Shor’s Algorithm

第4讲：Shor算法原理一

Shor算法原理

过 程

01 概述

02 问题转化

03 执行步骤

04 线路框架

05 态的演化

06 确认周期

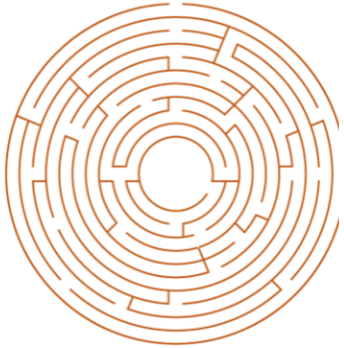
1. 算法概述

本 源 量 子

本源
量子

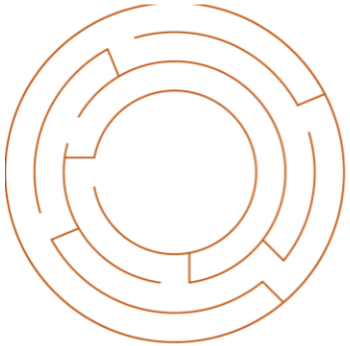
时间复杂度比较

（n，表示素数乘积的位数）



$O\left(\exp\left(\sqrt[3]{\frac{64}{9}n(\log n)^2}\right)\right)$

使用传统计算机，解决素数分解的最佳复杂度.



$O(n^3 \log n)$

Shor的算法可以将复杂度大幅降低

提供了超多项式执行加速

复杂度的降低，使RSA加密算法处在危险中！

Shor算法思想

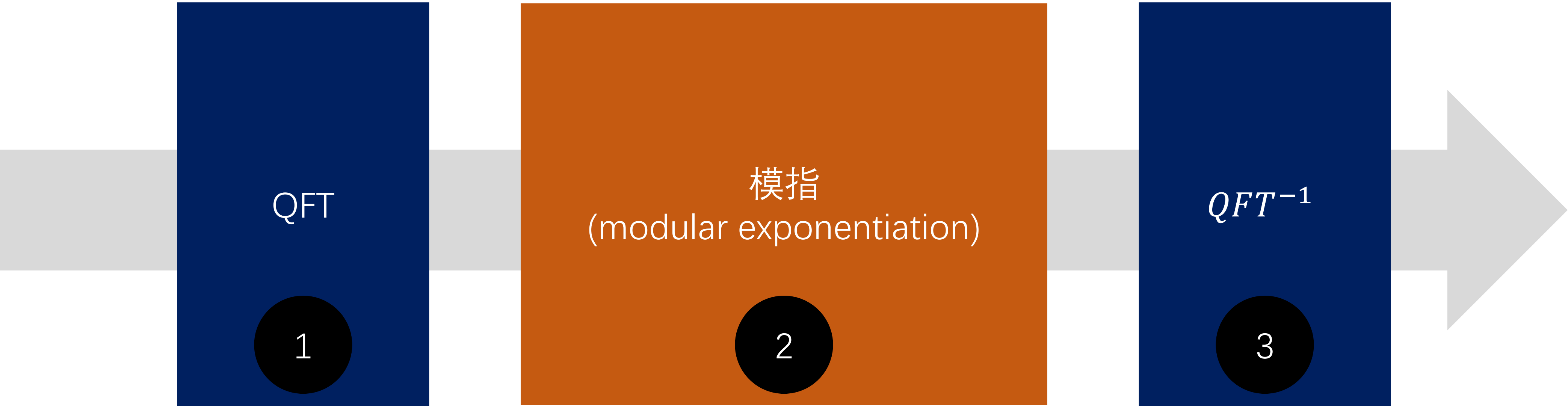
r

关键思想：

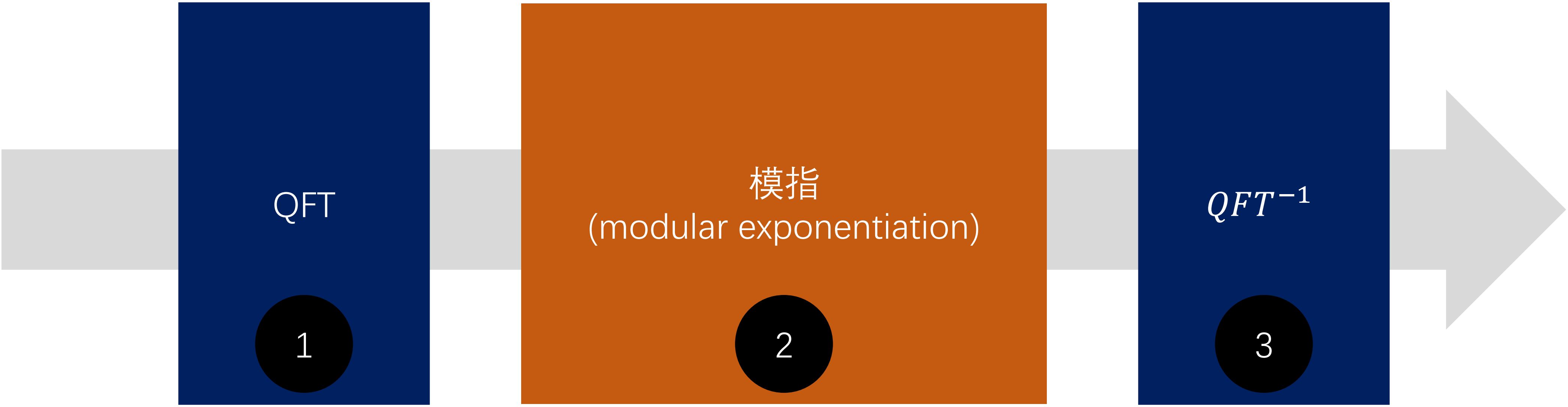
将分解问题转化为寻找模指数电路的周期问题，构建模指数电路，通过逆QFT找到模指数电路的周期。

本 源
量 子

核心线路



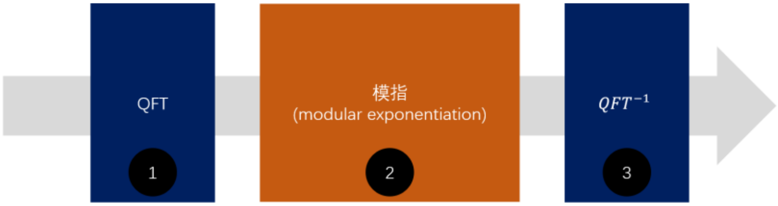
核心线路



Origin Q

本源量子

核心线路



1. QFT傅里叶变换。

2. 模指线路U_f计算函数:

$2 \leq x < N^2$

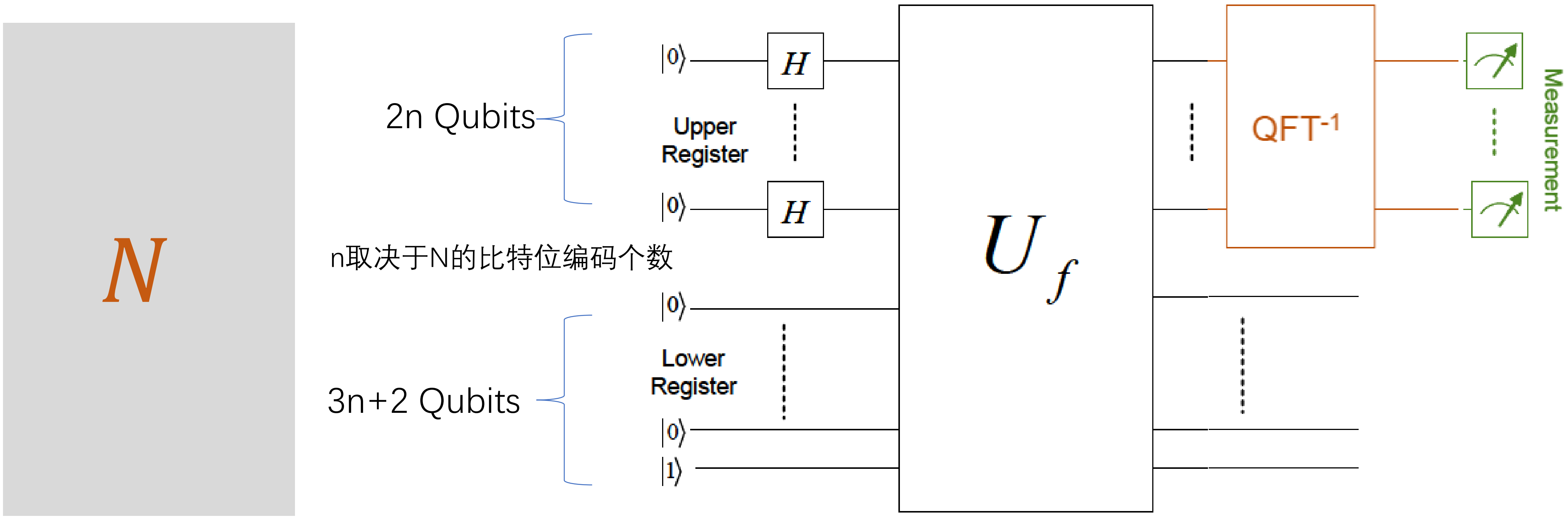
$$f(x) = a^x \bmod N$$

$2 \leq a < N$

将要分解的数

3. QFT^{-1}，逆傅里叶变换

线路图总览



本源Shor算法实施线路图

2. 问题转化

本源量子

问题转化

假设分解的数为 N，任取$a \in [2, N-1]$, 满足a和N互质, 且

$$a^r = 1 \bmod N \quad \text{(其中r为偶数)}$$

$$\left(a^{\frac{r}{2}}+1\right)\left(a^{\frac{r}{2}}-1\right) = kN$$

如果

$$a^{\frac{r}{2}} \neq -1 \bmod N, a^{\frac{r}{2}} \neq 1 \bmod N$$

得到N的两个因子p_1和p_2

$$p_1 = gcd\left(a^{\frac{r}{2}}+1, N\right) \text{ 和 } p_2 = gcd\left(a^{\frac{r}{2}}-1, N\right)$$

问题转化

假设分解的数为 N，任取$a \in [2, N-1]$, 满足a和N互质, 且

$$a^r = 1 \bmod N$$

（其中r为偶数）

特殊情况：

如果$N = p^m$，则无法用如上所述方法经行转化，所以算法开始时候还需做如下判定:

判断$\sqrt[k]{N} \in Z$是否为真，*其中*$k \leq \log_2 N$

得到N的两个因子p_1和p_2

$$p_1 = gcd\left(a^{\frac{r}{2}} + 1, N\right) \text{ 和 } p_2 = gcd\left(a^{\frac{r}{2}} - 1, N\right)$$

本 源
量 子

追本溯源 高掌远跖

https://www.originqc.com.cn