THE UNIVERSITY of EDINBURGH
informatics

Introduction to Quantum Computing

Lecture 19: Quantum Phase Estimation

Raul Garcia-Patron Sanchez

THE UNIVERSITY of EDINBURGH
informatics

Recap Fourier Transform

Quantum Fourier Transform over $\mathbb{Z}_{2^n}$

Binary representation of integers: $z \equiv z_1 z_2 .... z_n$

$$z = z_1 2^{n-1} + z_2 2^{n-2} + ... + z_{n-l} 2^l + z_{n-l+1} 2^{l-1} + ... + z_{n-1} 2 + z_n$$

Binary fraction: $0.w_1 ....w_m = \frac{w_1}{2} + ... + \frac{w_m}{2^m}$

- Encode $\varphi \in [0, 1[$ into a phase $e^{2\pi i \varphi}$

$$\frac{z}{2^l} = z_1 2^{n-1-l} + ... + z_{n-l} + \frac{z_{n-l+1}}{2} + ... + \frac{z_n}{2^l}$$

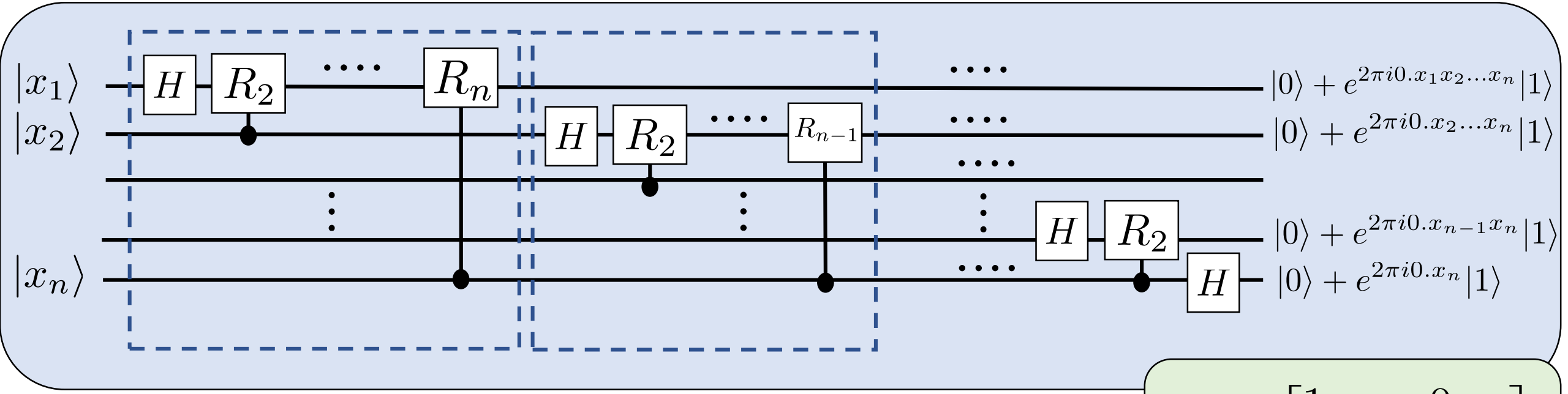
$$e^{2\pi i z 2^{-l}} = e^{2\pi i (z_1 2^{n-l-1} + z_2 2^{n-l-2} + ... + z_{n-l})} e^{2\pi i 0.z_{n-l+1} z_{n-l+2} ... z_n} = e^{2\pi i 0.z_{n-l+1} z_{n-l+2} ... x_n}$$

$$\varphi = 0.w_1 ....w_m$$

$$e^{2\pi i 2\varphi} = e^{2\pi i (2 \cdot 0.w_1 w_2 ....w_m)} = e^{2\pi i (w_1 + 0.w_2 ....w_m)} = e^{2\pi i 0.w_2 ....w_m}$$

Quantum Fourier Transform over $\mathbb{Z}_{2^n}$

$$|x_1, x_2, ..., x_{n-1}, x_n\rangle \rightarrow \frac{1}{2^{n/2}}(|0\rangle + e^{2\pi i 0.x_n}|1\rangle)...(|0\rangle + e^{2\pi i 0.x_2...x_n}|1\rangle)(|0\rangle + e^{2\pi i 0.x_1 x_2...x_n}|1\rangle)$$



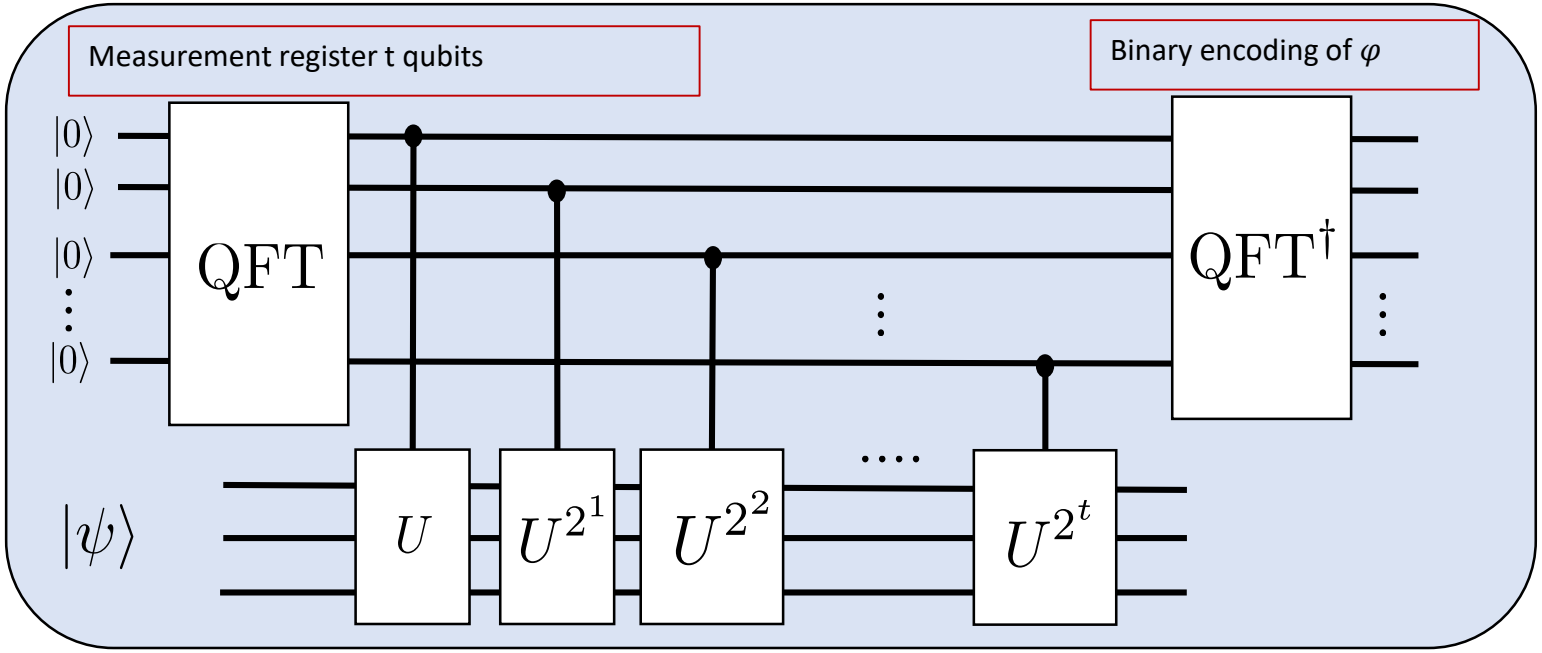
$$R_k = \begin{bmatrix} 1 & 0 \\ 0 & e^{i2\pi/2^k} \end{bmatrix}$$

- QFT up to a reverse of the order of qubits.
- Unitary as composed of unitary gates.
- $n + (n-1) + ... + 1 = n(n+1)/2$ gates are required
  $+n/2$ SWAP gates (3 CNOT)

$\Theta(n^2)$ gates

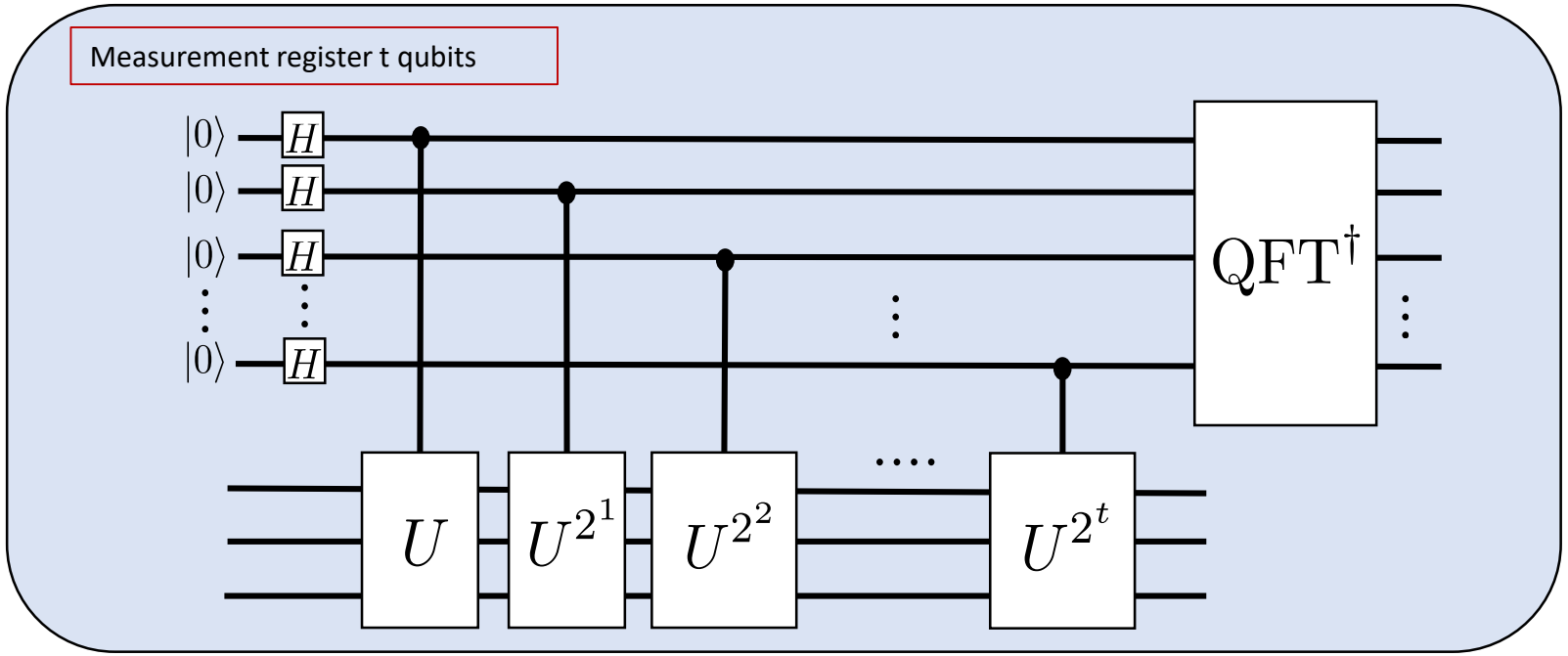
Quantum phase estimation

Quantum phase estimation: applications



- Factoring: Shor's algorithm
- Quantum counting = Grover + Quantum phase estimation
- Quantum chemistry and many-body physics: energies estimation
- Quantum Metropolis Sampling

Quantum phase estimation: applications



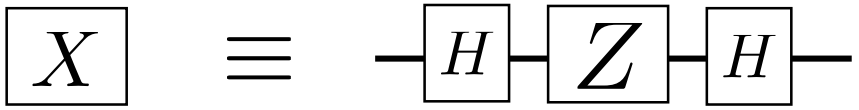
- Factoring: Shor's algorithm
- Quantum counting = Grover + Quantum phase estimation
- Quantum chemistry and many-body physics: energies estimation
- Quantum Metropolis Sampling

The eigenspace and eigenvalues of unitary matrices

Spectral theorem Unitary $U : UU^\dagger = U^\dagger U = I$

$$\exists V : VUV^\dagger = D = \mathrm{diag}(e^{2\pi i\varphi_1}, ..., e^{2\pi i\varphi_N})$$

- N eigenvalues in the unit circle: $\lambda_i = e^{2\pi i\varphi_i}$
- $U = \sum_{i=1}^{N} e^{2\pi i\varphi_i} |u_i\rangle\langle u_i|$, and $V = \sum_{i=1}^{N} |i\rangle\langle u_i|$



The eigenspace and eigenvalues of unitary matrices

Spectral theorem

Unitary $U : UU^\dagger = U^\dagger U = I$

$$\exists V : VUV^\dagger = D = \mathrm{diag}(e^{2\pi i\varphi_1}, ..., e^{2\pi i\varphi_N})$$

- N eigenvalues in the unit circle: $\lambda_i = e^{2\pi i\varphi_i}$
- $U = \sum_{i=1}^{N} e^{2\pi i\varphi_i} |u_i\rangle\langle u_i|$, and $V = \sum_{i=1}^{N} |i\rangle\langle u_i|$

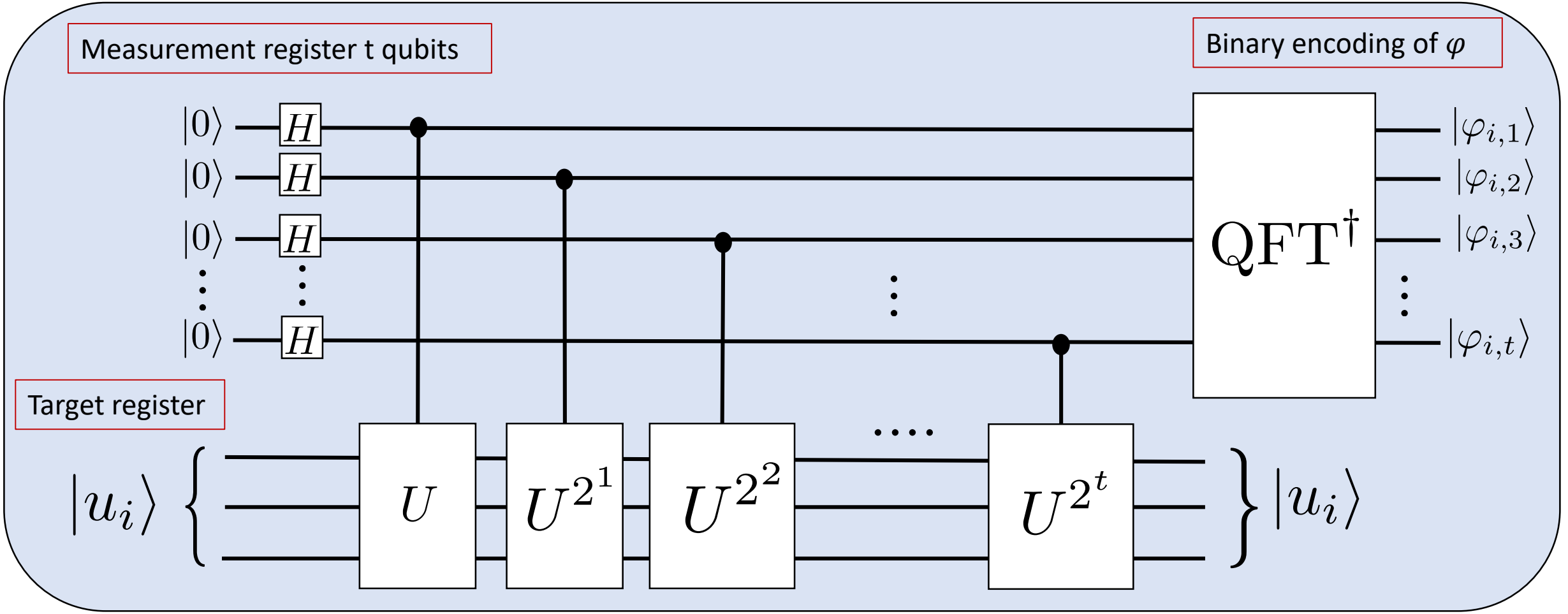
Degeneracy

- $U = \sum_{i=1}^{L} e^{2\pi i\varphi_i} P_i$
- $\sum_{i=1}^{L} P_i = I$
- $r_i = \mathrm{rank}(P_i) : \sum_{i=1}^{L} r_i = N$

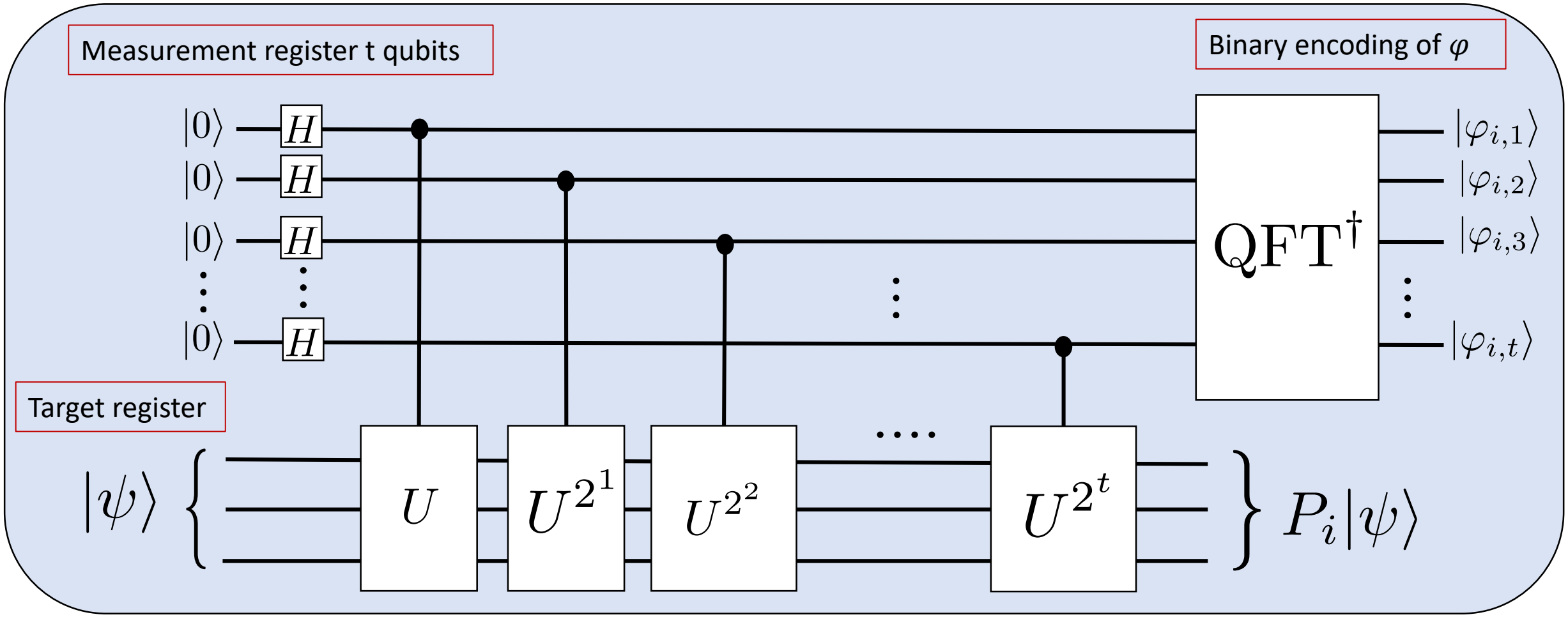
Quantum phase estimation

Projective measurement on the basis $|u_i\rangle$ with outcome $\varphi_i \in [0, 1]$

Assumptions:
- we can perform the controled-U^{2^x} operation
- All φ_i have at most t digits in binary encoding



Quantum phase estimation



$$|0^n\rangle \otimes |\psi\rangle = |0^n\rangle \otimes (\sum_i P_i|\psi\rangle) = \sum_i |0^n\rangle \otimes P_i|\psi\rangle \rightarrow \sum_i |\varphi_i\rangle \otimes P_i|\psi\rangle$$

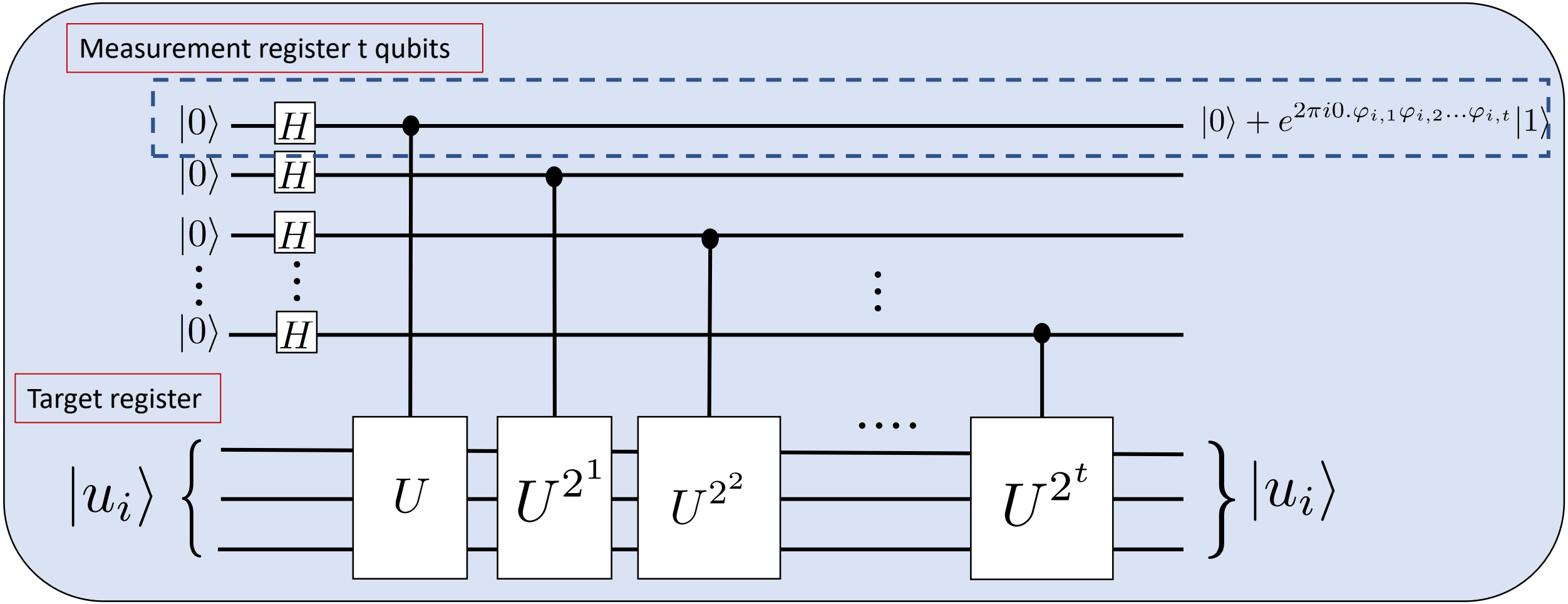
- With probability $||P_i|\psi\rangle||^2$ the measurement outputs $|\varphi_i\rangle$
- and the target register is projected to the subspace $P_i|\psi\rangle$

Quantum phase estimation: Proof

$$\varphi_i \in [0,1[$$
$$U|u_i\rangle = e^{2\pi i\varphi_i}|u_i\rangle$$

$$\varphi_i = 0.\varphi_{i,1}\varphi_{i,2}....\varphi_{i,t} = \frac{\varphi_{i,1}}{2} + \frac{\varphi_{i,2}}{2^2} + ... + \frac{\varphi_{i,t}}{2^t}$$

$$(|0\rangle + |1\rangle) \otimes |u_i\rangle \rightarrow (|0\rangle + e^{2\pi i\varphi_i}|1\rangle) \otimes |u_i\rangle$$



Quantum phase estimation: Proof

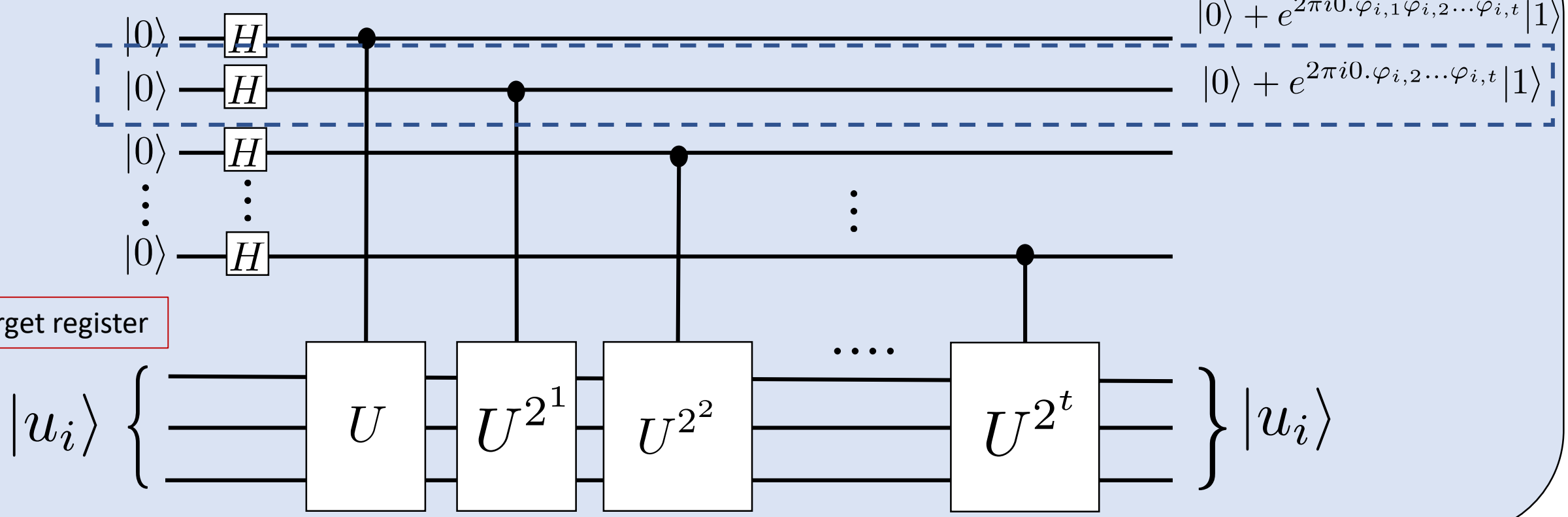
$$U|u_i\rangle = e^{2\pi i\varphi_i}|u_i\rangle$$
$$U^{2^k}|u_i\rangle = e^{2\pi i 2^k\varphi_i}|u_i\rangle$$

$$2\varphi_i = \varphi_{i,1} + \frac{\varphi_{i,2}}{2} + \ldots + \frac{\varphi_{i,t}}{2^{t-1}}$$

$$|0\rangle + e^{2\pi i 2\varphi_i}|1\rangle = |0\rangle + e^{2\pi i 0.\varphi_{i,2}\ldots\varphi_{i,t}}|1\rangle$$

Measurement register t qubits

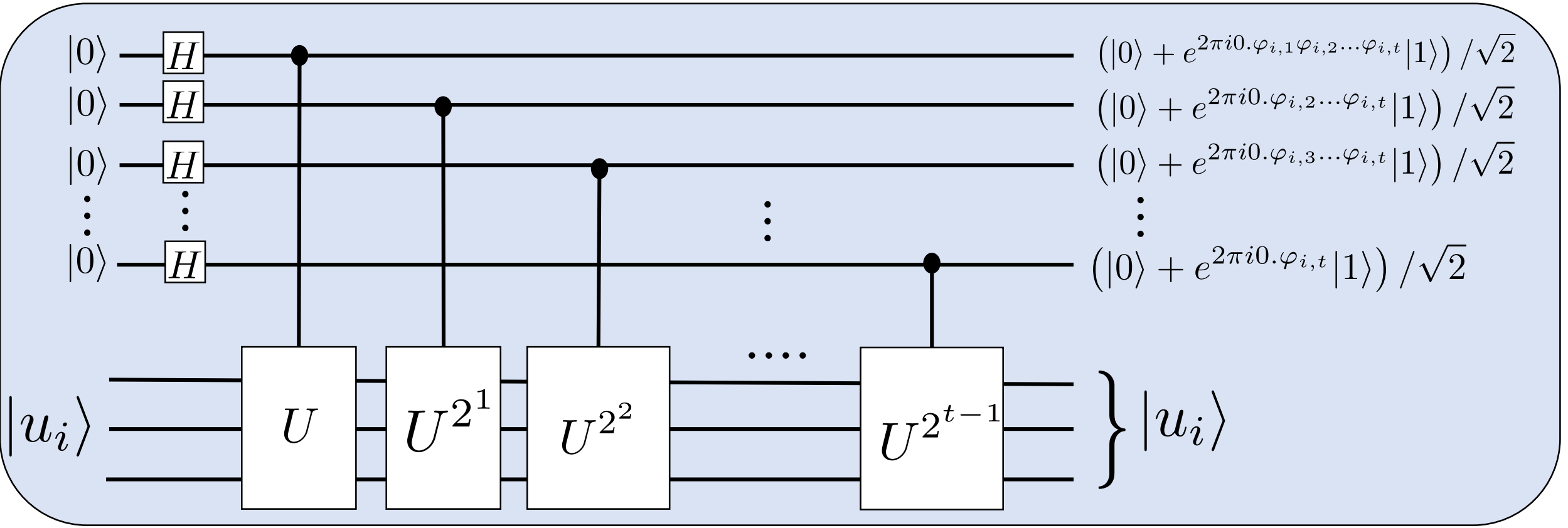
Target register



Quantum phase estimation: Proof

$$\varphi_i \in [0,1[\qquad \varphi_i = 0.\varphi_{i,1}\varphi_{i,2}....\varphi_{i,t} = \frac{\varphi_{i,1}}{2} + \frac{\varphi_{i,2}}{2^2} + ... + \frac{\varphi_{i,t}}{2t}$$

$$e^{2\pi i 2^k \varphi} = e^{2\pi i (2^{k-1}\varphi_{i,1} + ... + \varphi_{i,k})} e^{0.\varphi_{i,k+1}\cdots\varphi_{i,t}} = e^{0.\varphi_{i,k+1}\cdots\varphi_{i,t}}$$

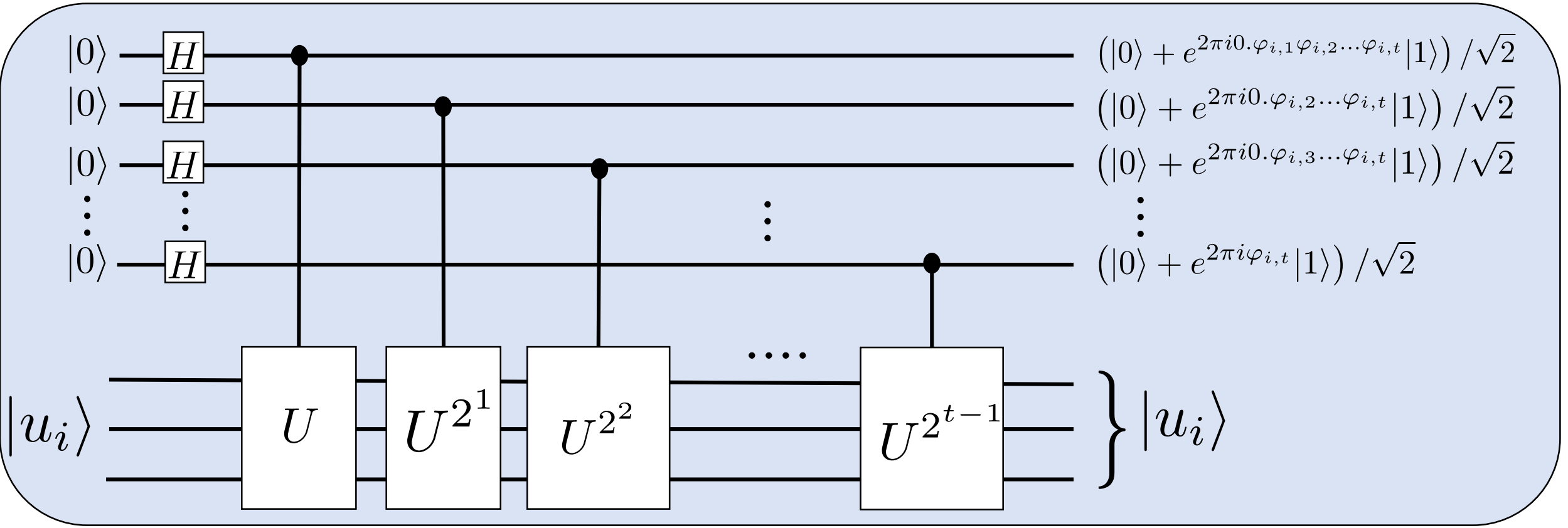


Quantum phase estimation: Proof

$$\varphi_i \in [0,1[\qquad \varphi_i = 0.\varphi_{i,1}\varphi_{i,2}....\varphi_{i,t} = \frac{\varphi_{i,1}}{2} + \frac{\varphi_{i,2}}{2^2} + ... + \frac{\varphi_{i,t}}{2t}$$

$$|x_1, x_2, ..., x_{n-1}, x_n\rangle \rightarrow \frac{1}{2^{n/2}}(|0\rangle + e^{2\pi i 0.x_n}|1\rangle)(|0\rangle + e^{2\pi i 0.x_{n-1}x_n}|1\rangle)...(|0\rangle + e^{2\pi i 0.x_1 x_2 ... x_n}|1\rangle)$$

QFT

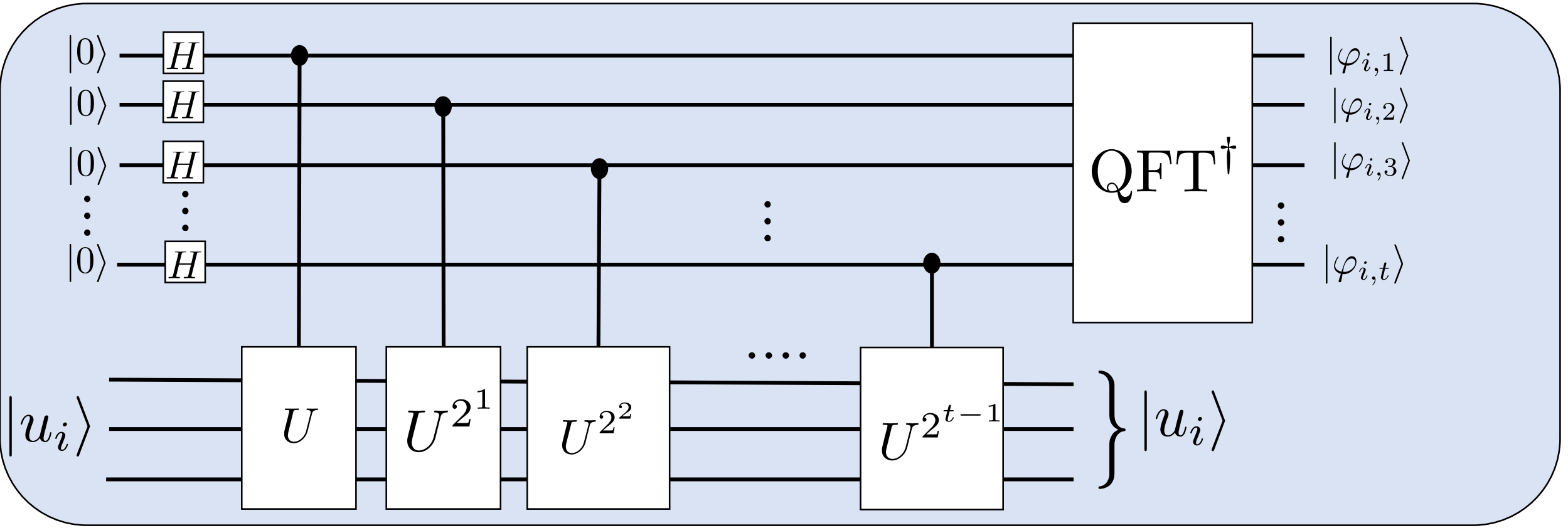


Quantum phase estimation: Proof

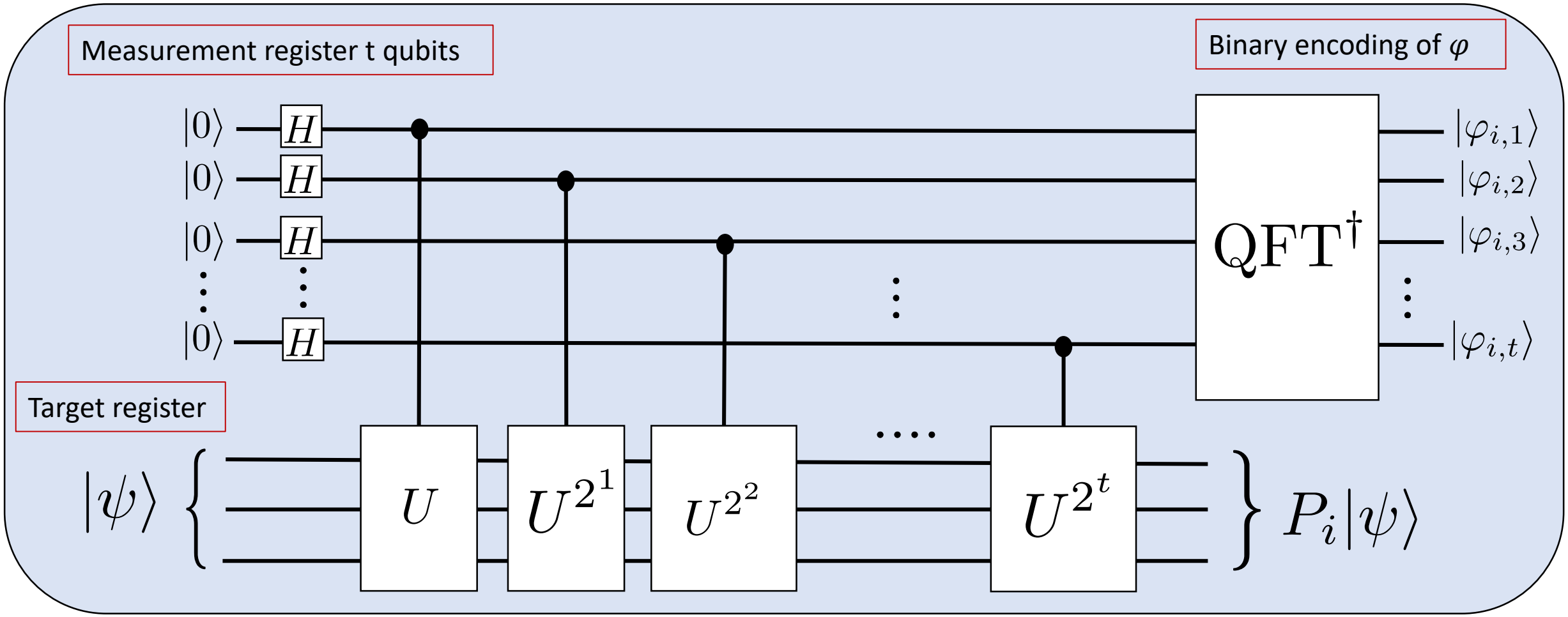
$$\varphi_i \in [0,1[\qquad \varphi_i = 0.\varphi_{i,1}\varphi_{i,2}....\varphi_{i,t} = \frac{\varphi_{i,1}}{2} + \frac{\varphi_{i,2}}{2^2} + ... + \frac{\varphi_{i,t}}{2^t}$$

$$|x_1, x_2, ..., x_{n-1}, x_n\rangle \rightarrow \frac{1}{2^{n/2}}(|0\rangle + e^{2\pi i 0.x_n}|1\rangle)(|0\rangle + e^{2\pi i 0.x_{n-1}x_n}|1\rangle)...(|0\rangle + e^{2\pi i 0.x_1 x_2 ... x_n}|1\rangle)$$

QFT



Quantum phase estimation

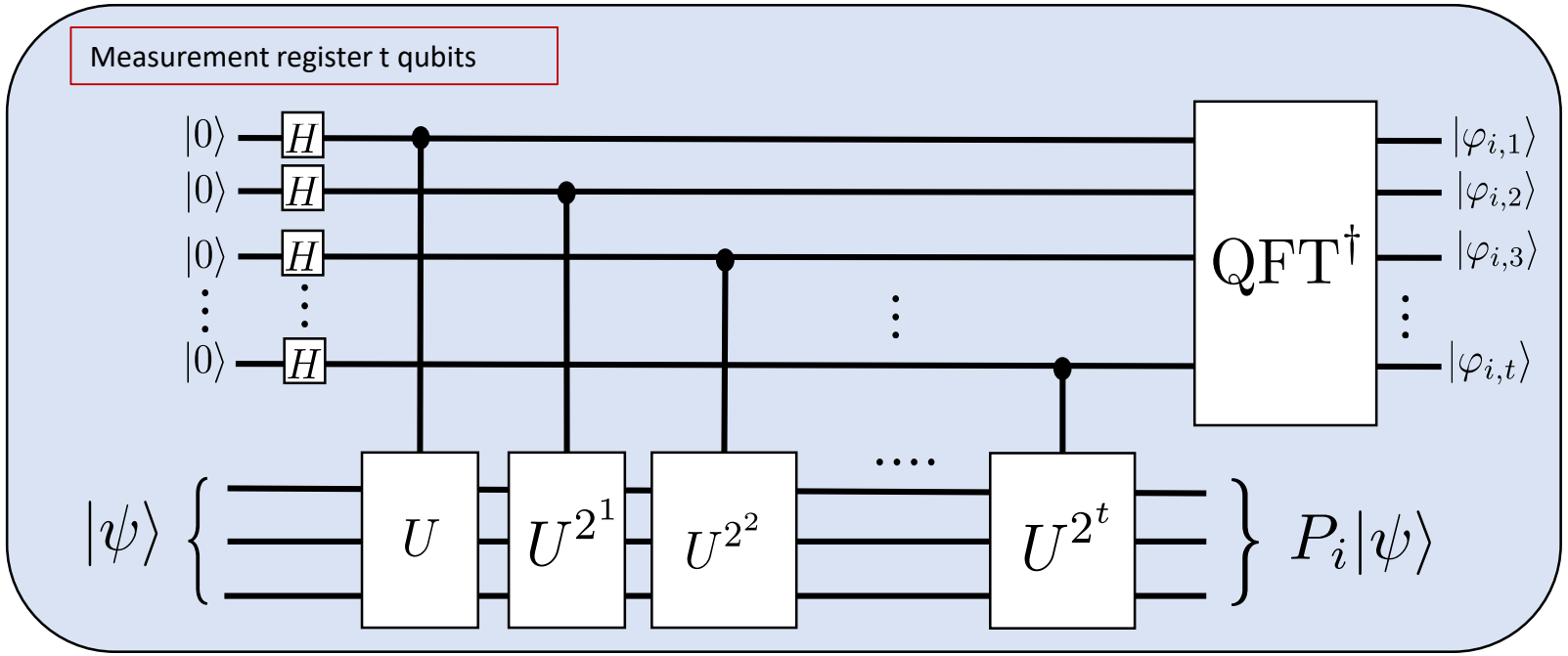


$$|0^n\rangle \otimes |\psi\rangle = |0^n\rangle \otimes (\sum_i P_i|\psi\rangle) = \sum_i |0^n\rangle \otimes P_i|\psi\rangle \rightarrow \sum_i |\varphi_i\rangle \otimes P_i|\psi\rangle$$

- With probability $||P_i|\psi\rangle||^2$ the measurement outputs $|\varphi_i\rangle$
- and the target register is projected to the subspace $P_i|\psi\rangle$

Application and Discussion

$$|0^n\rangle \otimes |\psi\rangle \rightarrow \sum_i |\varphi_i\rangle \otimes P_i|\psi\rangle$$



- Can we implement U^{2^k} efficiently?
  - Sometimes YES!!, see Shor's algorithm.
  - Most of the time not! or we could exp-accelerate quantum simulation.
- To obtain φ accurate to n bits with probability of error ϵ
  - we need to satisfy: $t = n + \lceil \log(2 + \frac{1}{2\epsilon}) \rceil$

Shor algorithm:

QPE for modular exponentiation

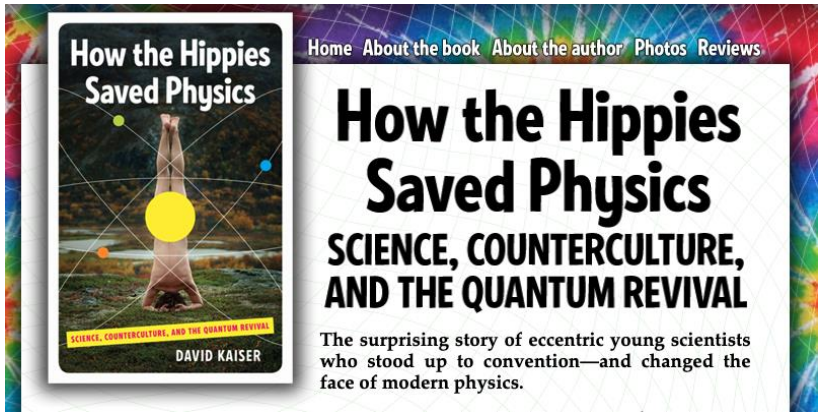
Shor's Algorithm for Factoring

Input: $N \in \mathbb{N}$. An n digits integer number.
Promise: $N = p_1 p_2$ where p_1, p_2 are prime numbers.
Problem: find p_1 and p_2

- Major breakthrough in 1994

Classical: $O(2^{n^{1/3}})$

Quantum: $O(n^3)$



- Changed the field of quantum computation

UK NATIONAL QUANTUM TECHNOLOGIES PROGRAMME

Summary Factoring

- Pick $\kappa \in \mathbb{N} : \kappa < N$ at random.

$$N = p_1 \cdot p_2$$

- Compute $GCD(\kappa, N)$ Using Euclid's Algorithm.

$$\text{If } GCD(\kappa, N) \neq 1 \Rightarrow GCD(\kappa, N) = p_1 \text{ or } p_2$$

As unlikely as random guessing 

$$f_{N,\kappa}(x) = \kappa^x (\mathrm{mod} N) \quad \text{Least positive } r : \kappa^r (\mathrm{mod} N) = 1$$

- We call ORDER FINDING to obtain r.
- $\mathrm{GCD}(\kappa^{r/2} - 1, N) = p_1 \quad \mathrm{GCD}(\kappa^{r/2} + 1, N) = p_2$

H1 r is even: $r/2 \in \mathbb{N}$. H2 $\kappa^{r/2} + 1 \neq 0 \ (\mathrm{mod} N)$

- We have a verification of solution.

$$P\left[\kappa < N : \text{H1} \cap \text{H2}\right] > 1/2$$

THE UNIVERSITY of EDINBURGH
informatics

Order finding

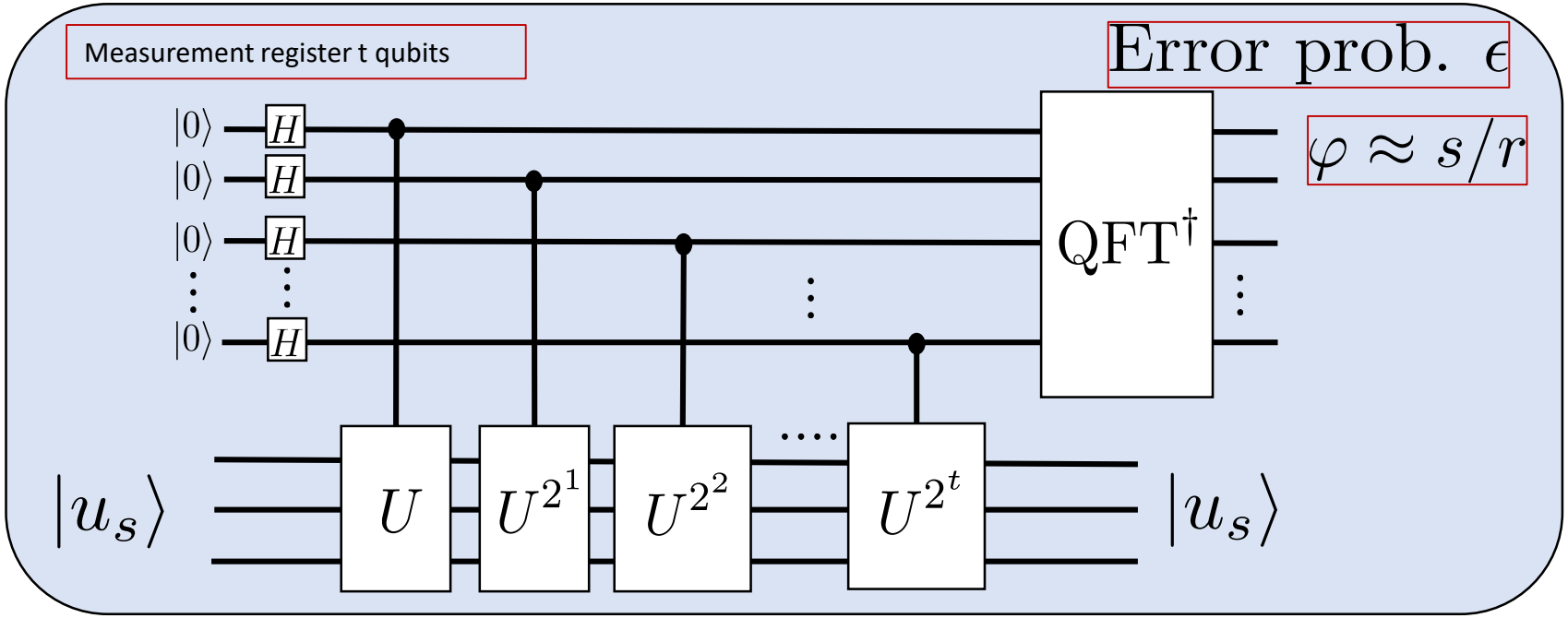
Phase-estimation for order finding

$$U|y\rangle \equiv |\kappa y (\mathrm{mod} N)\rangle$$

Unitary as $\mathrm{GCD}(\kappa, N) = 1$

Binary encoding of N

$L \equiv \lceil \log(N) \rceil$



- $|u_s\rangle$ is eigenvector of U of eigenvalue $e^{2\pi i s/r}$ with $s \in \{0, r-1\}$

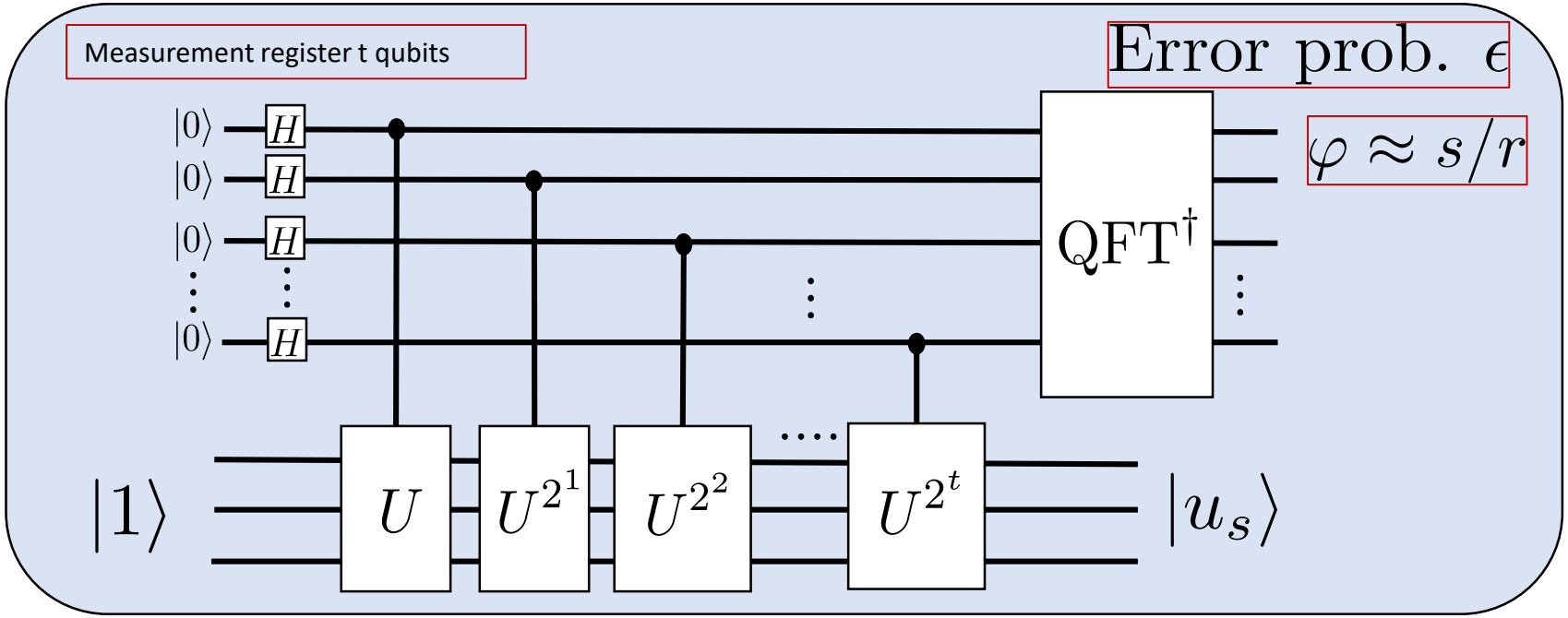
$$|u_s\rangle = \frac{1}{r}\sum_{l=0}^{r-1} e^{-2\pi i s l/r} |\kappa^l (\mathrm{mod}) N\rangle \qquad U|u_s\rangle = e^{2\pi i s/r}|u_s\rangle$$

- Continued fractions extract s/r from φ
- Approximation φ of $2L+1$ bits, if $t = 2L + 1 + \lceil \log(2 + \frac{1}{2\epsilon}) \rceil$

The input state

$$U|y\rangle \equiv |\kappa y (\mathrm{mod} N)\rangle$$

Unitary as $\mathrm{GCD}(\kappa, N) = 1$



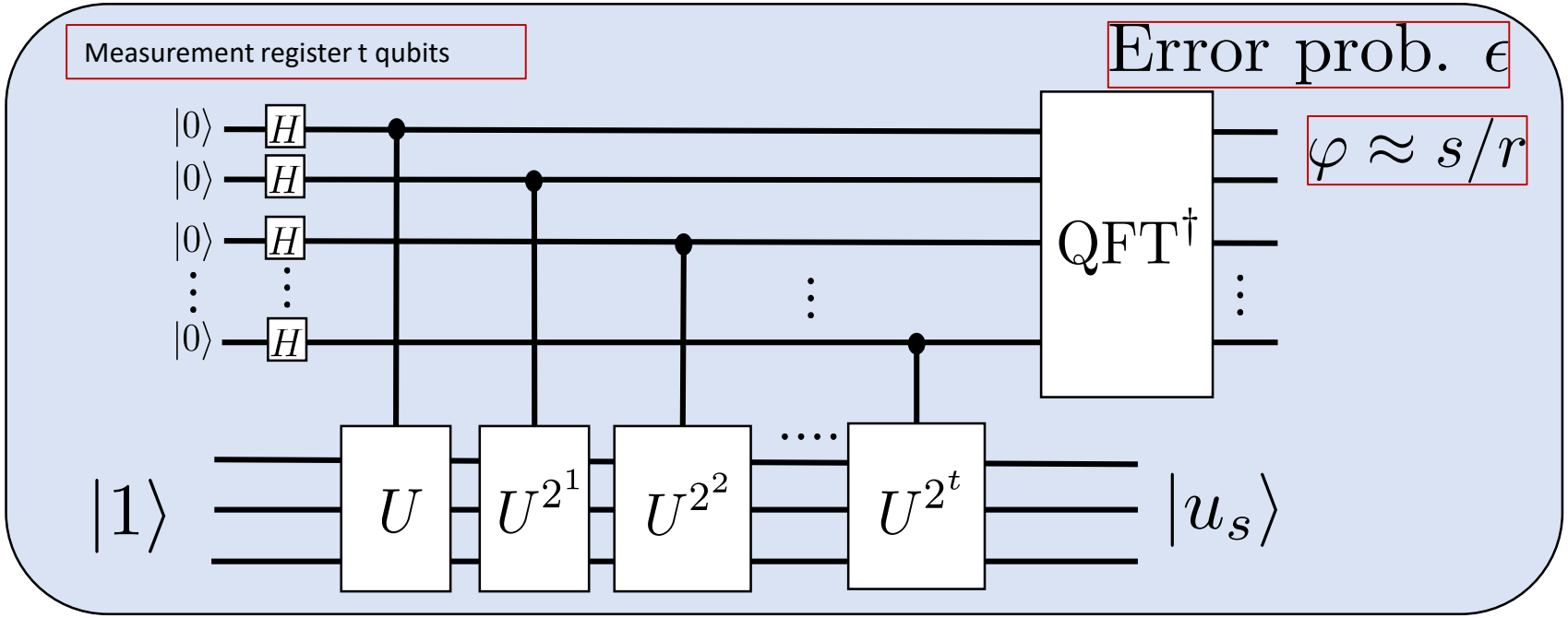
- $|u_s\rangle$ is eigenvector of U of eigenvalue $e^{2\pi i s/r}$
- But to generate $|u_s\rangle$ we need r!

$$\frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} |u_s\rangle = |1\rangle = |0\rangle \otimes .... \otimes |0\rangle \otimes |1\rangle$$

Post-processing: potential error

$$U|y\rangle \equiv |\kappa y (\mathrm{mod} N)\rangle$$

Unitary as $\mathrm{GCD}(\kappa, N) = 1$



- Continued fractions computes the nearest s'/r' such that $\mathrm{GCD}(s', r') = 1$
- Error if $s'/r' = s/r$ and $\mathrm{GCD}(s, r) \neq 1$
  - For random $s \in \{0, r-1\}$ high prob. $\mathrm{GCD}(s, r) = 1$

#co-primes: $\Omega(r/\log\log r) \Rightarrow$ repeat $O(\log L)$

$$|1\rangle = \frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} |u_s\rangle$$

References

Reading references

1. Phase estimation: NC 5.2
2. Phase estimation when φ my have more than t digits (approximation with error): NC 5.2.1 (NEM)
3. Additional references RdW Ch4, G Ch9
4. Order finding and factoring NC 5.3, RdW Ch5, G Ch10

NC ≣ Michael Nielsen and Isaac Chuang, Quantum Computing and Quantum Information Cambridge University Press (2010)

RdW ≣ Quantum Computing Lecture Notes, Ronald de Wolf, https://arxiv.org/abs/1907.09415

G ≣ Introduction to Quantum Computation, Sevag Gharibian, Lectures notes.

Number Theory

1. Michael Nielsen and Isaac Chuang, Quantum Computing and Quantum Information, Cambridge University Press (2010) [Appendix 4]
2. Ivan Niven, Herbert S. Zuckerman, Hugh L. Montgomery, *An Introduction to the Theory of Numbers*, John Wiley & Sons (1991)
3. Victor Shoup, *A Computational Introduction to Number Theory and Algebra*, Cambridge University Press (2008)

Probability of hypothesis H1 and H2

1. Ronal de Wolf, Quantum Computing: Lecture Notes, arXiv:1907.09415v1 (2019) [Footnote page 36].
2. See also Nielsen and Chuang [Chapter 5: page 233].

Public Key Cryptography and RSA

1. Michael Nielsen and Isaac Chuang, Quantum Computing and Quantum Information, Cambridge University Press (2010) [Appendix 5]
2. Victor Shoup, *A Computational Introduction to Number Theory and Algebra*, Cambridge University Press (2008)