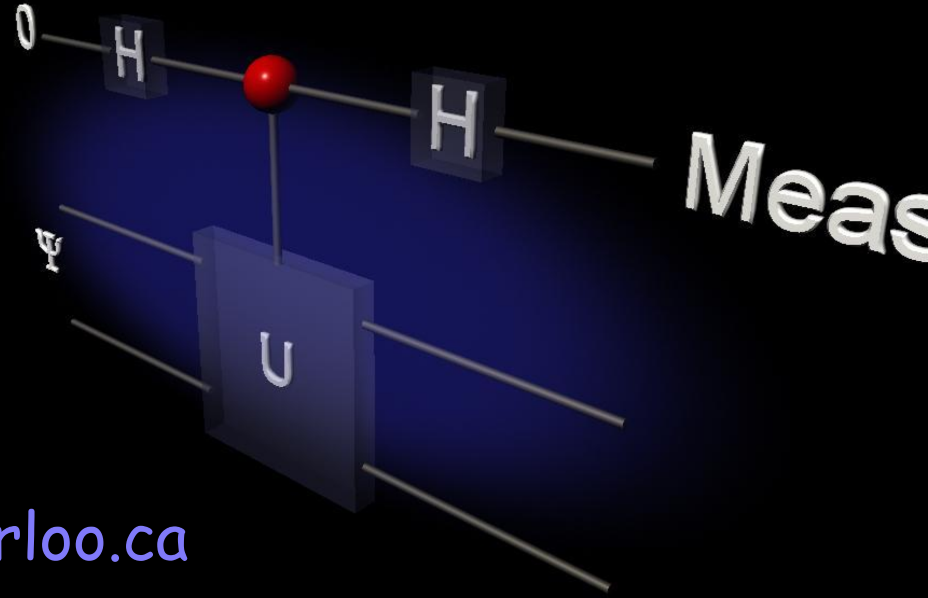
Introduction to Quantum Information Processing

CO481 CS467 PHYS467



Michele Mosca mmosca@iqc.uwaterloo.ca

Tuesdays and Thursdays 10am-11:15am

Overview

- Reading: sections 7.4, 7.5, 7.6

Discrete Logarithm Problem

Consider two elements $a, b \in G$ from a group G satisfying

$$a^r = 1$$

$$b = a^s$$

Find s.

$$U_a |x\rangle = |ax\rangle$$

Discrete Logarithm Problem

We know U_a has eigenvectors

$$|\psi_k\rangle = \sum_{j=0}^{r-1} e^{-i2\pi j\frac{k}{r}} |a^j\rangle$$

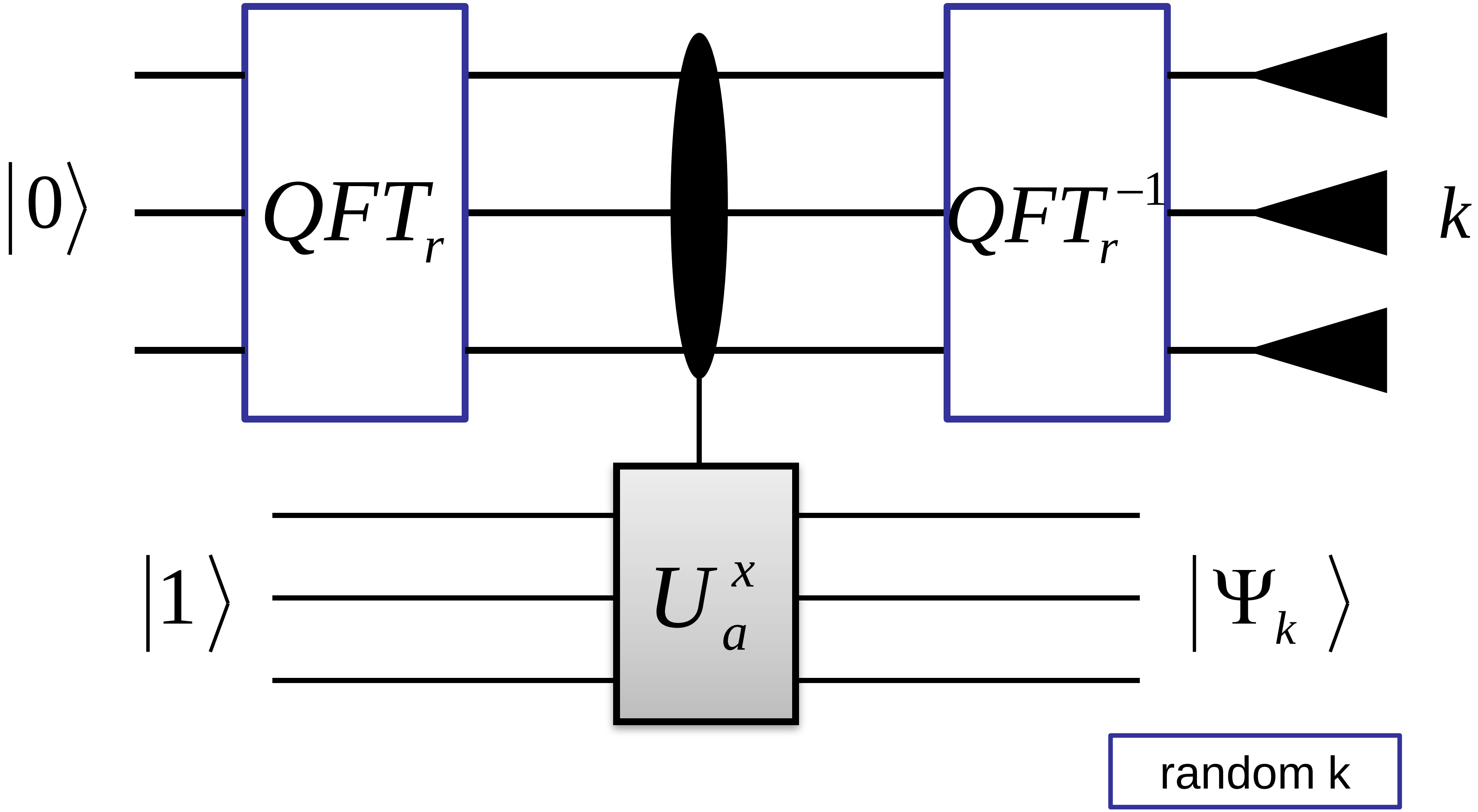
$$U_a|\psi_k\rangle = e^{i2\pi\frac{k}{r}} |\psi_k\rangle$$

Discrete Logarithm Problem

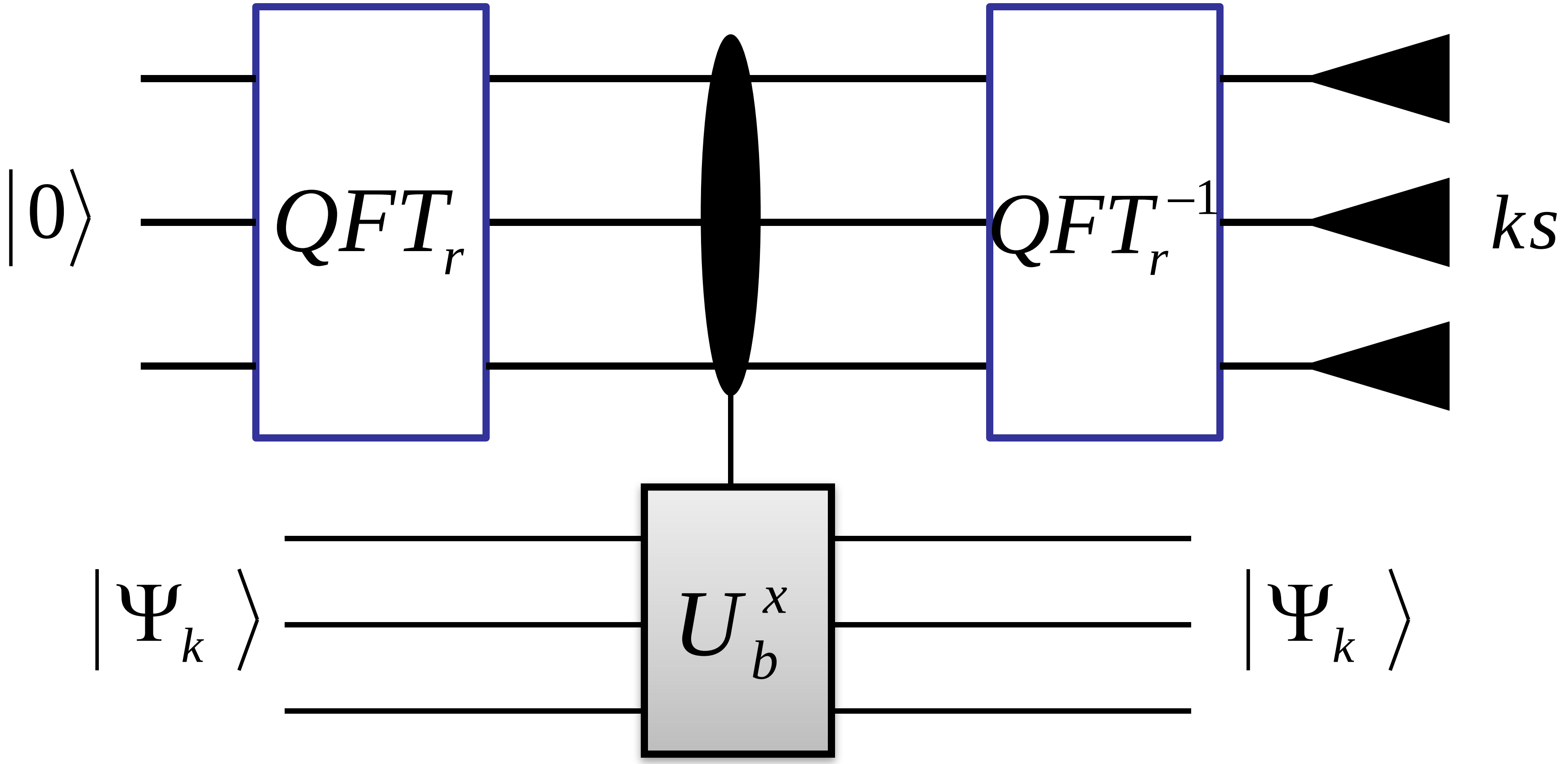
Thus U_{b} has the same eigenvectors but with eigenvalues exponentiated to the power of s

$$U_{b}\left|\psi_k\right\rangle = U_{a^s}\left|\psi_k\right\rangle = e^{i2\pi\frac{ks}{r}}\left|\psi_k\right\rangle$$

Discrete Logarithm Problem

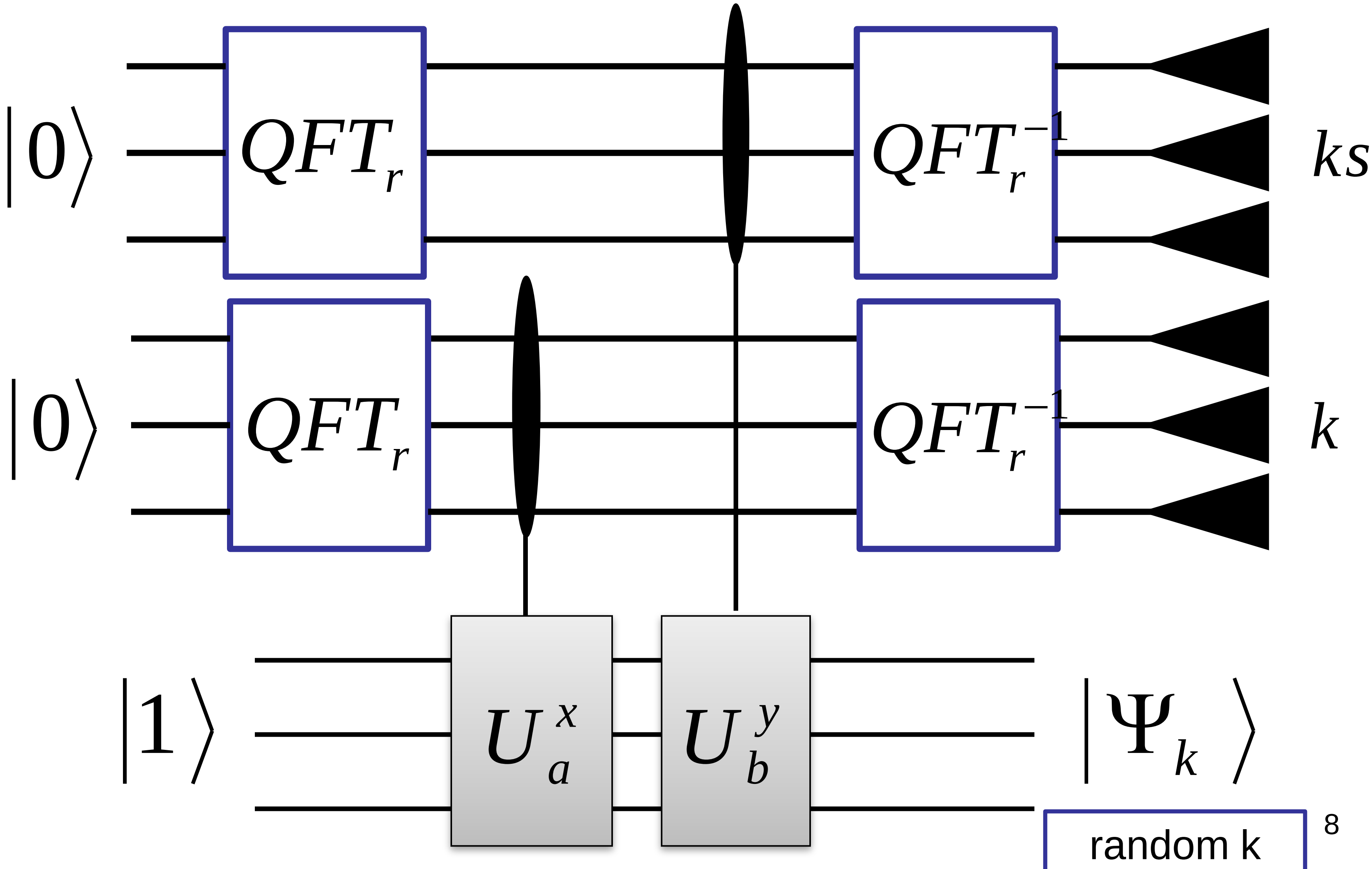


Discrete Logarithm Problem



Given k and ks, we can compute $s \bmod r$
(provided k and r are coprime)

Complete Circuit



Generalization of Simon's problem, order-finding and DLP: "Hidden subgroup problem"

- A unifying framework was developed for these problems

$$f : G \to X$$

$$f(x) = f(y) \quad \textbf{iff} \quad x + S = y + S$$

for some $S \leq G$

- If G is Abelian, finitely generated, and represented in a reasonable way, we can efficiently find S.

Example (I)

Deutsch's Problem:

$$G = \{0,1\} \qquad X = \{0,1\}$$

$S = \{0\}$ or $\{0,1\}$

Order finding:

$G = Z$ $\qquad X$ any group

$$f(x) = a^x$$

$$S = rZ$$

Example (II)

Discrete Log of $b = a^k$ to base a :

$$G = Z_r \times Z_r \qquad X \quad \text{any group}$$

$$f(x, y) = a^x b^y$$

$$S = \langle (k, -1) \rangle$$

Example (III)

Self-shift equivalences:

$$G = GF(q)^n \qquad X = GF(q)[X_1, X_2, \ldots, X_n]$$

$$f(a_1, a_2, \ldots, a_n) = P(X_1 - a_1, \ldots, X_n - a_n)$$

$$S = \{(a_1, \ldots, a_n) :$$
$$P(X_1 - a_1, \ldots, X_n - a_n) = P(X_1, \ldots, X_n)\}$$

Other applications of Abelian HSP

- Any finite Abelian group G is the direct sum of finite cyclic groups

$$\langle g_1 \rangle \oplus \langle g_2 \rangle \oplus \cdots \oplus \langle g_n \rangle$$

But finding generators $g_1, g_2, \cdots, g_n$ satisfying $G = \langle g_1 \rangle \oplus \langle g_2 \rangle \oplus \cdots \oplus \langle g_n \rangle$ is not always easy, e.g. for $G = Z_N^*$ it's as hard as factoring N

- Given any polynomial sized set of generators, we can use the Abelian HSP algorithm to find new generators that decompose G into a direct sum of finite cyclic groups.

What about non-Abelian HSP

- Consider the symmetric group $G = S_n$
- $\mathrm{S_n}$ is the set of permutations of n elements
- Let G be an n-vertex graph

- Let $X_G = \{\pi(G) \mid \pi \in S_n\}$
- Define $f_G : S_n \to X_G \qquad f_G(\pi) = \pi(G)$
- Then $f_G(\pi_1) = f_G(\pi_2) \Leftrightarrow \pi_1 S = \pi_2 S$

where $S = AUT(G) = \{\pi \mid \pi(G) = G\}$

Graph automorphism problem

- So the hidden subgroup of f_G is the automorphism group of G
- This is a difficult problem in NP that is believed not to be in BPP and yet not NP-complete.
- A solution to the graph automorphism problem gives a solution to the graph isomorphism problem.