Quantum Information and Quantum Computation

Yuanyuan Chen

College of Physical Science and Technology

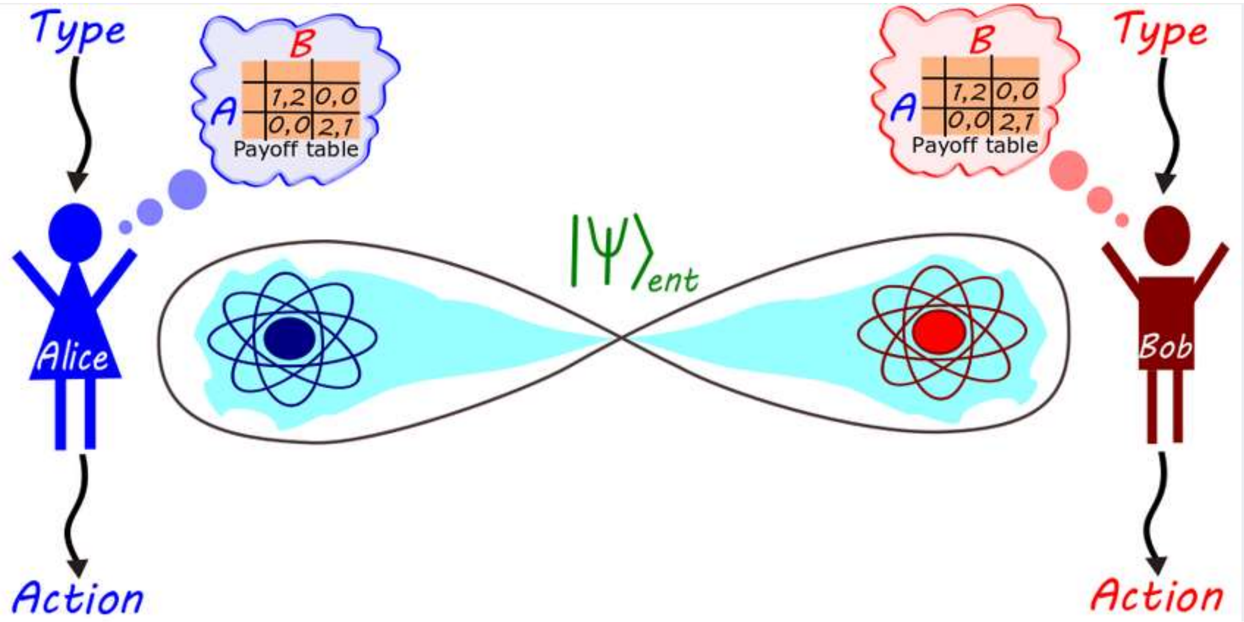
Xiamen University

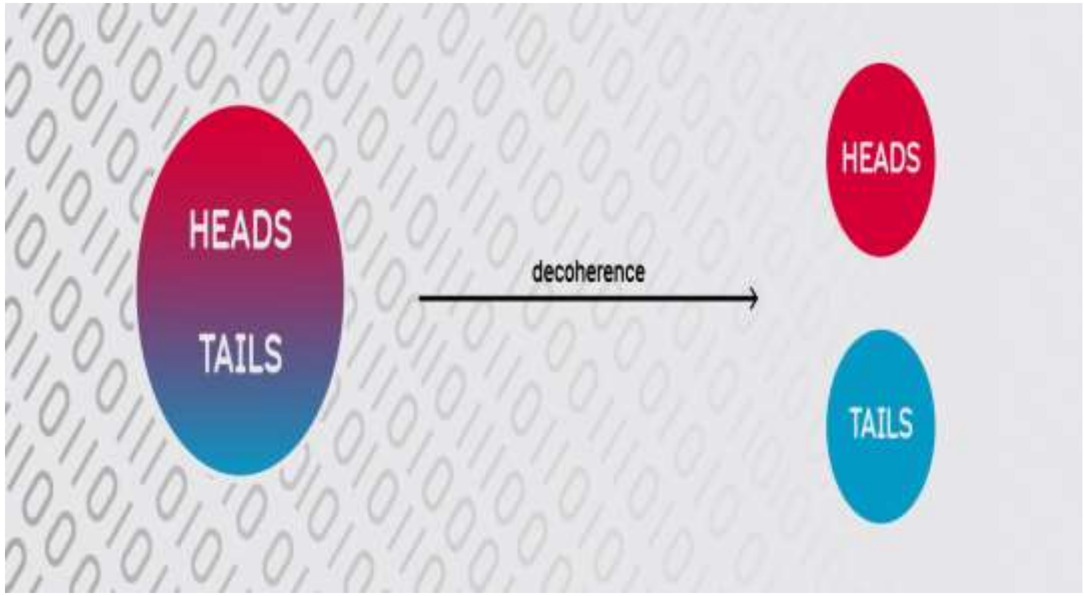
Email: chenyy@xmu.edu.cn

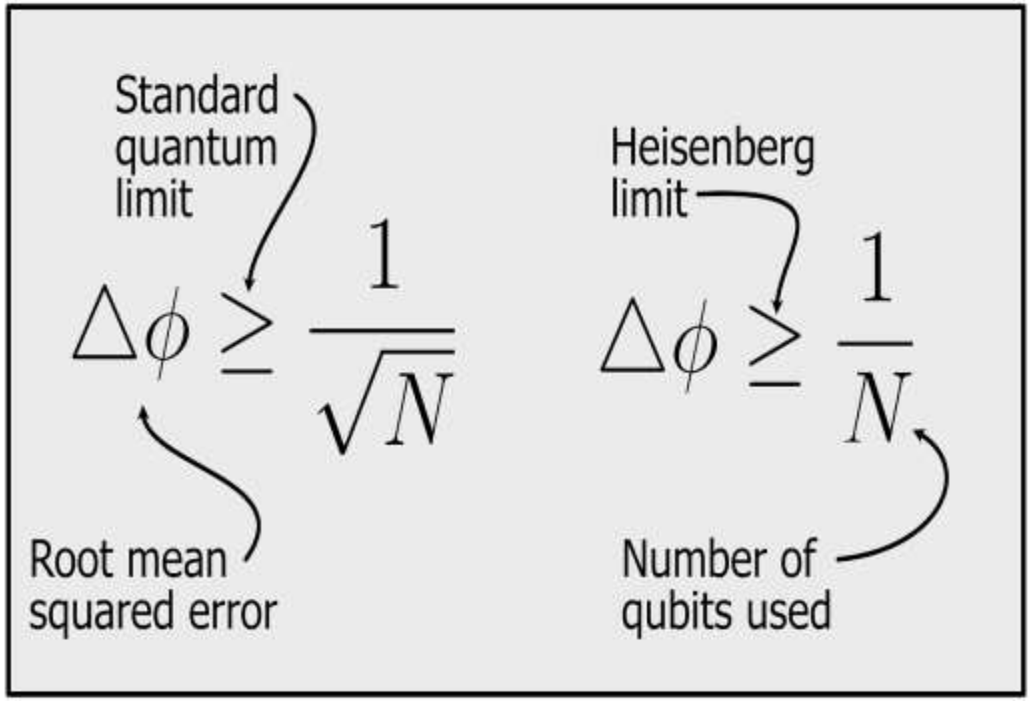
http://qolab.xmu.edu.cn

Course assessment and requirements

- Attendance（10%）and class performance （20%）
- Midterm exam: Quantum mechanics project （20%）
- Final exam： Dissertation on quantum information science （50%）


Type
B
A
1,2 0,0
0,0 2,1
Payoff table
Alice
$|\Psi\rangle_{ent}$
Bob
Action


HEADS
TAILS
decoherence
HEADS
TAILS


Standard quantum limit
$\Delta\phi \geq \frac{1}{\sqrt{N}}$
Root mean squared error
Heisenberg limit
$\Delta\phi \geq \frac{1}{N}$
Number of qubits used


Quantum sensor
Quantum clocking
Quantum security
Quantum imaging
Quantum thermodynamics
Quantum material
Quantum computer
Quantum simulation
Machine learning
Material and drug design
Finances
Cryptography
Quantum application
Classical application

1. 5人左右为一个小组，准备6-7分钟的PPT，课堂上随机抽选一名同学作报告。

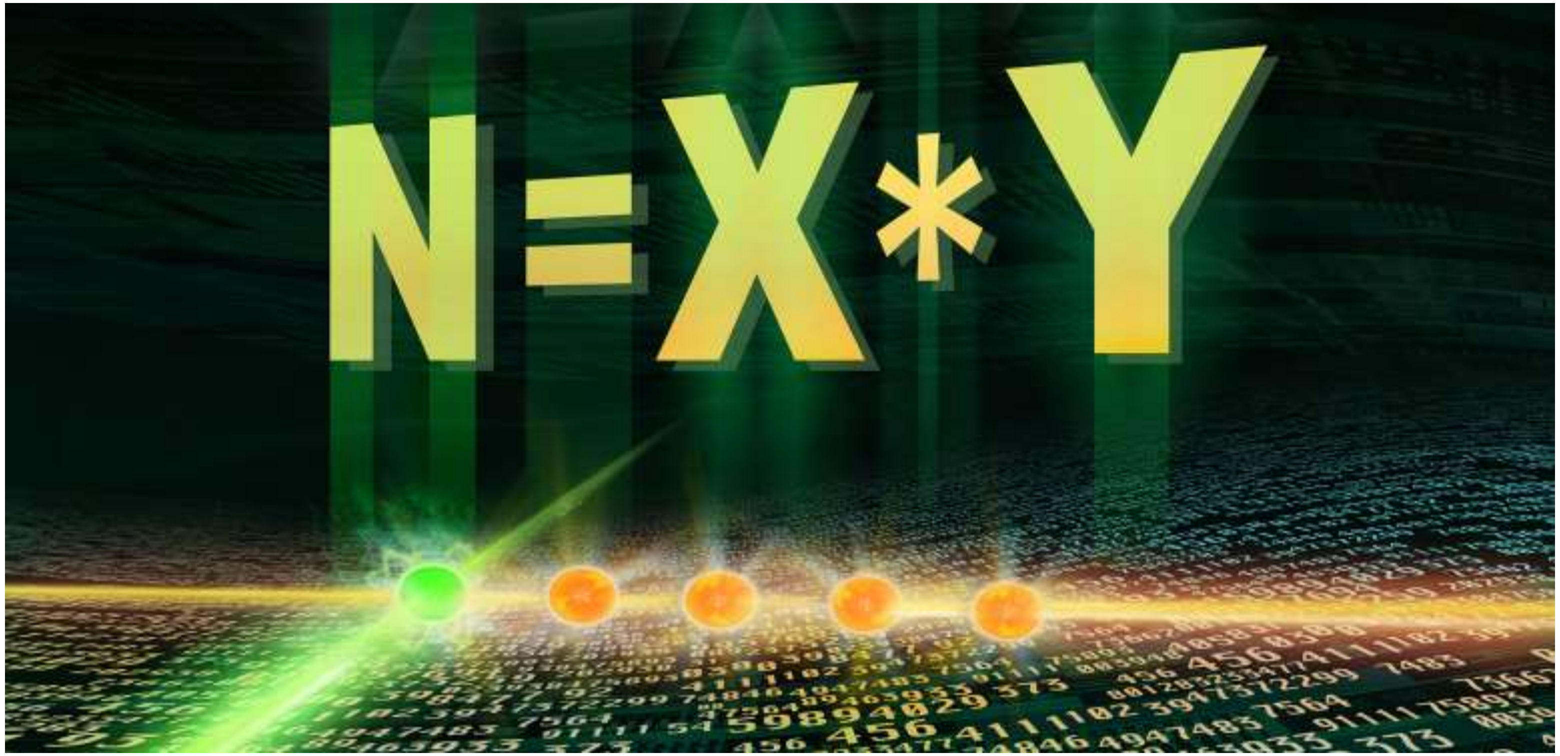
2. 选题内容应与课程相关，鼓励前沿科学探索。

3. 12月4日12:00之前将报告题目和PPT发至邮箱chenyy@xmu.edu.cn.

4. 因选课人数较多，估计需要两次课时间，即12月5日，12月12日，发送邮件时可注明理想的报告时间。若大多数人选择同一时间点，无法安排，将根据发送邮件时间进行排序。

Lecture 12

Quantum factorization algorithm



下列表格给出各种形式的最大已知素数。有些素数使用分散式计算找到。2009年，互联网梅森素数大搜索因为第一个发现具至少1,000万个数位的素数，而获得10万美元的奖金。电子前哨基金会亦为具至少1亿个数位及10亿个数位的素数分别提供15万美元及25万美元的奖金

类型	素数	数位	日期	发现者
梅森素数	$2^{82589933}-1$	23,249,425	2018年12月21日	互联网梅森素数大搜索
非梅森素数（普罗斯数）	$19,249\times2^{13,018,586}+1$	3,918,990	2007年3月26日	十七或者破产
阶乘素数	$150209!+1$	712,355	2011年10月	PrimeGrid[25]
素数阶乘素数	$1098133\#-1$	476,311	2012年3月	PrimeGrid[26]
孪生素数s	$3756801695685\times2^{666669}\pm1$	200,700	2011年12月	PrimeGrid[27]

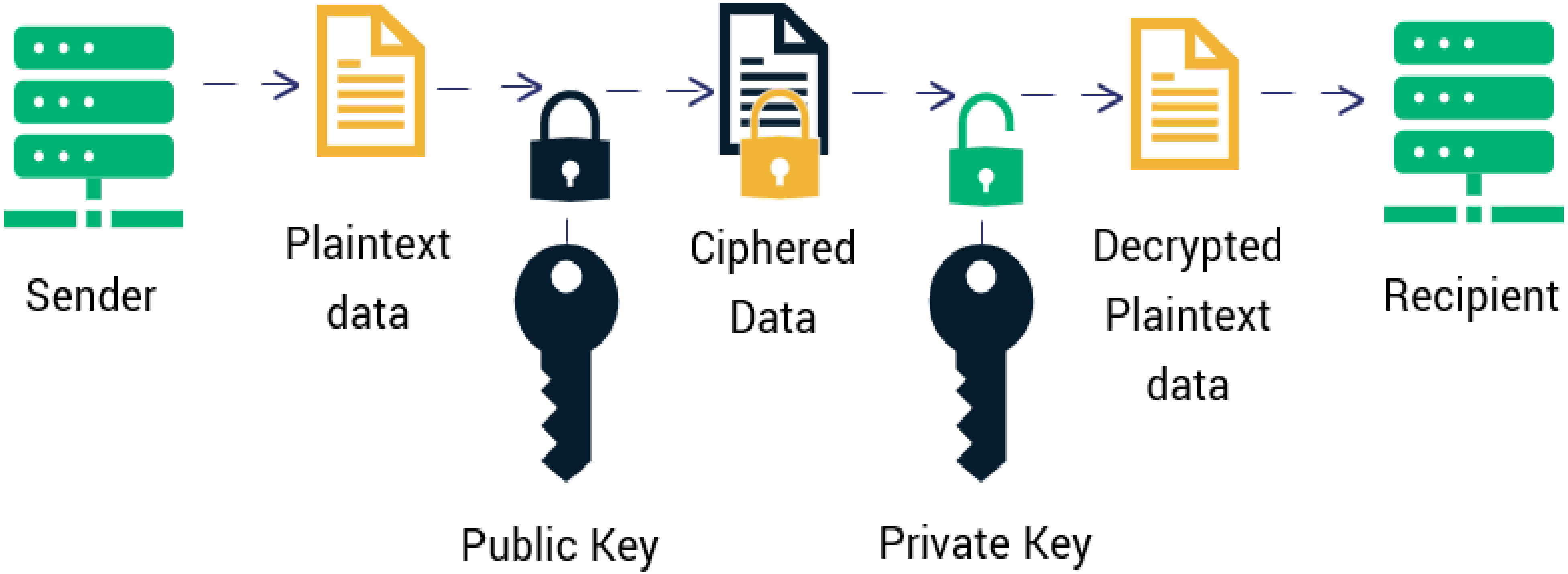
黎曼发现了质数分布的奥秘完全蕴藏在一个特殊的函数之中，尤其是使那个函数取值为零的一系列特殊的点对质数分布的细致规律有着决定性的影响。那个函数如今被称为黎曼ζ函数，那一系列特殊的点则被称为黎曼ζ函数的非平凡零点。

黎曼ζ函数ζ(s)被定义为一无穷级数

$$\zeta(s)=\sum_{n=1}^{\infty}\frac{1}{n^s},$$

其中，s为实数部分大于1的一个复数。

How RSA Encryption Works



1.1 欧拉函数

欧拉函数 $\phi(n)$ ：表示小于 n 且与 n 互质的正整数的个数。

若 $n = p \cdot q$ ，且 p 和 q 都为质数，则 $\phi(n) = (p-1)(q-1)$

1.2 同余计算

$$23 \div 7 = 3 \ldots 2$$
$$65 \div 7 = 9 \ldots 2$$

可把同余计算记为

$$23 \equiv 65(mod\ 7) \equiv 2(mod\ 7)$$

同余计算有几条简单性质：

①、若 $a = b + k\,m$ ，则 $a = b(mod\ m)$ 或者 $a = b(mod\ k)$

②、同余加法

若 $a \equiv b(mod\ m)$, $c \equiv d(mod\ m)$ ，则 $(a+c) \equiv (b+d)(mod\ m)$

③、同余乘法

若 $a \equiv b(mod\ m)$, $c \equiv d(mod\ m)$ ，则 $a * c \equiv (b * d)(mod\ m)$

④、同余逆元

若 $ab = 1(mod\ m)$ ，则称 a ，b 是互为关于 m 的同余逆元

1.3 欧拉定理

若 $\gcd(a,\ n) = 1$ *，则* $a^{\phi(n)} = 1(\mathrm{mod}\ n)$ 。

①、这里的 $\gcd(a,\ n)$ 表示求 a 和 n 的公约数，$\gcd(a,\ n) = 1$ 表示 a 和 n 互质。

②、费马小定理是欧拉定理的一个特例。

费马小定理：若 n 是一个质数，且 a 不是 n 的倍数，则 $a^{n-1} = 1(mod\ n)$

③、费马小定理不予证明，只说一下为什么它是欧拉定理的一个特例：

若 n 是一个质数，且 a 不是 n 的倍数，则 $\phi(n) = n - 1$ ， a 和 n 必然互质。

举例： $n = 3,\ a = 5,\ (a, n) = 1, a^{n-1} = 5^2 = 25 = 1(mod\ n)$

1.4 RSA 算法

信息传输问题：发信人 Alice，收信人 Bob，间谍 Eve。

1.4.1 公钥和秘钥

①、获得两个大质数 p_1，p_2 ,则 $n=p_1*p_2$，$\phi(n)=(p_1-1)(p_2-1)$ 。注意如果仅知道 n ，不知道 p_1，p_2 ，是很难知道 $\phi(n)$ 的。这个 $\phi(n)$ 仅收信人Bob知道。

②、Bob构造一个整数 e ，要求：

$$1 \ll e < \phi(n),\ \ \gcd(e,\ \phi(n)) = 1,\ \ e \neq p_1, p_2$$

③、求出 e 对同余 $\phi(n)$ 的逆元 d：

$$e*d = 1(mod\ \phi(n)) \Leftrightarrow e*d = 1 + k*\phi(n)$$

④、任意整数 a 只要 $1 \leq a < n,\ a \neq p_1, p_2$ ，必有 $\gcd(a,\ n) = 1$

$$\Rightarrow a^{\phi(n)} = 1(mod\ n)\ (\text{费马小定理})$$

$$\Rightarrow a^{k*\phi(n)} = 1(mod\ n)\ (\text{同余乘法})$$

$$\Rightarrow a^{k*\phi(n)+1} = a(mod\ n)\ (\text{同余加法})$$

$$\Rightarrow a^{e*d} = a^{k*\phi(n)+1} = a(mod\ n)$$

所以若构造一个整数 $c = a^e(mod\ n)$,则 $c^d = a^{ed}(mod\ n) = a(mod\ n)$

这时候我们就得到了我们的公钥和私钥

$$\text{公钥}:\{n, e\} \text{——所有人都可见}$$

$$\text{私钥}:\{n, d\} \text{——仅收件人可见}$$

1.4.2 RSA 的信息加密-传输-解密方案为:

①、Alice加密：把明文 a 经过公钥 $\{n, e\}$ 加密成密文 $c = a^e (mod\, n)$

②、信息传递：通过任何信息传递手段（电报，邮件，书信等）把密文 c 发送给Bob

③ Bob解密：通过私钥 $\{n, d\}$ 解密 $c^d = a(mod\, n)$ ，获得明文 a

Example

RSA-768

It has 232 decimal digits and was factored over the span of 2 years:

$$
\begin{array}{l}
1230186684530117755130494958384962720772853569595 3 \\
\end{array}
$$

素数因子分解问题，用数学的语言描述就是：

已知一合数 N *，它存在唯一的质因子分解* $N = P_1 \cdot P_2$ *，但* P_1 *，* P_2 *未知，求* P_1 *，* P_2 *。*

有以下的步骤来解决质因子分解问题。

第一步，随机取正整数 y ，要求 $y < N$ ，且互质（ $gcd(y, N) = 1$ ）。

定义阶数：使 $y^r = 1 (\bmod N)$ 的最小正整数 r 称为 y 关于 N 的阶数。

存在一个算法——可在多项式复杂度求得 y **关于** N **的阶数（order）** $r = \mathrm{ord}_N(y)$

第二步，若 r 为奇数，则再要一个 y ，继续求 r ，直到 r 为偶数。

第三步， r 为偶数，取 $x=y^{r/2}(\mathrm{mod}\ N)$ ，则 $x^2=1(\mathrm{mod}\ N)$ ，进而

$$(x+1)(x-1)=0(\mathrm{mod}\ N)$$

于是可设

$$(x+1)(x-1)=t\cdot N=tP_1P_2=r\cdot sP_1P_2\ ,\ (t=r\cdot s)$$

进而有

$$(x+1)(x-1)=(rP_1)\cdot(sP_2)$$

上式解为

$$\begin{aligned} x+1=0(\mathrm{mod}\ P_1)\ &\Rightarrow\ P_1=\gcd(x+1,N) \\ x-1=0(\mathrm{mod}\ P_2)\ &\Rightarrow\ P_2=\gcd(x-1,N) \end{aligned}$$

而求解 $\gcd(x,N)$ 可用辗转相除法（多项式难度）。需要注意的是，有可能存在这样一组平庸解：

$$\begin{aligned} P_1&=\gcd(x+1,N)=N \\ P_2&=\gcd(x-1,N)=1 \end{aligned}$$

这时候需要选一个新的 y ，继续以上操作。

$$N = 21 = 3 \times 7 \quad , \quad P_1 = 3, P_2 = 7$$

取 $y = 4,$

$$4^r = 1(\text{mod}21) \Rightarrow r = 3$$ 奇数，不行

取 $y = 5,$

$$5^r = 1(\text{mod}21) \Rightarrow r = 6$$ 偶数，可以

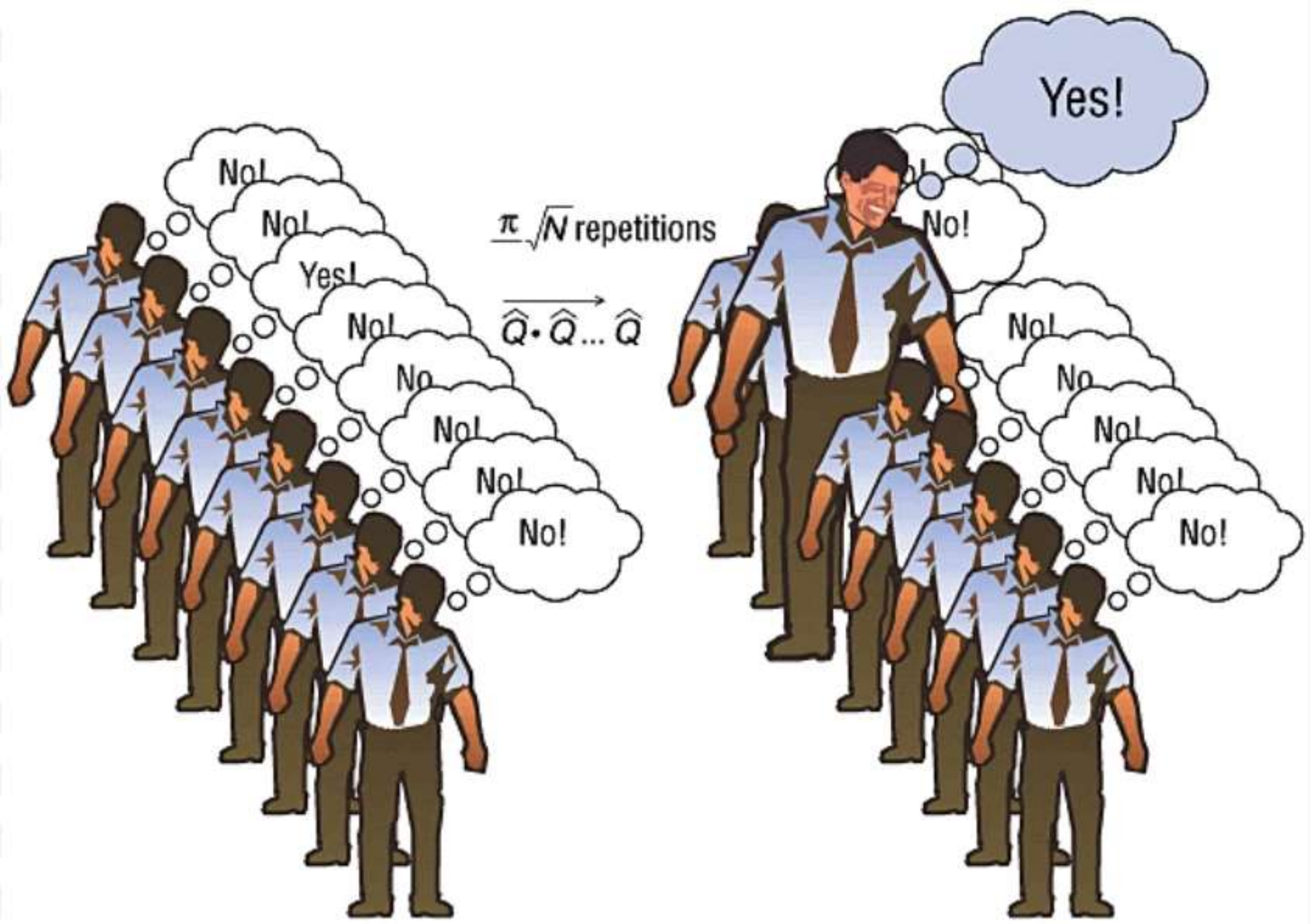
$$\Rightarrow x = y^{r/2} = 5^3 = 125$$
$$\Rightarrow (x+1)(x-1) = 15624 = 744 * 21 = 0(\text{mod } 21)$$
$$\Rightarrow P_1 = \gcd(x+1, N) = \gcd(126, 21) = 21$$
$$\Rightarrow P_2 = \gcd(x-1, N) = \gcd(124, 21) = 1$$

这个 y 不行，再取一个 $y = 8$ (6不行，6和21不互质)

$$8^r = 1(\text{mod}21) \Rightarrow r = 2$$
$$\Rightarrow x = y^{r/2} = 8^1 = 8$$
$$\Rightarrow (x+1)(x-1) = 63 = 3 * 21 = 0(\text{mod}21)$$
$$\Rightarrow P_1 = \gcd(x+1, N) = \gcd(9, 21) = 3$$
$$\Rightarrow P_2 = \gcd(x-1, N) = \gcd(7, 21) = 7$$

Example: Factoring n=21

1. Choose x
2. Determine q
3. Initialize first register (r_1)
4. Initialize second register (r_2)
5. QFT on first register
6. Measurement
7. Continued Fraction Expansion $\rightarrow$ determine r
8. Check r $\rightarrow$ determine factors


No!
No!
Yes!
No!
No
No!
No!
No!
π √N repetitions
$\overrightarrow{\hat{Q}\cdot\hat{Q}\ldots\hat{Q}}$
Yes!
No!
No!
No
No!
No!
No!

1. Choose a random integer x, $1 < x < n$

- if it is not coprime with n, e.g. $x = 6$:
  $\rightarrow \gcd(x, n) = \gcd(6, 21) = 3 \rightarrow 21/3 = 7 \rightarrow$ done!
- if it is coprime with n, e.g. $x = 11$:
  $\rightarrow \gcd(11, 21) = 1 \rightarrow$ continue!

2. Determine q

- $n^2 = 244 \leq q = 2^l < 2n^2 = 882$
  $\rightarrow q = 512 = 2^9$
- Initial state consisting of two registers of length l:
  $|\Phi_i\rangle = |0\rangle_{r_1} |0\rangle_{r_2} = |0\rangle^{\otimes 2^l}$

3. Initialize r_1

- ▷ initialize first register with superposition of all states $a(\mod q)$:

$$|\Phi_0\rangle = \frac{1}{\sqrt{512}} \sum_{a=0}^{511} |a\rangle\,|0\rangle$$

- ▷ this corresponds to $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ on all bits

4. Initialize r_2

▷ initialize second register with superposition of all states $x^a \pmod n$:

$$|\Phi_1\rangle = \frac{1}{\sqrt{512}} \sum_{a=0}^{511} |a\rangle \, |11^a \pmod{21}\rangle$$
$$= \frac{1}{\sqrt{512}} (|0\rangle\,|1\rangle + |1\rangle\,|11\rangle + |2\rangle\,|16\rangle + |3\rangle\,|8\rangle + ...)$$

a	0	1	2	3	4	5	6	7	8	9	10	...
$11^a(mod 21)$	1	11	16	8	4	2	1	11	16	8	4	...

▷ $r = 6$, but not yet observable

5. Quantum Fourier Transform

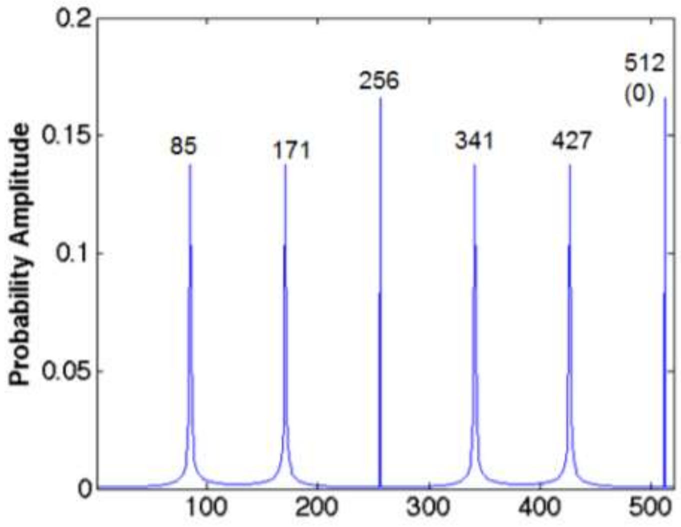
▷ apply the QFT on the first register:

$$|\tilde{\Phi}\rangle = \frac{1}{512}\sum_{a=0}^{511}\sum_{c=0}^{511} e^{2\pi iac/512}\,|c\rangle\,|11^a(mod21)\rangle$$

6. Measurement!

- probability for state $|c, x^k(\mod n)\rangle$, e.g. $k = 2 \to |c, 16\rangle$ to occur:

$$p(c) = \left| \frac{1}{512} \sum_{a:11^a \mod 21=16}^{511} e^{2\pi iac/512} \right|^2 = \left| \frac{1}{512} \sum_b e^{2\pi i(6b+2)c/512} \right|^2$$



- peaks for $c = \frac{512}{6} \cdot d$, $d \in \mathbb{Z}$:

7. Determine the period r

- Assume we get 427: $\left|\frac{c}{q} - \frac{d}{r}\right| = \left|\frac{427}{512} - \frac{d}{r}\right| \leq \frac{1}{1024}$
- Continued fraction expansion:

$$\frac{c}{q} = a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \frac{1}{\cdots}}}, \quad d_0 = a_0, \quad d_1 = 1 + a_0 a_1, \quad d_n = a_n d_{n-1} + d_{n-2}$$

$$r_0 = 1, \quad r_1 = a_1, \quad r_n = a_n r_{n-1} + r_{n-2}$$

$$\frac{427}{512} = 0 + \frac{1}{1 + \frac{1}{5 + \frac{1}{42 + \frac{1}{2}}}}, \quad d_0 = 0, \quad d_1 = 1, \quad d_2 = 5, \quad d_3 = 427$$

$$r_0 = 1, \quad r_1 = 1, \quad r_2 = 6, \quad r_3 = 512$$

- ▷ as $\frac{d_0}{r_0} = 0$ and $\frac{d_1}{r_1} = 1$ obviously don't work, try $\frac{d_2}{r_2} = \frac{5}{6} \rightarrow r = 6$
  $\rightarrow$ it works! $=)$
- ▷ for $\frac{c}{q} = \frac{171}{512}$ we would get $\frac{d}{r} = \frac{1}{3}$, so using $r = 3$ this would not work.
  $\rightarrow$ it only works if d and r are coprime!
  $\rightarrow$ if it doesn't work, try again!

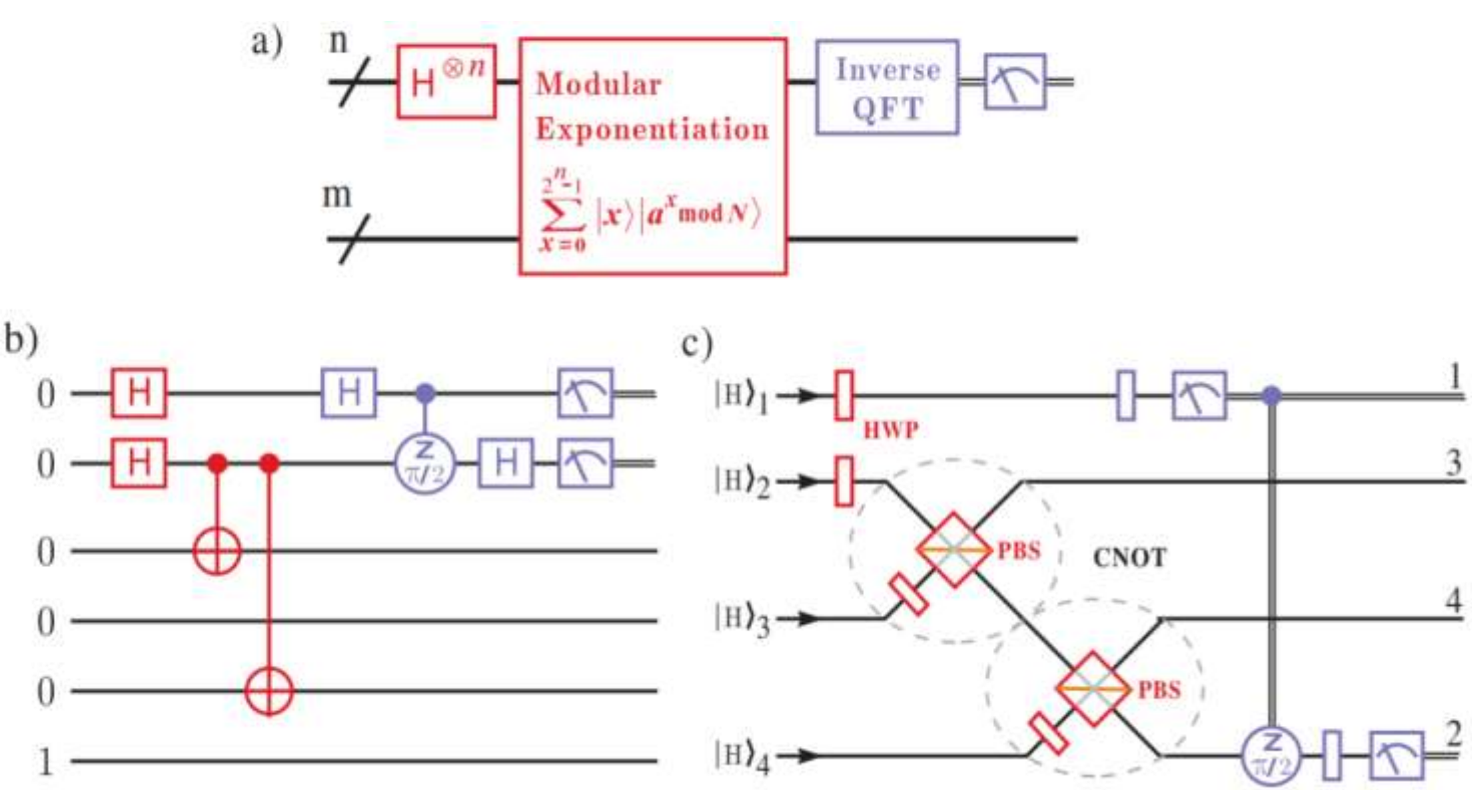
8. Check r

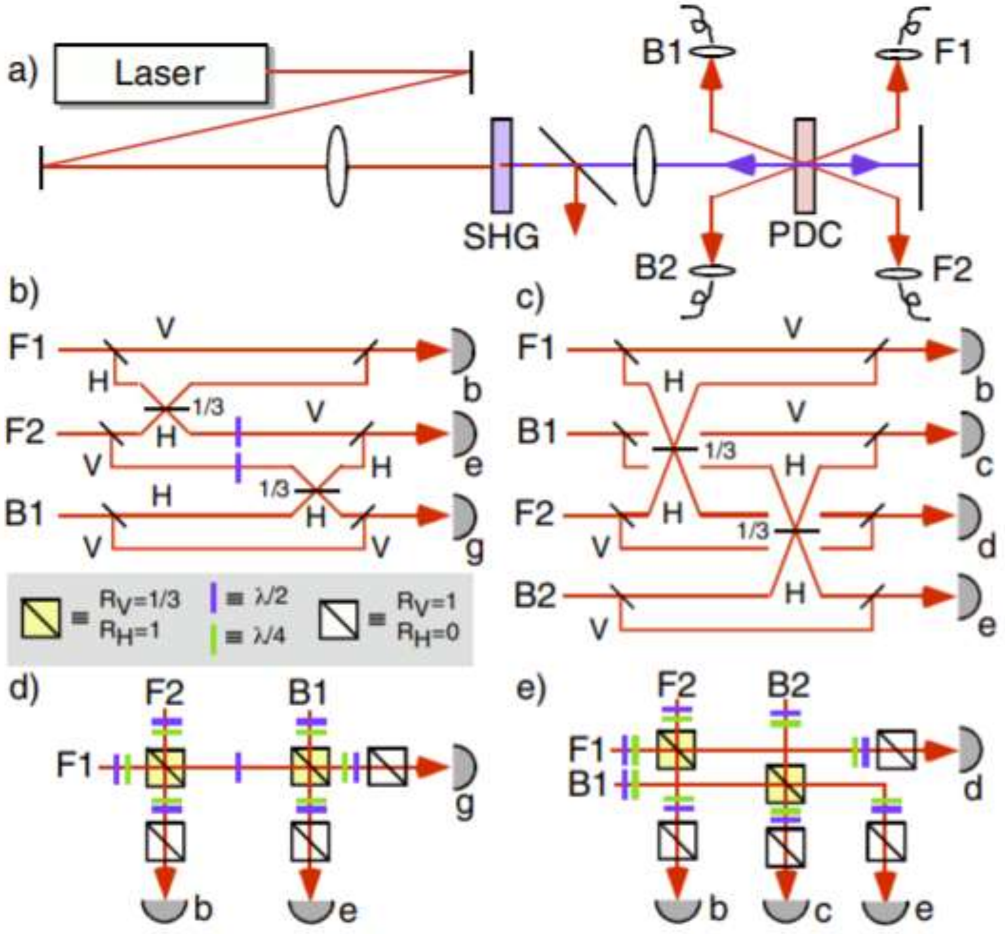
- check if r is even ✓
- check if $x^{r/2} \mod n \neq -1$ ✓
- as both holds, we can determine the factors:

$$x^{r/2} \mod n - 1 = 11^3 \mod 21 - 1 = 7$$
$$x^{r/2} \mod n + 1 = 11^3 \mod 21 + 1 = 9$$

→ the two factors are $\gcd(7, 21) = 7$ and $\gcd(9, 21) = 3$

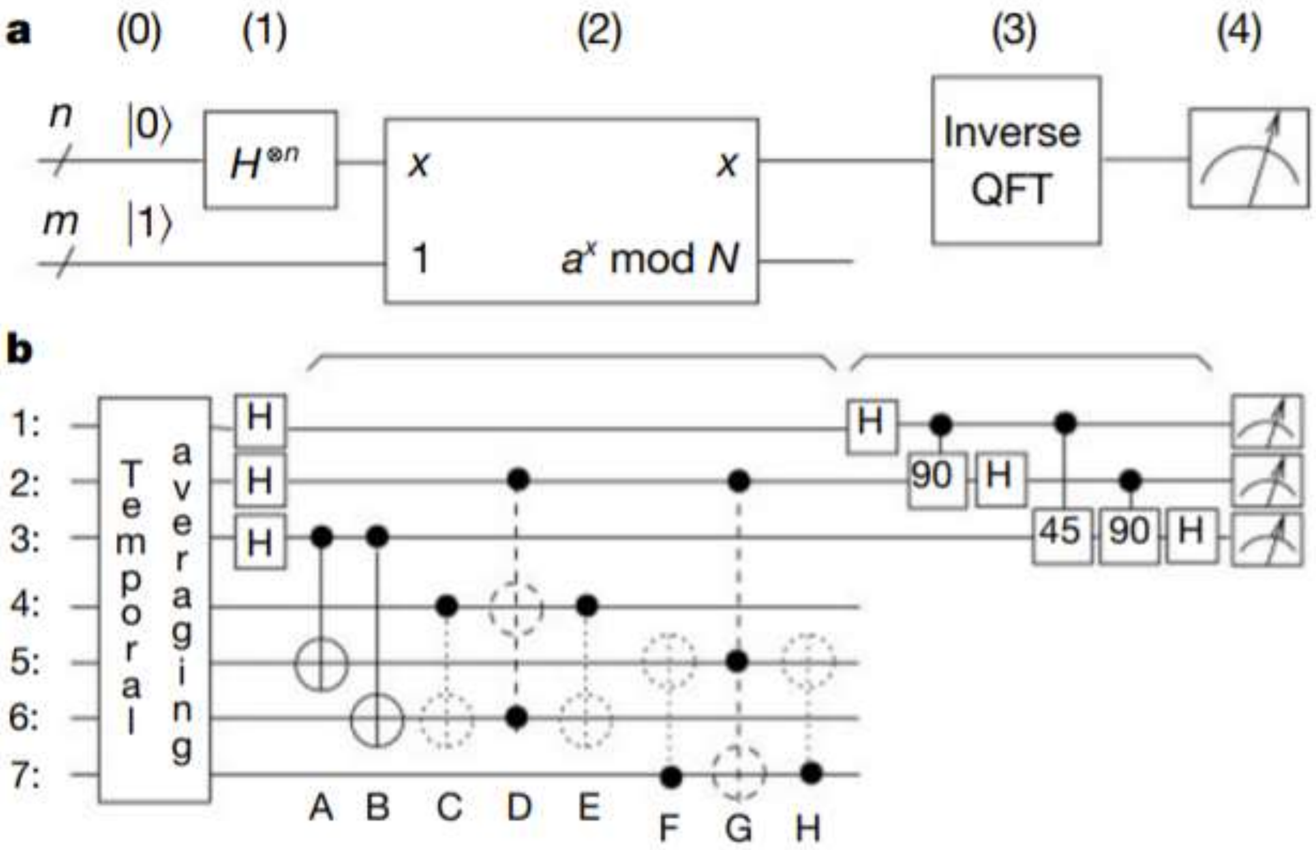
Experimental implementation of Shor’s algorithm



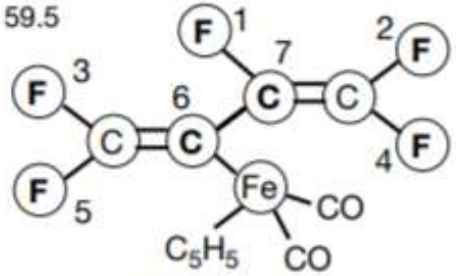


Experimental Demonstration of a Compiled Version of Shor's Algorithm with Quantum Entanglement, Phys. Rev. Lett. 99, 250505 (2007).

Demonstration of a Compiled Version of Shor's Quantum Factoring Algorithm Using Photonic Qubits, Phys. Rev. Lett. 99, 250504 (2007)



i	$\omega_i/2$	$T_{1,i}$	$T_{2,i}$	J_{7i}	J_{6i}	J_{5i}	J_{4i}	J_{3i}	J_{2i}
1	−22052.0	5.0	1.3	−221.0	37.7	6.6	−114.3	14.5	25.16
2	489.5	13.7	1.8	18.6	−3.9	2.5	79.9	3.9	
3	25088.3	3.0	2.5	1.0	−13.5	41.6	12.9		
4	−4918.7	10.0	1.7	54.1	−5.7	2.1			
5	15186.6	2.8	1.8	19.4	59.5				
6	−4519.1	45.4	2.0	68.9					
7	4244.3	31.6	2.0						



Experimental realization of Shor's quantum factoring algorithm using nuclear magnetic resonance, Nature volume 414, pages883–887 (2001)