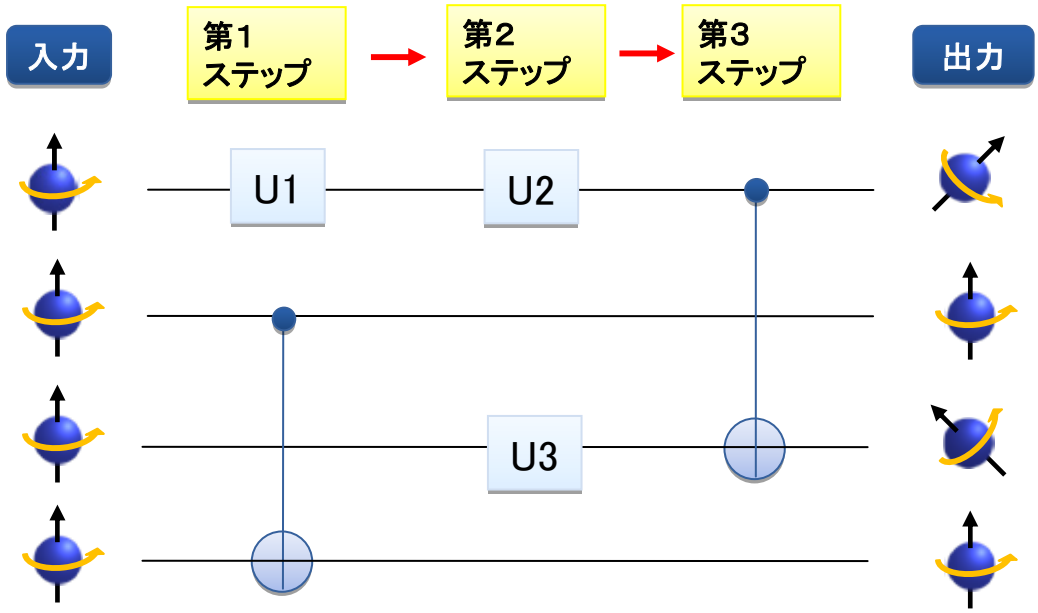


量子回路

基本ユニタリ演算を組み合わせて，量子コンピュータに計算をさせるための手順を表したもの

基本ユニタリ演算

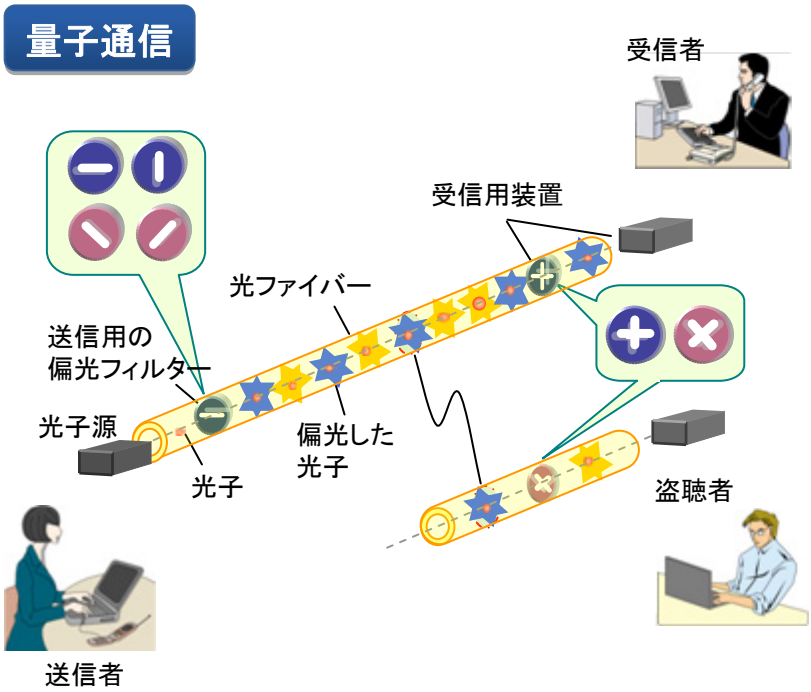




量子通信とは

光子の一個一個に情報をのせて送る，究極の通信方式

暗号に応用すると、量子力学の不確定性原理により
無条件安全性が保証できる



研究の目的

新しい量子通信プロトコルの発見により，量子通信の潜在的能力を明らかにする

将来どのように役に立つか

- 無条件安全な暗号通信
- 無条件安全なデジタル署名

などへの応用が期待されている

量子通信の現状と課題

量子鍵配送に関しては，すでに実用段階

	現状	課題
ソフトウエア	• 秘密鍵配送方式として BB84，E91，B92 などが有名 • 一部のプロトコルは，無条件安全性が証明されている • 近年，量子公開鍵暗号なども盛んに研究されている	• 量子公開鍵暗号 • 量子デジタル署名 • 量子ゼロ知識証明 • 無条件安全性証明 （当研究所の研究ターゲット）
ハードウエア	• 市販の端末装置が存在 - 通信距離数十km - 通信速度数kbit/s • 既存の光ファイバが利用可能	• 単一光子発生デバイス，量子中継器などの開発