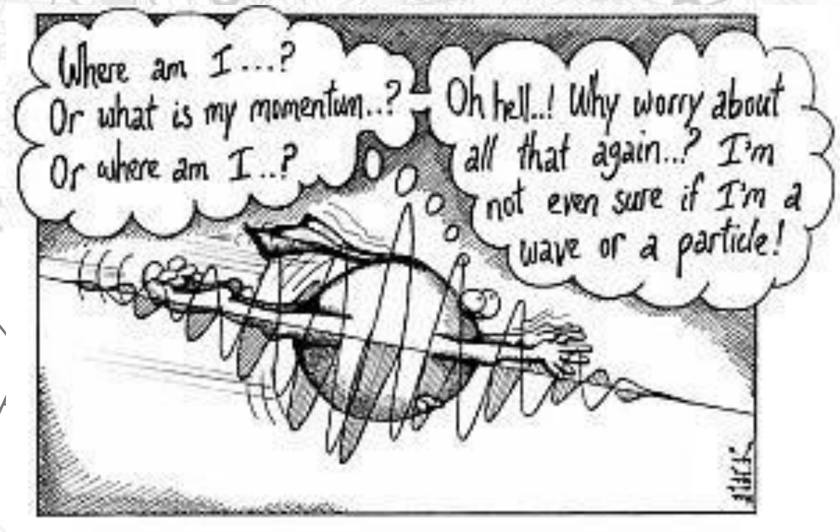
HÁLÓZATI REN
ÉS SZOLGÁLTA
TANSZÉK



Photon self-identity problems.

QFT and the Shor-algorithm

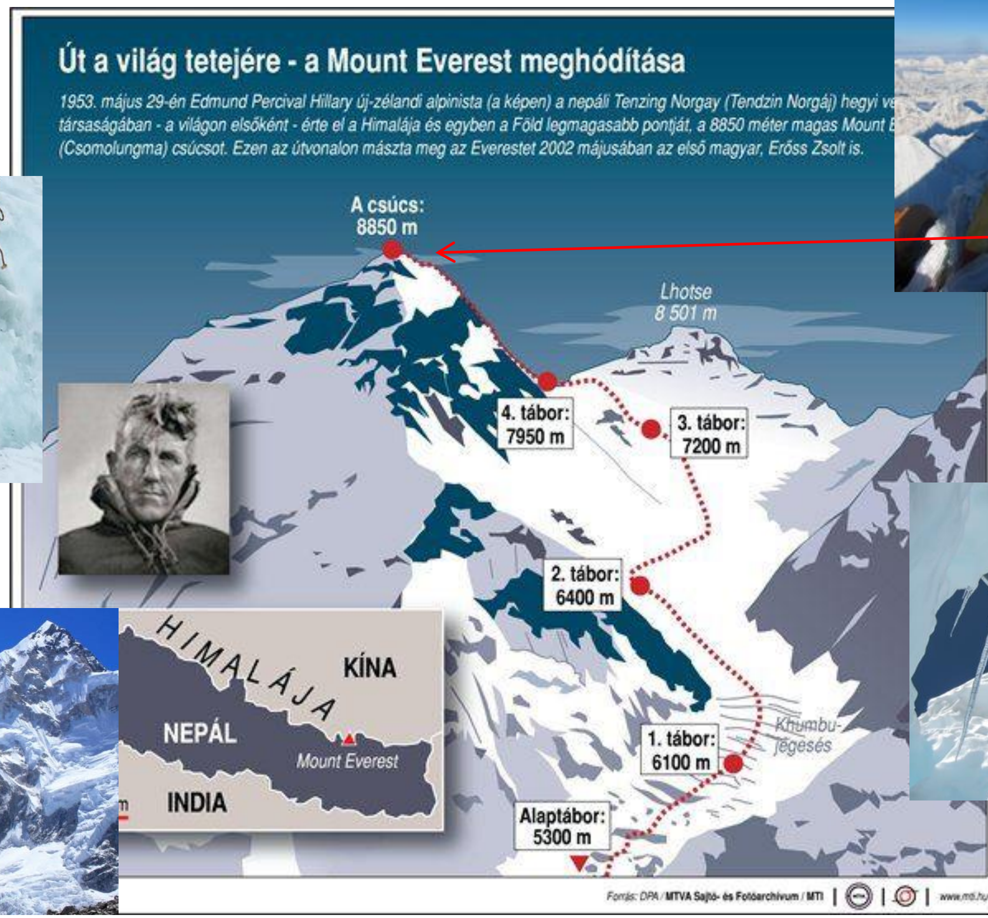
Quantum Computers and its Applications (BMEVIHIAD00)
Spring 2025

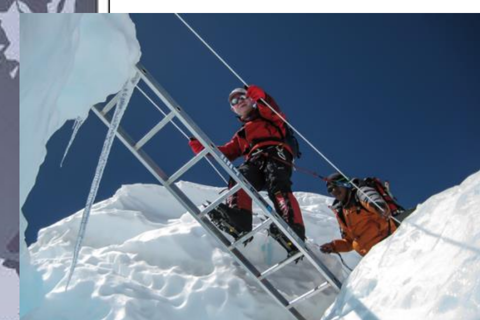
Prof. Sándor Imre, Dr. László Bacsárdi, Kitti Oláh

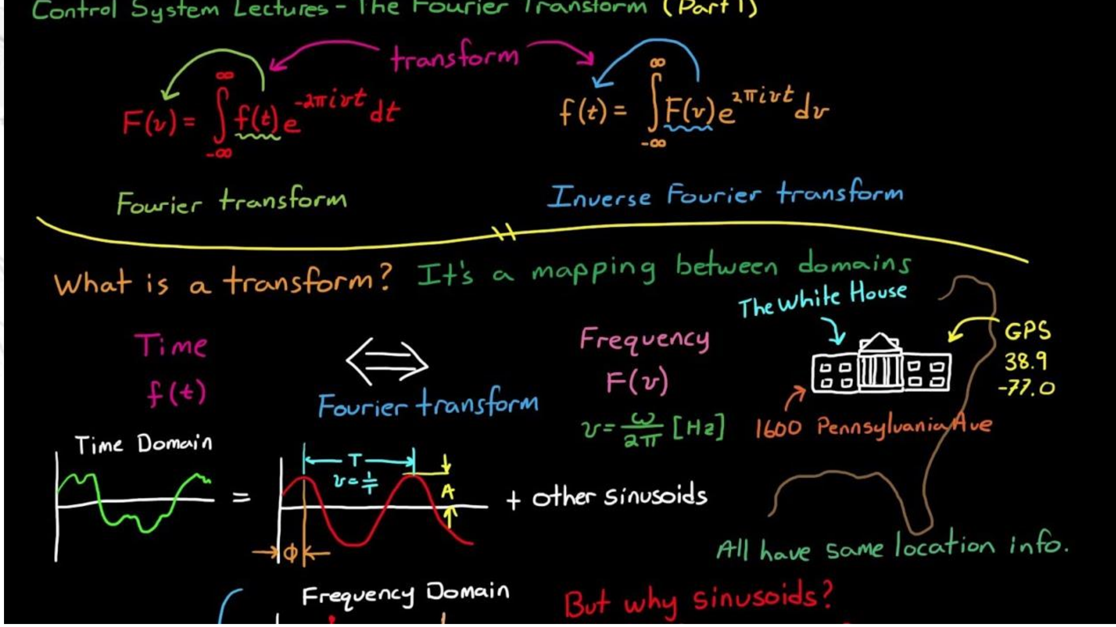
BME Department of Networked Systems and Services
imre@hit.bme.hu

MŰEGYETEM 1782

TODAY PROGRAM – MOUNT EVEREST





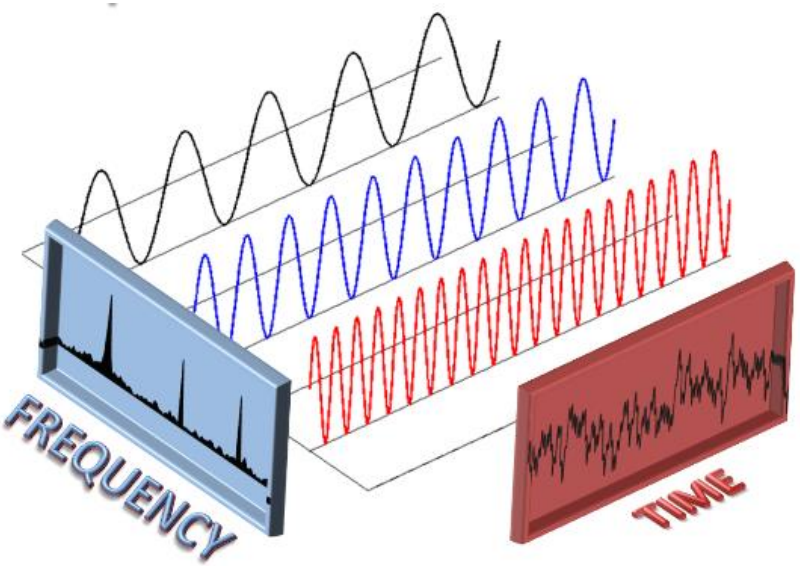


QUANTUM FOURIER TRANSFORM

Definition and decomposition

Base camp – 6100m

FOURIER Jean Baptiste Joseph (1768-1830)



CLASSICAL → QUANTUM

- Classical Discrete Fourier Transform (DFT)

$$\mathbf{x} = [x_0, x_1, \dots, x_{N-1}]^T \quad x_i \in \mathbb{C}$$

$$\mathbf{y} = \mathrm{DFT}\{\mathbf{x}\}$$

$$y_k \triangleq \frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} x_i e^{j\frac{2\pi}{N}ik}$$

- Quantum Discrete Fourier Transform (QFT)

$$|\varphi\rangle = \sum_{i=0}^{N-1} \varphi_i |i\rangle$$

$$|\psi\rangle = F|\varphi\rangle$$

$$\boxed{\psi_k \triangleq \frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} \varphi_i e^{j\frac{2\pi}{N}ik}}$$

Exercise 6.1. Prove that operator F is unitary!

Exercise 6.2. Determine the matrix of QFT!

DEFINITIONS

- For computational basis states

$$F|i\rangle = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{j\frac{2\pi}{N}ik} |k\rangle$$

- For arbitrary superposition

$$|\psi\rangle = \sum_{k=0}^{N-1} \psi_k |k\rangle = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} \sum_{i=0}^{N-1} \varphi_i e^{j\frac{2\pi}{N}ik} |k\rangle$$

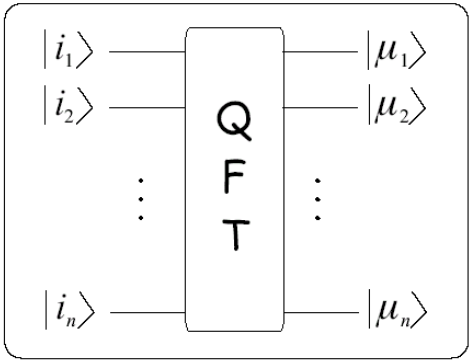
- Inverse Fourier Transform (IQFT)

$$\varphi_i \triangleq \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} \psi_k e^{-j\frac{2\pi}{N}ik}$$

$$\boxed{F^\dagger |k\rangle = \frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} e^{-j\frac{2\pi}{N}ik} |i\rangle}$$

HOW TO IMPLEMENT QFT 1

- The goal: to find an efficient circuit implementing QFT built from elementary quantum gates.
- The way: we prepare an equivalent tensor product representation of QFT which advises us what shall we do on each quantum wire separately.



- Binary representation of integer and real numbers:

An integer number $k \in \{0, 1, ..., 2^n - 1\}$ can be represented in the binary form of $(k_1, k_2, .., k_n) = k_1 2^{n-1} + k_2 2^{n-2} + ... + k_n 2^0$, where $k_l \in \{0, 1\}$. Let us introduce moreover for $h \geq 0$ the binary notation of

$$0.k_l k_{l+1} ... k_{l+h} \triangleq \frac{k_l}{2^1} + \frac{k_{l+1}}{2^2} + ... + \frac{k_{l+h}}{2^{h+1}}; k_m \in \{0, 1\}.$$

HOW TO IMPLEMENT QFT 2

- Now, we start the reformulation from the original definition

$$F|i\rangle = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{j\frac{2\pi}{N}ik}|k\rangle = \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} e^{j2\pi i \sum_{l=1}^{n} k_l \frac{2^{n-l}}{2^n}}|k\rangle$$

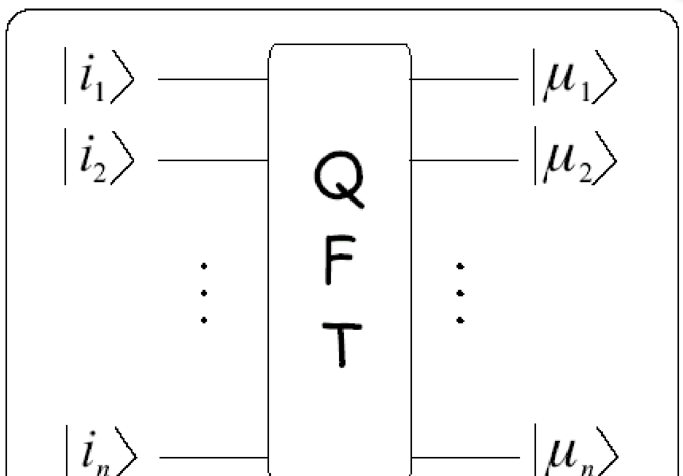
Recognizing that $\frac{2^{n-l}}{2^n} = 2^{-l}$ furthermore exploiting that $|k\rangle = |k_1, k_2, .., k_n\rangle = |k_1\rangle \otimes |k_2\rangle \otimes ... \otimes |k_n\rangle$ and $e^{\alpha+\beta} \equiv e^{\alpha}e^{\beta}$

$$F|i\rangle = \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} \prod_{l=1}^{n} e^{j2\pi i k_l 2^{-l}} \bigotimes_{l=1}^{n} |k_l\rangle = \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} \bigotimes_{l=1}^{n} e^{j2\pi i k_l 2^{-l}} |k_l\rangle$$

HOW TO IMPLEMENT QFT 3

Considering that $k_l \in \{0,1\}$ we collect the factors of the tensor product into two groups whit respect to $|0\rangle$ and $|1\rangle$

$$F|i\rangle = \frac{1}{\sqrt{2^n}} \bigotimes_{l=1}^{n} \left(e^{j2\pi i(k_l=0)2^{-l}} |0\rangle + e^{j2\pi i(k_l=1)2^{-l}} |1\rangle \right) = \frac{1}{\sqrt{2^n}} \bigotimes_{l=1}^{n} \left(|0\rangle + e^{j2\pi i 2^{-l}} |1\rangle \right)$$

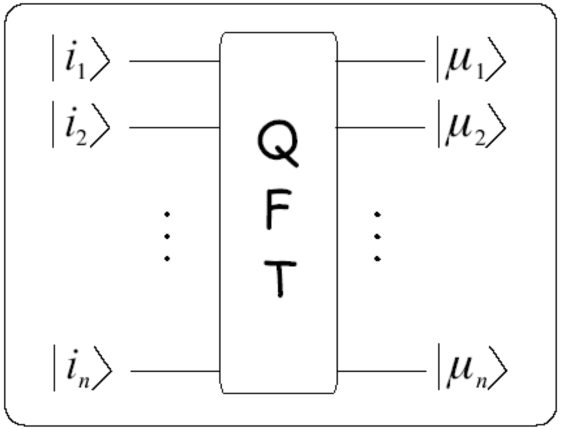


HOW TO IMPLEMENT QFT 4

$$\boxed{|\mu_l\rangle \triangleq \frac{1}{\sqrt{2}}\left(|0\rangle + e^{j2\pi i 2^{-l}}|1\rangle\right)}$$

$$i = \sum_{l=1}^{n} i_l 2^{n-l}$$

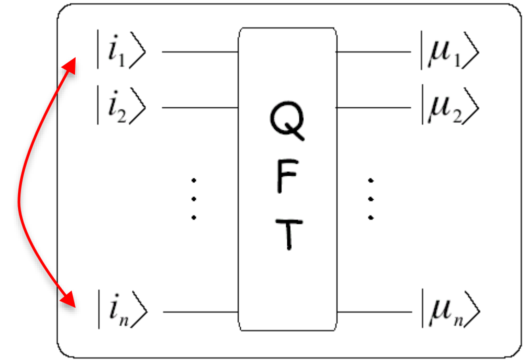
$$\left(2\pi i 2^{-l}\right) \mod 2\pi = 0.i_{l-n} i_{l-n+1} \ldots i_n$$



$$F|i\rangle = \underbrace{\left(\frac{|0\rangle + e^{j2\pi 0.i_n}|1\rangle}{\sqrt{2}}\right)}_{|\mu_1\rangle} \otimes \underbrace{\left(\frac{|0\rangle + e^{j2\pi 0.i_{n-1} i_n}|1\rangle}{\sqrt{2}}\right)}_{|\mu_2\rangle} \otimes \ldots \otimes \underbrace{\left(\frac{|0\rangle + e^{j2\pi 0.i_1 i_2 \ldots i_n}|1\rangle}{\sqrt{2}}\right)}_{|\mu_n\rangle} \tag{6.10}$$

HOW TO IMPLEMENT QFT 4

- Now, we have the tensor product representation in our hand. For the sake of easier implementation we apply a SWAP gate at the output of the QFT circuit, hence we are interested in



$$U_l \; : \quad |i_l\rangle \rightarrow |\mu_{n-l+1}\rangle$$

- Let us investigate first U_n.

$$\underbrace{\left(\frac{|0\rangle + e^{j2\pi 0.i_n}|1\rangle}{\sqrt{2}}\right)}_{|\mu_1\rangle}$$

$$\boxed{U_n = H}$$

$$i_n = 0, 1$$

$$e^{j2\pi 0.i_n} = \pm 1$$

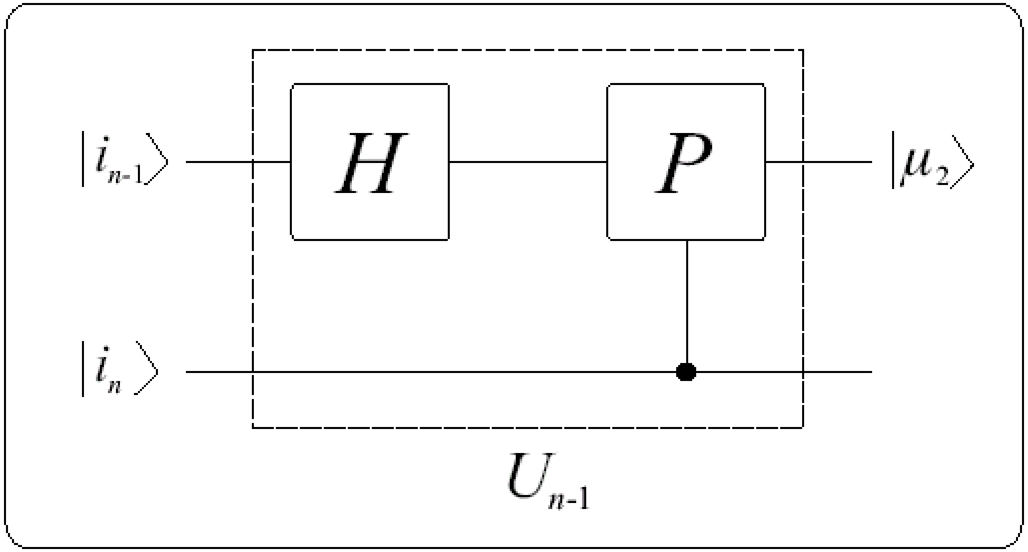
$$|\mu_1\rangle = \begin{cases} \frac{|0\rangle + |1\rangle}{\sqrt{2}} & \text{if } i_n = 0 \\ \frac{|0\rangle - |1\rangle}{\sqrt{2}} & \text{if } i_n = 1. \end{cases}$$

HOW TO IMPLEMENT QFT 5

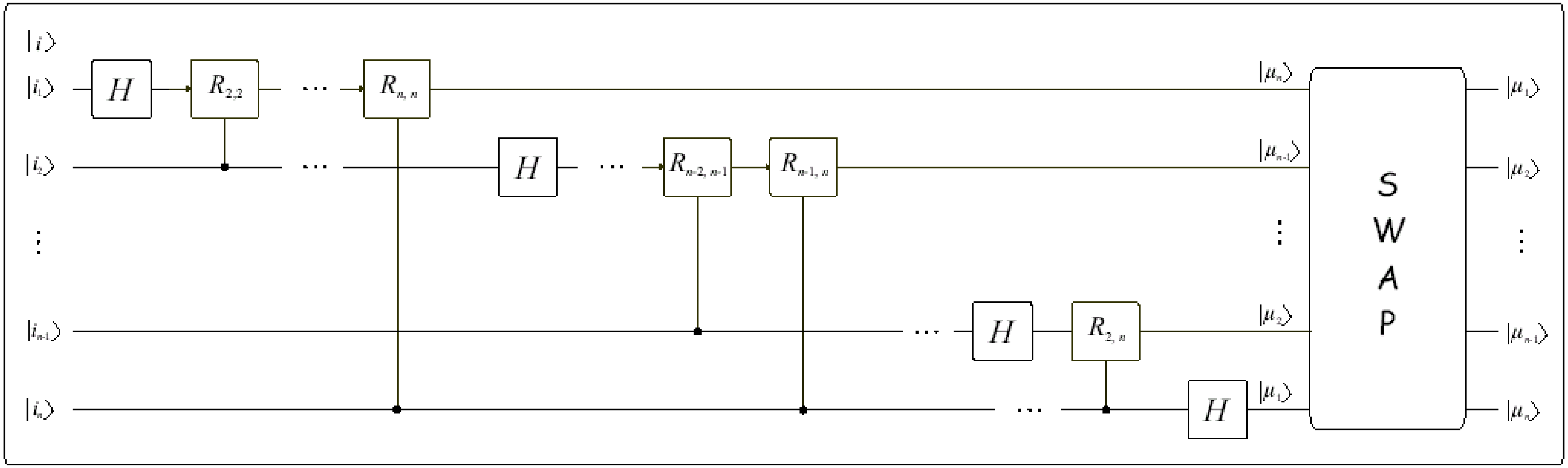
- Next we turn to $U_{n-1} : |i_{n-1}\rangle \rightarrow |\mu_2\rangle$

$$\underbrace{\left(\frac{|0\rangle + e^{j2\pi 0.i_{n-1}i_n}|1\rangle}{\sqrt{2}}\right)}_{|\mu_2\rangle}$$

$$|\mu_2\rangle = \frac{1}{\sqrt{2}}\left[|0\rangle + e^{j2\pi 0.i_{n-1}} \cdot \left\{ \begin{array}{cc} P(2\pi\frac{1}{2^2})|1\rangle & \text{if } i_n = 1 \\ 1|1\rangle & \text{if } i_n = 0 \end{array} \right\}\right]$$



HOW TO IMPLEMENT QFT 6



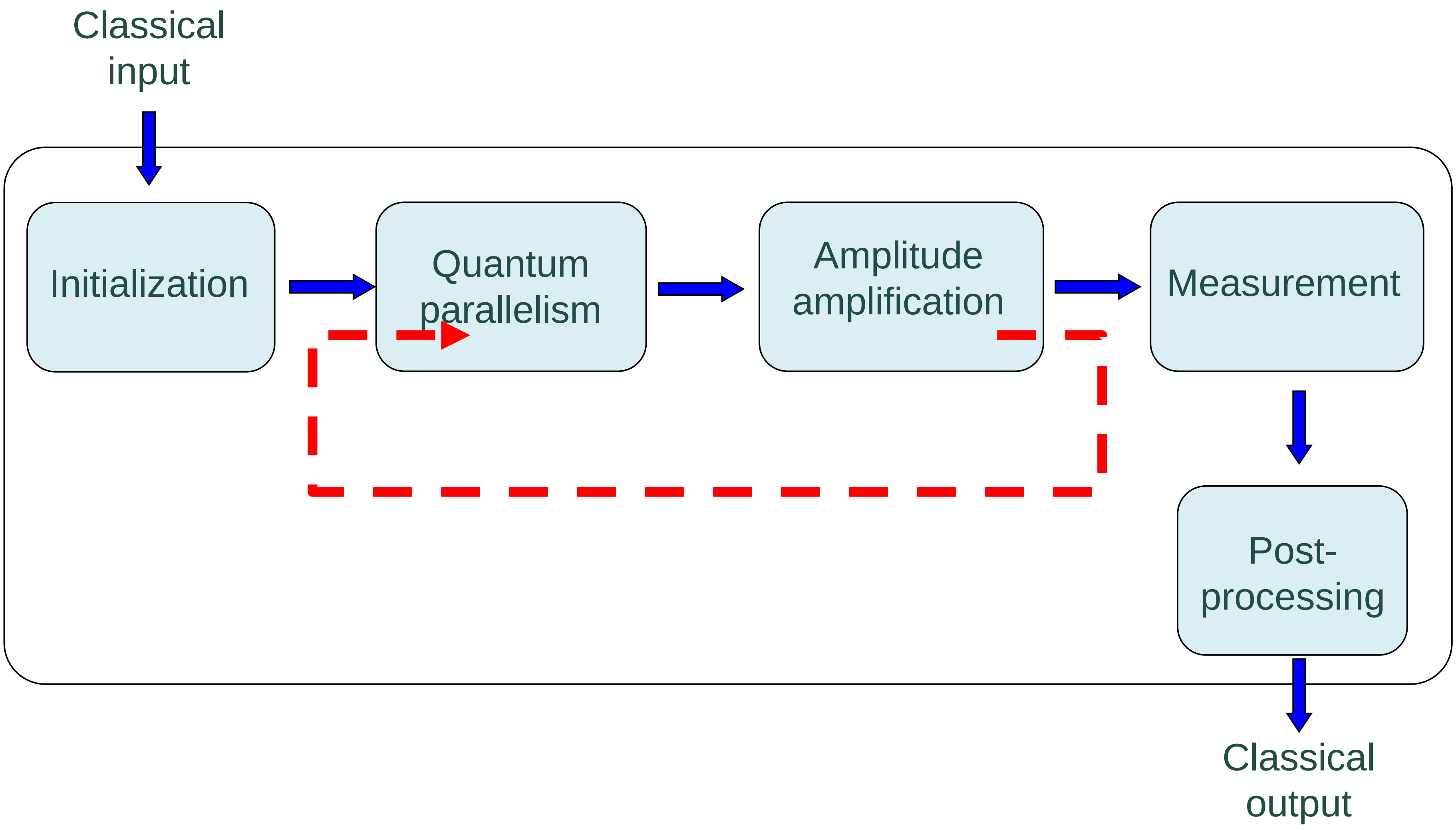
$$R_{h,p} \triangleq \begin{cases} P(2\pi \frac{1}{2^h}) & \text{if } i_p = 1 \\ 1 & \text{if } i_p = 0 \end{cases}$$

- Remarks
  - Complexity: $O(n^2)$
  - QFT is not for computing Fourier coefficients in a faster way since they are represented by probability amplitudes!

QUANTUM PHASE ESTIMATION –

Second camp– 6400m

QUANTUM ALGORITHM DESIGN



THE PROBLEM

- Each unitary transform U having eigenvector $|u\rangle$ has eigenvalues in the form of $e^{j\alpha_u}$.

$$\boxed{U = \sum_u \omega_u |u\rangle\langle u|}$$

- Phase ratio: $\kappa_u \in [0,1) : \alpha_u = 2\pi\kappa_u$

IDEALISTIC CASE

$$\kappa_u \in [0,1) : \alpha_u = 2\pi\kappa_u$$

$$\boxed{\kappa_u = i/2^n \text{ and } i \in \{0, 1, \ldots, 2^n - 1\}}$$

$$N = 2^n \qquad i/2^n = \kappa_u$$

IQFT

$$F|i\rangle = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{j\frac{2\pi}{N}ik}|k\rangle. \quad \longrightarrow \quad \boldsymbol{i} \qquad (6.4)$$

Decomposition of QFT

$$|\mu_l\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + e^{j2\pi 2^{n-l}\kappa_u}|1\rangle\right). \qquad (6.12)$$

$$|\mu_l\rangle = \frac{1}{\sqrt{2}} \underbrace{\left(|0\rangle + e^{j2\pi 2^{n-l} \kappa_u} |1\rangle \right)}_{} . \qquad (6.12)$$

Hadamard gate + special transform controlled by $|1\rangle$.

$|\mu_l\rangle$ ➡ $2^0 = 1$ is replaced by 2^{n-l}

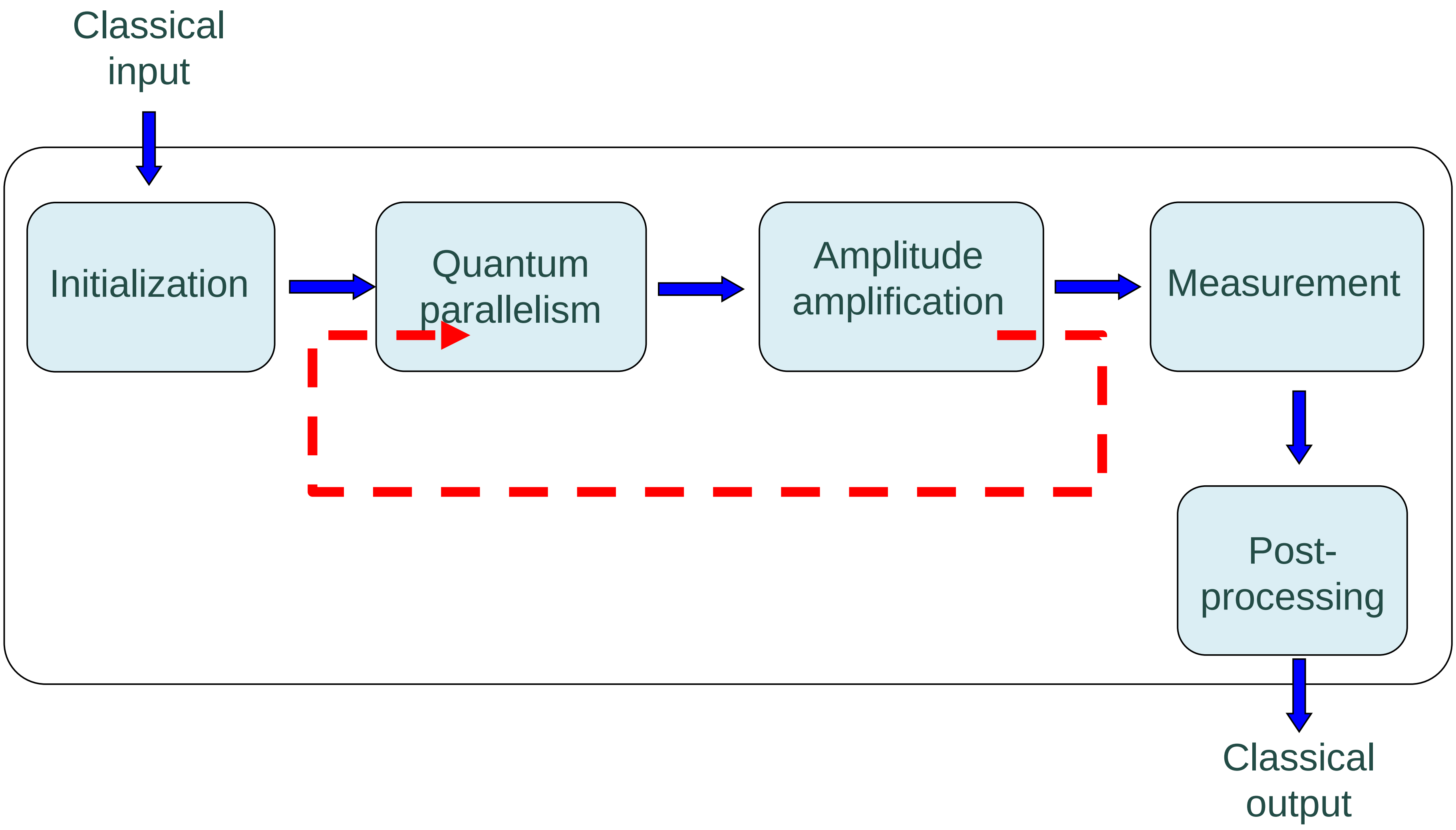
$$U^h \triangleq \underbrace{UU \dots U}_{h},$$

$$U^h|u\rangle = \underbrace{e^{j2\pi\kappa_u} e^{j2\pi\kappa_u} \dots e^{j2\pi\kappa_u}}_{h} |u\rangle = e^{j2\pi h\kappa_u} |u\rangle$$

eigenvalue

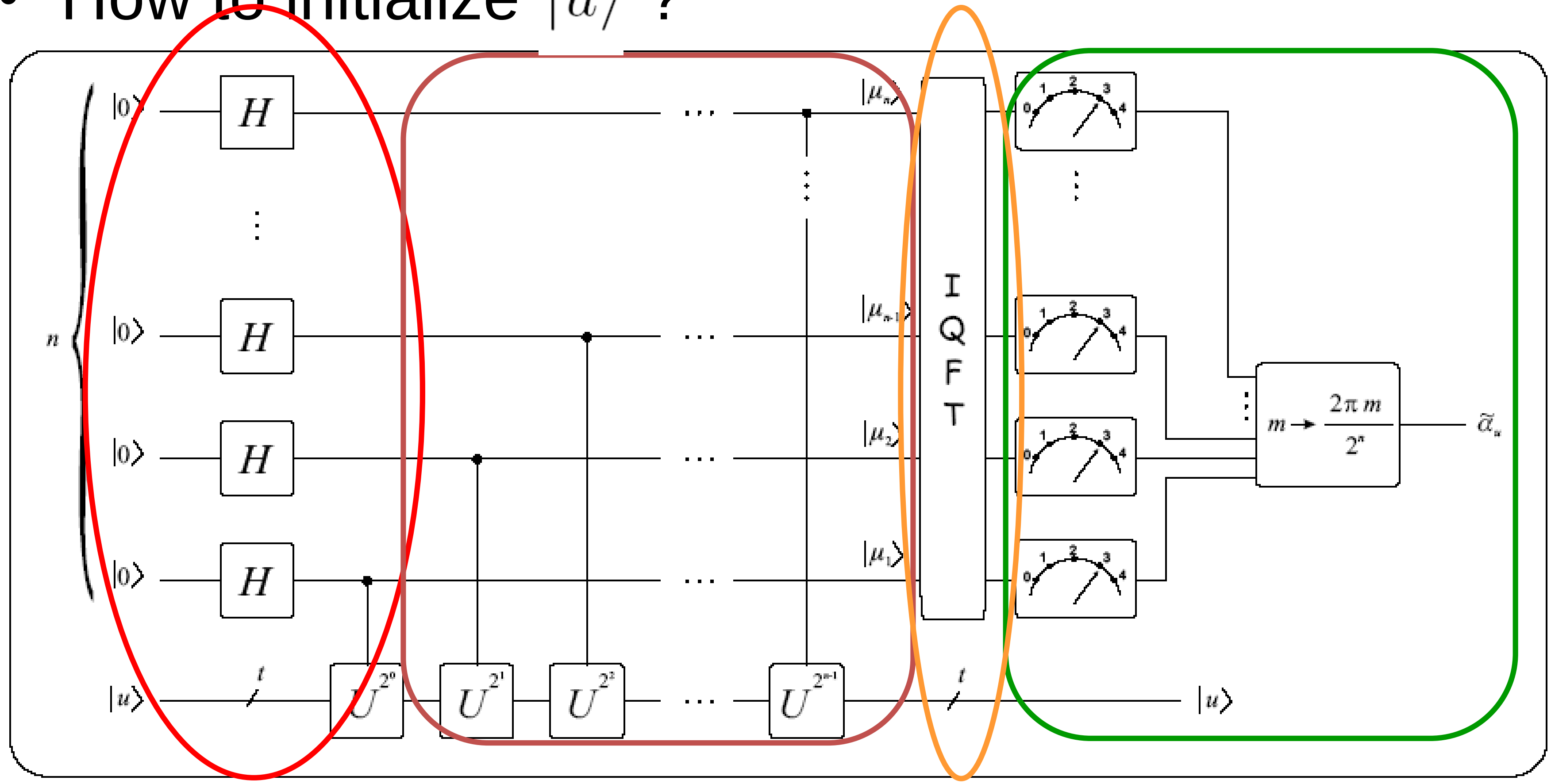
eigenvector

QUANTUM ALGORITHM DESIGN



QUANTUM PHASE ESTIMATOR

- How to initialize $|u\rangle$?



PRACTICAL CASE

we allow arbitrary $\kappa_u \in [0,1)$ $\quad \kappa_u \cancel{=} i/2^n$

- IQFT will not work correctly!

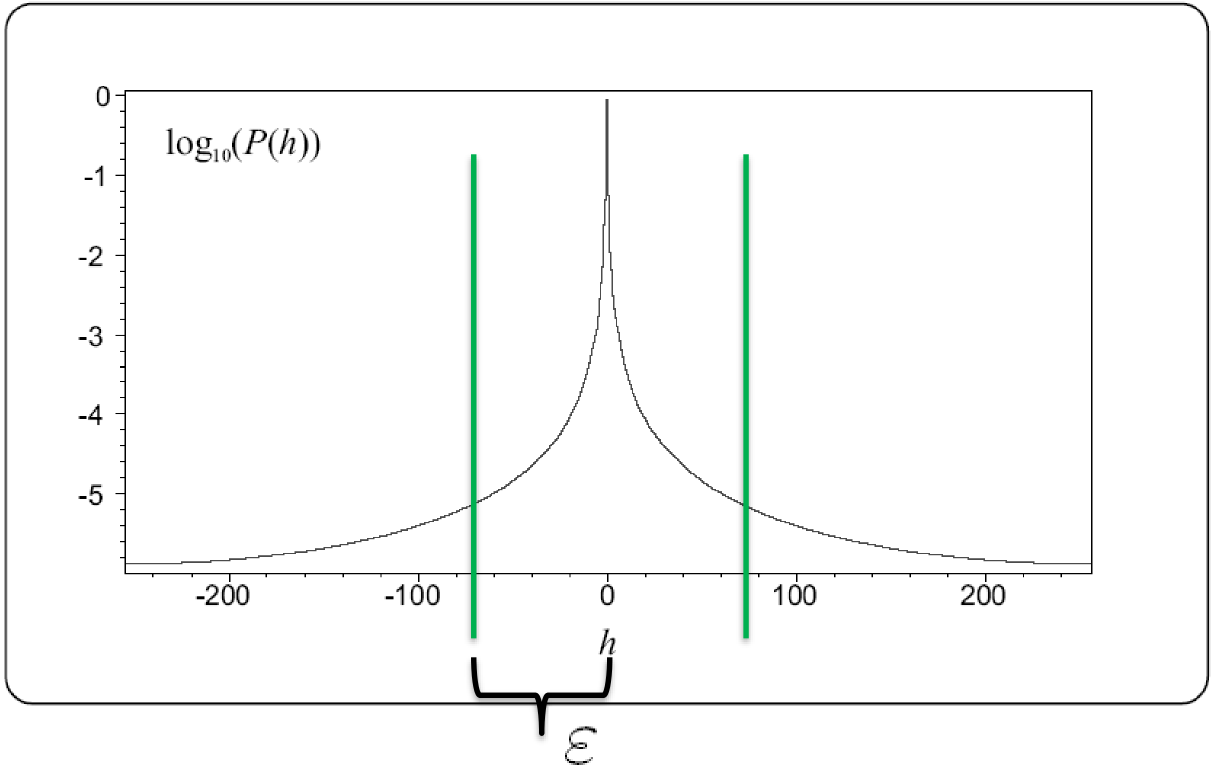
IQFT

$$F^\dagger|\mu\rangle = \sum_{k=0}^{2^n-1} \frac{1}{\sqrt{2^n}} e^{j2\pi k \kappa_u} \underbrace{\frac{1}{\sqrt{2^n}} \sum_{i=0}^{2^n-1} e^{-j2\pi \frac{i}{2^n} k}|i\rangle}_{\text{IQFT}}$$

$$= \frac{1}{2^n} \sum_{k=0}^{2^n-1} \sum_{i=0}^{2^n-1} e^{j2\pi k(\kappa_u - \frac{i}{2^n})}|i\rangle = \sum_{i=0}^{2^n-1} \sum_{k=0}^{2^n-1} \frac{1}{2^n} \left(e^{j2\pi(\kappa_u - \frac{i}{2^n})}\right)^k |i\rangle.$$

$\varphi_i \cancel{=} 1$

PROB. AMPLITUDES



$$\varphi_i = \frac{1}{2^n}\frac{1-q^{2^n}}{1-q} = \frac{1}{2^n}\frac{1-e^{j2\pi(2^n\kappa_u - i)}}{1-e^{j2\pi(\kappa_u - \frac{i}{2^n})}}$$

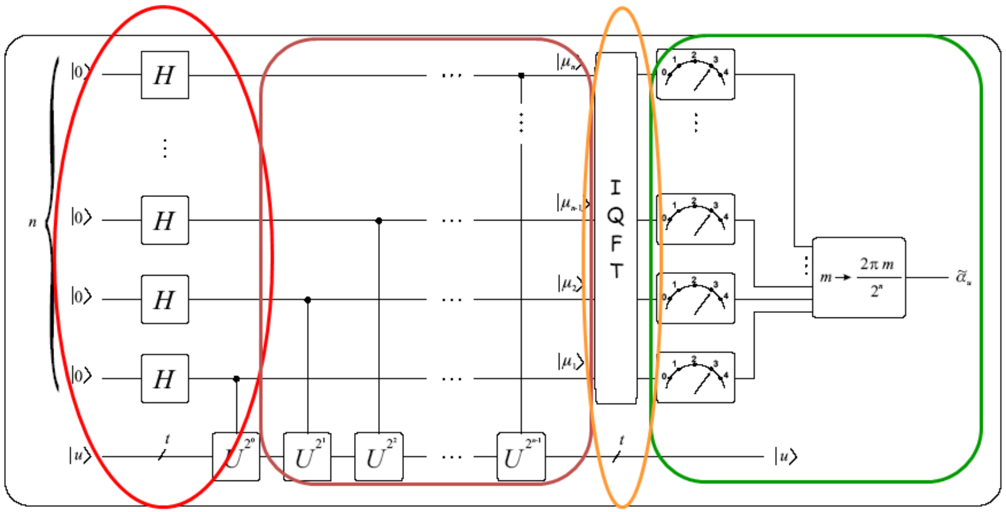
$$P_s = \frac{1}{2^{2c-2}}\frac{\sin^2(\pi 2^{c-1}2^{-c})}{\sin^2(\pi 2^{-c})} = \frac{4}{2^{2c}}\frac{\sin^2(\pi/2)}{\sin^2(\pi 2^{-c})} = \frac{4}{2^{2c}\sin^2(\pi 2^{-c})}$$

ERROR ANALYSIS

$$n = c - 1 + p$$

$$2\varepsilon = 2^p \Rightarrow \varepsilon = 2^{p-1}$$

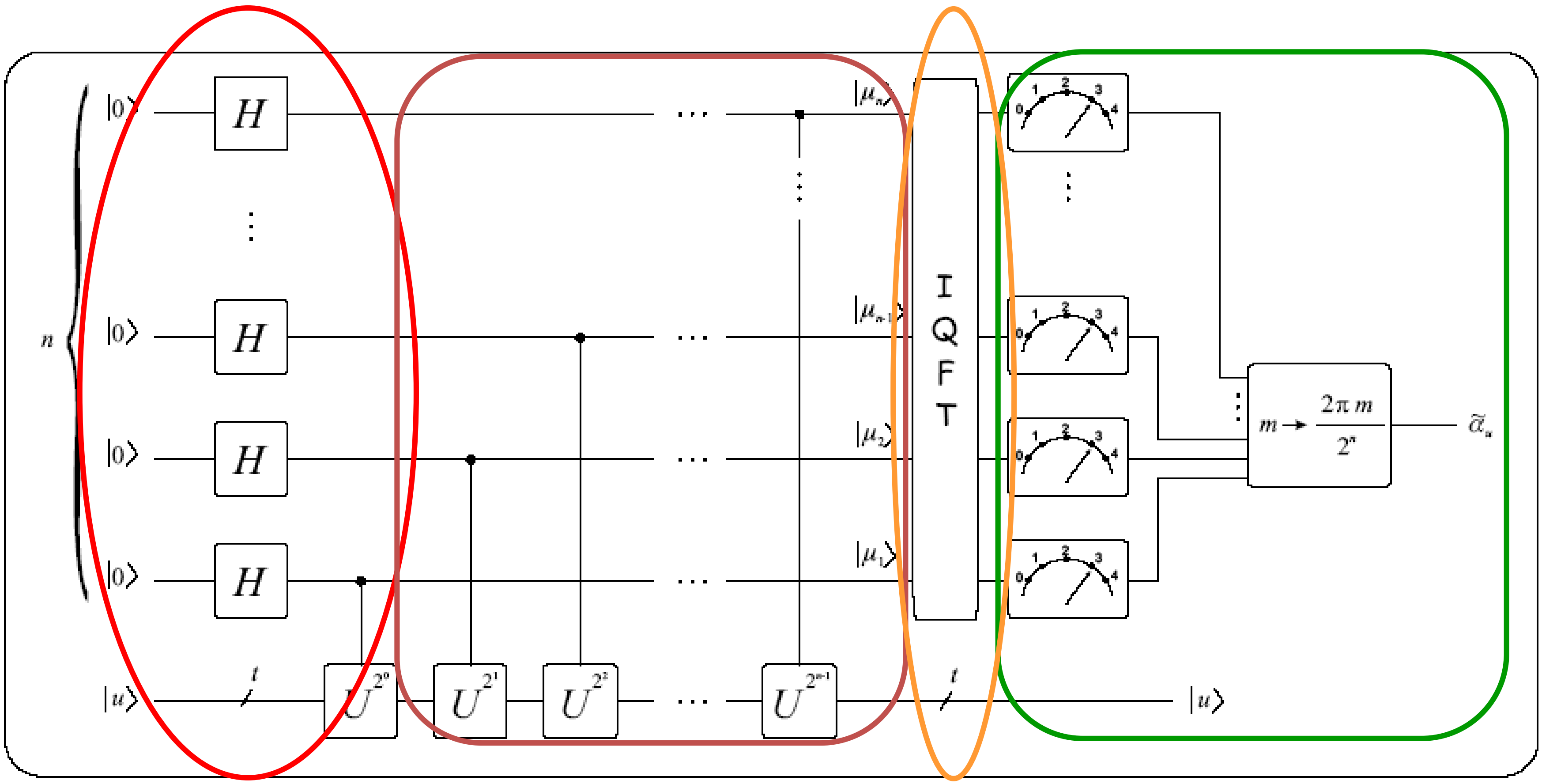
$$p \geq \operatorname{ld}\left(3 + \frac{1}{\breve{P}_\varepsilon}\right)$$



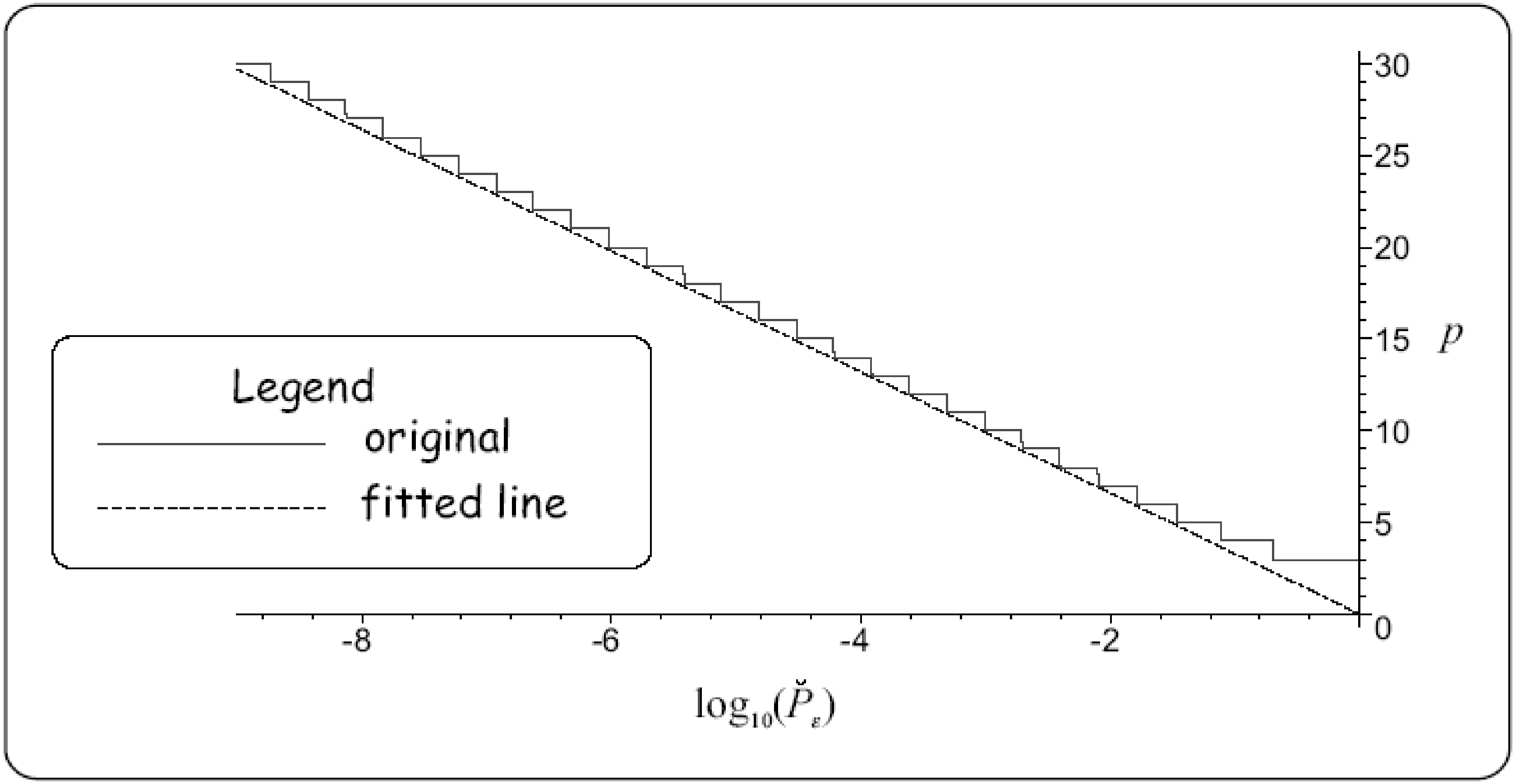
$$n = c - 1 + \left\lceil \operatorname{ld}\left(3 + \frac{1}{\breve{P}_\varepsilon}\right) \right\rceil$$

$$n = c - 1 + \left\lceil \operatorname{ld}(2\pi) + \operatorname{ld}\left(3 + \frac{1}{\breve{P}_\varepsilon}\right) \right\rceil$$

QUANTUM PHASE ESTIMATOR



ERROR ANALYSIS

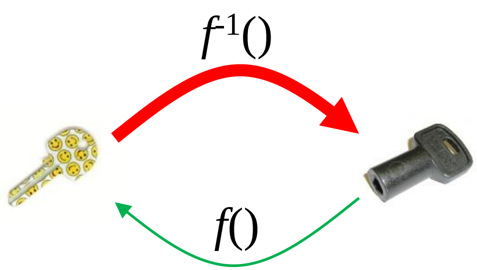


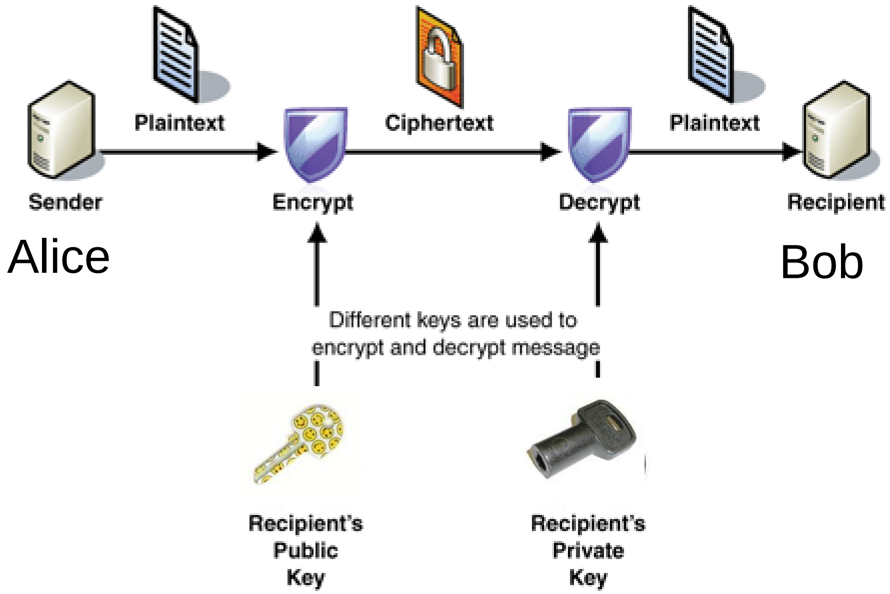
- Complexity in elementary gates: $\boxed{O(n^3)}$

THE RSA ALGORITHM

3rd camp – 7200m

PUBLIC KEY CRIPTOGRAPHY



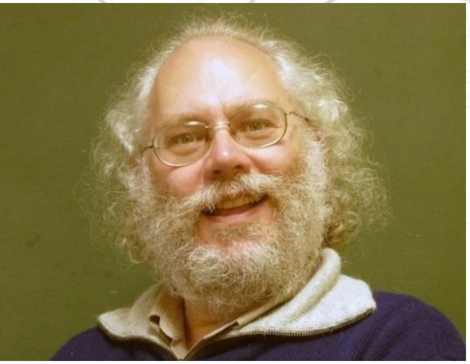


- Public ciphering key
- Secret de-ciphering key
- Key generation: multiplication of 2 large prime numbers
- Hacking: prime factorization
- To date, it has not been proven that there is no effective hacking algorithm. In any case, no such classical algorithm has been found so far.

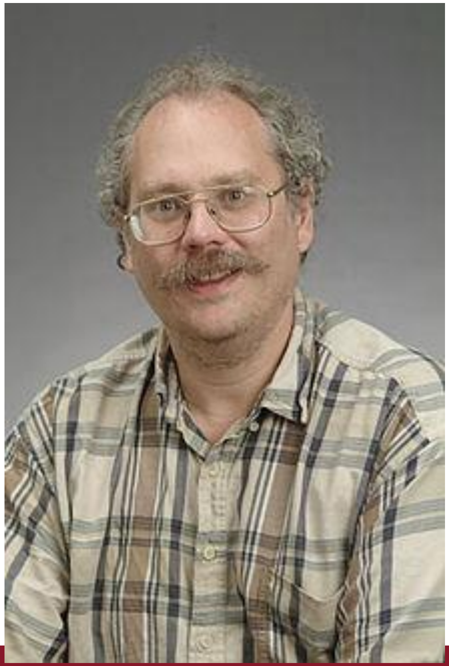
1. Bob selects randomly two large prime numbers p and q such that $p \neq q$.
2. He calculates $N = p \cdot q$.
3. Bob selects randomly a small odd number a such that $\gcd(\varphi(N), a) = 1$, where $\varphi(N)$ denotes the corresponding Euler function (see Section 12.3.2). Since N is a product of two prime numbers we can utilize Theorem 12.2 resulting in $\varphi(N) = (p-1) \cdot (q-1)$.
4. Next he calculates the multiplicative inverse (see Section 12.3.2) of a in modulo $\varphi(N)$ sense using Euclid's algorithm (see Section 12.3.3) and denotes it with b: $(a \cdot b) \bmod \varphi(N) = 1$. Moreover he knows that b always exists because of Theorem 12.3.
5. Bob announces the public key $K_B = (a, N)$ and
6. keeps secret the private key $L_B = (b, N)$.

Encryption and decryption are performed by means of the following special functions

$$\begin{aligned} E &= e(P, K_B) = (P^a) \bmod N, \\ P &= d(E, L_B) = (E^b) \bmod N. \end{aligned} \tag{9.10}$$



Peter Shor (1959-)



ORDER FINDING – SHOR ALGORITHM

4th camp – 7950m

CONNECTION BETWEEN FACTORING AND ORDER FINDING

Let us assume two positive integers $x < N$ that are co-primes, i.e. $\gcd(x, N) = 1$. The *order* of x in modulo N sense is defined as the least natural number r such that

$$x^r \bmod N = 1 \tag{6.40}$$

and it is easy to see that $1 < r < N$, too. The order of x is in close connection with the period of the function $f(z) = x^z \bmod N$ since

$$f(z+r) = x^{z+r} \bmod N = ((x^z \bmod N) \cdot (\underbrace{x^r \bmod N}_{\equiv 1})) \bmod N = f(z). \tag{6.41}$$

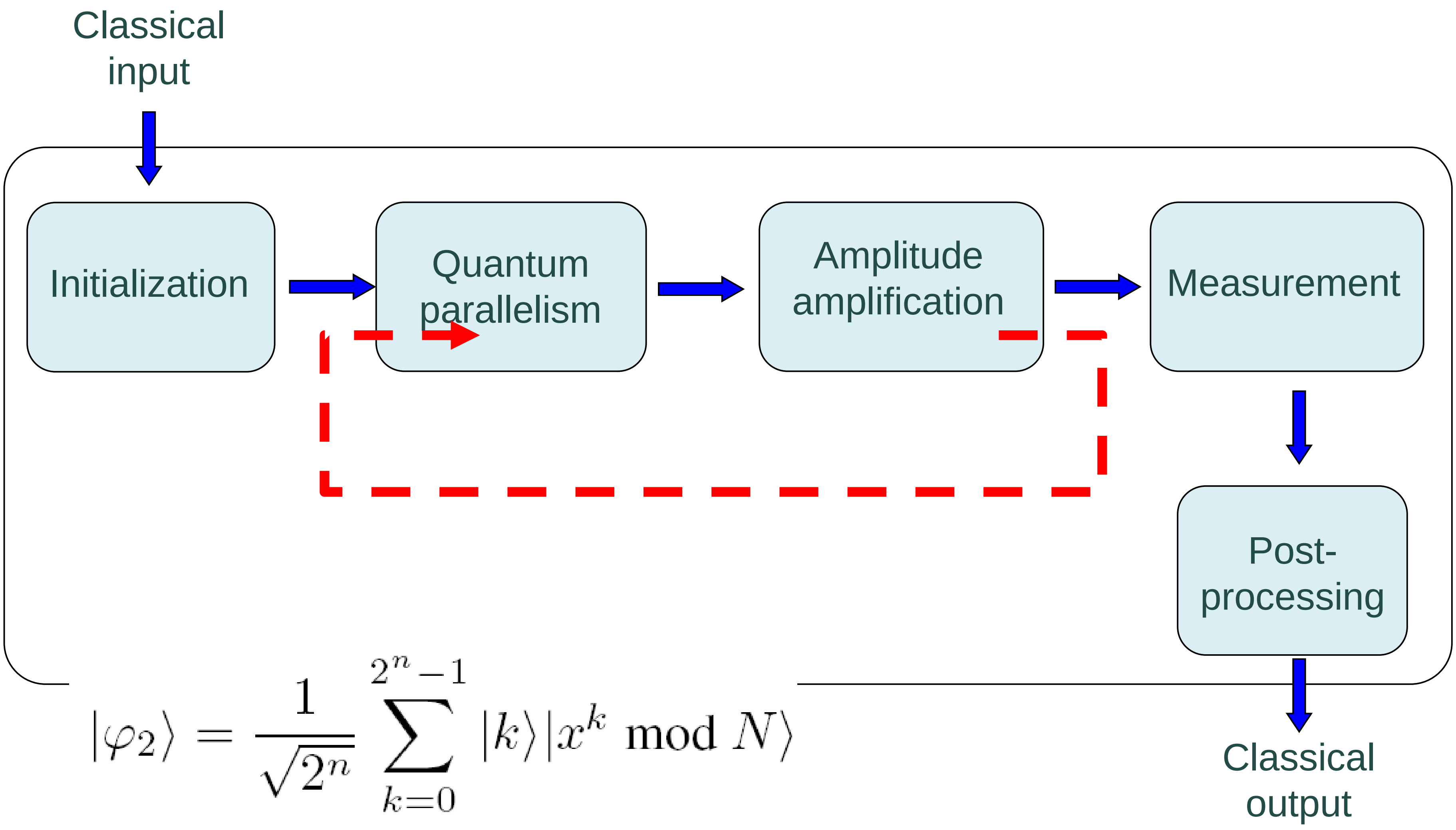
Factorize $A = 66$! To find the order use exhaustive search.

Solution: Since 66 is even we divide it by 2. $N = 33$ is a composite odd integer and it is easy to see that 33 does not prove to be a prime power. Therefore we cast a 32-faced dice and we get say $x = 5$. Now we are seeking for the order r of 5 in modulo 33 sense using an exhaustive search, i.e. we try to determine $r : x^r \bmod N = 1$

$$\begin{aligned} 5^1 \bmod 33 &= 5, & 5^6 \bmod 33 &= 16, \\ 5^2 \bmod 33 &= 25, & 5^7 \bmod 33 &= 14, \\ 5^3 \bmod 33 &= 26, & 5^8 \bmod 33 &= 4, \\ 5^4 \bmod 33 &= 31, & 5^9 \bmod 33 &= 20, \\ 5^5 \bmod 33 &= 23, & \boxed{5^{10} \bmod 33 = 1.} \end{aligned}$$

So $r = 10$ is even thus $y = x^{\frac{r}{2}} = 5^5$. Next we have to calculate $b_{+1} = (y+1) \bmod N = 24$ and $b_{-1} = (y-1) \bmod N = 22$. Fortunately neither of them equals zero (i.e. $x^{\frac{r}{2}} \bmod N \neq \pm 1$), which enables us to compute nontrivial factors $c_{+1} = \gcd(24, 33) = 3$ and $c_{-1} = \gcd(22, 33) = 11$. In order to check the results it is worth calculating $3 \cdot 11 = 33$.

QUANTUM ALGORITHM DESIGN



$$|\varphi_2\rangle = \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} |k\rangle |x^k \bmod N\rangle$$

CONNECTION BETWEEN ORDER FINDING AND PHASE ESTIMATION

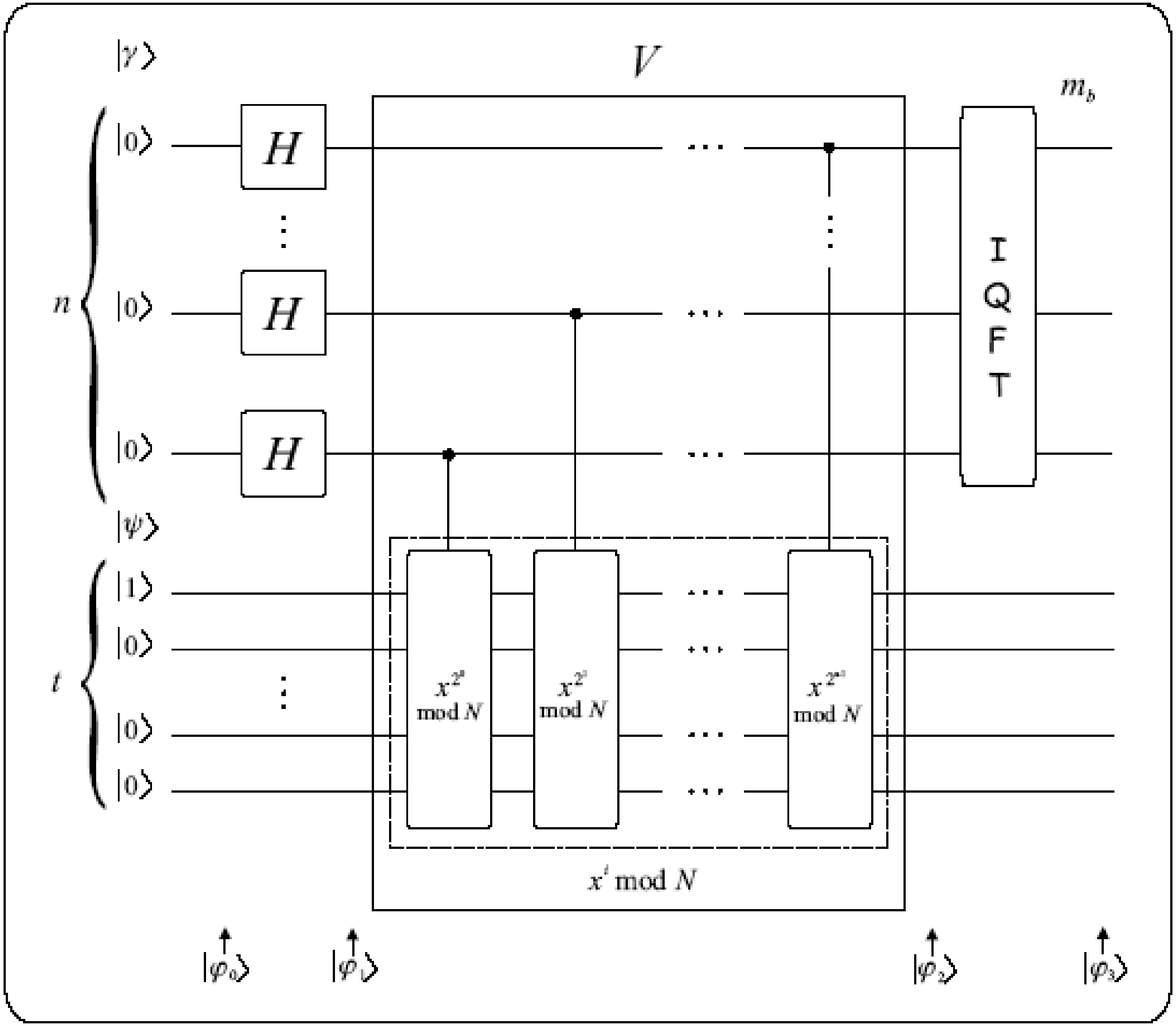
$$|\varphi_2\rangle = \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} |k\rangle |x^k \bmod N\rangle$$

$$x^k \bmod N = \prod_{l=1}^{2^n} \left(x^{k_l 2^{n-l}} \bmod N \right)$$
$$= \left(x^{k_1 2^{n-1}} \bmod N \right) \left(x^{k_2 2^{n-2}} \bmod N \right) \ldots \left(x^{k_n 2^0} \bmod N \right)$$

- Eigenvalues and vectors of : $U : |q\rangle \to |(qx) \bmod N\rangle$

Phase estimation!

$$\kappa_b = \frac{b}{r}, \quad |u_b\rangle = \sum_{s=0}^{r-1} \frac{e^{-j2\pi \frac{b}{r} s}}{\sqrt{r}} |x^s \bmod N\rangle$$


$|\gamma\rangle$
V
m_b
$|0\rangle$
$|0\rangle$
$|0\rangle$
n
H
H
H
IQFT
$|\psi\rangle$
$|1\rangle$
$|0\rangle$
$|0\rangle$
$|0\rangle$
t
x^{2^0} mod N
x^{2^1} mod N
$x^{2^{n-1}}$ mod N
x^i mod N
$|\varphi_0\rangle$
$|\varphi_1\rangle$
$|\varphi_2\rangle$
$|\varphi_3\rangle$

$$\kappa_b = \frac{b}{r}, \qquad |u_b\rangle = \sum_{s=0}^{r-1} \frac{e^{-j2\pi \frac{b}{r} s}}{\sqrt{r}} |x^s \bmod N\rangle$$

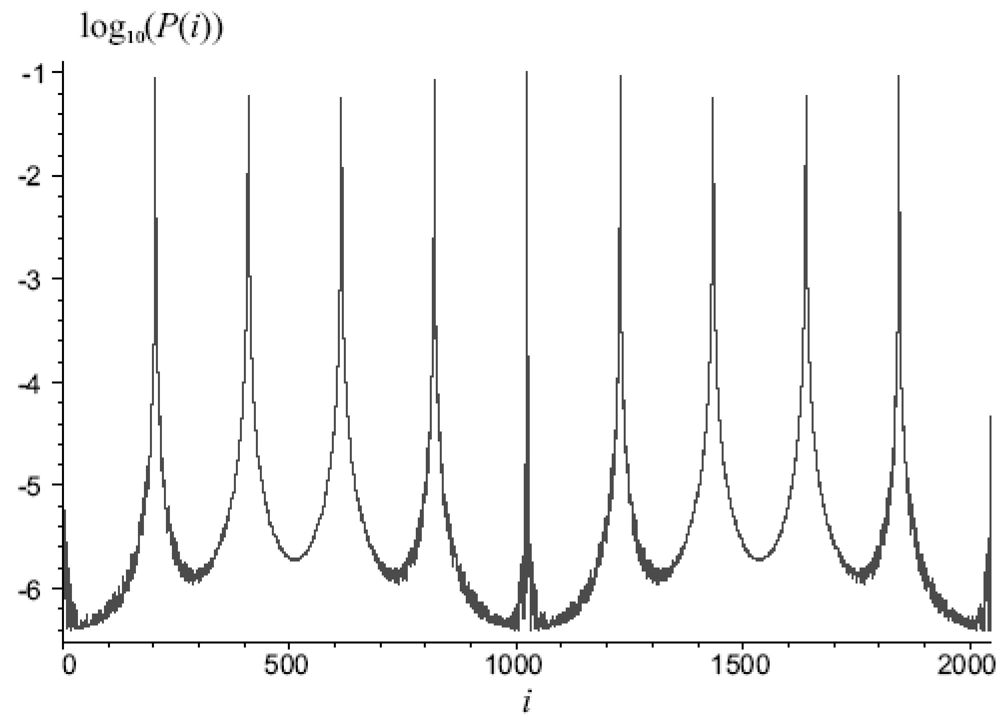


Fig. 6.16 $\log_{10}(P(i))$ assuming $n = 11, N = 33, x = 5, r = 10$

USING SHOR’S ORDER FINDING ALGORITHM TO BREAK RSA

Before the peak – 8790m

RSA

1. Bob selects randomly two large prime numbers p and q such that $p \neq q$.
2. He calculates $N = p \cdot q$.
3. Bob selects randomly a small odd number a such that $\gcd(\varphi(N), a) = 1$, where $\varphi(N)$ denotes the corresponding Euler function (see Section 12.3.2). Since N is a product of two prime numbers we can utilize Theorem 12.2 resulting in $\varphi(N) = (p-1) \cdot (q-1)$.
4. Next he calculates the multiplicative inverse (see Section 12.3.2) of a in modulo $\varphi(N)$ sense using Euclid's algorithm (see Section 12.3.3) and denotes it with b: $(a \cdot b) \bmod \varphi(N) = 1$. Moreover he knows that b always exists because of Theorem 12.3.
5. Bob announces the public key $K_B = (a, N)$ and
6. keeps secret the private key $L_B = (b, N)$.

Encryption and decryption are performed by means of the following special functions

$$
\begin{aligned}
E &= e(P, K_B) = (P^a) \bmod N, \\
P &= d(E, L_B) = (E^b) \bmod N.
\end{aligned}
\tag{9.10}
$$

www.hit.b

És me

Eve – our evil character in this story – downloads Bob's public key $K_B = (a, N)$ from the free database and launches the following process:

1. First she calculates the order of E in modulo N sense using the Shor algorithm and denotes it with r that is $((P^a)^r) \bmod N = 1$. This step requires that E and N are relative primes. If not Eve can apply Euclid's algorithm (see Section 12.3.3) to eliminate the common factors, which provides p and q.
2. Next she computes the modulo r multiplicative inverse of a. The existence of this inverse $b^\sharp$ requires that a is co-prime to r. Since $(E^r) \bmod N = 1$ and Euler's theorem (see Section 12.5) states that $(E^{\varphi(N)}) \bmod N = 1$ thus $\varphi(N) = k \cdot r$ for certain integer k, that is prime factors of r form a subset of those of $\varphi(N)$. Keeping in view that $\gcd(\varphi(N), a) = 1$, a and $\varphi(N)$ are relative primes, because of the operation of RSA algorithm, we can conclude that a is co-prime to r, too.
3. Furthermore Eve recalls from the RSA algorithm that $(a \cdot b) \bmod \varphi(N) = 1$ while she obtained in Point 2 that $(a \cdot b^\sharp) \bmod r = 1$ and $\varphi(N) = k \cdot r$ hence $b^\sharp = b + k \cdot r$.
4. Now, in possession of $b^\sharp$ Eve replaces in her decipher the unknown b with it. Hence

$$\left((P^a)^{b^\sharp}\right) \bmod N = \left(P^{ab+akr}\right) \bmod N = \left(P^{ab} \cdot (P^{ar})^k\right) \bmod N = P,$$

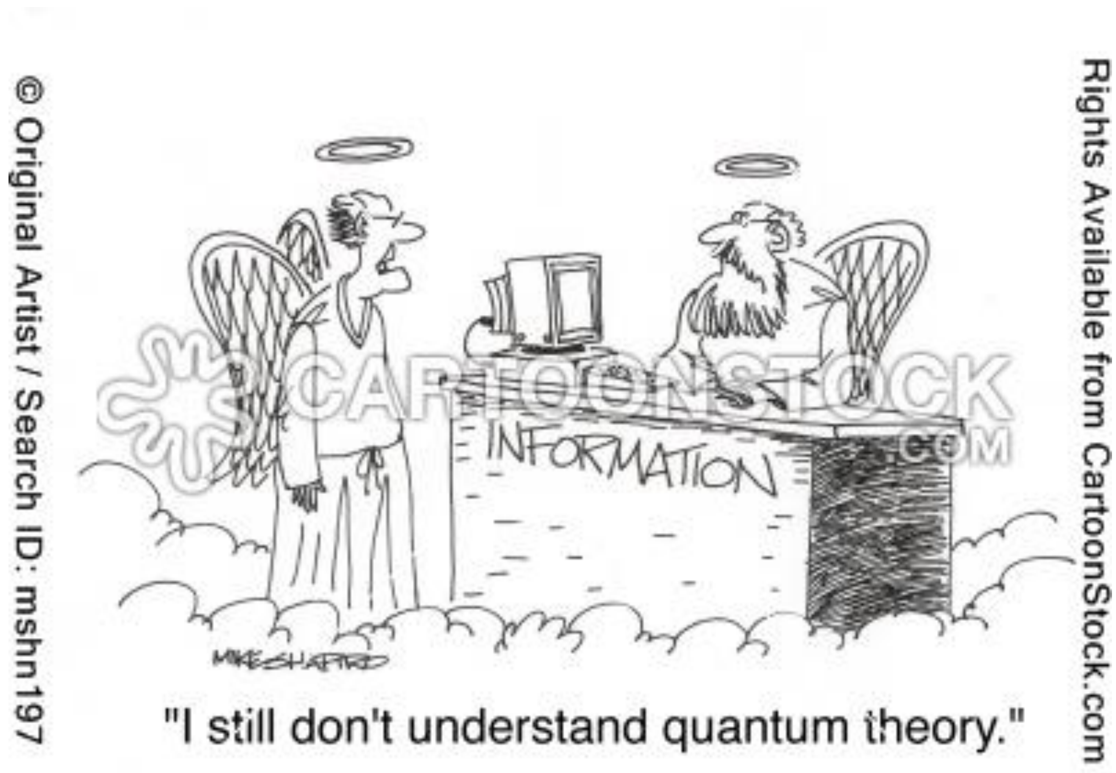
- Although the Grover algorithm is dedicated to find items efficiently in an unsorted data base it can be used to crack the RSA.
- The space of the potential prime factors of *N* can be regarded as a database and we need to find one prime number *p* which divides *N* = *p* x *q* without remainder.
- Since it is enough to search for *p* below $\sqrt{N}$ therefore the computational complexity becomes $\sqrt{\sqrt{N}} = 2^{\frac{n}{4}}$.

Table 9.1 Code-breaking methods and related complexity

Method	$n = 128$	$n = 128$	$n = 1024$	$n = 1024$	1s barrier
BF	$1.8 \cdot 10^7$ s	0.58 year	$1.3 \cdot 10^{142}$ s	$4 \cdot 10^{134}$ year	80 bit
BC	$6 \cdot 10^{-4}$ s	$1.9 \cdot 10^{-11}$ year	$3.5 \cdot 10^8$ s	11.29 year	273 bit
G	$4 \cdot 10^{-3}$ s	$1.3 \cdot 10^{-10}$ year	$1.1 \cdot 10^{65}$ s	$3.7 \cdot 10^{57}$ year	159 bit
S	$2 \cdot 10^{-5}$ s	$6.6 \cdot 10^{-14}$ year	**0.01** s	$3.4 \cdot 10^{-11}$ year	**10000** bit

- BF: *brute force* classical method which scans the integer numbers from 2 to $\lceil \sqrt{N} \rceil$ with complexity $O(\sqrt{N})$,
- BC: *best classical* method requiring $O(\exp[c \cdot \mathrm{ld}^{\frac{1}{3}}(N)\mathrm{ld}^{\frac{2}{3}}(\mathrm{ld}(N))])$ steps,
- G: *Grover* search based scheme with $O(N^{\frac{1}{4}})$,
- S: *Shor* factorization with $O(\mathrm{ld}(N)^3)$. ⟵ Extreme!

WE REACHED THE PEAK! - 8850M


© Original Artist / Search ID: mshn197
INFORMATION
CARTOONSTOCK.COM
"I still don't understand quantum theory."
Rights Available from CartoonStock.com