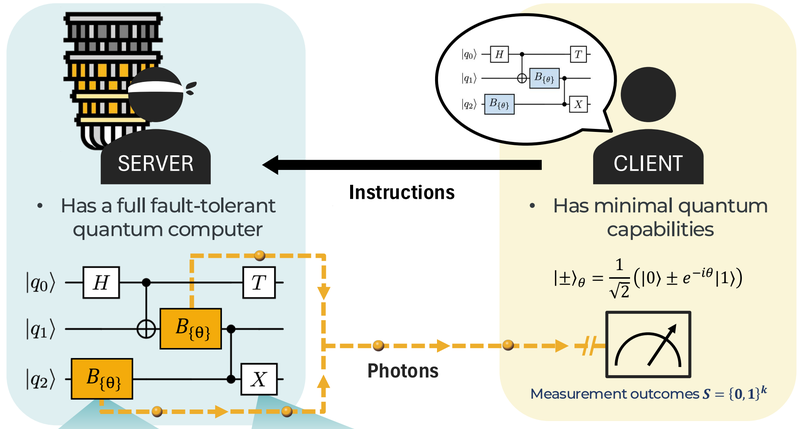
Designing a Blind Quantum Algorithm for Secure Robot Path Planning

[1,2]Sunny Kang, [3]Iria W. Wang, [1]Raisa Trubko, [2]Carlo Pinciroli

[1]Department of Physics, WPI, [2]Department of Robotics Engineering, WPI, [3]Department of Physics, Harvard University

BLIND QUANTUM COMPUTING: HYBRID LIGHT-MATTER

Blind Quantum Computing allows a client to delegate a quantum computation to a server without revealing any information about it



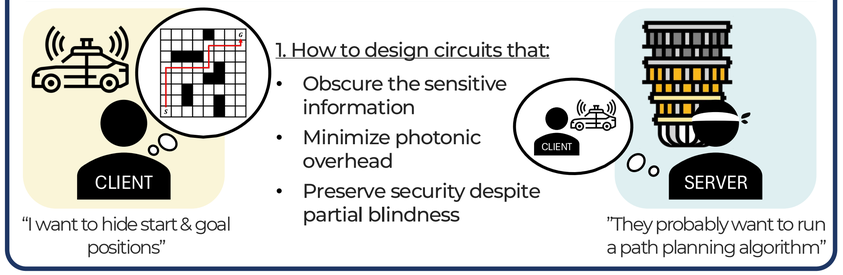
Blindness:

Density matrix that sees, $\rho_{out} = \frac{1}{2^k}\sum_S C(\vec{\theta}, S)\rho_{in}C^\dagger(\vec{\theta}, S)$, is independent of $\vec{\theta}$

Key Advantages:

- Clients can customize the circuit and choose what parts are **blind vs non-blind: balancing security and efficiency**

MOTIVATION & PROBLEM STATEMENT



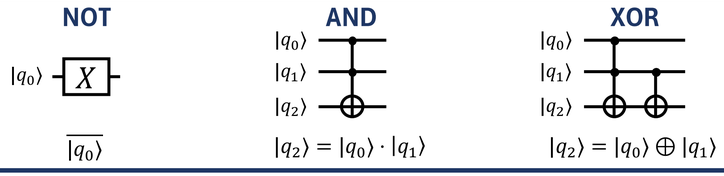
"I want to hide start & goal positions"

1. How to design circuits that:

- Obscure the sensitive information
- Minimize photonic overhead
- Preserve security despite partial blindness

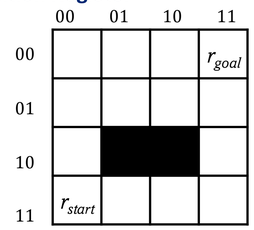
"They probably want to run a path planning algorithm"

BOOLEAN LOGIC GATES AS QUANTUM GATES



PROBLEM SETUP

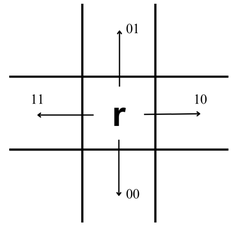
Position Register



$N \times N$ grid map

- # of qubits : $n_{\text{pos}} = 2 \cdot \log_2(N)$
- Position state : $|r\rangle = |\underbrace{r_0 r_1 \ldots}_{\text{row index}} \underbrace{r_{n-2} r_{n-1}}_{\text{column index}}\rangle$

Movement Register



- degrees of freedom : k
- # of qubits : $n_{\text{move}} = \log_2(k)$
- movement state : $|m\rangle = |m_0 m_1 \ldots m_{n-2} m_{n-1}\rangle$

PATH PLANNING WITH GROVER'S ALGORITHM

A parallel search over all possible solution states, with a feedback loop that amplifies the correct solution

State Preparation

Encode all N candidate solutions (e.g. paths, configurations) into a quantum superposition state

$$|\psi\rangle = \frac{1}{\sqrt{N}}\sum_{x=0}^{N-1}|x\rangle \quad = \quad \sqrt{\frac{S}{N}}|\omega\rangle + \sqrt{\frac{N-S}{N}}|v\rangle$$

- $|\omega\rangle = \frac{1}{\sqrt{S}}\sum_{x\in\Omega}|x\rangle$ = superposition of all solution states
- $|v\rangle = \frac{1}{\sqrt{N-S}}\sum_{x\notin\Omega}|x\rangle$ = superposition of all non-solution states
- $S = |\Omega|$ = number of solution states, Ω = set of all solution states

1. Grover Oracle U_ω

Marks the correct solution

$$f(x) = \begin{cases} 1 & \text{If } x \text{ is a valid solution} \\ 0 & \text{otherwise} \end{cases}$$

- Is the path collision-free?
- Is the path within the map?
- Does the configuration reach the target?

$$U_\omega|\psi\rangle = (-1)^{f(x)}\sqrt{\frac{S}{N}}|\omega\rangle + \sqrt{\frac{N-S}{N}}|v\rangle$$

2. Grover Diffuser U_ψ

Amplify probability amplitude of the solution state

- Increases the probability of valid solutions
- Decreases the probability of invalid solutions

$$U_\psi = 2|\psi\rangle\langle\psi| - I$$

For at most $\frac{\pi}{4}\sqrt{\frac{N}{S}}$

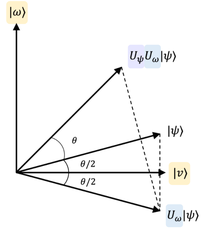
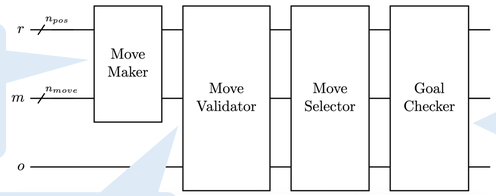


Fig 1: Geometric representation of Grover's algorithm

GROVER ORACLE



Move Maker

- Increments / decrements row, column indices by one

Goal Checker

- Checks if the goal position has been reached

Move Validator

- Obstacle collision check
- Map boundary check

$$o = \prod_{i=0}^{n_{\text{pos}}/2-1}\overline{(r_i \oplus \overline{y_i})} \cdot \prod_{i=n_{\text{pos}}/2}^{n_{\text{pos}}-1}\overline{(r_i \oplus \overline{y_i})}$$

r_i = initial index, y_i = updated index

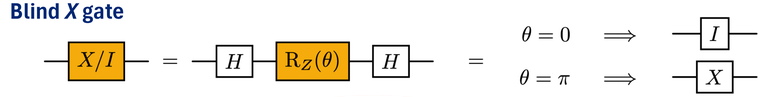
Move Selector

- Selects a valid move

$$r_i' = r_i' = \overline{(y_i \cdot o)} \cdot \overline{(r_i \cdot \overline{o})}, \quad 0 \le i \le n_{\text{pos}} - 1$$

BLIND TRASNFORMATION

Blind X gate



1. Hiding Start Position

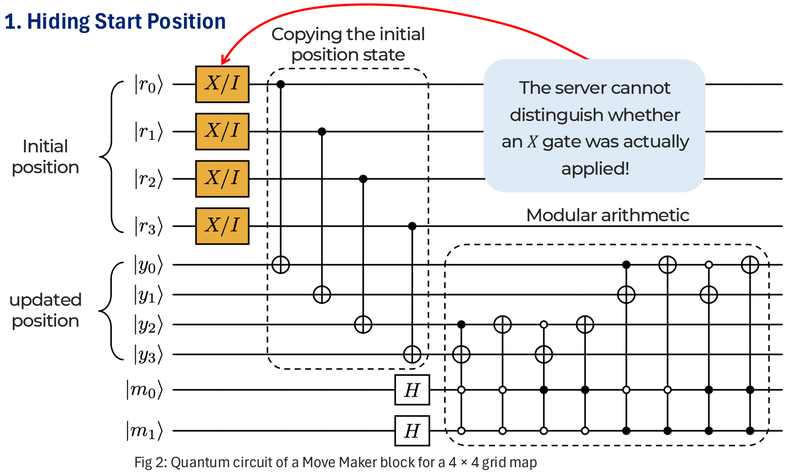
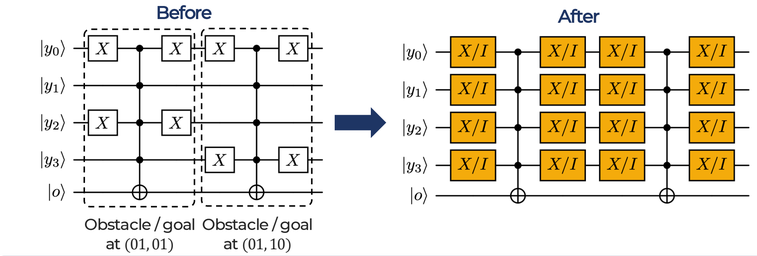


Fig 2: Quantum circuit of a Move Maker block for a 4 × 4 grid map

2 Hiding Obstacle & Goal Position



[1] G. Baranes *et al.*, *Designing Fault-Tolerant Blind Quantum Computation*. 2025. [Online]. Available: https://arxiv.org/abs/2505.21621
[2] Chella et al., 2022. "A Quantum Planner for Robot Motion." Mathematics 10 (14). https://doi.org/10.3390/math10142475.