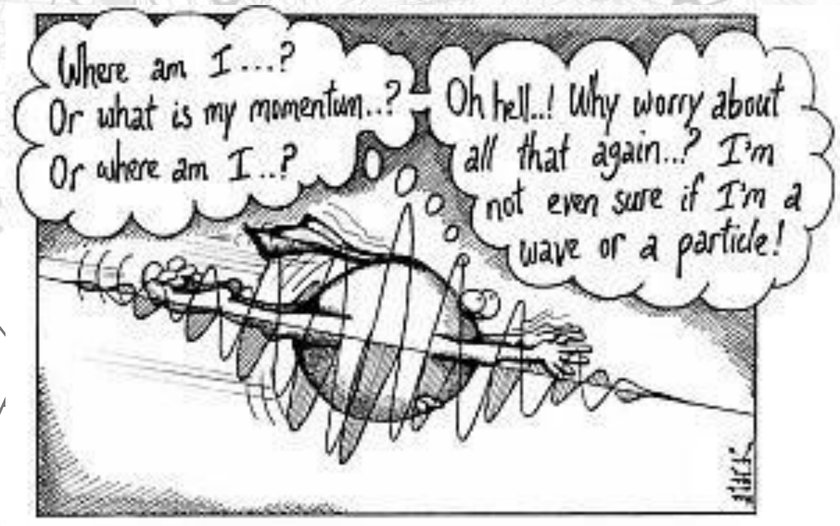


Photon self-identity problems.

QFT és a Shor-algoritmus

Kvantuminformatikai alkalmazások

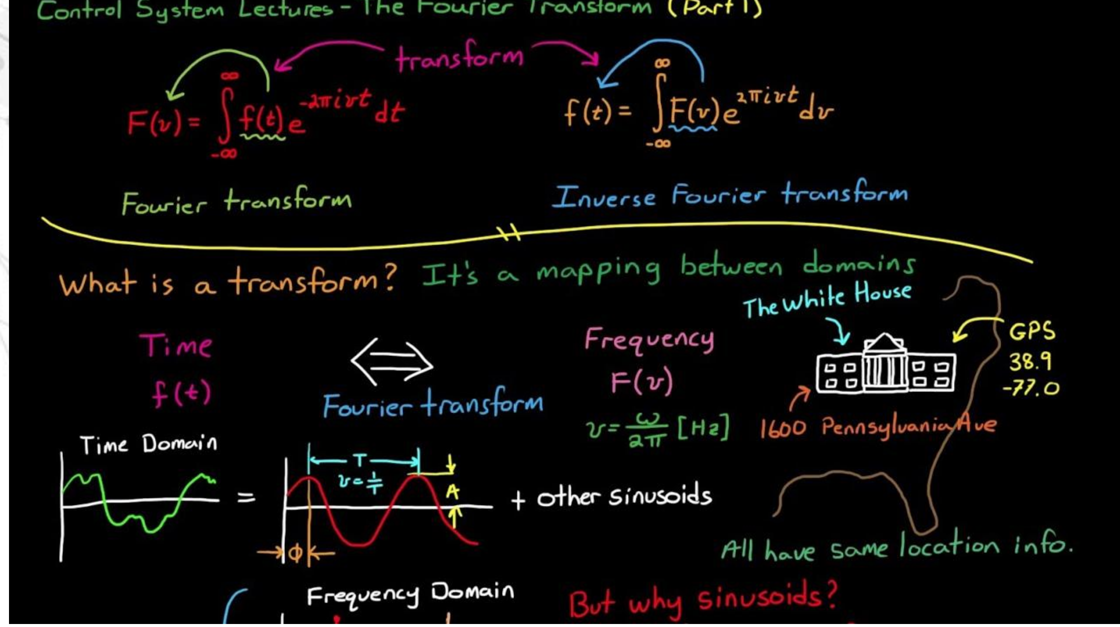
Dr. Imre Sándor , Dr. Bacsárdi László

BME Hálózati Rendszerek és Szolgáltatások Tanszék

imre@hit.bme.hu

Budapest,
2025. 11. 04.

MAI PROGRAM – MOUNT EVEREST OXIGÉNPALACKKAL

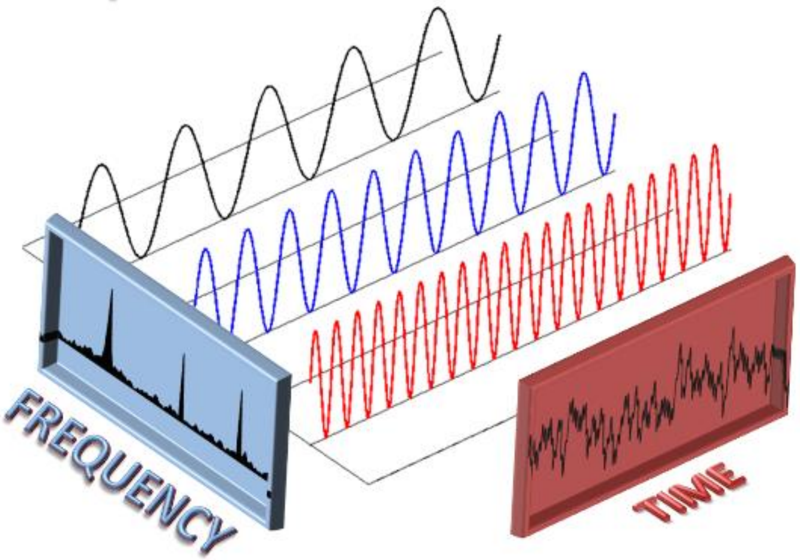


KVANTUM FOURIER-TRANSZFORMÁCIÓ

Avagy hogyan építhető fel egy bonyolult unitér transzformáció elemi kapukból

Indulás az 1. táborból – 6100m

FOURIER Jean Baptiste Joseph (1768-1830)



KLASSZIKUS ⟶ KVANTUM

- Klasszikus Diszkrét Fourier-Transzformáció (DFT)

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

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

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

- Kvantumos Diszkrét Fourier Transzformáció (QFT)

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

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

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

Exercise 6.1. Prove that operator F is unitary!

Exercise 6.2. Determine the matrix of QFT!

DEFINITIONS

- Klasszikus bázisállapotokra

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

- Tetszőleges szuperpozícióra

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

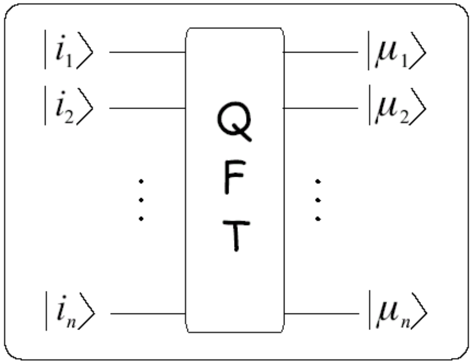
- Inverz Fourier-Transzformáció (IQFT)

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

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

HOGYAN IMPLEMENTÁLJUK A QFT-T?

- A cél: egy hatékony, QFT-t megvalósító áramkör megtalálása, amely elemi kvantumkapukból épül fel.
- A módszer: elkészítjük a QFT egy ekvivalens tenzorszorzat-reprezentációját, amely külön-külön megmondja, hogy mit tegyünk az egyes kvantumhuzalokkal.



- Egész és valós számok bináris ábrázolása:

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

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

HOGYAN IMPLEMENTÁLJUK A QFT-T?

- Most az eredeti definícióból kezdjük az újrafogalmazást/felírást:

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

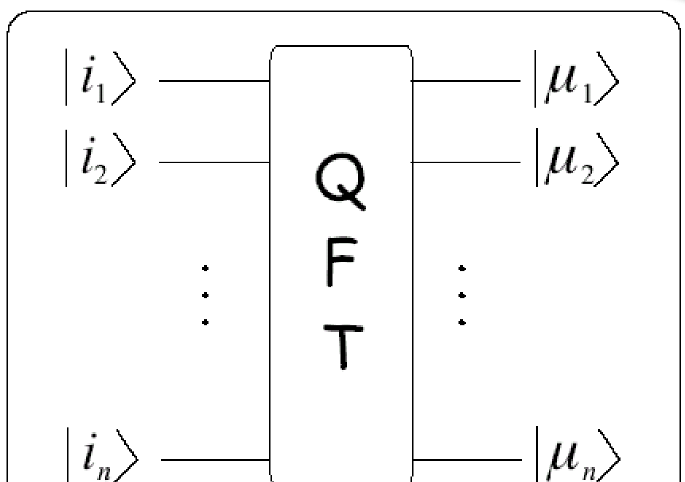
Recognizing that $\frac{2^{n-l}}{2^n} = 2^{-l}$ furthermore exploiting that $|k\rangle = |k_1, k_2, .., k_n\rangle = |k_1\rangle \otimes |k_2\rangle \otimes ... \otimes |k_n\rangle$ and $e^{\alpha+\beta} \equiv e^{\alpha}e^{\beta}$

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

HOGYAN IMPLEMENTÁLJUK A QFT-T?

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

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

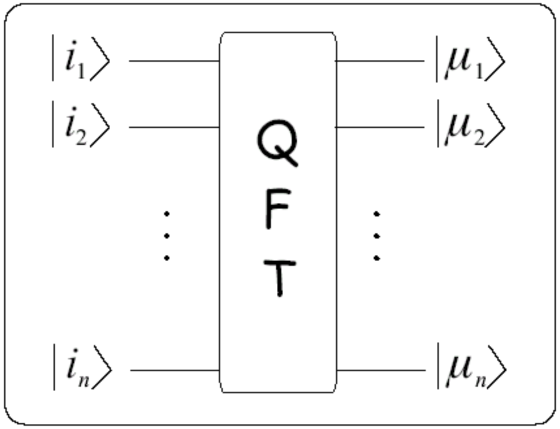


HOGYAN IMPLEMENTÁLJUK A QFT-T?

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

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

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

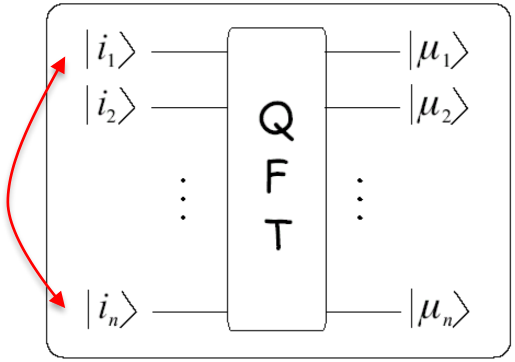


$$F|i\rangle = \underbrace{\left(\frac{|0\rangle + e^{j2\pi 0.i_n}|1\rangle}{\sqrt{2}}\right)}_{|\mu_1\rangle} \otimes \underbrace{\left(\frac{|0\rangle + e^{j2\pi 0.i_{n-1}i_n}|1\rangle}{\sqrt{2}}\right)}_{|\mu_2\rangle} \otimes \ldots \otimes \underbrace{\left(\frac{|0\rangle + e^{j2\pi 0.i_1 i_2 \ldots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

HOGYAN IMPLEMENTÁLJUK A QFT-T?

- Most már a kezünkben van a tenzorszorzat reprezentációja. A könnyebb megvalósítás érdekében egy SWAP kaput alkalmazunk a QFT áramkör kimenetén, ezért a következők érdekelnek minket:

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



- Elsőként vizsgáljuk meg: U_n.

$$i_n = 0, 1$$

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

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

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

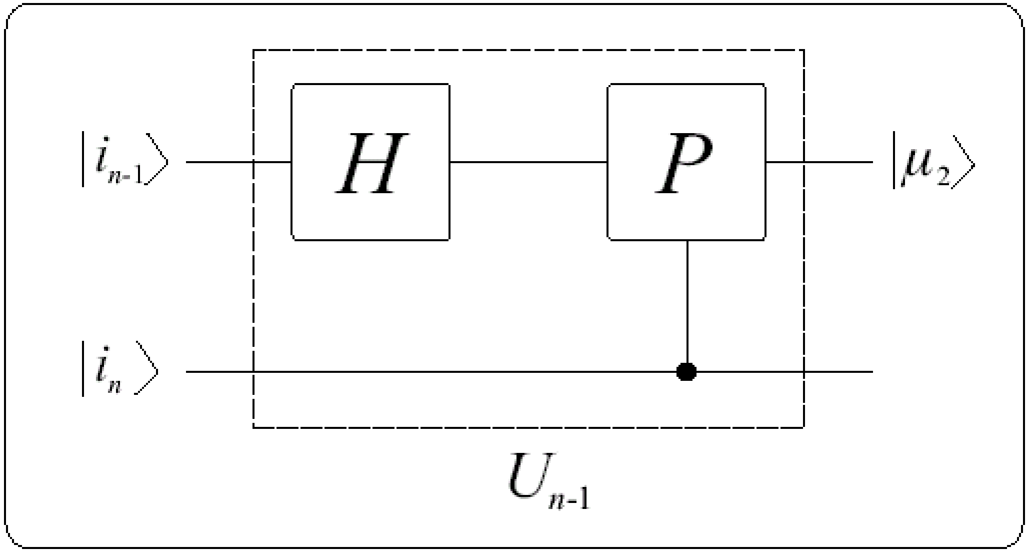
$$\boxed{U_n = H}$$

HOGYAN IMPLEMENTÁLJUK A QFT-T?

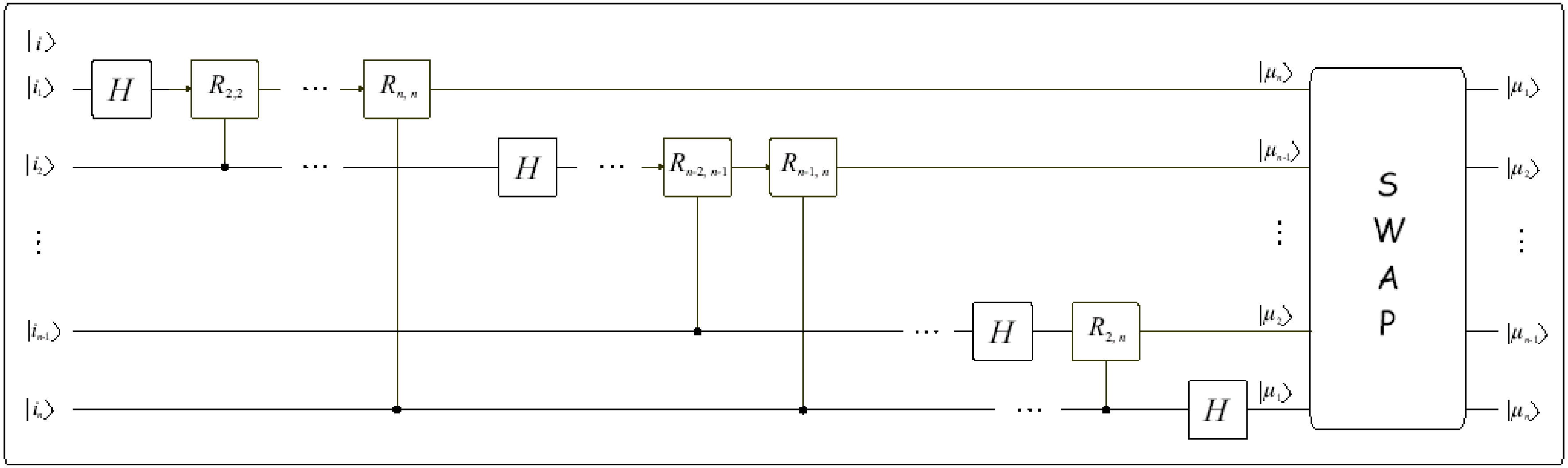
- Ezután: $U_{n-1} : |i_{n-1}\rangle \rightarrow |\mu_2\rangle$

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

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



HOGYAN IMPLEMENTÁLJUK A QFT-T?



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

- Megjegyzések
  - Komplexitás: $O(n^2)$
  - A QFT nem a Fourier-együtthatók gyorsabb kiszámítására szolgál, mivel azokat valószínűségi amplitúdók képviselik!

KVANTUMUS FÁZISBECSLÉS

Indulás az 2. táborból – 6400m

A PROBLEMA

- Minden sajátvektorral rendelkező unitér U transzformáció $e^{j\alpha_u}$ sajátértékei a következő formában vannak.

$|u\rangle$

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

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

IDEÁLIS ESET

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

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

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

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

IQFT → i

Decomposition of QFT

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

IDEÁLIS ESET

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

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

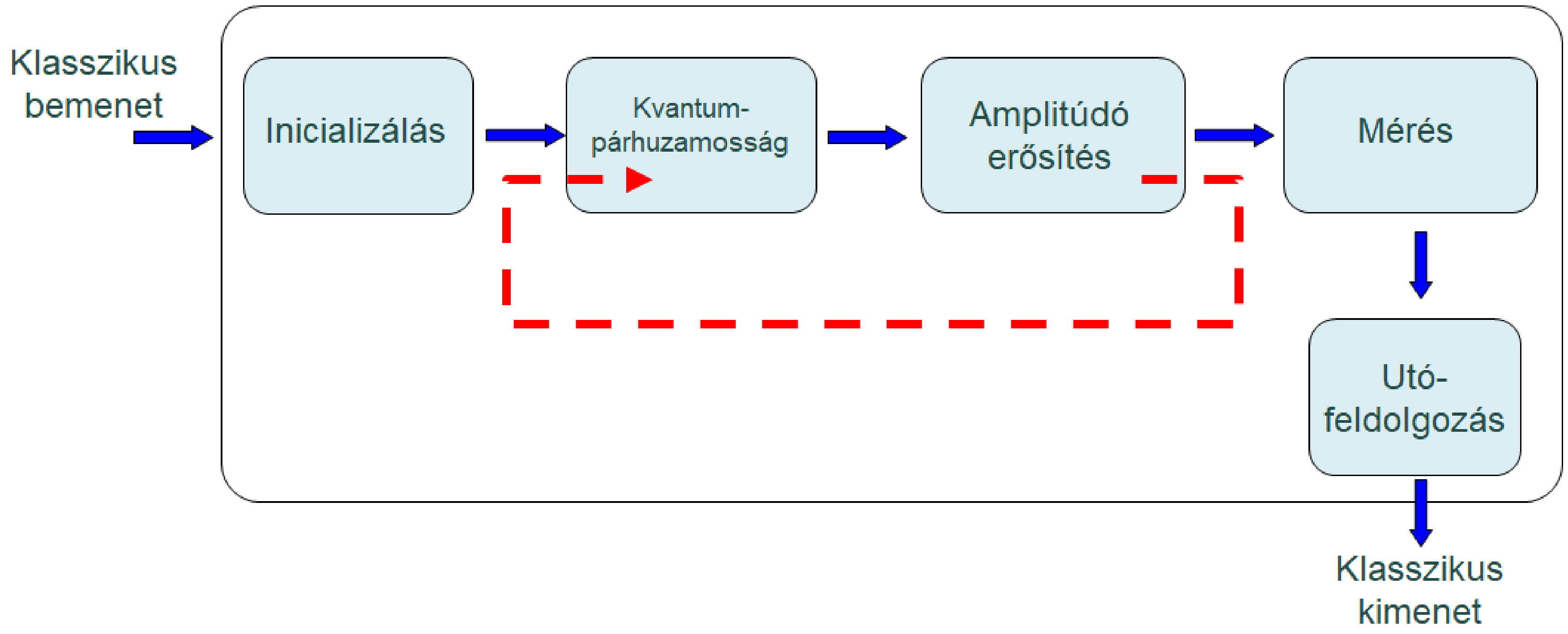
$$U^h \triangleq \underbrace{UU\ldots U}_{h},$$

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

sajátérték

sajátvektor

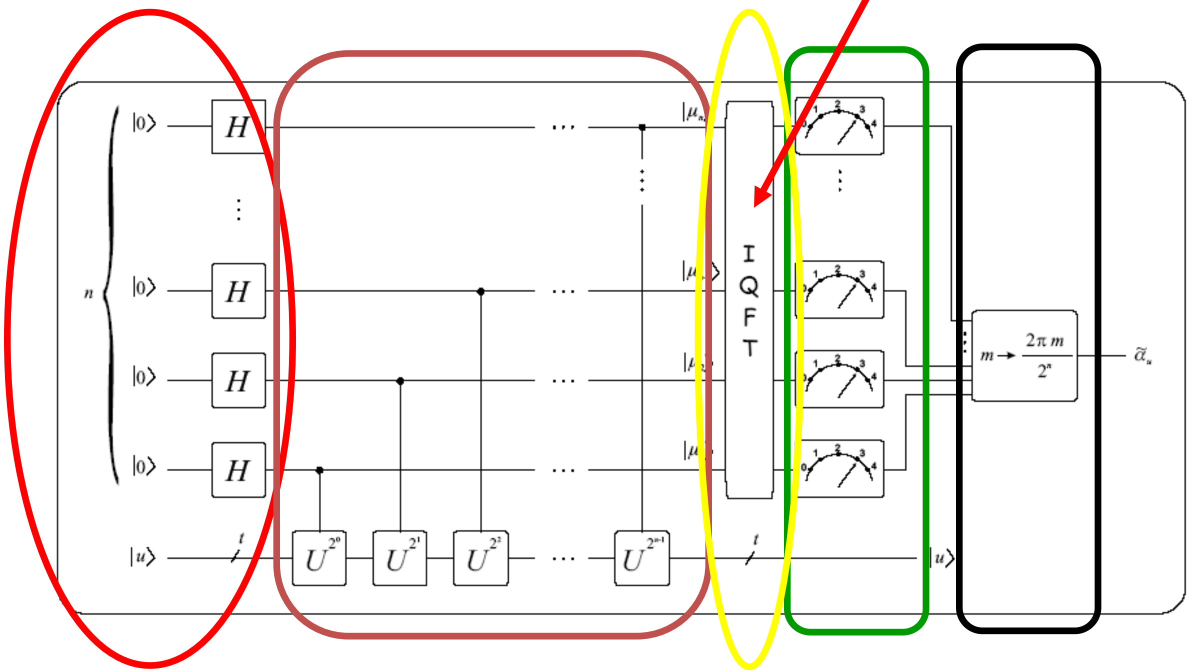
KVANTUMALGORITMUSOK TERVEZÉSI RECEPTJE

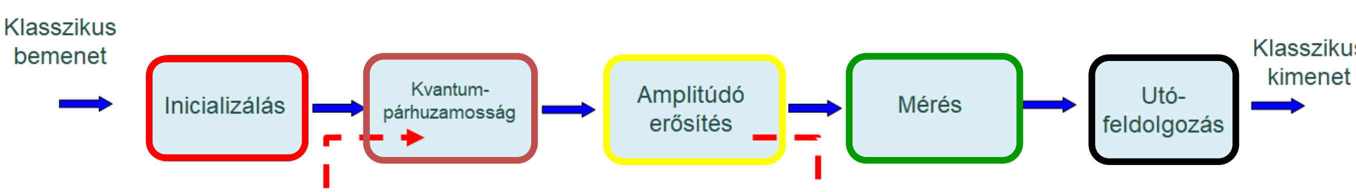


QUANTUM PHASE ESTIMATOR

- How to initialize $|u\rangle$?

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





GYAKORLATI ESET

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

- IQFT will not work correctly!

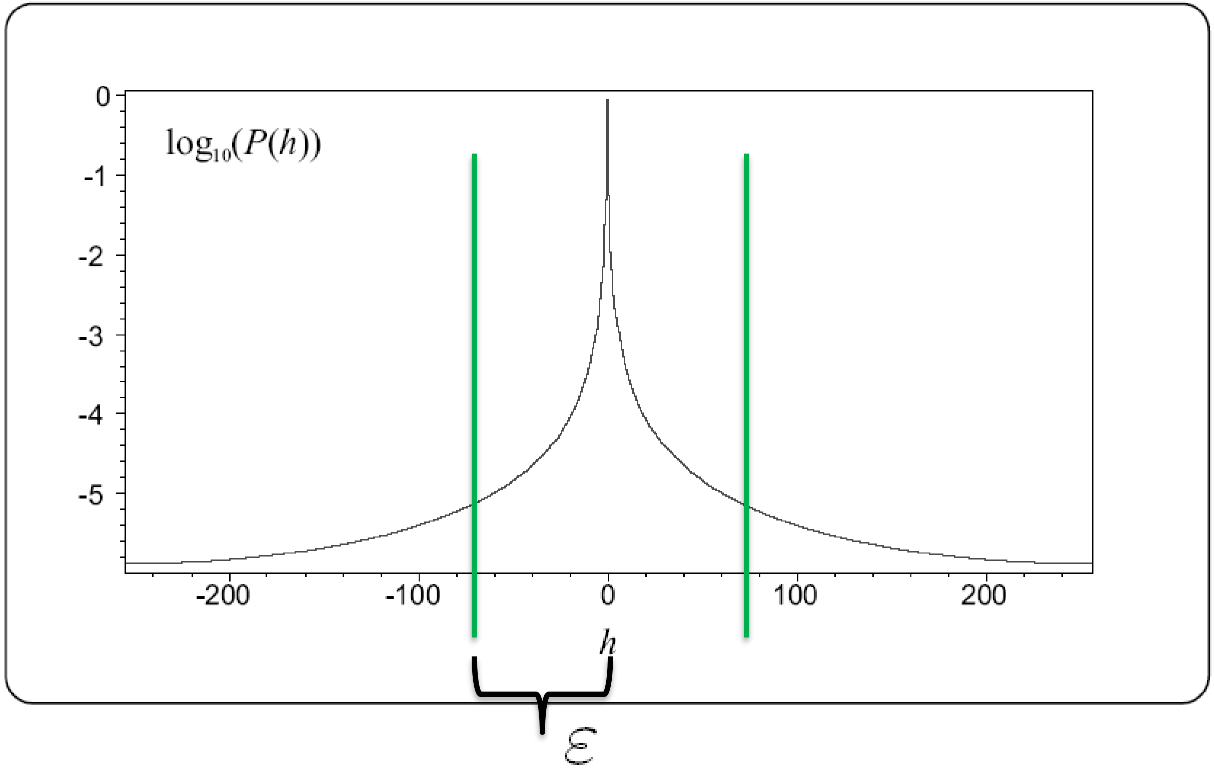
IQFT

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

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

$\varphi_i \cancel{=} 1$

VALÓSZÍNŰSÉGI AMPLITÚDÓK



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

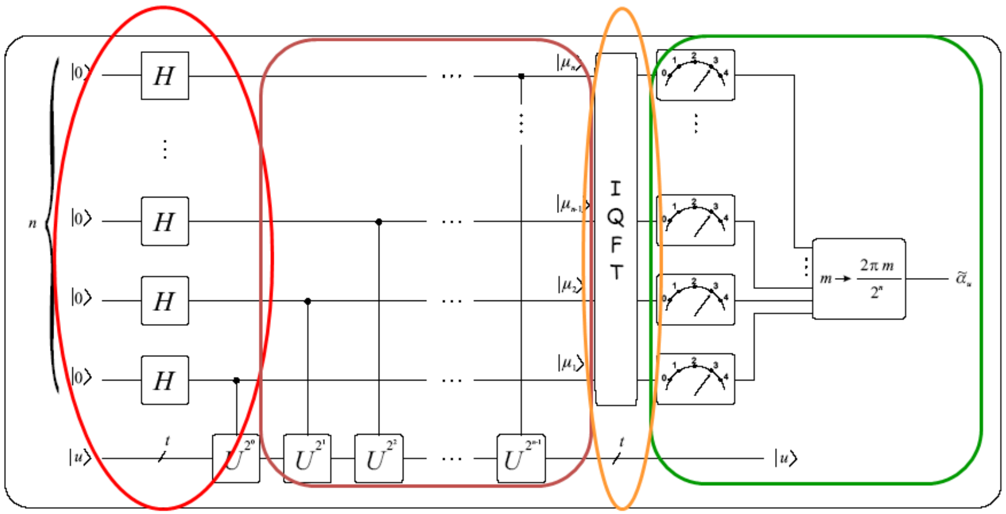
$$P_s = \frac{1}{2^{2c-2}}\frac{\sin^2(\pi 2^{c-1}2^{-c})}{\sin^2(\pi 2^{-c})} = \frac{4}{2^{2c}}\frac{\sin^2(\pi/2)}{\sin^2(\pi 2^{-c})} = \frac{4}{2^{2c}\sin^2(\pi 2^{-c})}$$

HIBAANALÍZIS

$$n = c - 1 + p$$

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

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

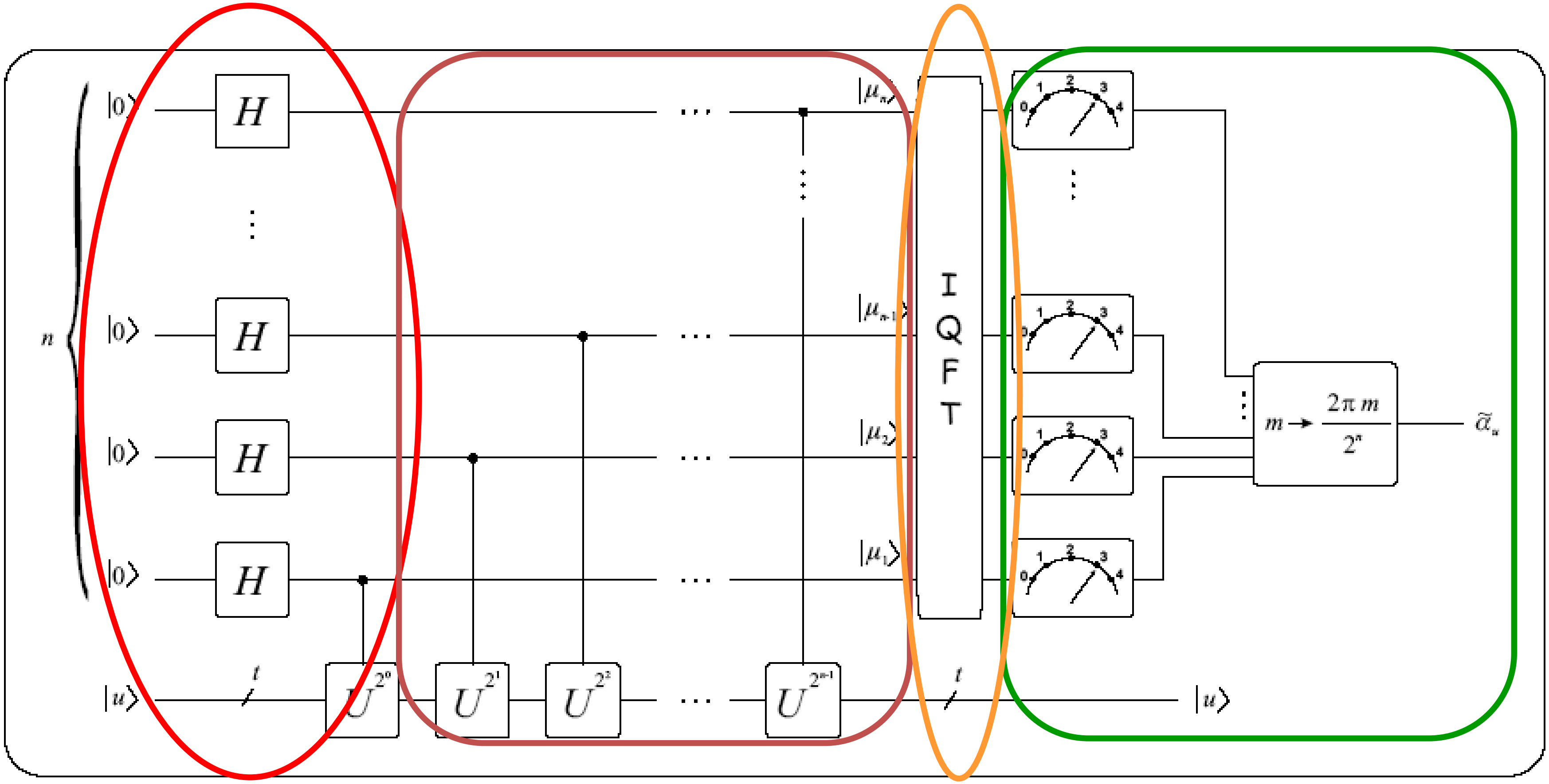


$$n = c - 1 + \left\lceil \mathrm{ld}\left(3 + \frac{1}{\breve{P}_\varepsilon}\right) \right\rceil$$

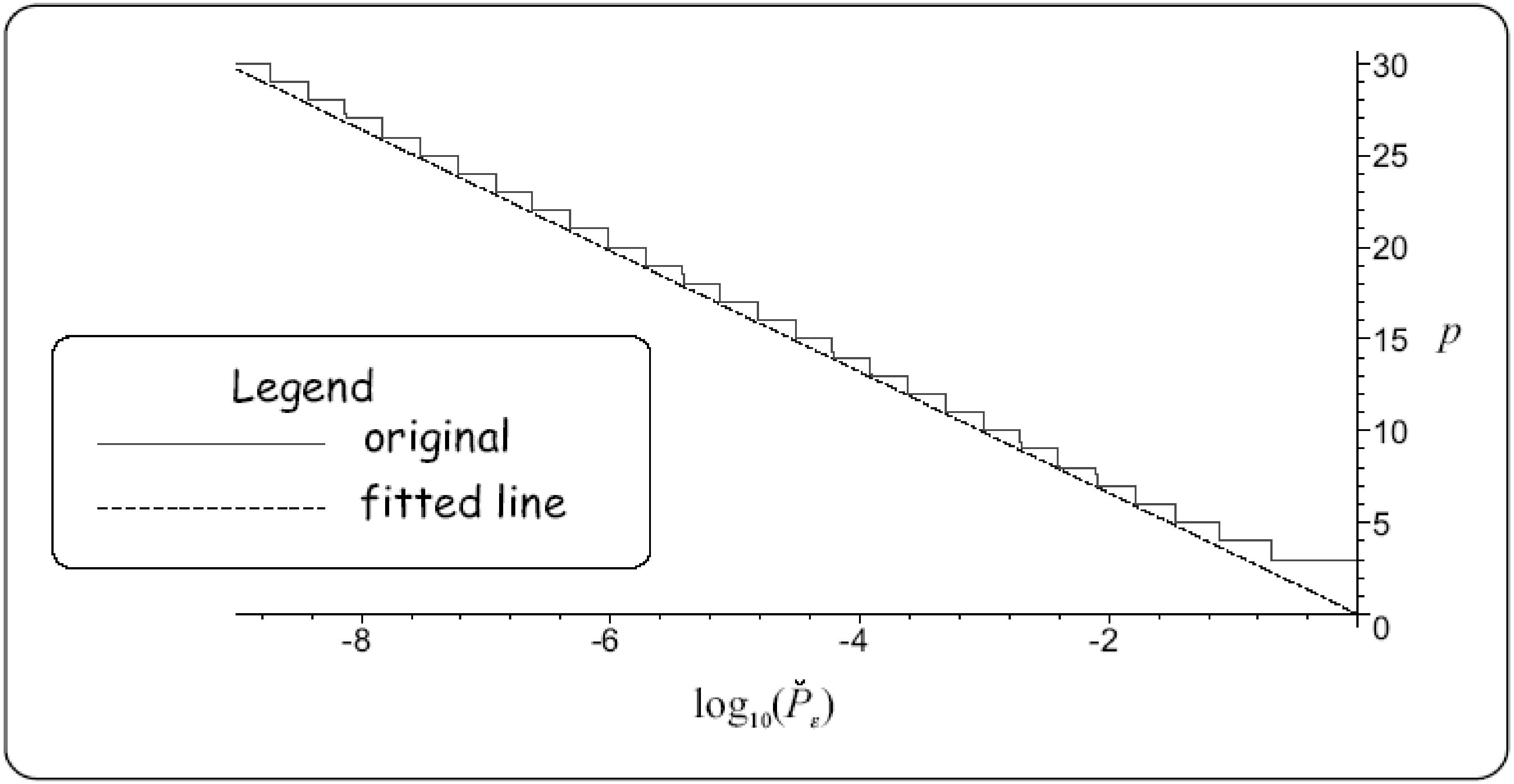
$$n = c - 1 + \left\lceil \mathrm{ld}(2\pi) + \mathrm{ld}\left(3 + \frac{1}{\breve{P}_\varepsilon}\right) \right\rceil$$

HÁLÓZATI RENDSZEREK
ÉS SZOLGÁLTATÁSOK
TANSZÉK
www.hit.bme.hu

KVANTUMOS FÁZISBECSLŐ



HIBAANALÍZIS

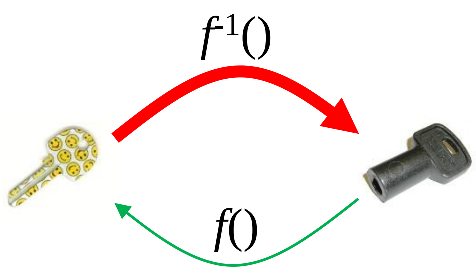


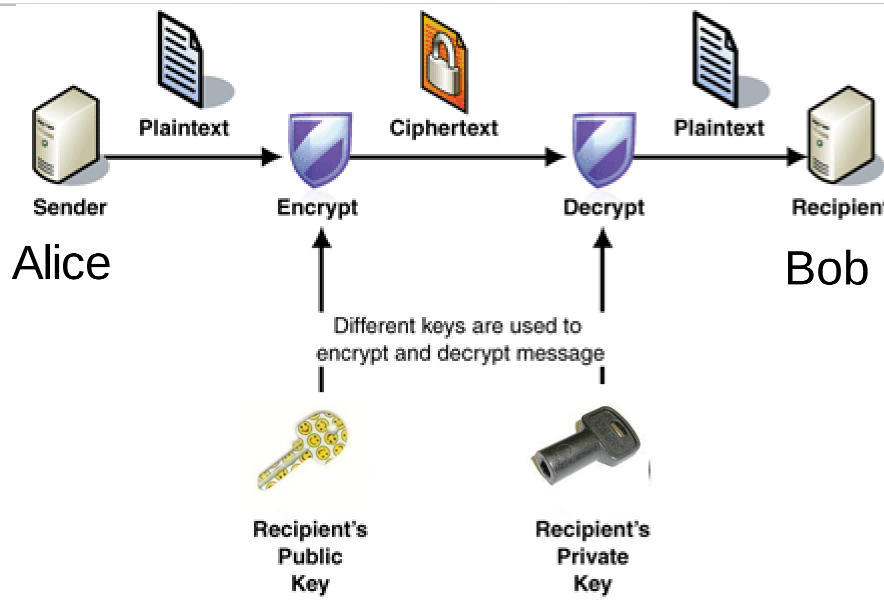
- Complexity in elementary gates: $\boxed{O(n^3)}$

AZ RSA ALGORITMUS

Indulás az 3. táborból – 7200m

NYÍLVÁNOS KULCSÚ TITKOSÍTÁS



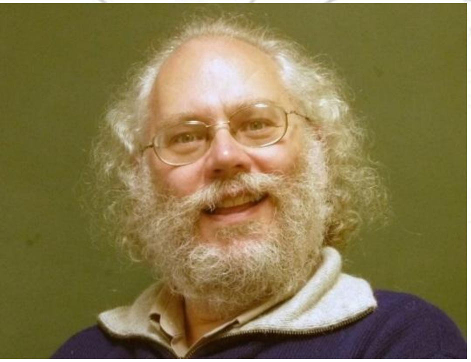


- Nyílvános kulcsú titkosítás
  - nyilvános titkosítókulcs, titkos fejtőkulcs
  - kulcsok előállítása: két nagy prímszám szorzatát felhasználva
  - feltörés: a törzstényezők meghatározása
- A mai napig nem sikerült bebizonyítani, hogy nincs hatékony algoritmus a feltörésre. Mindenesetre eddig nem sikerült ilyen klasszikus algoritmust találni.
- **De kvantumosat IGEN!**

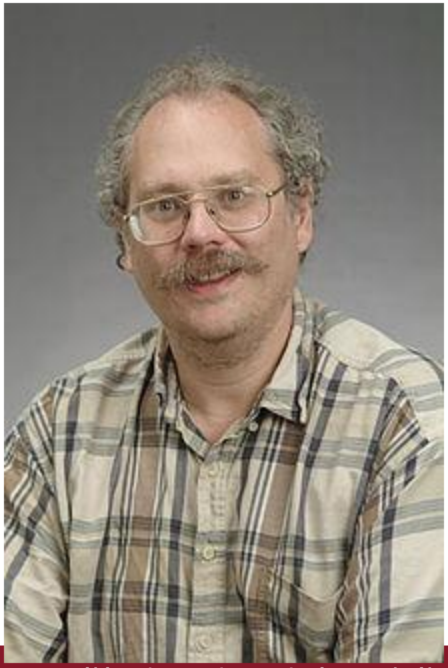
1. Bob selects randomly two large prime numbers p and q such that $p \neq q$.
2. He calculates $N = p \cdot q$.
3. Bob selects randomly a small odd number a such that $\gcd(\varphi(N), a) = 1$, where $\varphi(N)$ denotes the corresponding Euler function (see Section 12.3.2). Since N is a product of two 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

$$E = e(P, K_B) = (P^a) \bmod N,$$
$$P = d(E, L_B) = (E^b) \bmod N. \qquad (9.10)$$



Peter Shor (1959-)



RENDKERESÉS– SHOR ALGORITMUS

Indulás az 4. táborból – 7950m
Csúcstámadás!

FAKTORIZÁLÁS ÉS RENDKERESÉS KAPCSOLATA

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

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

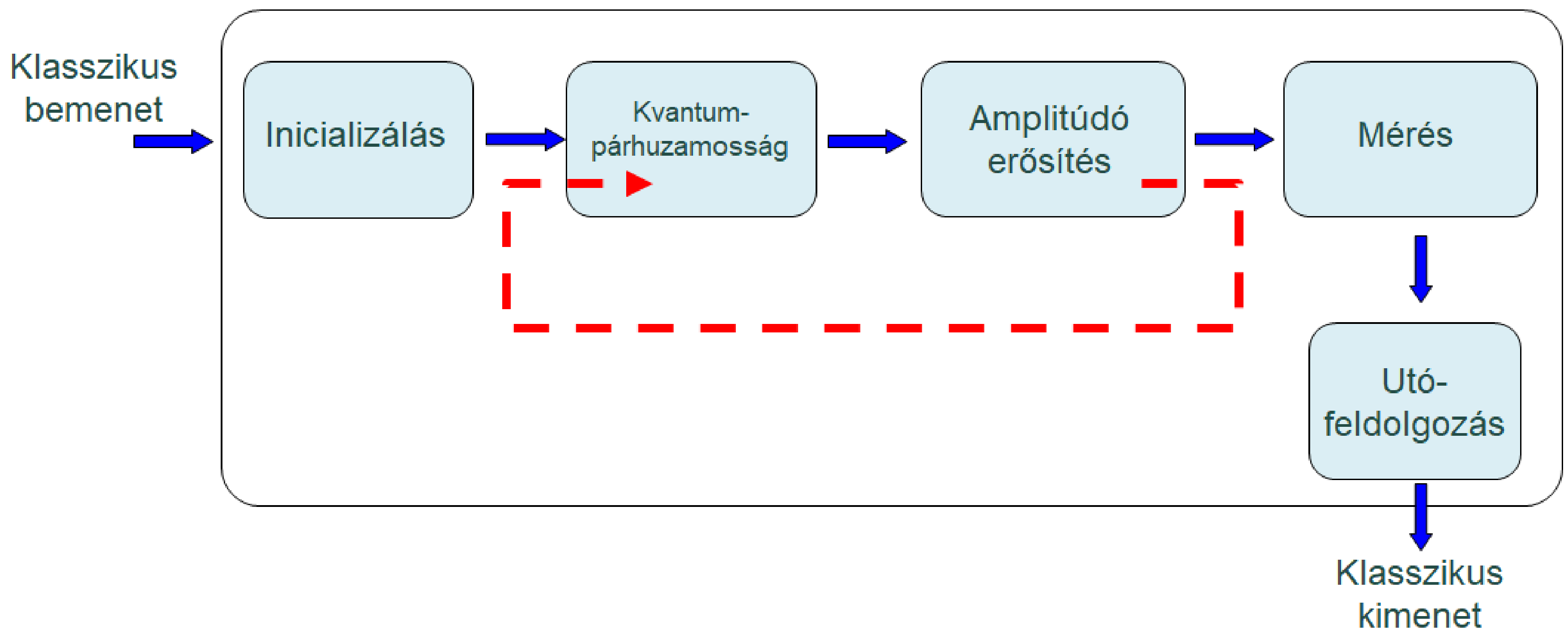
FAKTORIZÁLJUK A 66-OT!

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 $r : x^r \bmod N = 1$

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

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 $3 \cdot 11 = 33$.

KVANTUMALGORITMUSOK TERVEZÉSI RECEPTJE



FAKTORIZÁLÁS ÉS RENDKERESÉS KAPCSOLATA

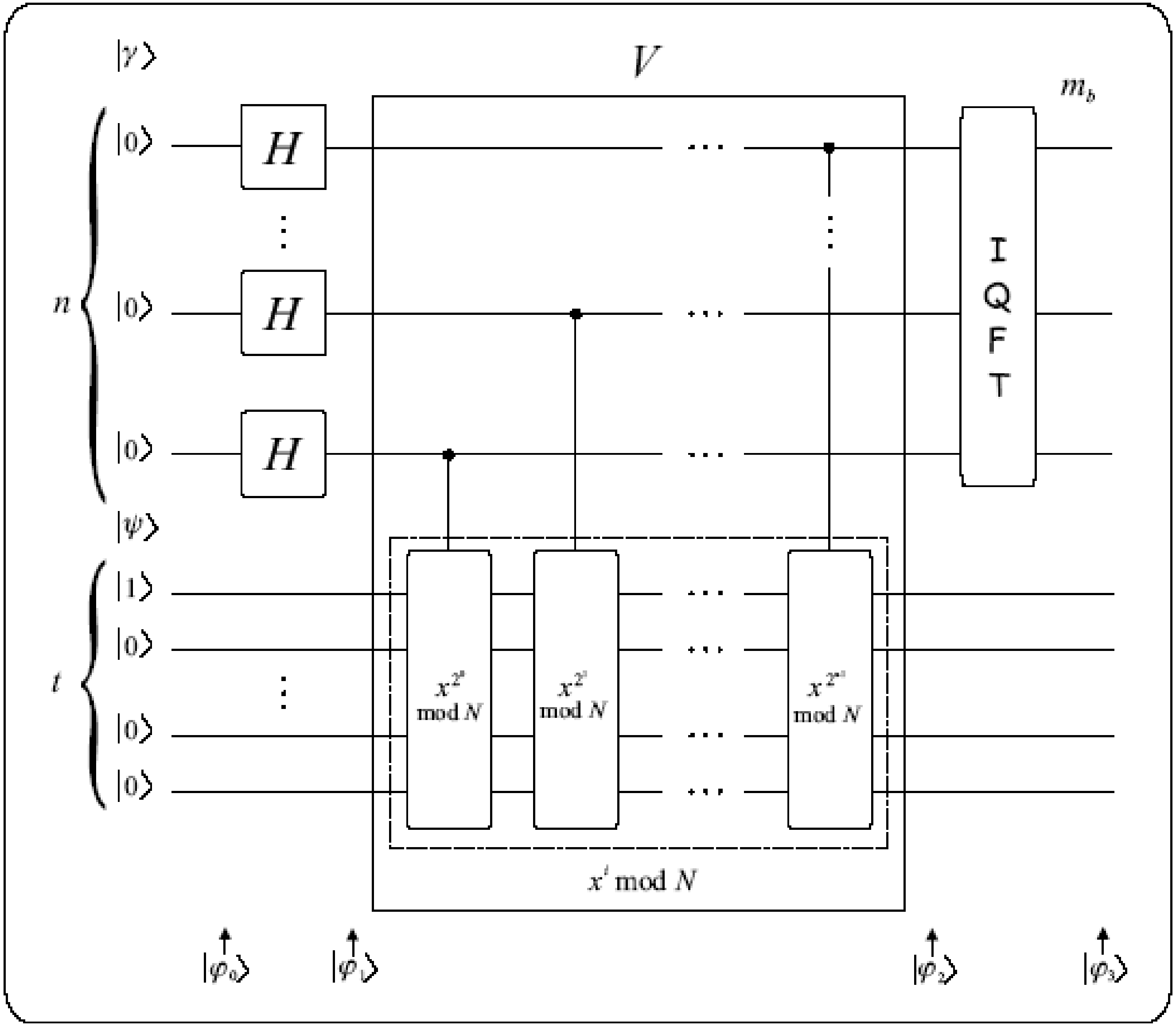
$$|\varphi_2\rangle = \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} |k\rangle |x^k \bmod N\rangle$$

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

$$= \left(x^{k_1 2^{n-1}} \bmod N \right) \left(x^{k_2 2^{n-2}} \bmod N \right) \dots \left(x^{k_n 2^0} \bmod N \right)$$

- *U* sajátértékei és vektorai: $U : |q\rangle \rightarrow |(qx) \bmod N\rangle$

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


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

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

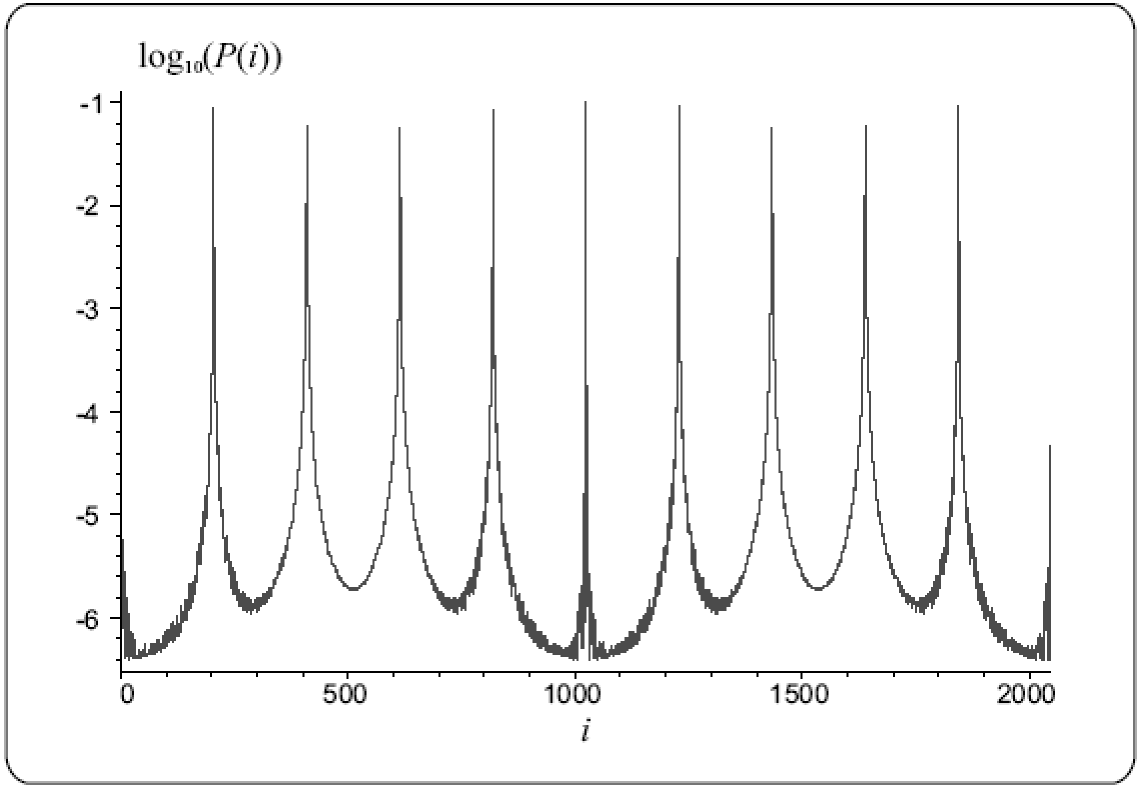


Fig. 6.16 $\log_{10}(P(i))$ assuming $n = 11, N = 33, x = 5, r = 10$

Theorem 12.1. *If* $m_b/2^n$ *is a rational fraction and* b *and* r *are positive integers that satisfy*

$$\left|\frac{b}{r} - \frac{m_b}{2^n}\right| \leq \frac{1}{2r^2}$$

then b/r *is a convergent of the continued fraction of* $\frac{m_b}{2^n}$.

LÁNCTÖRTEK (CONTINUED FRACTION)

If a and b are integers then a/b is called the *rational fraction* or *rational number*. *Continued fraction* representation of a rational fraction can be derived from Euclid's algorithm.

$$\begin{aligned}
a &= q_1 b + r_1 && \Rightarrow \quad \frac{a}{b} = q_1 + \frac{1}{\frac{b}{r_1}} \\
b &= q_2 r_1 + r_2 && \Rightarrow \quad \frac{b}{r_1} = q_2 + \frac{1}{\frac{r_1}{r_2}} \\
&\vdots && \Rightarrow \quad \vdots \\
r_k &= q_{k+2} r_{k+1} + r_{k+2} && \Rightarrow \quad \frac{r_k}{r_{k+1}} = q_{k+2} + \frac{1}{\frac{r_{k+1}}{r_{k+2}}} \\
&\vdots && \Rightarrow \quad \vdots \\
r_{l-2} &= q_l r_{l-1} && \Rightarrow \quad \frac{r_{l-2}}{r_{l-1}} = q_l .
\end{aligned}$$

LÁNCTÖRTEK ÉS KONVERGENSEK

Thus using the right-hand side equivalences we can describe $\frac{a}{b}$ as

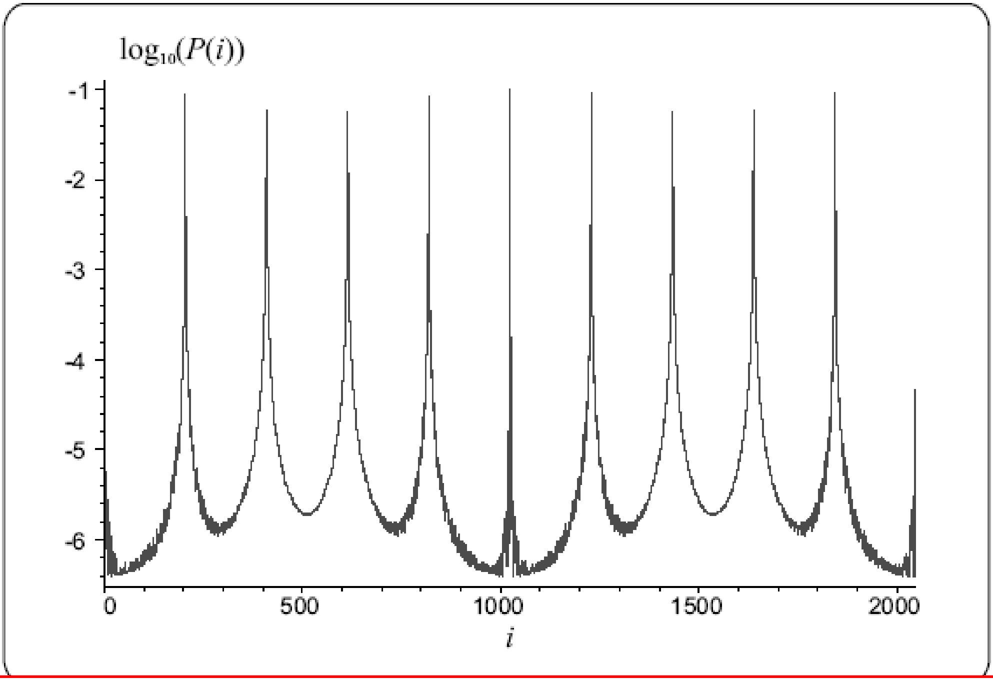
$$\frac{a}{b} = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \cdots + \cfrac{1}{q_l}}}.$$

Convergents of rational number $\frac{a}{b}$ are the following rational fractions

$$\zeta_1 = q_1, \quad \zeta_2 = q_1 + \frac{1}{q_2}, \quad \zeta_3 = q_1 + \frac{1}{q_2 + \frac{1}{q_3}}, \quad \ldots, \quad \zeta_l = \frac{a}{b}.$$

VISSZA A PÉLDÁHOZ

Peaks can be observed at $0, 205, 410, 614, 819, 1024, 1229, 1434, 1638, 1843$ which are the closest integers to $b2^n/r$ with periodicity $\approx 2^n/r = 205$. Related peak probability values are $0.1, 0.0875, 0.0573, 0.0573, 0.08753, 0.1, 0.08753, 0.0573, 0.0573, 0.08753$.



The probability of measuring one of them is 0.779.

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

- A hibavalószínűség kontrollálása:

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

- Példánk esetében:

Let us assume $m_b = 614$. The corresponding convergents are: $\frac{1}{3}, \frac{2}{7}, \frac{3}{10}, \frac{152}{507}, \frac{307}{1024}$. Among them $\frac{3}{10}$ is the closest one to $\frac{614}{2048}$ with denominator less than N. Therefore we check $5^{10} \bmod 33$ which equals 1 thus we managed to find r.

a ***r*** ***N***

USING SHOR’S ORDER FINDING ALGORITHM TO BREAK RSA

Hillary-lépcső – 8790m

AZ RSA MŰKÖDÉSE

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

$$E = e(P, K_B) = (P^a) \bmod N,$$
$$P = d(E, L_B) = (E^b) \bmod N. \qquad (9.10)$$

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

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

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 $O(\mathrm{ld}(N)^3)$.

$\longleftarrow$ Brutális!

FELÉRTÜNK A CSÚCSRA! - 8850M

REVELATIONS!

A QFT MINT ÁLTALÁNOSÍTOTT HADAMARD TRANSZFORMÁCIÓ

- Hadamard:

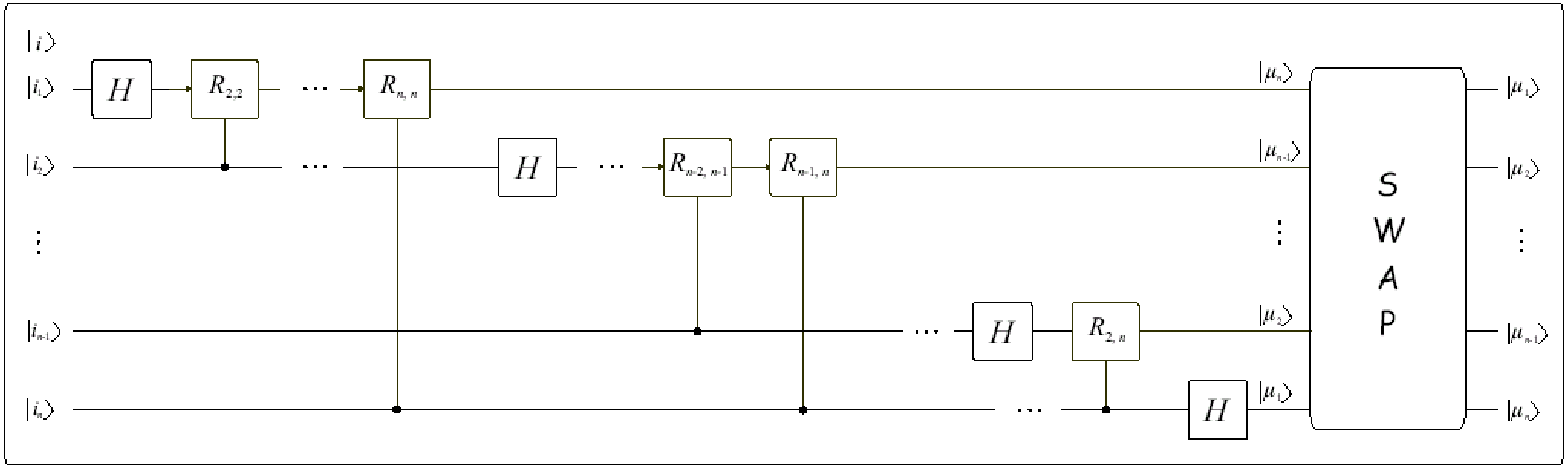
$$H^{\otimes 1}|i\rangle = \frac{1}{\sqrt{2^1}} \sum_{k\in\{0,1\}^1} (-1)^{ik}|k\rangle = \frac{1}{\sqrt{2}} \sum_{k=0}^{1} (-1)^{ik}|k\rangle$$

$$-1 = e^{j2\pi\frac{1}{2}} \Rightarrow H|i\rangle = \frac{1}{\sqrt{2}} \sum_{k=0}^{1} e^{j2\pi\frac{ik}{2}}|k\rangle$$

- QFT:

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

- A *H* kapuk $(\mathbb{Z}_2)^n = \mathbb{Z}_{N=2^n}$ Fourier-trafók. Néhány *R* kapuval kiegészítve $\mathbb{Z}_N$ feletti Fourier-trafók lesznek ☺



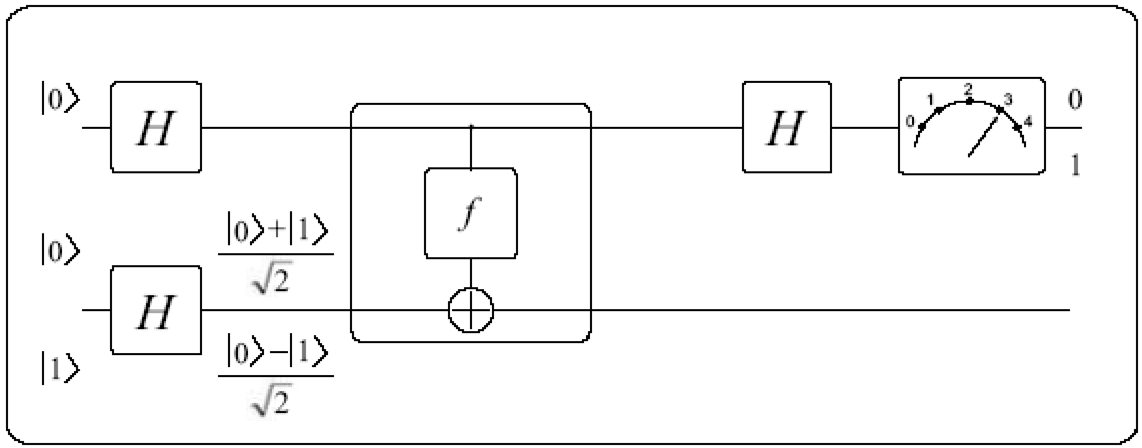
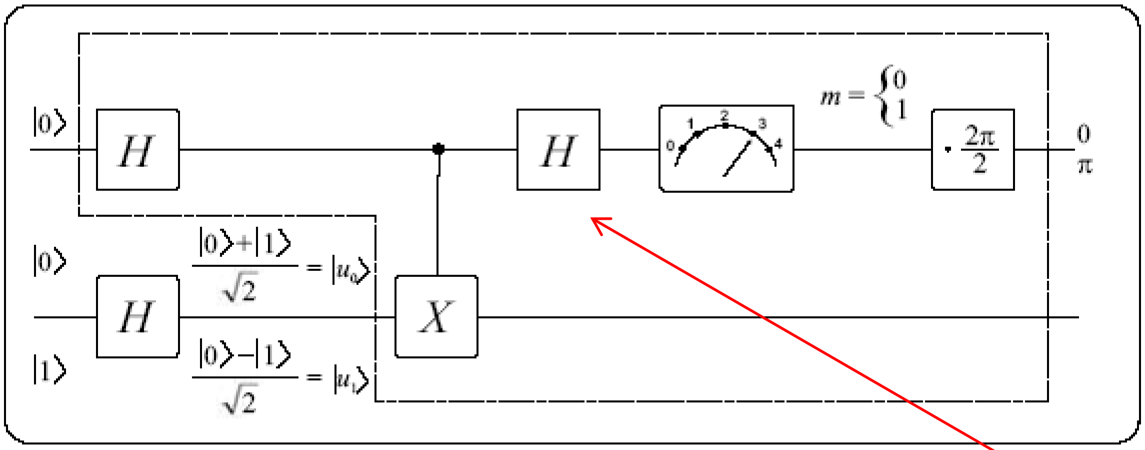
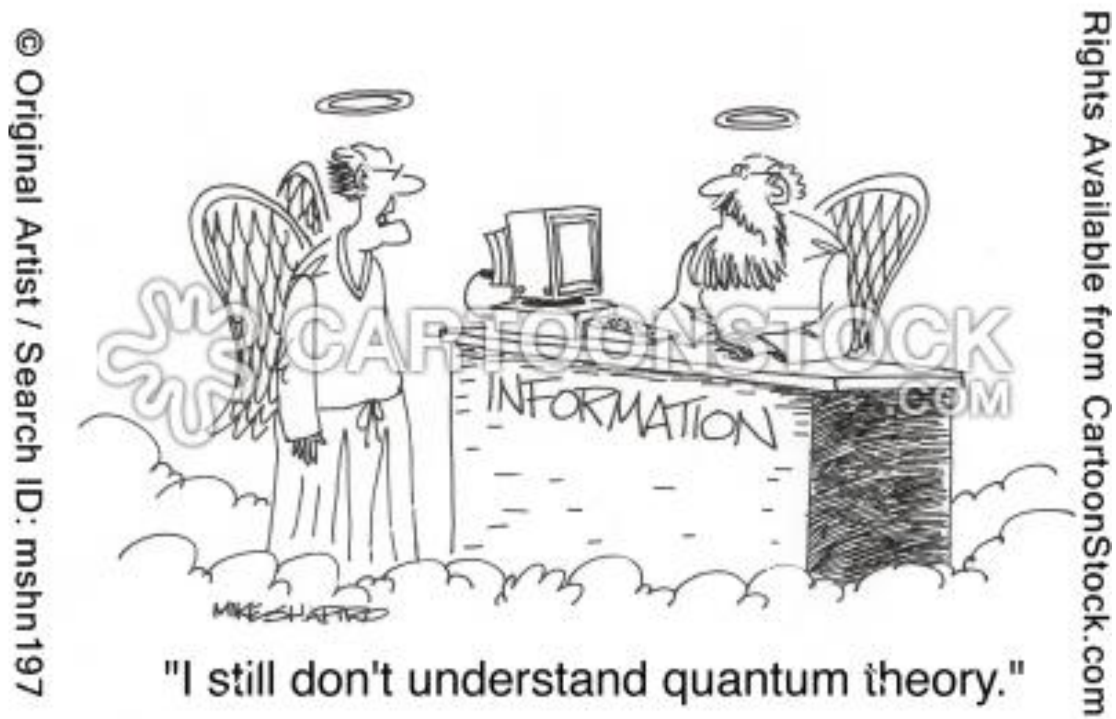


Fig. 6.17 Deutsch–Jozsa circuit as a decision maker whether f is constant or varying



IQFT ☺

Fig. 6.18 Deutsch–Jozsa circuit as a simple phase estimator


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