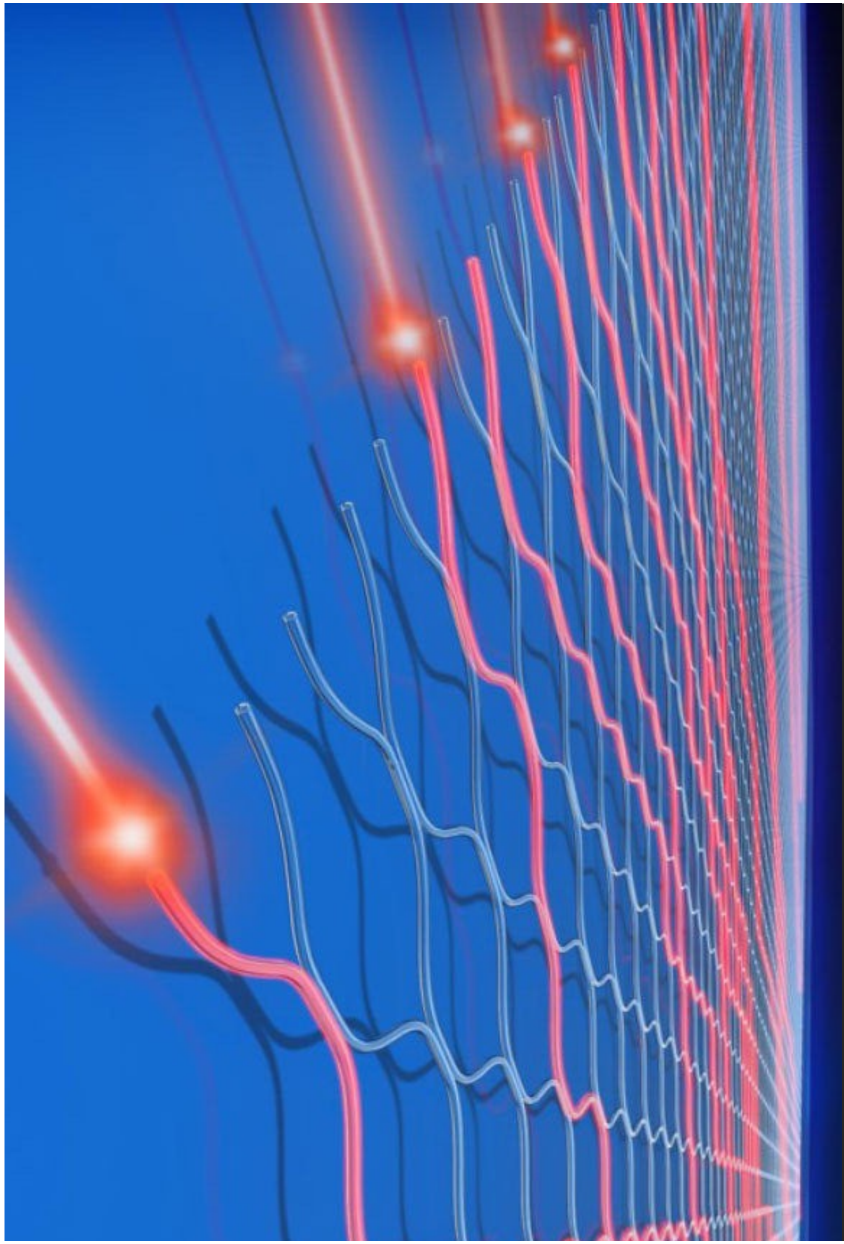


Lecture 13:
Quantum Supremacy & Summary

COMP3366
Quantum algorithms & computing architecture

Instructor: Yuxiang Yang

Department of Computer Science, HKU

Objectives:

- **[O1] Concepts:**

  Quantum supremacy, boson sampling.

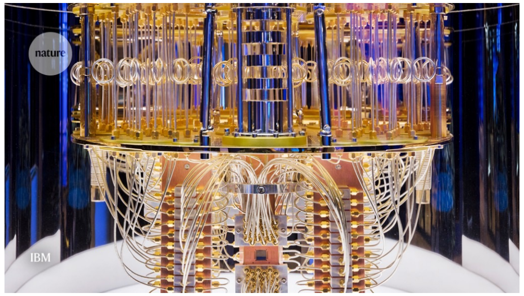
Part I:
Quantum supremacy

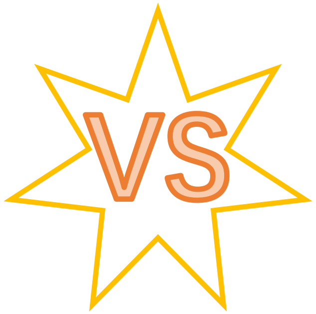
A Race for Supremacy

Image: *Katy Dannenberg*

- How to demonstrate the power of quantum computers as soon as possible.

Discussion: How to convince a billionaire to make investment in building quantum computers?





Mr. Stark, please support our research in quantum computing.

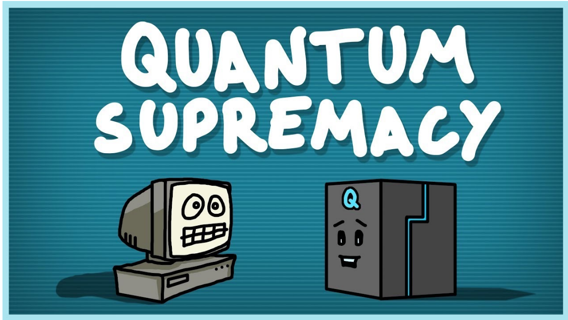
I can … but for what? I have already got the fastest supercomputer.

- How would you persuade the billionaire?
- "Achieving quantum supremacy":

  To find a computational task and to prove that:

  1. no classical computer can solve it within a reasonable amount of time and
  2. there is a quantum algorithm that solves it efficiently.

     (To prove this point, we need to demonstrate the quantum algorithm.)



Images from YouTube

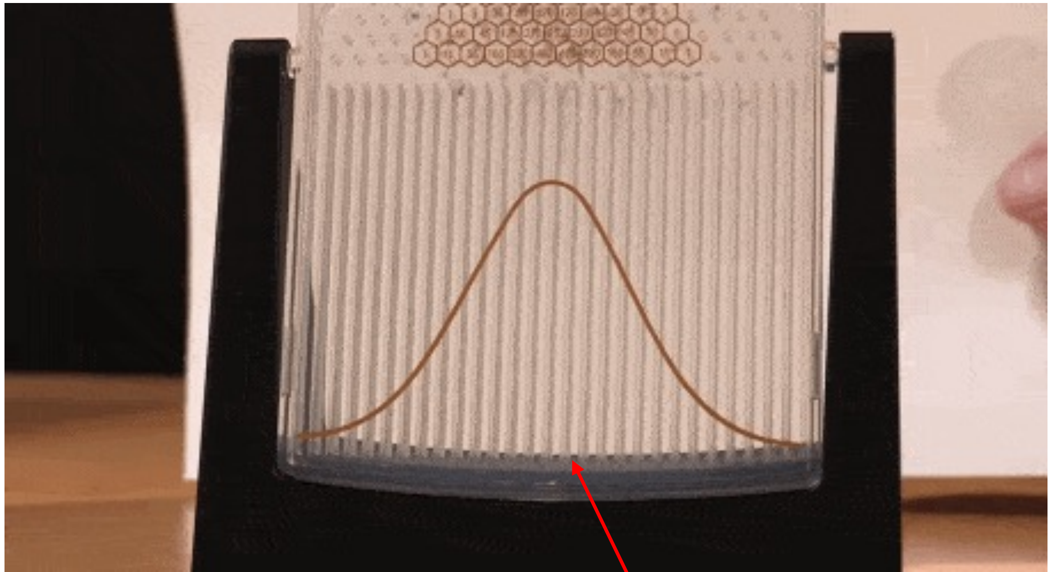
- **Discussion:**

  Could you propose some candidates for this task?

Sampling problems

- Challenge: the quantum algorithm must be “NISQ-compatible”.
- For example, factorization is hard for any classical computer, but it is also hard for NISQ devices!
- Instead, people often consider sampling problems: Sampling problems are those which output random numbers according to a particular probability distribution.

• Example: Galton’s board



Output: Balls whose locations obey the binomial distribution approximately!

- Boson sampling (Aaronson-Arkhipov'13)

The m-th detector getting s_m "clicks"

- Input: photons in the first n out of m ports

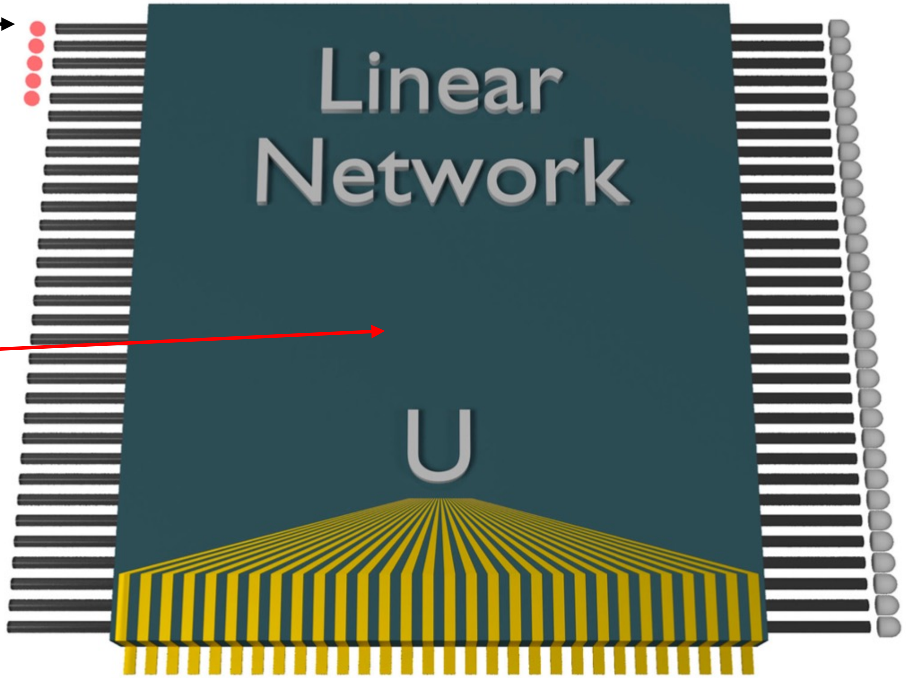
  Output: n "clicks" with random locations with $p_{\vec{s}}$ for the event $\vec{s} = (s_1, \ldots, s_m)$

Permanent (see later)

$$p_{\vec{s}} = \frac{Perm(A_{\vec{s}})^2}{s_1! \cdots s_m!}$$

A $n \times n$ matrix that depends on U and $\vec{s}$

1 ball = 1 photon



Quantum circuit U implemented by linear quantum optical gadgets (≈ semitransparent glasses)

The circuit can be adjusted freely, just like adjusting the positions of pillars in a Galton board.

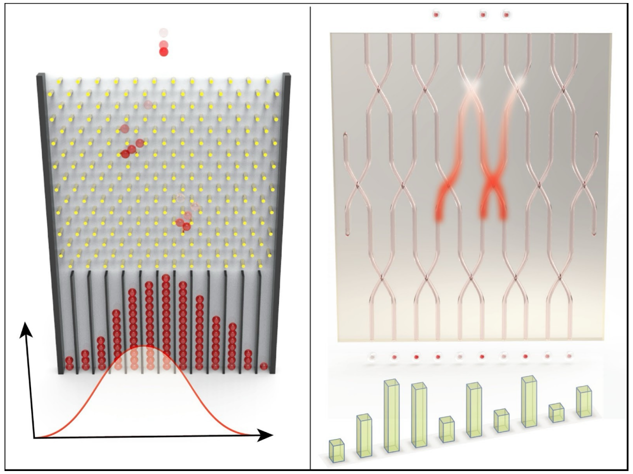
Photon detectors ("click" when a photon arrives)

Quantum supremacy with boson sampling

- The distribution $p_{\vec{s}} = \frac{Perm(A_{\vec{s}})^2}{s_1! \cdots s_m!}$ depends on the permanent of a $n-$ dimensional matrix.
- Computing the permanent of a large matrix is very hard for classical computers (#P-complete; harder than any problem in NP!).
- If we could design a quantum algorithm that efficiently computes the permanent, we could show quantum supremacy!
- … And we already did ~

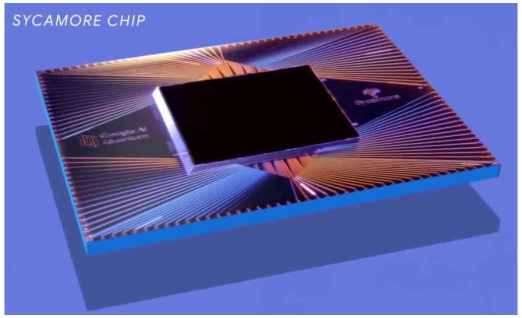
Quantum supremacy with Boson sampling

- There is a way to embedded a matrix into a quantum circuit for Boson sampling.
- Then, we can run Boson sampling with this circuit, and estimate $p_{\vec{s}}$ (like in the case of the Galton board) by counting photons.
- This gives us the permanent as desired, since $p_{\vec{s}}$ is proportional to the permanent!
- **Conclusion:**
  Boson sampling can efficiently estimate the permanent of a large random matrix, which is computationally hard for any classical computer!

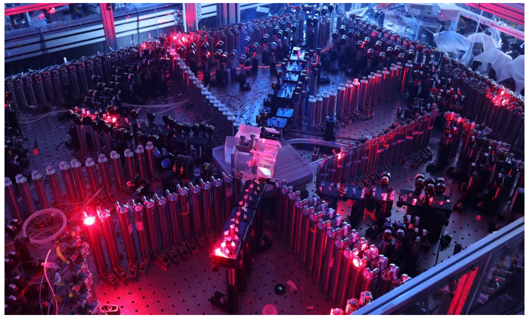


Timeline of quantum supremacy

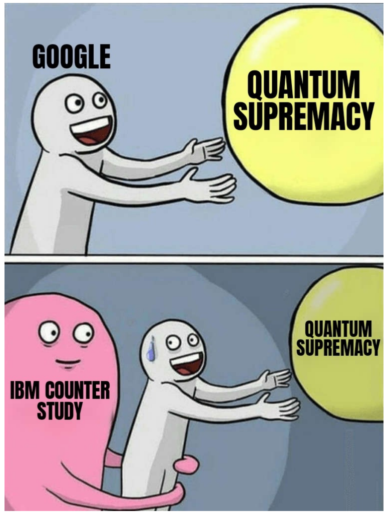
- **2019**: Sycamore executes a sampling task (XEB) in 200 seconds. Google claims that it takes 10,000 years for a classical supercomputer.
- **2020**: Photonic quantum computer Jiuzhang achieves supremacy in boson sampling.
- **2021-now**: Jiuzhang 2.0 and other QCs demonstrated boson sampling with larger circuits.
- **2021**: the same sampling task of Sycamore was finished in 15 hours on a supercomputer, after optimization of its algorithm.
- Consequently, sycamore did not achieve a good demonstration of supremacy (but others are more solid).



Google Sycamore



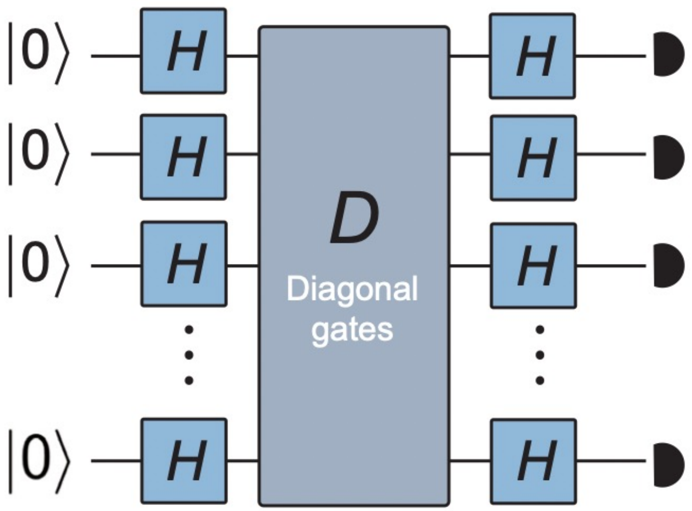
USTC Jiuzhang (九章)



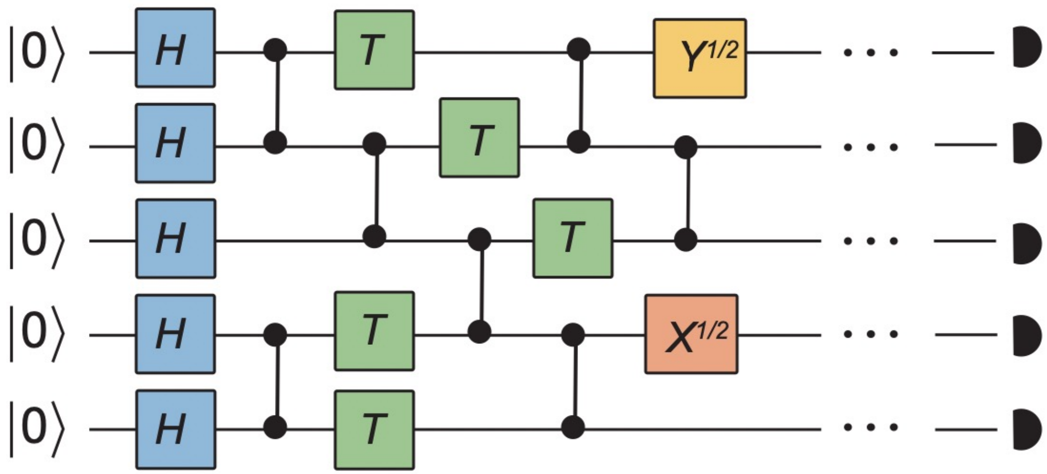
From Twitter
(John Martinis, a Nobel Prize Laurent in Physics, was in charge of Google quantum computing)

Can you propose some other tasks where a NISQ device outperforms classical computers?

Some alternatives to boson sampling



IQP (instantaneous quantum polynomial) circuits.

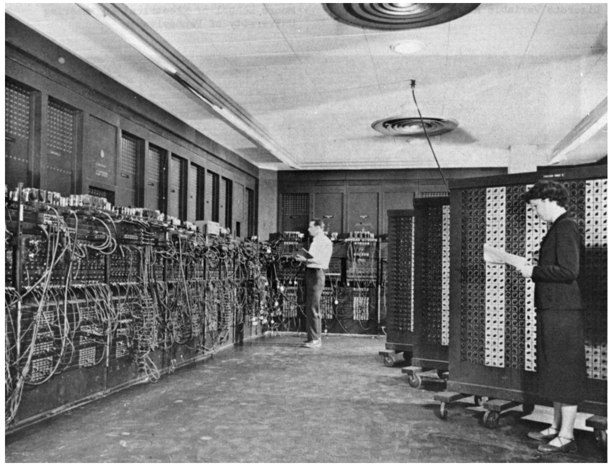


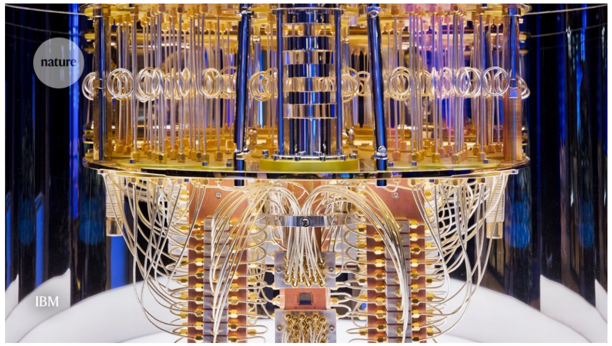
Chaotic quantum circuits (two-qubit gates are fixed whereas single-qubit gates are random)

Issue of IQP and Chaotic quantum circuits:
the quantum-classical separation is not robust against noise.

Concluding Remarks

- Quantum computers nowadays are just like classical computers in 1940-50.
- The “NISC” computers also had limited range of applications (e.g., in ballistics).
- In view of this, we expect full-fledged quantum computers to have revolutionary impacts!

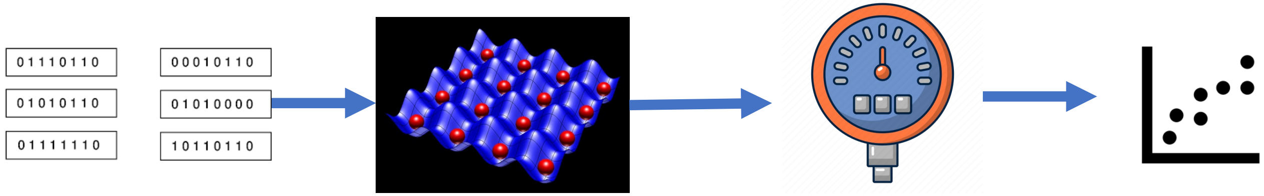




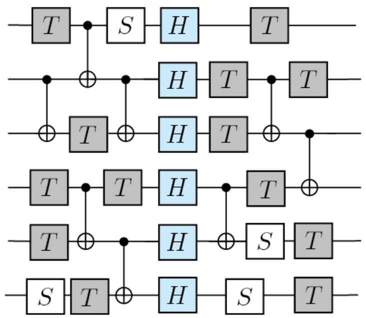
Part II:
Summary of the Course

Topic 1: Fundamentals of Quantum Computing

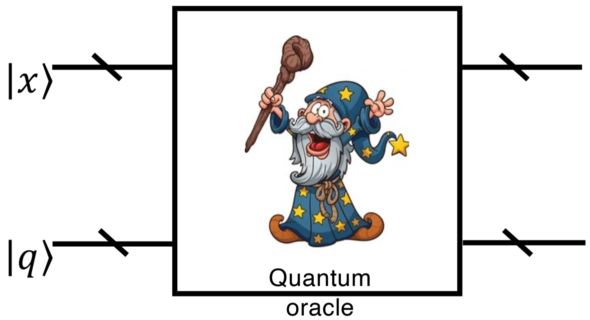
- States, gates, measurements.



- Universality.

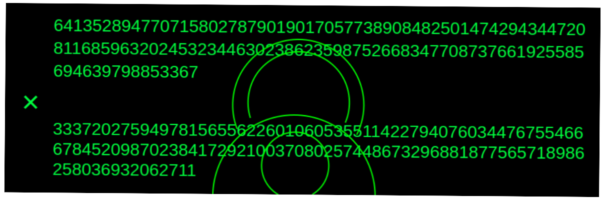


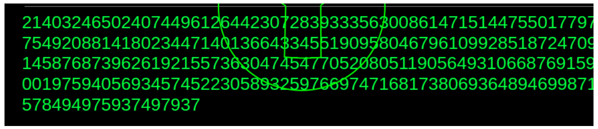
- Complexity & oracle model.



Topic 2: (post-FT) Quantum Algorithms

- QFT-based algorithms (exp. speedup): QPE, Shor, and HHL.





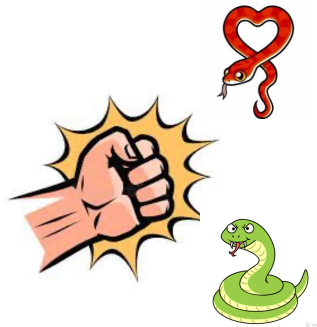
- QFT-independent algorithms: Grover

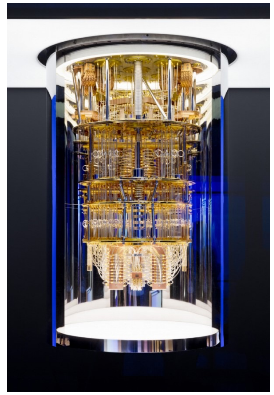
- Useful subroutines:

QFT, Hadamard transform, rejection sampling, uncomputation …

Topic 3: Realization of Quantum Computing

- Physical implementations: criteria for a good platform, NMR & Super-conducting platforms.

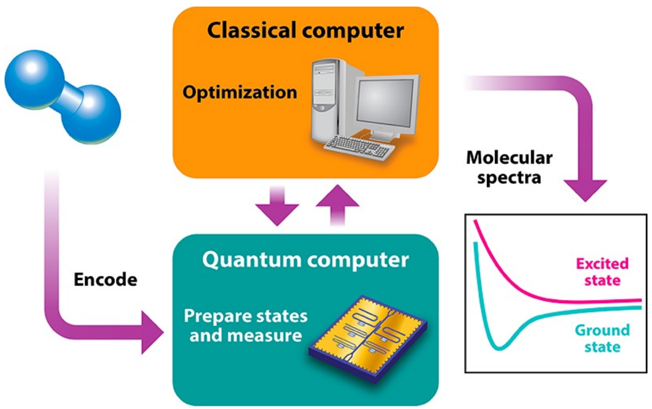


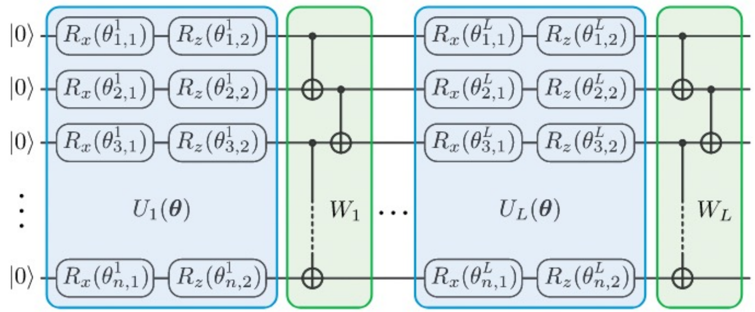


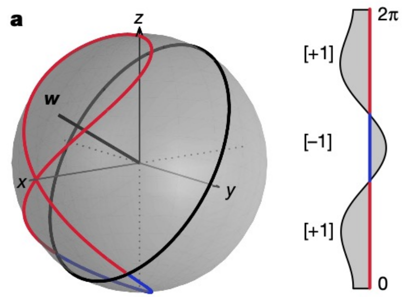
- Quantum error correction:
  the idea, syndrome detection, error types …
- Examples: repetition codes, Shor’s code, Steane code …
- Fault-tolerance: error propagation & threshold theorem.

Topic 4: NISQ Algorithms

- QAOA, VQE, and quantum chemistry:







- Quantum deep learning:

  quantum feature maps for classification, quantum autoencoder.

Part III:
Information on the final

Basic information

- 3 hours (December 22^{nd} 2:30-5:30 pm, Rm 103 Main Bldg.)
- Calculators: allowed;
  Cheat sheet: 1 A4 paper (both sides); other materials are not allowed.
- The exam will mainly focus on the first 3 topics, and the last topic (NISQ) will be tested at [O1] level.
  (Example: “Is the following statement true or false: QAOA does not require calculating any gradient.”)
- Complex algorithms (HHL, the full version of Shor) will only be tested at [O1] level.
- Bonus materials (those with *) will not be covered in the exam.

How to prepare

- Review all the course materials. Try the exercises therein.
- Review all assignments. Make sure you understand the solution.
- You can use the textbook “Quantum Computation and Quantum Information” for reference.
  You are welcome to try the exercises therein but be reminded that some of them are quite hard (so don’t get frustrated if you could not solve them).
- **Bonus consultation hours**: December 2nd (Tuesday) 10:00 – 12:00.
- Moodle forum & emails are welcome ~
  However, I will not be available from Dec. 13th to 21st

Levels of difficulty

- 40% of the questions are straightforward.
  (Like the examples in the next slides or slightly harder.)

- 40% of the questions have similar level of difficulty as those in Assignments 1-3.

- 20% of the questions (for the purpose of a tie-breaker for A) are relatively hard.

[01] Concepts & Knowledge

- Example 1:
  The 2-qubit quantum computer used in our course can run a quantum algorithm to factorize a large number, true or false?

- Example 2:
  Is $|\psi\rangle = (\frac{1}{2})(|00\rangle + |11\rangle)$ a quantum state? Justify your answer.

- Example 3:
  (True or False) Quantum supremacy was first demonstrated on an NMR quantum computing platform.

[02] Problem solving

- Example:
  Consider a qutrit (3-dimensional quantum) system with basis $\{|0\rangle, |1\rangle, |2\rangle\}$ and a quantum gate $U = |0\rangle\langle 1| + |1\rangle\langle 2| + |2\rangle\langle 0|$. Suppose the qutrit was initially in the Fourier basis $|e_1\rangle$ and then went through U. What is the probability of getting $|e_1\rangle$ if we measure it in the Fourier basis?

[03] Algorithm design

- Example:
  A 2-bit function $f: \{0,1\}^2 \to \{0,1\}$ is either balanced or constant.
  Design a quantum algorithm that tells these two cases apart using only 1 query to the oracle $O_f|x\rangle|a\rangle = |x\rangle|a \oplus f(x)\rangle$.

- Remarks: You should provide the concrete procedure
  (e.g., step 1: prepare the input register in $|00\rangle$ and the ancilla in $|1\rangle$,
  step 2: perform the Hadamard transform on both registers etc.)

- *The questions in the exam may concern algorithms that are variants of what we learned in the lectures; so be a bit more flexible.*

Tips

- **Be reminded to come to the exam!**

- Focus on mastering the basics.
  Bonus contents are not needed in the exam.

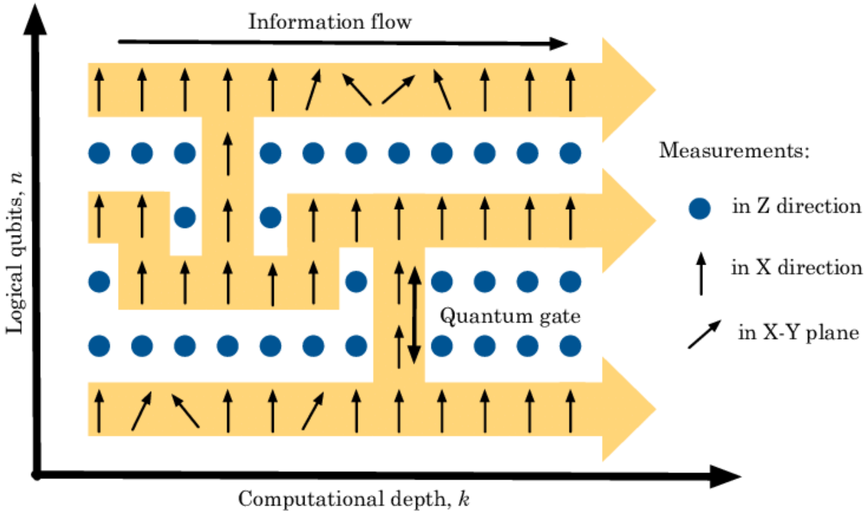
- You will be rewarded for attending most of the lectures.

- The solutions to most questions are quite short.

- Attempt all questions.
  But don’t spend too much time on a single question! If you find a question hard, try it after you finished the easier ones.

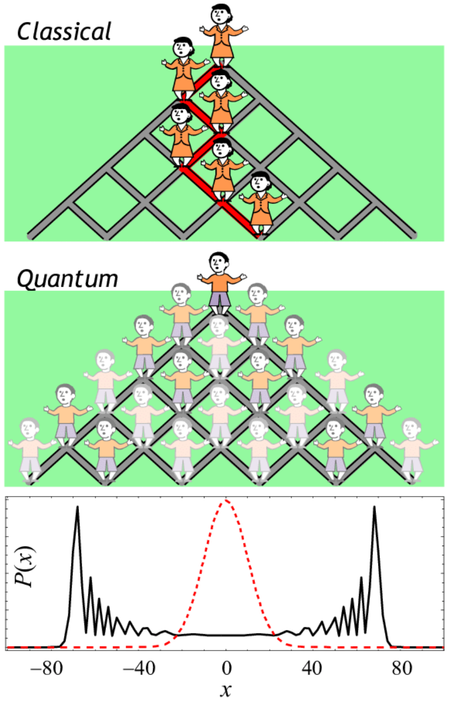
Part IV:
Beyond COMP3366

Other Models of Computing & Algorithms

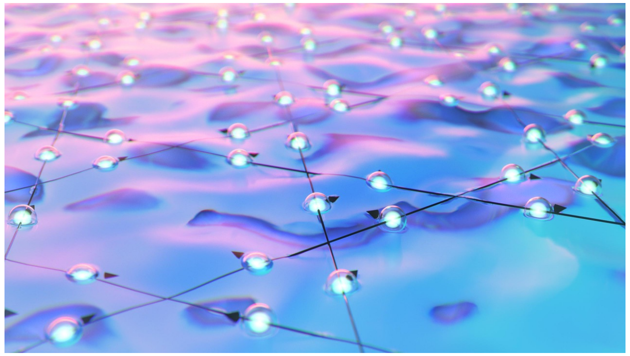


One-way quantum computers, or
measurement-based quantum computers (MBQCs)

Adiabatic quantum computing

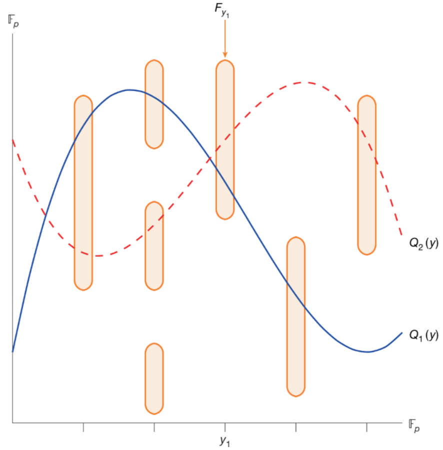


Quantum walk
(fig: Manouchehri, Wang,'18)



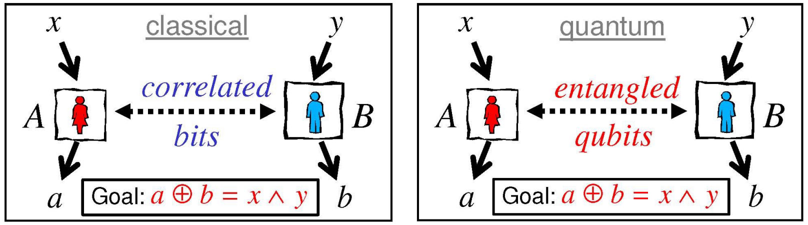
New candidates for exp. advantage
e.g., Decoded Quantum Interferometry
(Nature 646, 831 (2025))

Quantum simulation

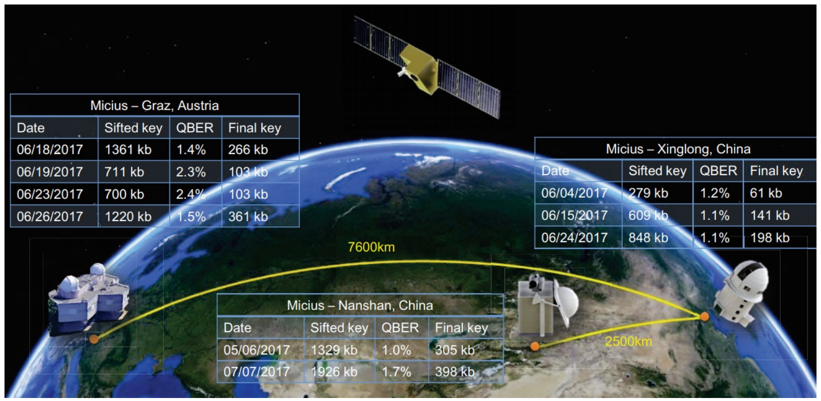


Quantum Communication & Cryptography

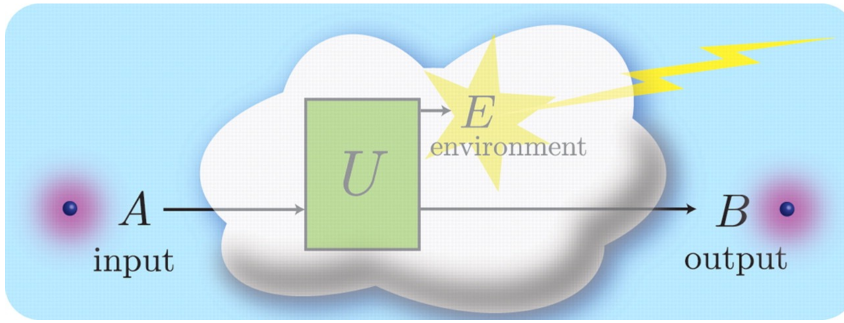
Samsung phones use quantum random number generators to enhance its security.



Bell test and nonlocality (its verification won Nobel Prize in Physics 2022)



Secure communication networks
via quantum key distribution



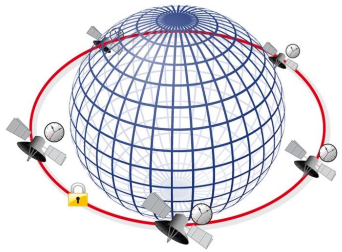
Quantum Shannon theory
(theory on noisy quantum gates and states:
density matrices & quantum channels)

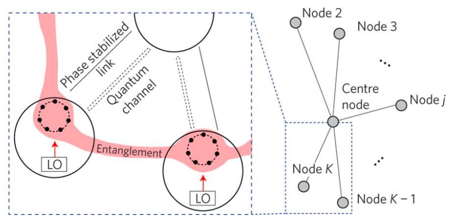
Some of the contents will be covered by COMP3316.
You may take it if you are interested ~

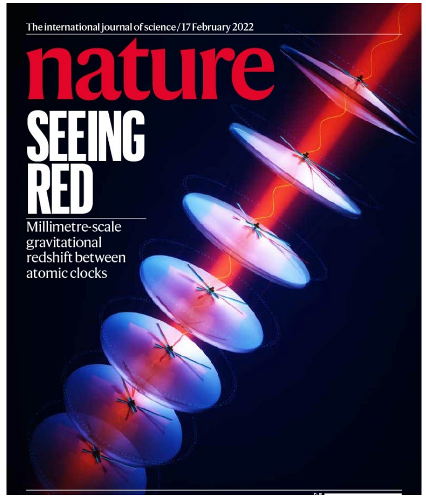
Quantum Sensing

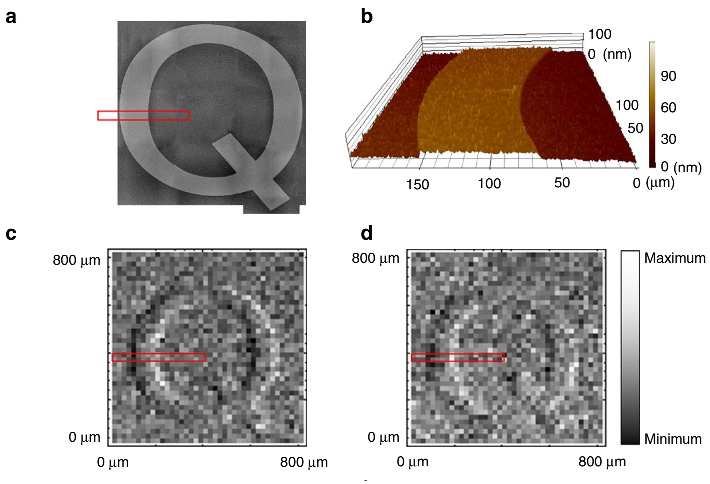
(my main research direction)

Quantum clocks and sensor networks



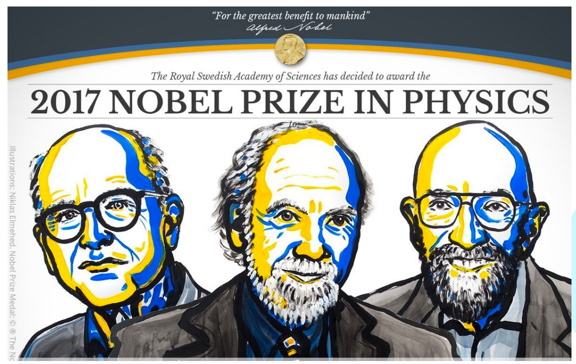


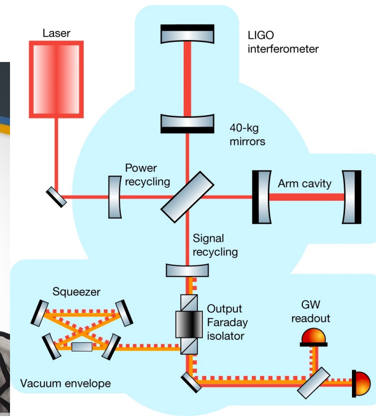




Quantum microscopes

Gravitational wave detection
(Nobel prize awarded to founders of LIGO)





Research opportunities

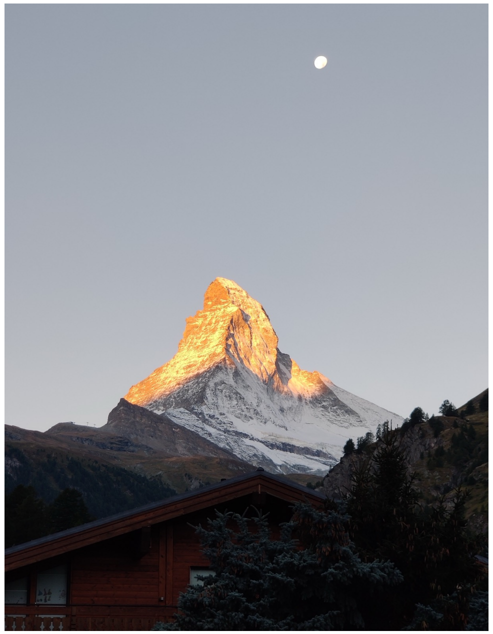
- I'd be glad to supervise research projects & FYP in quantum sensing and its connection with quantum computing & information theory.

- I'd also be recruiting PhDs every year.

- More information & news on https://yangyx09.github.io.

- Feel free to contact me (yuxiang@cs.hku.hk) if you are interested ;-)

That's all! Thanks for the journey ;-)



Any question?