Shor’s Algorithm

第5讲：Shor算法原理二

3. 执行步骤

本 源 量 子

（判断一个数是不是质数只需用多项式时间）

(1) 取一个待分解的数N，其中，N需要满足：非偶，非质，非某个质数的指数形式；

(2) 随机取一个数$a \in [2, N-1]$，若$\gcd(a, N) \neq 1$，返回$\gcd(a, N)$

(3) 找到函数$f(x) = a^x \bmod N$的周期r，若$r \pmod 2 = 0$（偶数）且$a^{\frac{r}{2}} \neq -1 \pmod N$，

求出$\gcd\left(a^{\frac{r}{2}} \pm 1, N\right)$；若$r$不满足上述条件，回步骤(2)，重复直到找到满足条件的a和r；

（判断一个数是不是质数只需用多项式时间）

（1）取一个待分解的数N，其中，N需要满足：非偶，非质，非某个质数的指数形式；

（2）

（3）……求 出

gcd(

补充：

$f(x) = a^x mod\ N$ 必然是周期函数，因为是模指函数，所以一定

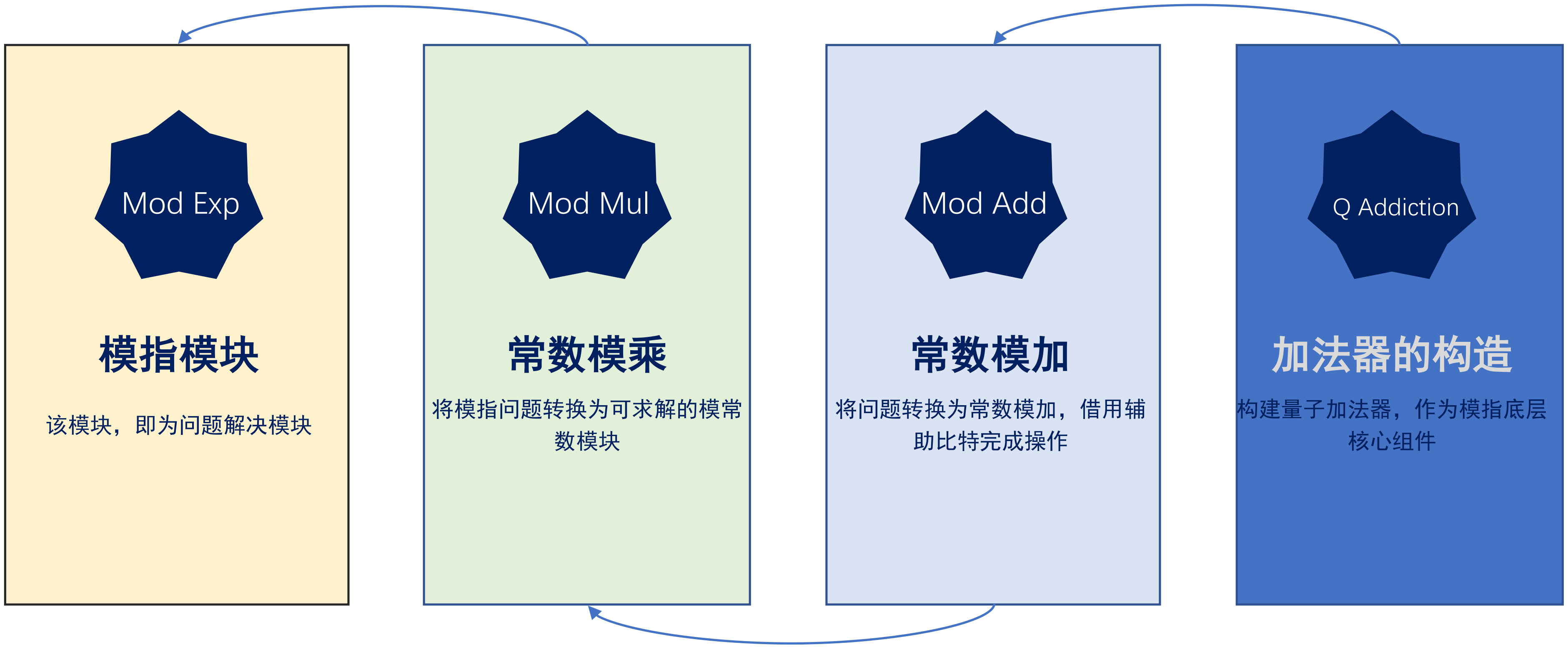
$\exists a, b(a < b) \rightarrow f(a) = f(b)$,则，

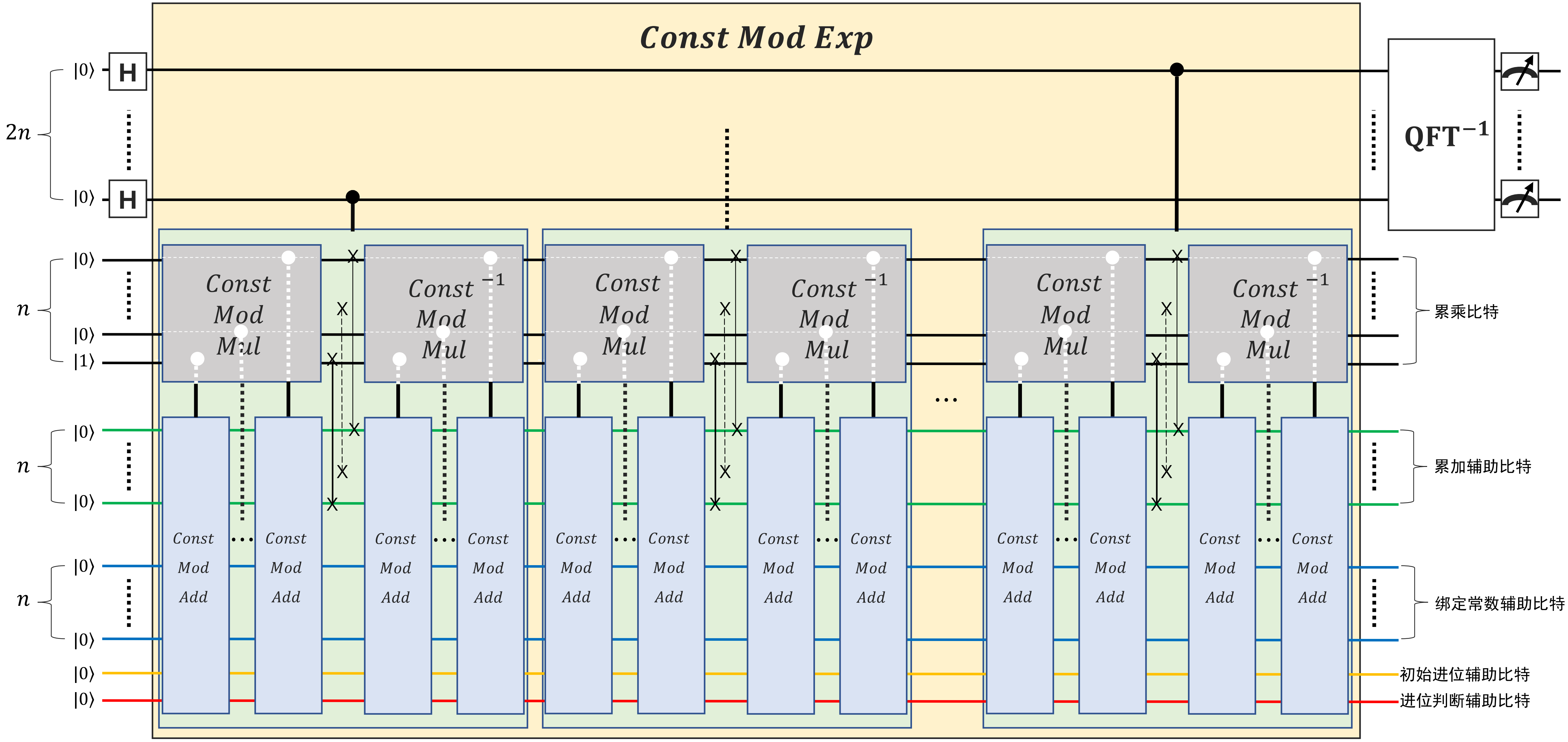
$\forall x$, 有$f(a+x) = a^{x+a}\ mod\ \ N\ = a^{x+b}\ mod\ N\ = f(b)$，从而

$f(x) = f(b-a+x)$，其中$b-a$为周期或周期的倍数；

4. 线路框架

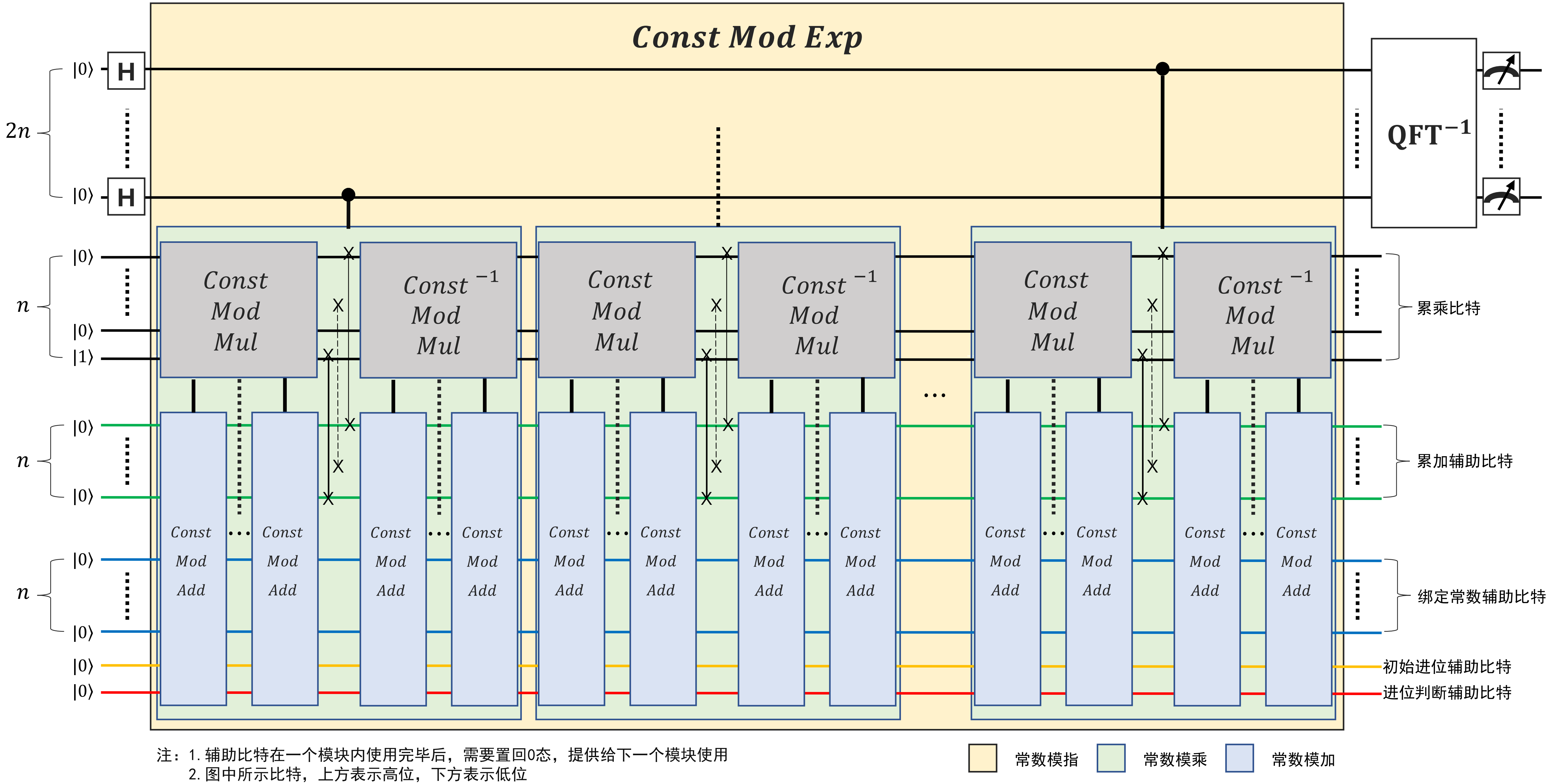
本 源 量 子


Mod Exp
模指模块
该模块，即为问题解决模块
Mod Mul
常数模乘
将模指问题转换为可求解的模常数模块
Mod Add
常数模加
将问题转换为常数模加，借用辅助比特完成操作
Q Addiction
加法器的构造
构建量子加法器，作为模指底层核心组件



注：1. 辅助比特在一个模块内使用完毕后，需要置回0态，提供给下一个模块使用
2. 图中所示比特，上方表示高位，下方表示低位

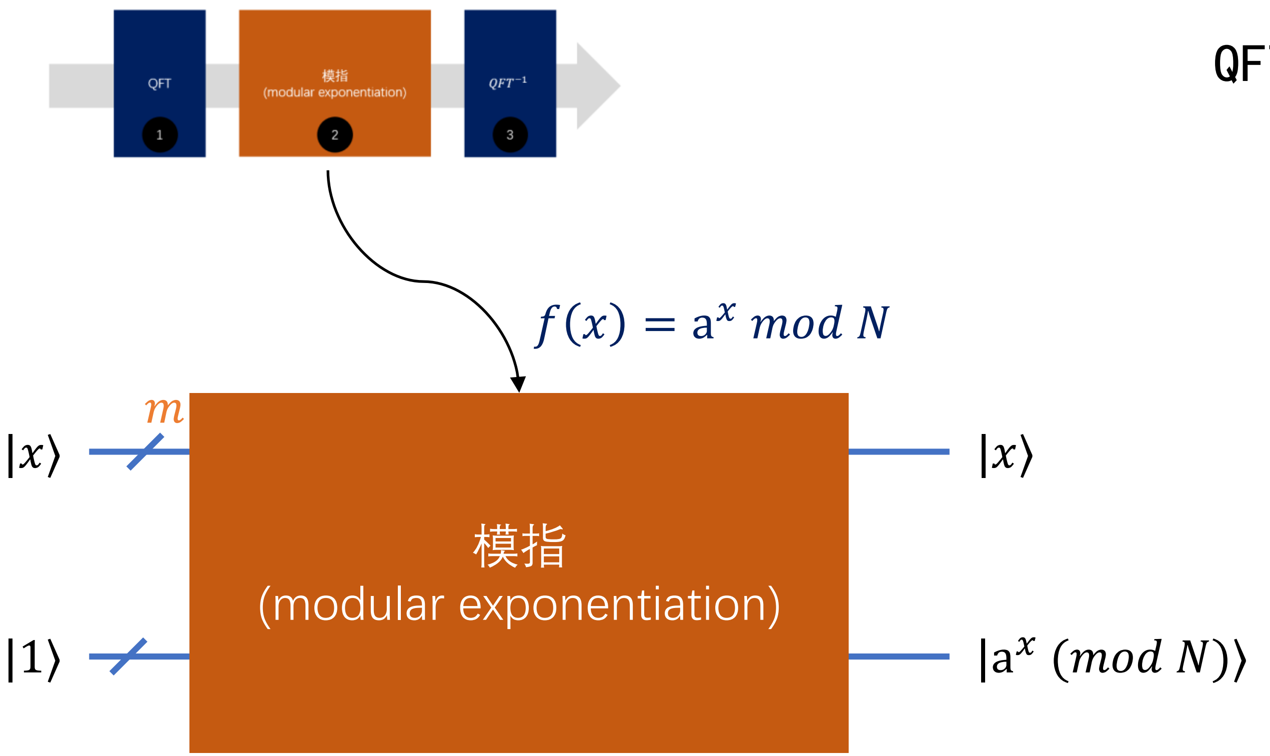
常数模指　常数模乘　常数模加



注：1. 辅助比特在一个模块内使用完毕后，需要置回0态，提供给下一个模块使用

2. 图中所示比特，上方表示高位，下方表示低位

线路组成：模指



$|x\rangle|1\rangle \rightarrow |x\rangle|f(x)\rangle$

QFT和模指数线路$f(x) = a^x mod \ N$

分析：

N对应的二进制长度为n，输入的x的位数m不固定，一般为$2n$位，即$m = 2n$

考虑 $\lceil log_2 N \rceil$ 是分解数N所需要表示的比特数

线路组成：模指转化为模乘

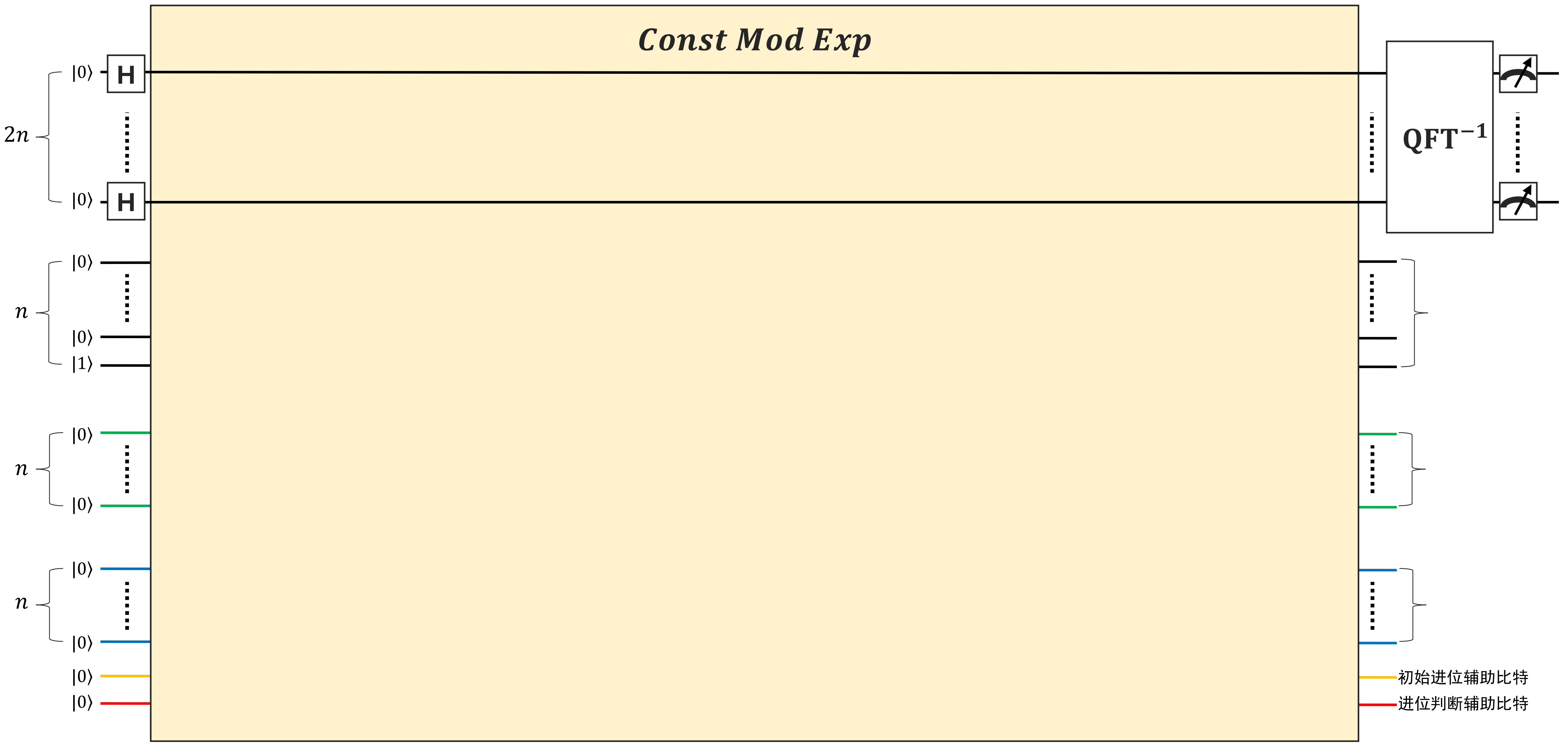
模指：$f(x) = a^x \ mod\ N$

x的二进制表达式

1 $x = (x_{2n-1}, \ldots, x_1, x_0) = \sum_{i=0}^{2n-1} x_i \times 2^i$ 其中， $x_i, (i = 0 \ldots 2n-1)$

2 $f(x)$可以写成：$f(x) = \prod_{i=0}^{t-1} a^{2^i x_i} \ mod\ N = a^{x_i \times \Sigma_i^{2n-1} a^i} \ mod\ N$

即：$(a^{2^0} \bmod N)^{x_0} \cdot (a^{2^1} \bmod N)^{x_1} \cdots (a^{2^{2n-1}} \bmod N)^{x_{2n-1}} \bmod N$



Const Mod Exp
QFT^{-1}
H
H
2n
n
n
n
|0⟩
|1⟩
初始进位辅助比特
进位判断辅助比特

线路组成:模指转化为模乘

模指：$f(x) = a^x \ mod \ N$

x的二进制表达式

1 $x = (x_{2n-1}, \ldots, x_1, x_0) = \sum_{i=0}^{2n-1} x_i \times 2^i$ 其中， $x_i, (i = 0 \ldots 2n-1)$

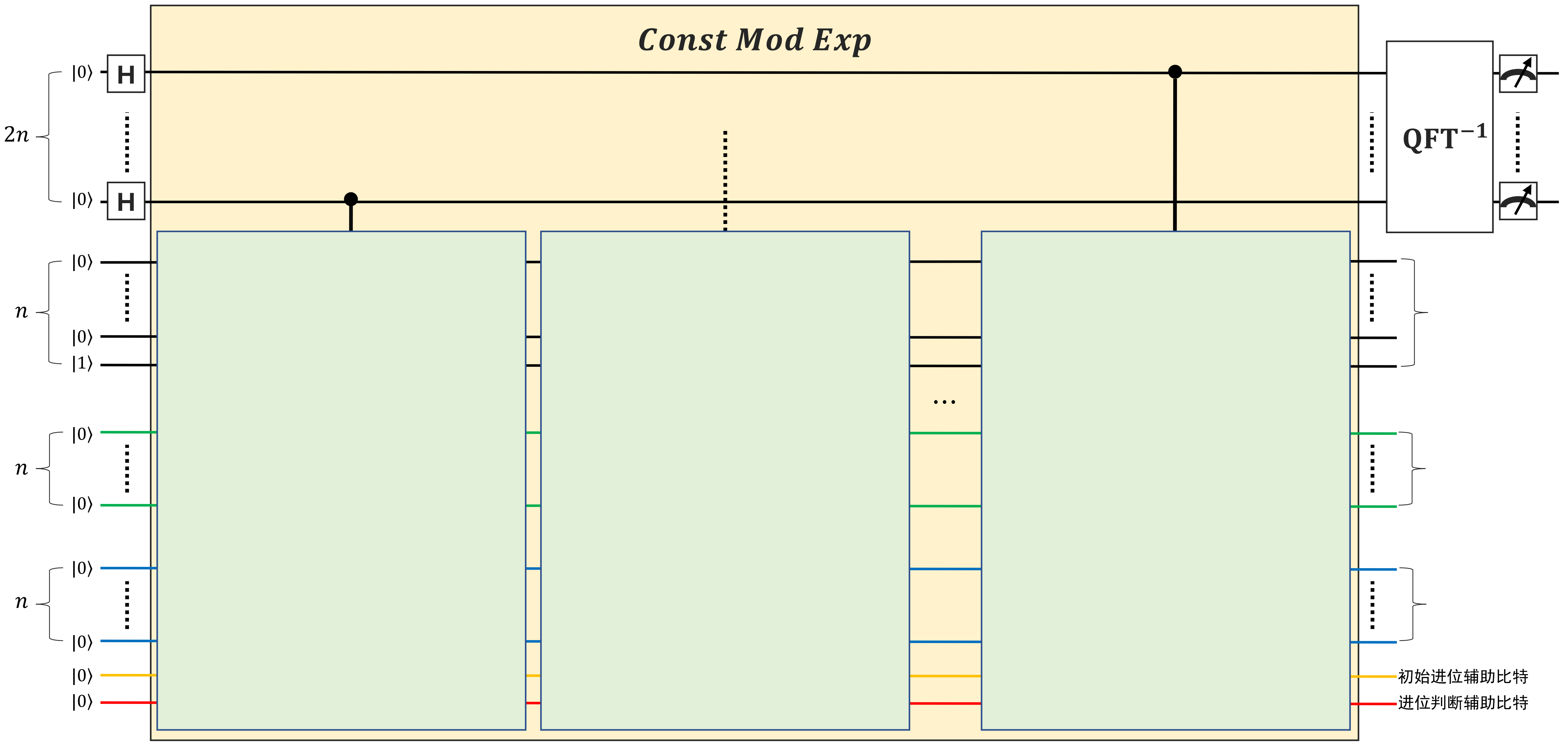
2 $f(x)$可以写成：$f(x) = \prod_{i=0}^{t-1} a^{2^i x_i} \ mod \ N = a^{x_i \times \sum_i^{2n-1} a^i} \ mod \ N$

即：$(a^{2^0} \bmod N)^{x_0} \cdot (a^{2^1} \bmod N)^{x_1} \cdots (a^{2^{2n-1}} \bmod N)^{x_{2n-1}} \bmod N$

3 假设有线路$U|y\rangle \rightarrow |Cy \ mod \ N\rangle$, 取$C$为$a^{2^i}$， $i = 0,1, \ldots, 2n-1$,将$|y\rangle$的初态设为$|1\rangle$,然后依次经过$C_i U_i$门:

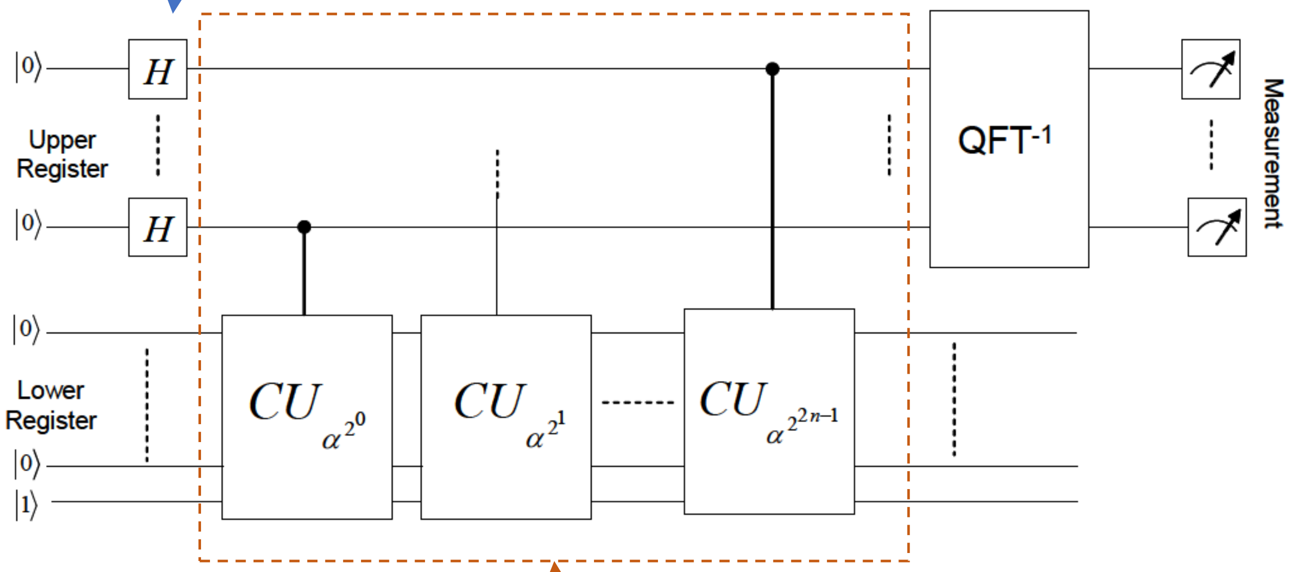
$$|1\rangle \rightarrow \left|a^{x_i \times \sum_i^{2n-1} a^i}\right\rangle \sim \sim |a^x \ mod \ N\rangle$$

常数模乘


Const Mod Exp
QFT^{-1}
2n
n
n
n
|0⟩
|1⟩
H
初始进位辅助比特
进位判断辅助比特

线路框架

QFT的初始态是$|0\rangle$时，等价于做H门操作



一系列的$C_i - U_i$门

分析：

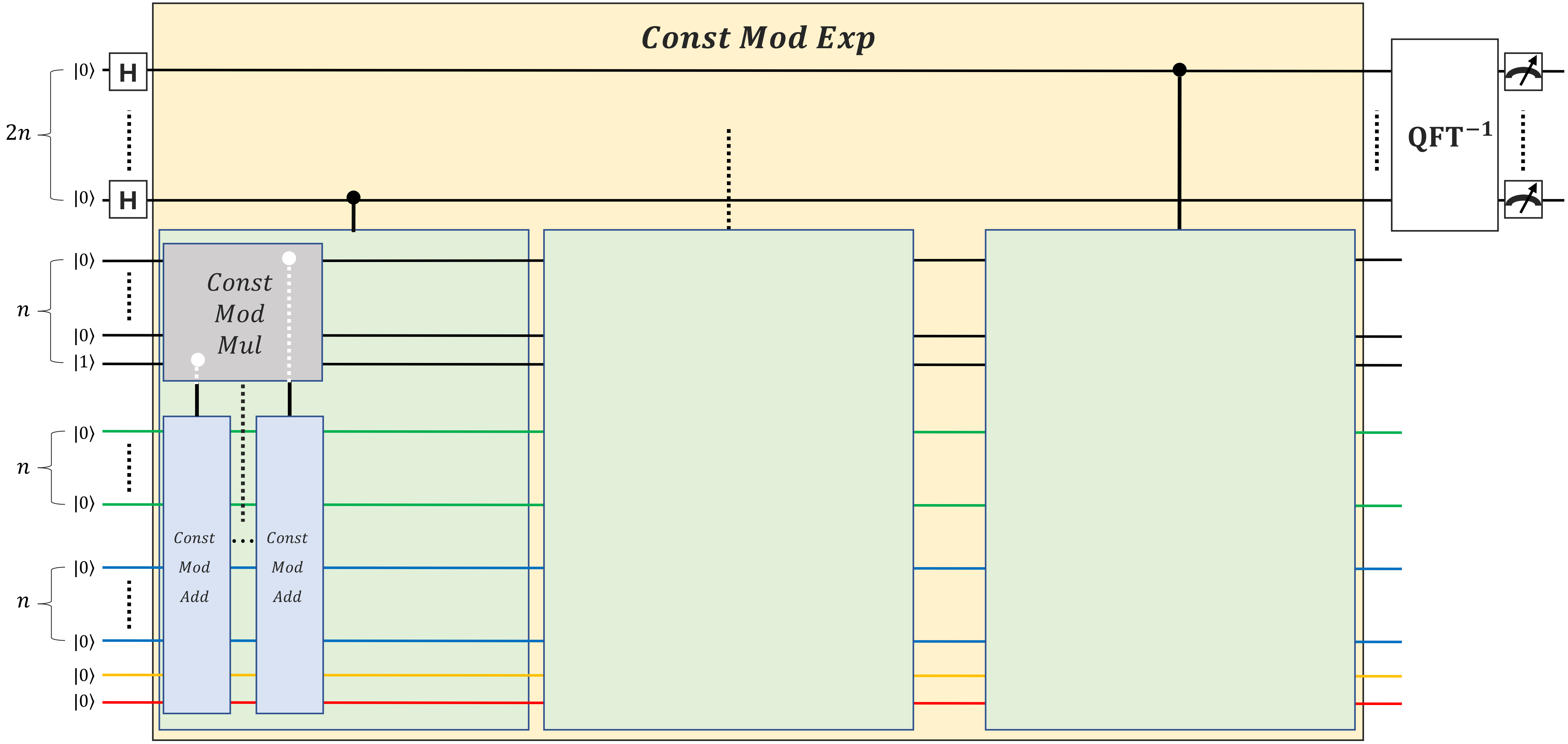
首先在$|x\rangle$上加QFT构成叠加态，同时将2^{2n-1}个x输入线路，用QFT^{-1}分析经过模指线路后的态的周期性，从而得到$f(x)$的周期；

这里总共有2n个控制U块。每个输入量子比特都控制着下方的模N乘法器 $CU_{a^{2^i}}$，注意这里设其常数为 a^{2^i}。

$$U|y\rangle \rightarrow |Cy \bmod N\rangle$$

1. 使用同样的方法，用二进制表示$y = \sum_{i=0}^{n-1} y_i \times 2^i$，同理 y_i 做控制位，

   将所需问题转化为加法$C_i - U(ADD)$:



Const Mod Exp
2n
|0⟩
H
|0⟩
H
n
|0⟩
|0⟩
|1⟩
Const Mod Mul
n
|0⟩
|0⟩
n
|0⟩
|0⟩
|0⟩
|0⟩
Const Mod Add
Const Mod Add
QFT^{-1}

$$U|y\rangle \rightarrow |Cy \bmod N\rangle$$

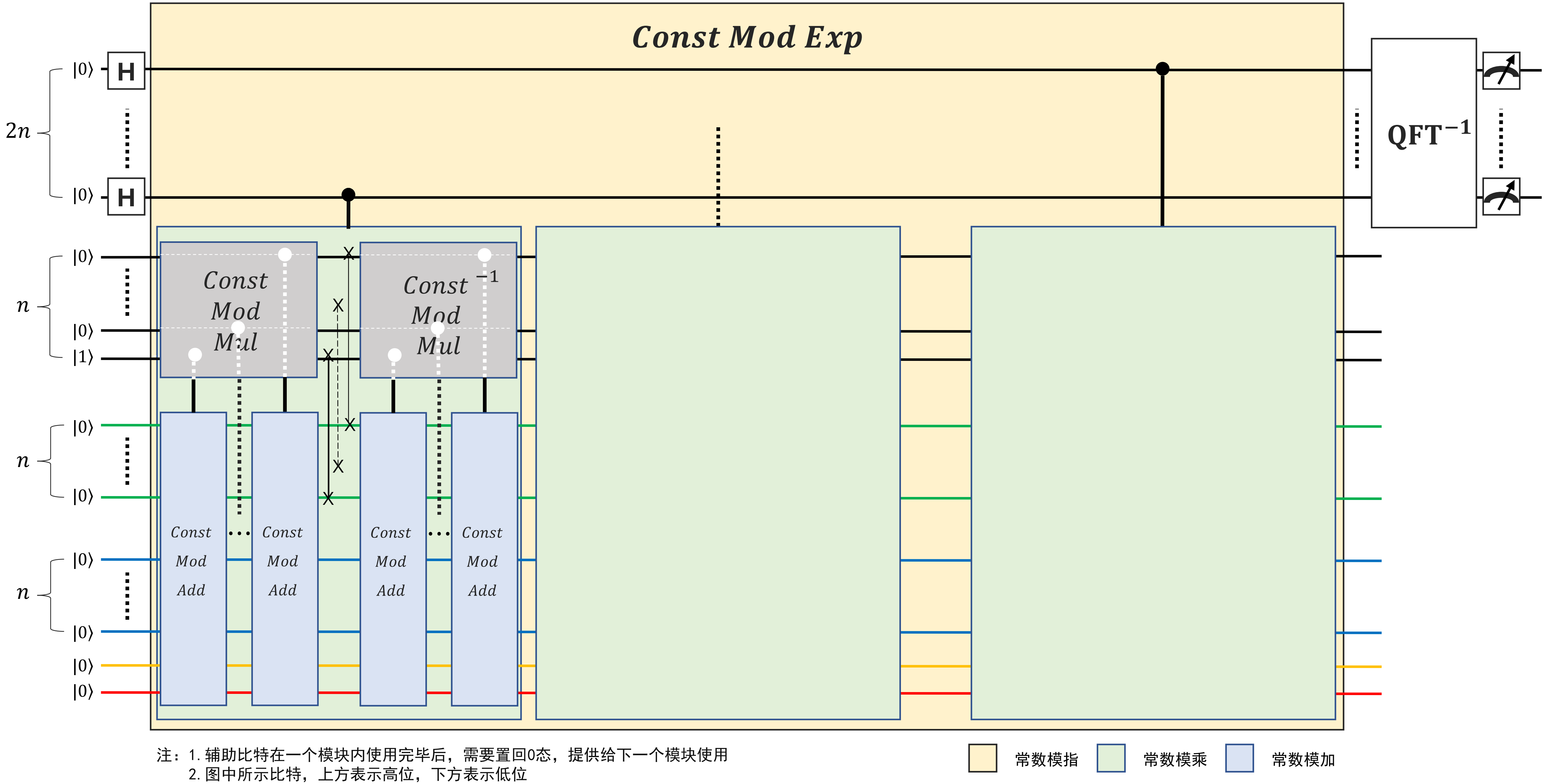
1 使用同样的方法，用二进制表示$y = \sum_{i=0}^{n-1} y_i \times 2^i$，同理 y_i 做控制位，可所需问题转化为加法$C_i - ADD$：

$$|y\rangle|z\rangle \rightarrow |y\rangle\left|z + C \times 2^i\right\rangle$$

2 $|z\rangle$初态置为$|0\rangle$，经过一连串$C_i - ADD$得到

$$|y\rangle|0\rangle \rightarrow |y\rangle|Cy \bmod N\rangle$$

3 通过交换操作：$|y\rangle|Cy \bmod N\rangle \rightarrow |Cy \bmod N\rangle\,|y\rangle$



注：1. 辅助比特在一个模块内使用完毕后，需要置回0态，提供给下一个模块使用
2. 图中所示比特，上方表示高位，下方表示低位

$U|y\rangle \rightarrow |Cy \; mod \; N\rangle$

1. 使用同样的方法，用二进制表示$y = \sum_{i=0}^{n-1} y_i \times 2^i$，同理 y_i 做控制位，

   可所需问题转化为加法$C_i - ADD$：

   $$|y\rangle|z\rangle \rightarrow |y\rangle\left|z + C \times 2^i\right\rangle$$

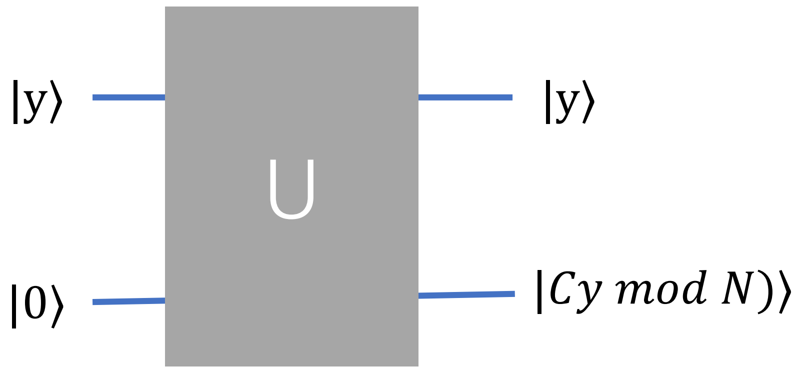
2. $|z\rangle$初态置为$|0\rangle$，经过一连串$C_i - ADD$得到

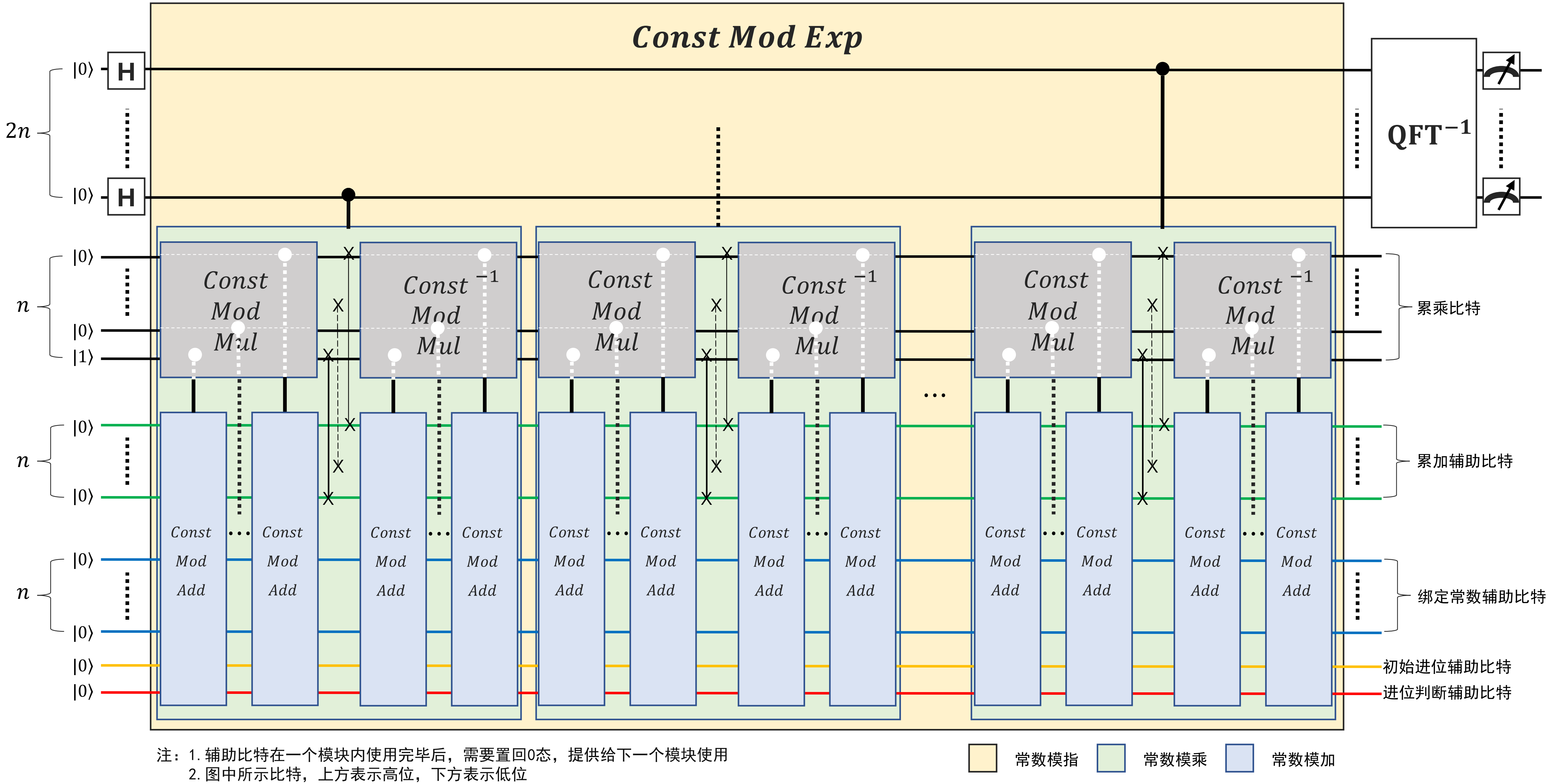
   $$|y\rangle|0\rangle \rightarrow |y\rangle|Cy \; mod \; N\rangle$$

3. 通过交换操作：$|y\rangle|Cy \; mod \; N\rangle \rightarrow |Cy \; mod \; N\rangle \, |y\rangle$

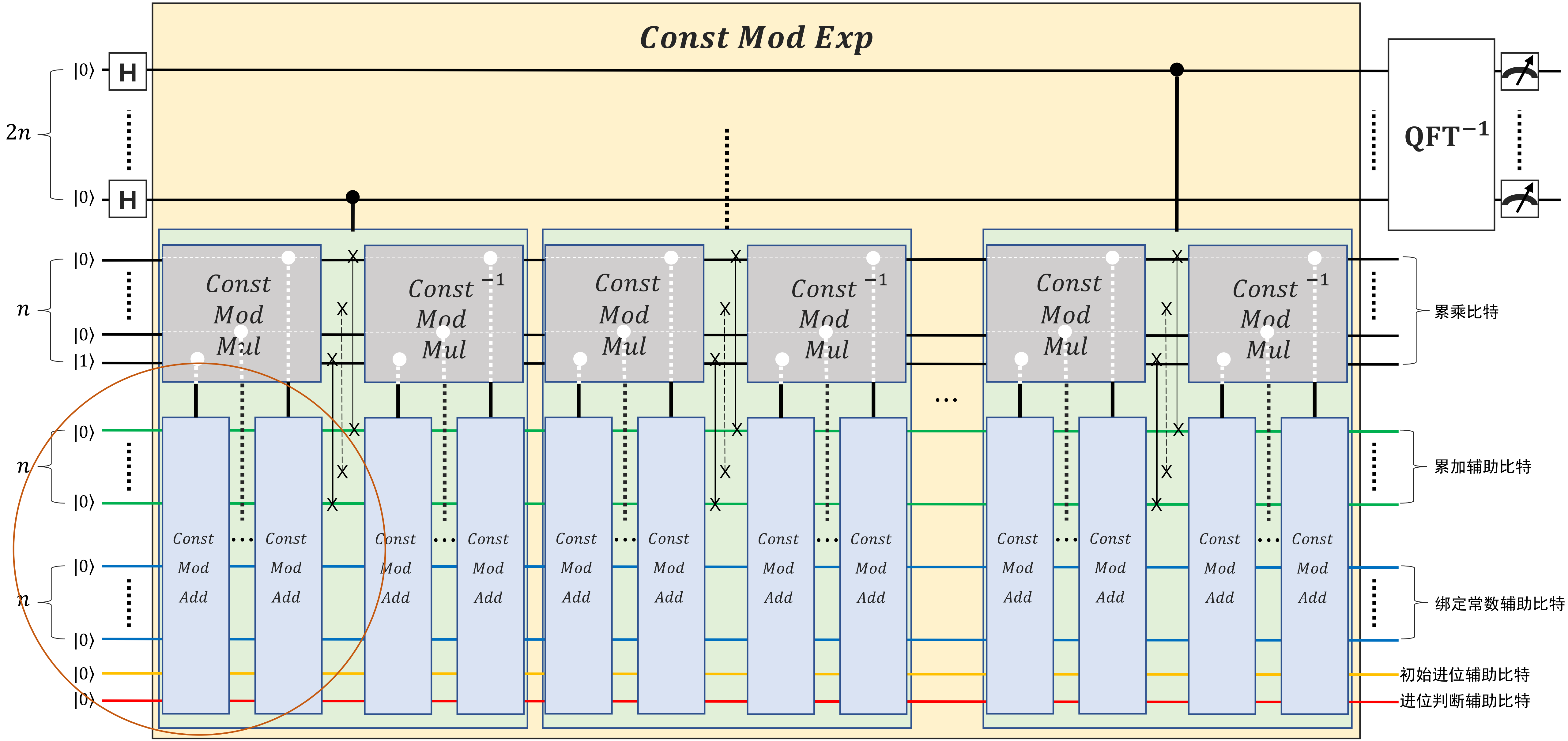
4. 最终目标：$|Cy \; mod \; N\rangle \, |y\rangle \rightarrow |Cy \; mod \; N\rangle \, |0\rangle$

   整个过程：$|y\rangle|0\rangle \rightarrow \; |Cy \; mod \; N\rangle \, |0\rangle$





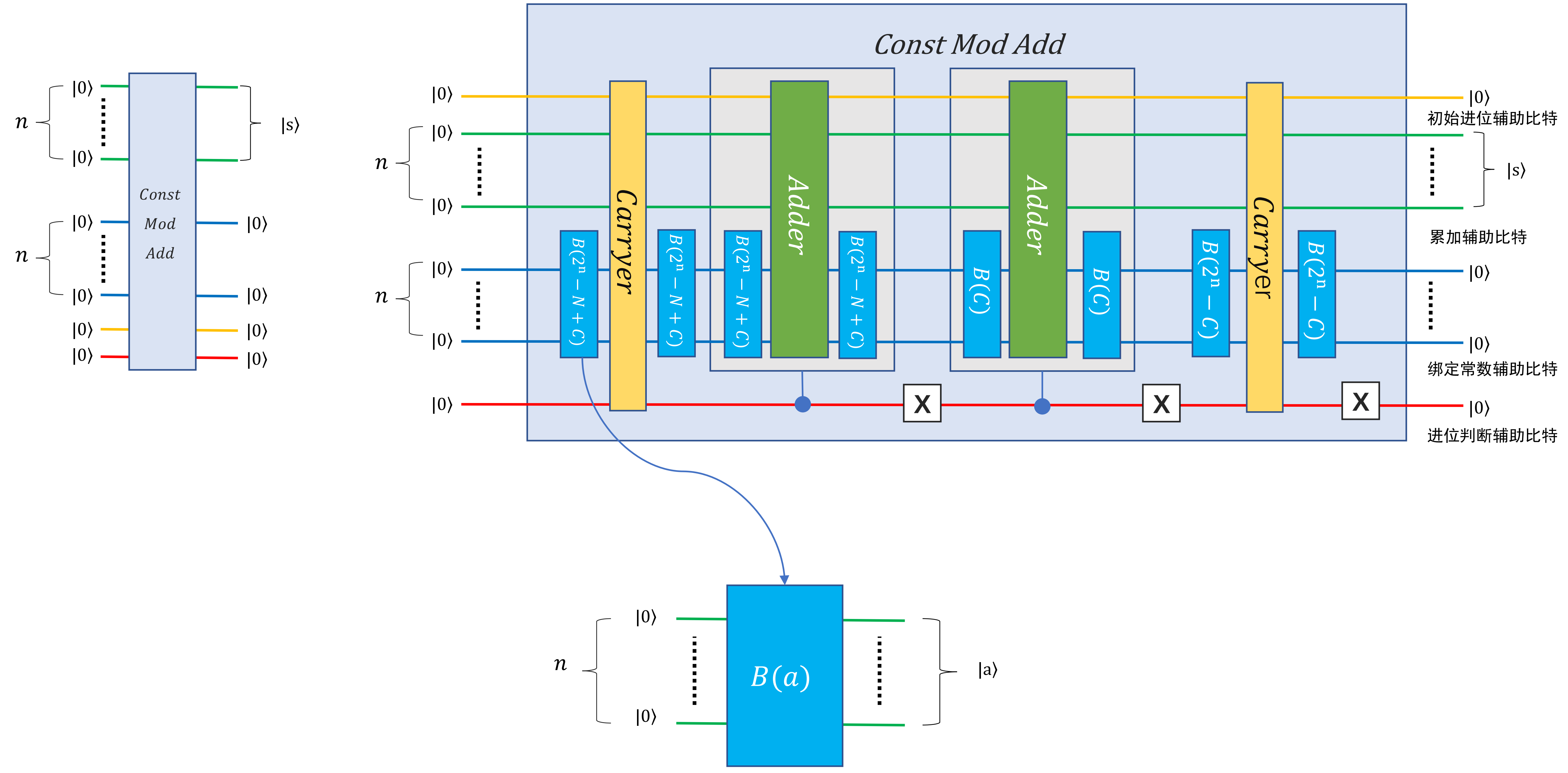
注：1. 辅助比特在一个模块内使用完毕后，需要置回0态，提供给下一个模块使用
2. 图中所示比特，上方表示高位，下方表示低位



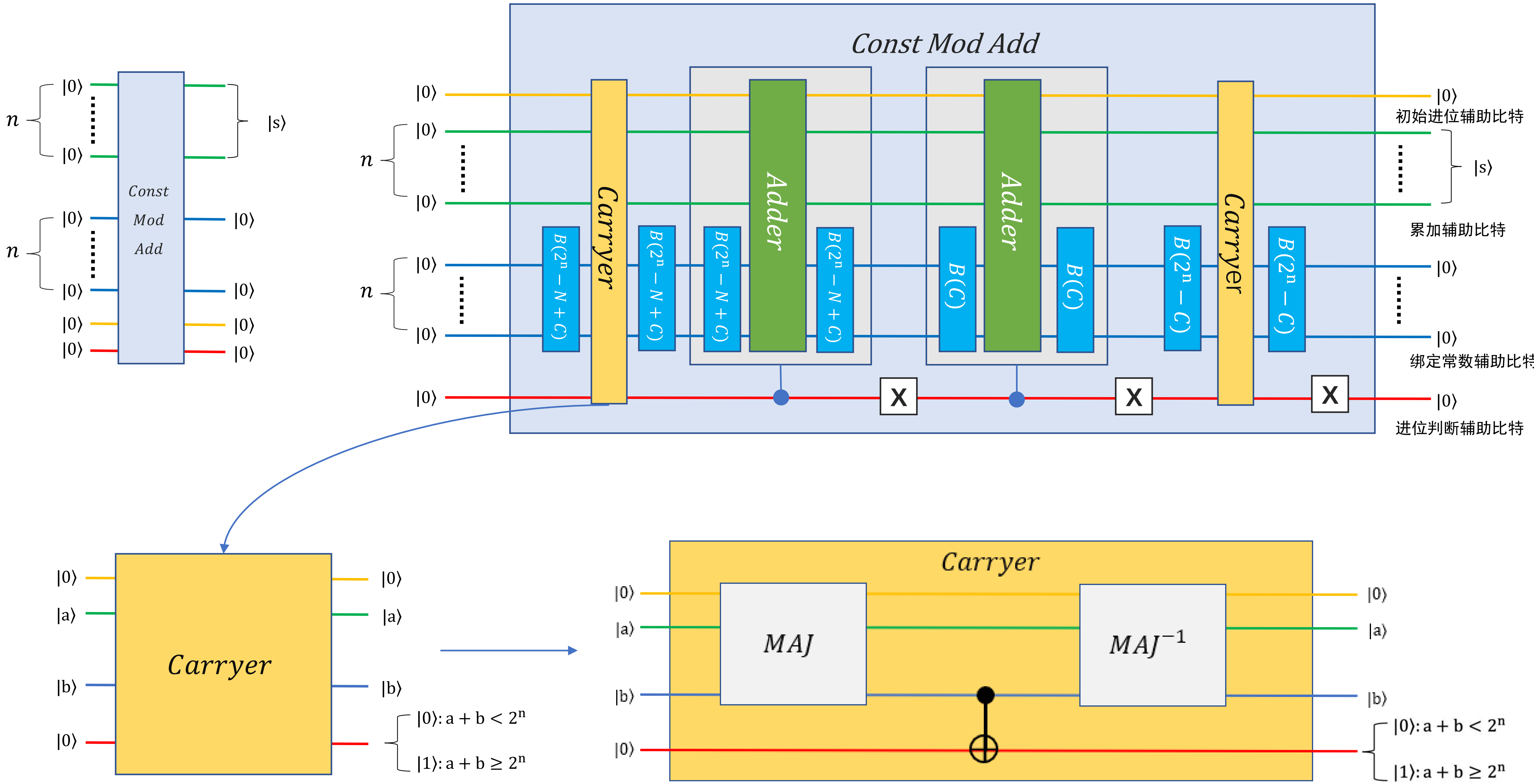
注：1. 辅助比特在一个模块内使用完毕后，需要置回0态，提供给下一个模块使用

2. 图中所示比特，上方表示高位，下方表示低位

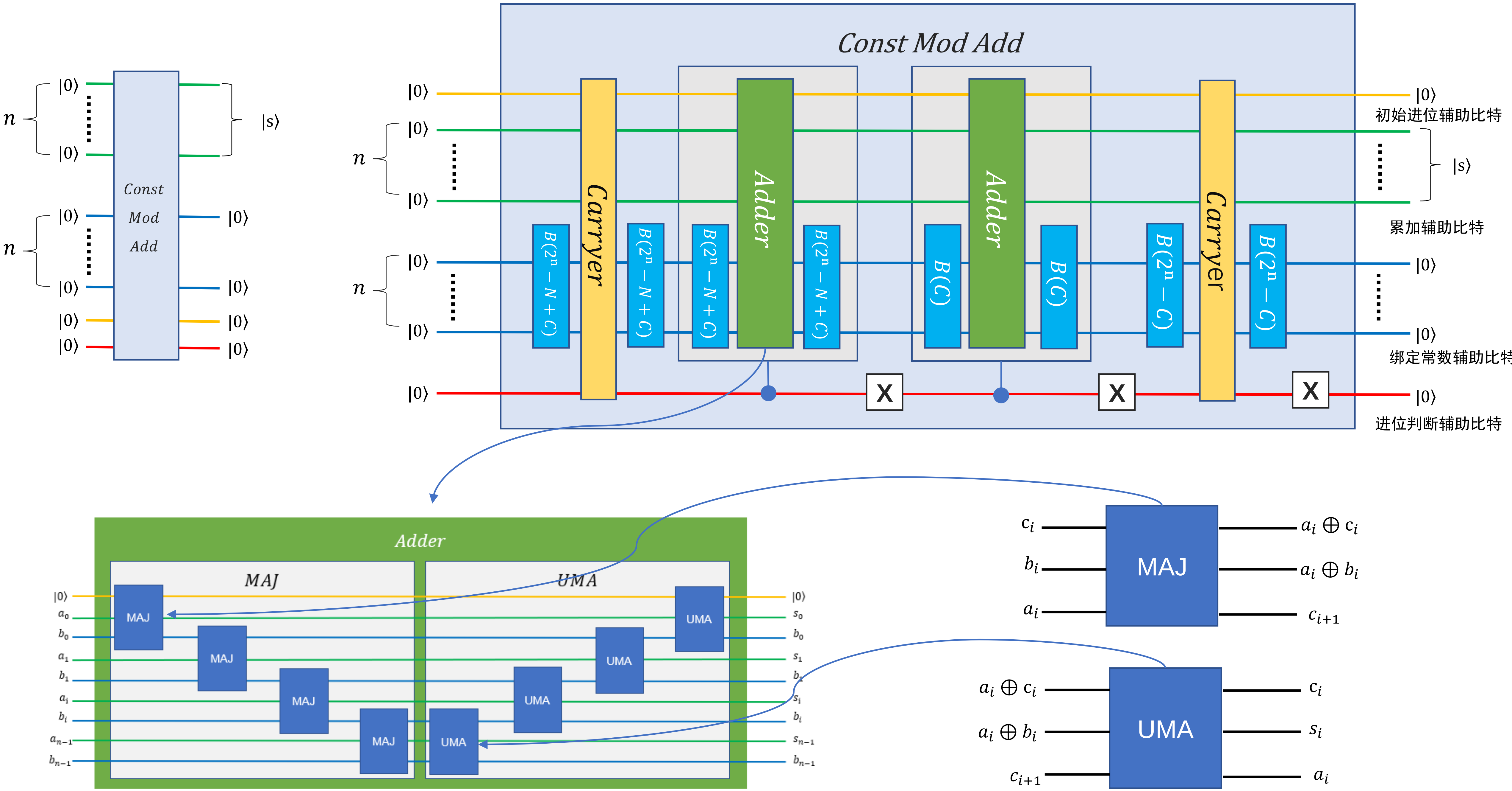
常数模指 常数模乘 常数模加



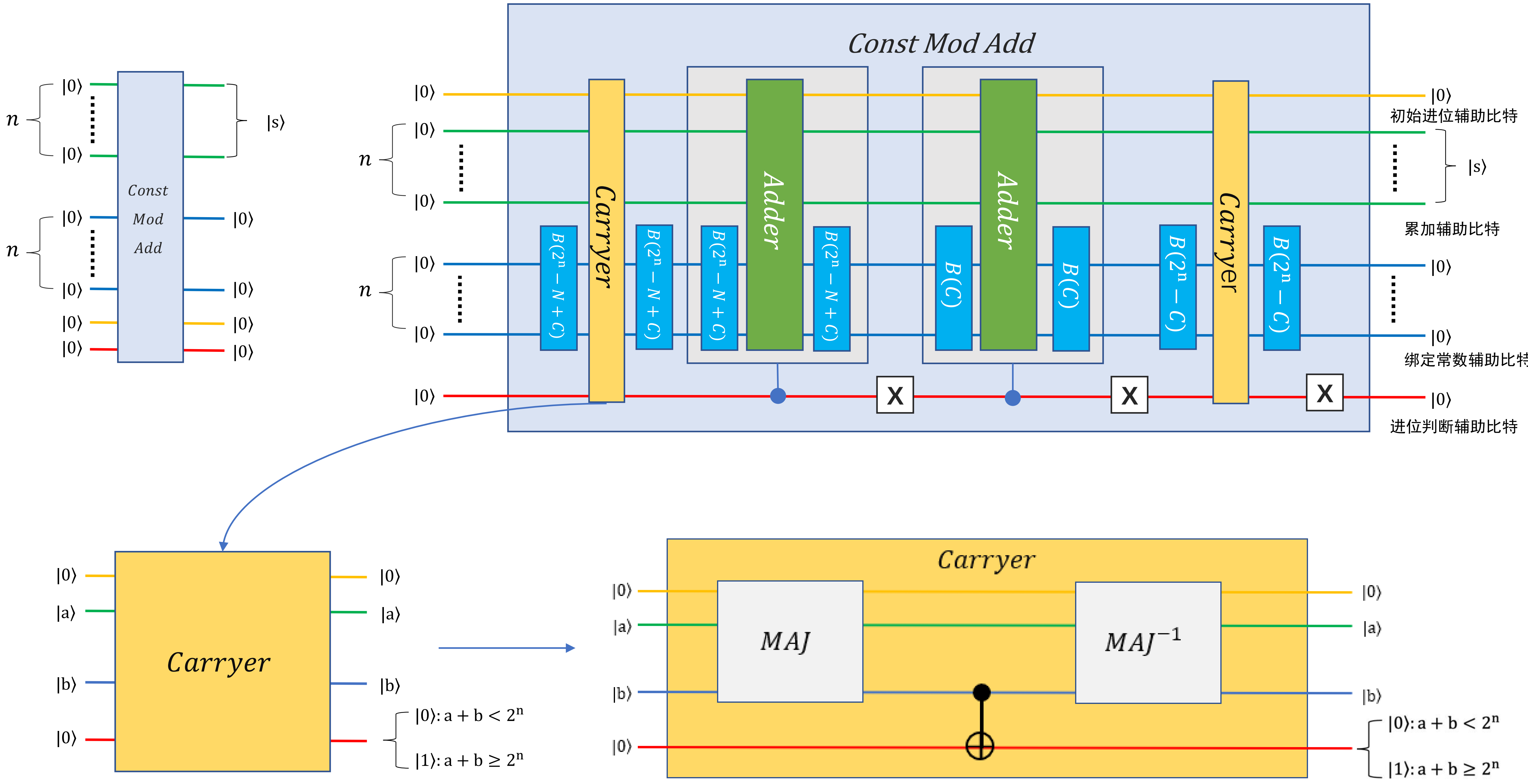
BindData(a)：绑定数据



Const Mod Add
Const
Mod
Add
|s⟩
Carryer
Adder
B(2^n − N + C)
B(C)
B(2^n − C)
X
初始进位辅助比特
累加辅助比特
绑定常数辅助比特
进位判断辅助比特
|0⟩
|a⟩
|b⟩
|0⟩: a + b < 2^n
|1⟩: a + b ≥ 2^n
MAJ
MAJ^{-1}
n



Const Mod Add
|0⟩
|s⟩
n
Carryer
Adder
B(C)
X
初始进位辅助比特
累加辅助比特
绑定常数辅助比特
进位判断辅助比特
MAJ
UMA



Const Mod Add
Const Mod Add
Carryer
Adder
Adder
Carryer
$B(2^n-N+C)$
$B(C)$
$B(2^n-C)$
X
|0⟩
|s⟩
|a⟩
|b⟩
n
初始进位辅助比特
累加辅助比特
绑定常数辅助比特
进位判断辅助比特
Carryer
MAJ
MAJ^{-1}
$|0\rangle: a+b<2^n$
$|1\rangle: a+b\geq 2^n$

本源量子

追本溯源 高掌远跖

https://www.originqc.com.cn