量子コンピュータと暗号解読

量子コンピュータ

- 量子系における性質（重ね合わせや量子もつれ等）を利用するコンピュータ
- 従来型コンピュータでは解けない問題（素因数分解等）を現実的な時間で解ける可能性がある
- 量子力学における本質的な制約やハードウェアの制約により、従来型コンピュータを置き換えるものではない（アクセラレータ的な利用）
- 量子ゲート型と量子アニーリング型に分類される
  - 量子ゲート型：量子回路（従来型の論理ゲートに相当）を組み合わせて「プログラミング」する。現実的な問題を解けるものは未開発。
  - 量子アニーリング型：特定の問題（組み合わせ最適化問題）に特化した量子コンピュータ

量子ビット(qubit)

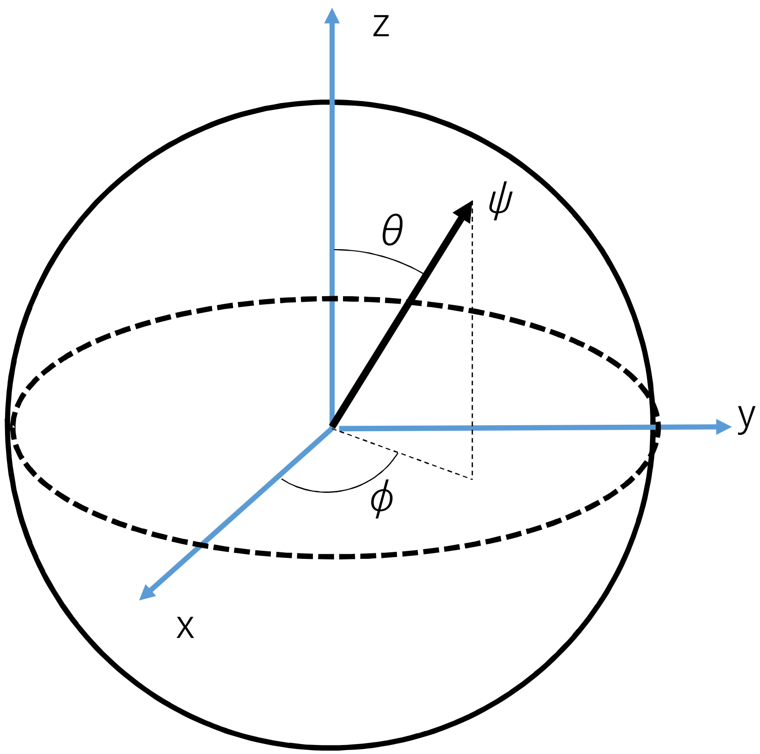
- 量子（光子や原子、イオン等）が持つ状態を情報(qubit)として扱う。ある状態ψ（一般に複素ベクトル）を$|\psi>$と表記する

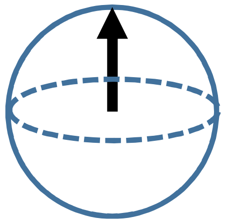
$$|\psi> = \alpha\ |0> + \beta\ |1>$$

  ただし、α、βは複素数で、$|\alpha|^2 + |\beta|^2 = 1$。
- $|\psi>$状態にある量子を「観測」すると、確率$|\alpha|^2$で状態0が、確率$|\beta|^2$で状態1が観測される。一旦観測されると量子の状態は失われる
- 状態0と状態1が等しく重ねあわされた独立な量子n個の系があると、2^n個の状態を同時に保持していることになる
  →うまく利用すれば、指数関数的な組み合わせの計算が可能

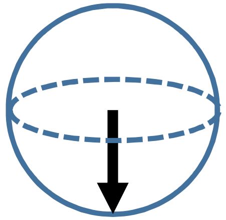
ブロッホ球

- １量子ビットの状態はブロッホ球（半径１の単位球）により表現できる

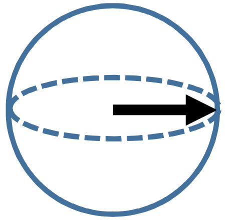




$$|\psi> = |0>$$



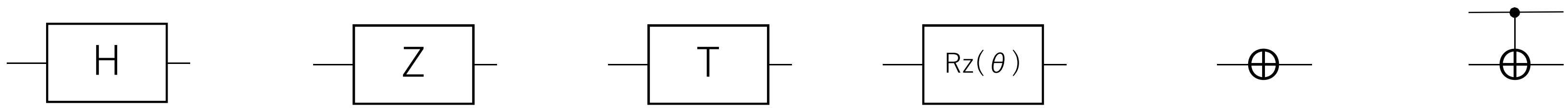
$$|\psi> = |1>$$



$$|\psi> = \frac{1}{\sqrt{2}}(|0> + |1>)$$

量子ゲート

- 従来型コンピュータの論理ゲートに相当する論理演算回路。ユニタリ変換で表現できる演算であり、処理自体はアナログ処理。



$\frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\1 & -1\end{bmatrix}$	$\begin{bmatrix}1 & 0\\0 & -1\end{bmatrix}$	$\begin{bmatrix}1 & 0\\0 & e^{i\pi/4}\end{bmatrix}$	$\begin{bmatrix}e^{-i\theta/2} & 0\\0 & e^{-i\theta/2}\end{bmatrix}$	$\begin{bmatrix}0 & 1\\1 & 0\end{bmatrix}$	$\begin{bmatrix}1000\\0100\\0001\\0010\end{bmatrix}$
|0>と|1>の重ね合わせ状態にする	|1> → -|1> |0>なら不変。	|1>ならπ/4回転。|0>なら不変	-θ/2位相回転	|0> →|1> |1> →|0>	制御ビット|1>のときNOT、|0>の時は不変
アダマール	パウリZ	T	Z-rotation	NOT	CNOT

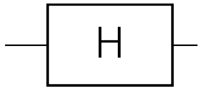
ユニタリ変換とは

- 複素正方行列Uにおいて、$U^*U = UU^* = E$を満たすとき（U^*はUの複素共役）、Uをユニタリ行列という
- 複素ベクトルxのUによる変換$y = Ux$をユニタリ変換と呼ぶ
- ユニタリ変換の重要な性質として全ての固有値λの絶対値が1。すなわち、$Uv = \lambda v$であるとき、$|\lambda| = 1$である。（$\lambda = e^{2\pi i\theta}(0 \leq \theta < 1)$と書ける）

量子ゲートの例（1）

- アダマールゲート

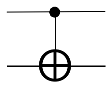
$$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$



初期状態$|0\rangle$に作用させると、$H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$となり、$|0\rangle$と$|1\rangle$の重ね合わせ状態を作ることができる。

- CNOTゲート

$$\Lambda(X) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$



CNOTゲートは、2量子ビット$|00\rangle, |01\rangle, |10\rangle, |11\rangle$に対して作用する。1つめのビットが$|0\rangle$なら何もせず、$|1\rangle$なら2つめのビットを反転させる。

量子ゲートの例（２）

- CNOTゲートの動作例（$\otimes$はテンソル積）

$$|\psi\rangle=\begin{pmatrix}|00\rangle\\|01\rangle\\|10\rangle\\|11\rangle\end{pmatrix}=(H|0\rangle)\otimes|0\rangle=\frac{1}{\sqrt{2}}\begin{pmatrix}1\\0\\1\\0\end{pmatrix}$$

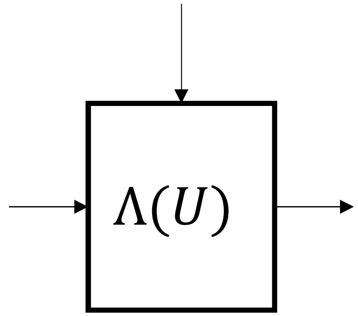
$$\Lambda(X)|\psi\rangle=\frac{1}{\sqrt{2}}\begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&0&1\\0&0&1&0\end{pmatrix}\begin{pmatrix}1\\0\\1\\0\end{pmatrix}=\frac{1}{\sqrt{2}}\begin{pmatrix}1\\0\\0\\1\end{pmatrix}=\frac{1}{\sqrt{2}}(|00\rangle+|11\rangle)$$

- 上記で得られた量子状態は、第1ビットの状態$|u\rangle$と第2ビットの状態$|v\rangle$とするとき、$|u\rangle\otimes|v\rangle$の形では表すことができない（第1ビットと第2ビットの間に量子的な相関がある）。
この状態を**量子エンタングルメント（量子もつれ）**という。

制御ユニタリー演算

- CNOTを一般のユニタリー演算U(d次元)に一般化することにより制御ユニタリー演算$\Lambda(U)$を以下のように構成できる

$$\Lambda(U)=\begin{pmatrix} I_d & 0 \\ 0 & U \end{pmatrix}$$



ただし、I_dは$d\times d$の単位行列である。

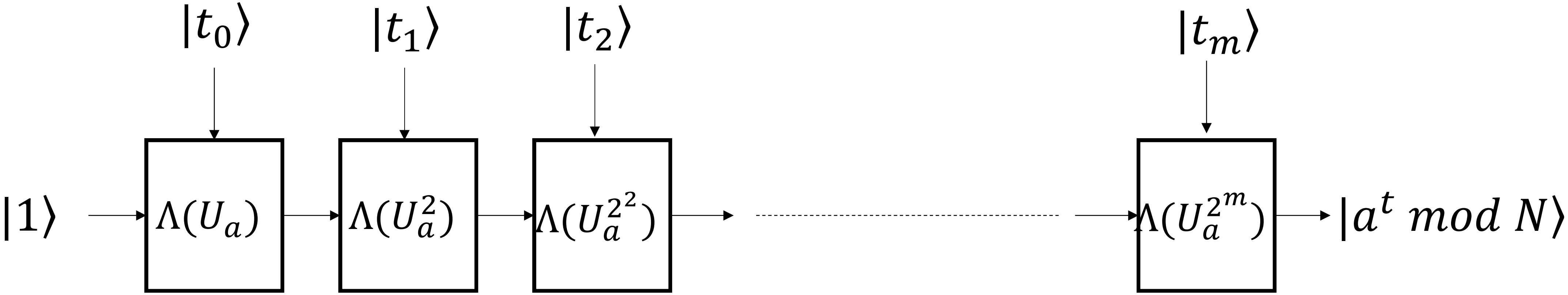
- いま、Uの固有状態を$|\psi\rangle$とし、その固有値をλとする。

$$\Lambda(U)(\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)\otimes|\psi\rangle)=\frac{1}{\sqrt{2}}(\Lambda(U)(|0\rangle\otimes|\psi\rangle)+\Lambda(U)(|1\rangle\otimes|\psi\rangle))$$
$$=\frac{1}{\sqrt{2}}(|0\rangle\otimes|\psi\rangle+|1\rangle\otimes U|\psi\rangle)=\frac{1}{\sqrt{2}}(|0\rangle+\lambda|1\rangle)\otimes|\psi\rangle$$

- 上記より、$\Lambda(U)$を適用した後の第1ビットの$|1\rangle$の係数として固有値λが現れていることがわかる。

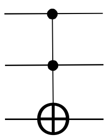
べき乗の計算

- $t = t_0 + t_1 \times 2 + t_2 \times 2^2 + \cdots + t_m \times 2^m \ (t_i \in \{0,1\})$と2進展開できるとき、$a^t (mod\ N)$を計算する量子回路はユニタリ演算子（$U_a|x\rangle = |ax\ mod\ N\rangle$）から作られる制御ユニタリ演算$\Lambda(U_a)$を用いて以下のように構成できる



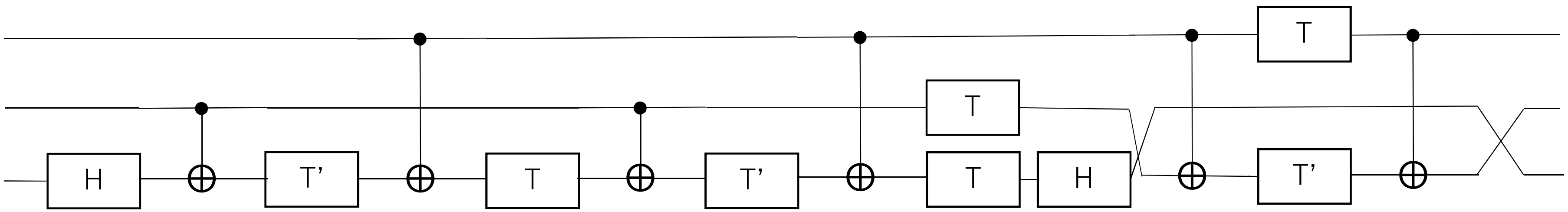
量子ゲートの組み合わせ

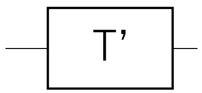
- 基本的な量子ゲート（H,T,CNOT)を組み合わせて、より複雑な任意の量子ゲートを作成できる



２つある制御ビットの両方が１であれば、入力ビットが反転する。
それ以外は、入力ビットは変化しない。

トフォリゲート





Tゲートの逆変換

ショアのアルゴリズム

- 量子コンピュータを用いることにより素因数分解および離散対数問題を高速に（多項式時間で）計算できるアルゴリズムが示された(1994)
- 素因数分解問題や離散対数問題は、現在用いられている多くの公開鍵暗号系(RSA暗号、エルガマル暗号、楕円曲線暗号など)においてその安全性の根拠となっているため、量子コンピュータが実用化されると、これらの暗号を利用できなくなる
- 現在、量子コンピュータを用いても解読できない暗号（耐量子計算機暗号(Post-Quantum Cryptography; PQC)の開発が進められている

ショアのアルゴリズムの原理

- 法$N(=pq)$において数aの周期rを求めると、高い確率でNの素因数が判明する。
- （例）$N = 35(= 5 \times 7)$とする。$a = 2$の周期を求めると、$2^{12} = 1\ (mod\ 35)$である。ここで、

$$\begin{aligned} 2^{12} - 1 &= \left(2^6 + 1\right)\left(2^6 - 1\right) \\ &= \left(2^6 + 1\right)\left(2^3 + 1\right)\left(2^3 - 1\right) \\ &= \left(2^6 + 1\right)\left(2^3 + 1\right) \times 7 \end{aligned}$$

  となり、素因数7が判明する。
- 上の例で、$a = 11$とすると、周期は$11^3 = 1(mod\ 35)$となり、この場合は素因数を求められない。
- 周期は多項式時間では求められないので（従来型の）コンピュータではこの方法は現実的でない。

ショアのアルゴリズムの流れ

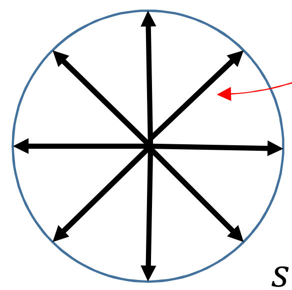
1. 合成数Nに対し、ランダムに$a(0 < x < N)$を選ぶ
   （$(a, N) = 1$とする。$(a, N) > 1$なら素因数が見つかったことになる）
2. $a^r = 1 (mod\ N)$となる位数rを量子コンピュータにより推定（量子位相推定）
3. 位数rが偶数でなければ1に戻る
4. $(a^{\frac{r}{2}} + 1, N)$または$(a^{\frac{r}{2}} - 1, N)$が1でなければ素因数が見つかったことになる。そうでなければ1に戻る

- 量子コンピュータで計算するのはステップ2のみ。他は従来型コンピュータでOK
- ステップ2で実際に求まるのは、$\frac{s}{r}\ (0 \leq s < r)$の近似値だが、ここから連分数展開により$r$を（従来型PCで）推定する

ショアのアルゴリズム（1）

- 以下のユニタリ演算子U_aを考える
$$U_a|x> = |ax \, mod \, N>$$
- 仮定より$(a, N) = 1$なので、全ての$x(0 < x < N)$は、$1 \sim N - 1$の値のどれかと1対1に対応するのでユニタリ変換であることがわかる
- aの周期（位数）をrとすると、U_aの固有状態$|u_s\rangle$は以下のように与えられる$(0 \leq s < r)$
$$|u_s\rangle = \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} e^{-\frac{2\pi isk}{r}} \left|a^k \, mod \, N\right\rangle$$
- これは、$U_a|u_s\rangle = e^{\frac{2\pi is}{r}}|u_s\rangle$となることから確認できる
- 固有状態$|u_s\rangle$に位数rが含まれている！この固有状態に対し量子位相推定という操作により位相$\frac{s}{r}$が推定できる。
（しかし、位数rが分からないので固有状態を直接作ることはできない）

ショアのアルゴリズム（２）

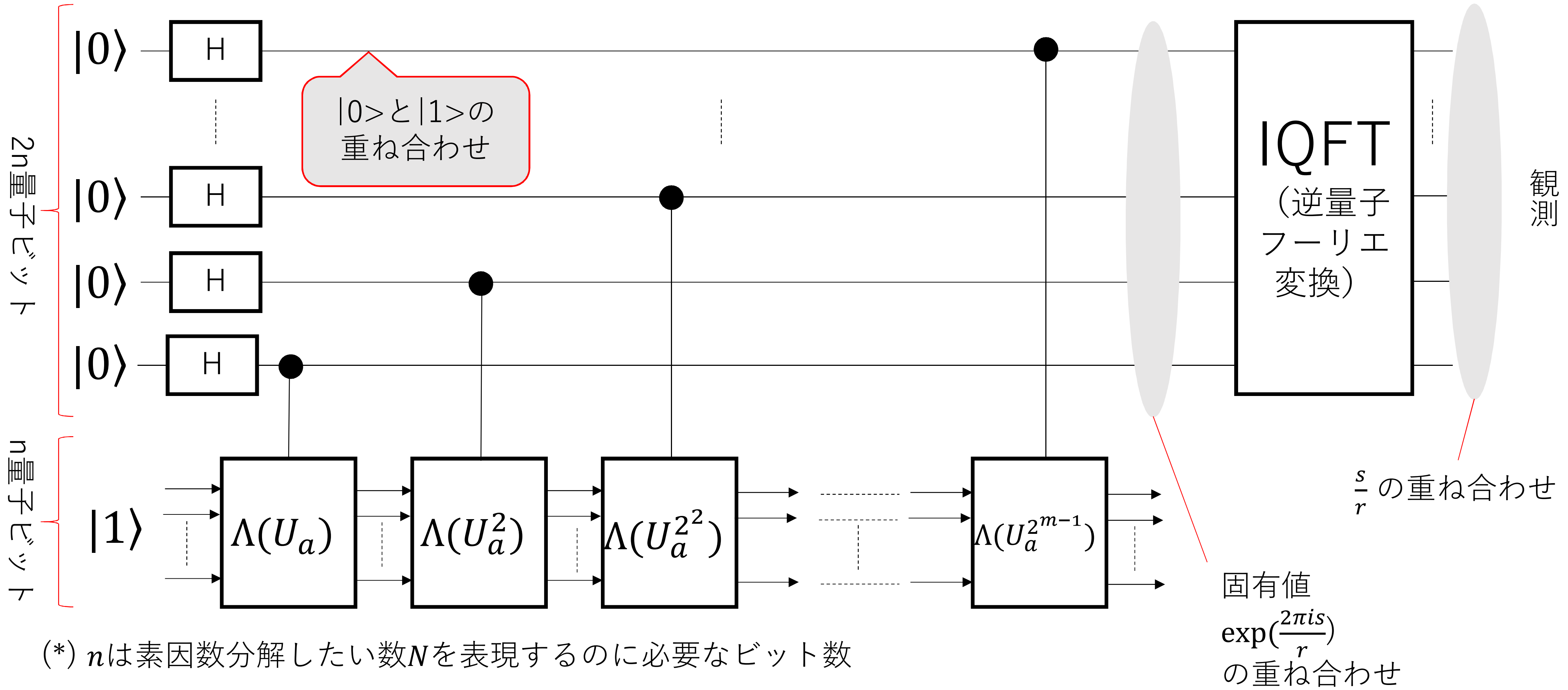


- 固有状態$|u_s\rangle$の和（重ね合わせ）を考える。
  以下が成り立つ（rが偶数のとき）

$$\frac{1}{\sqrt{r}}\sum_{s=0}^{r-1}|u_s\rangle = |1\rangle$$

- $|1\rangle$は簡単に作ることができるので、これに対して位相推定を行えば、最終的に$\frac{s}{r}$ $(0 \leq s < r)$のどれかを観測できる
- 観測された$\frac{s}{r}$の近似値に対して、連分数展開により分母rを求める

ショアのアルゴリズムの量子回路



(*) nは素因数分解したい数Nを表現するのに必要なビット数

量子コンピュータの今後

- ショアのアルゴリズムの計算量（ $O\left((\log N)^3\right)$
  - 素因数分解する数の桁数の多項式オーダーで計算可能になるので、鍵ビット長を長くしても対応できない。
- 現在実現している量子コンピュータの量子ビット数は5～7bit程度であり、$15 = 3 \times 5$や$21 = 3 \times 7$の素因数分解に成功している段階。2048bitの合成数を素因数分解するためには、6144量子ビット程度が必要であり、多くの技術的ブレイクスルーが必要
- 多量子ビットの計算では、途中でビット誤りが生じるため、誤り訂正を行いながら計算する技術(量子誤り訂正)も必要になる
- 量子状態を長時間保持する(デコヒーレンス)技術開発も求められる