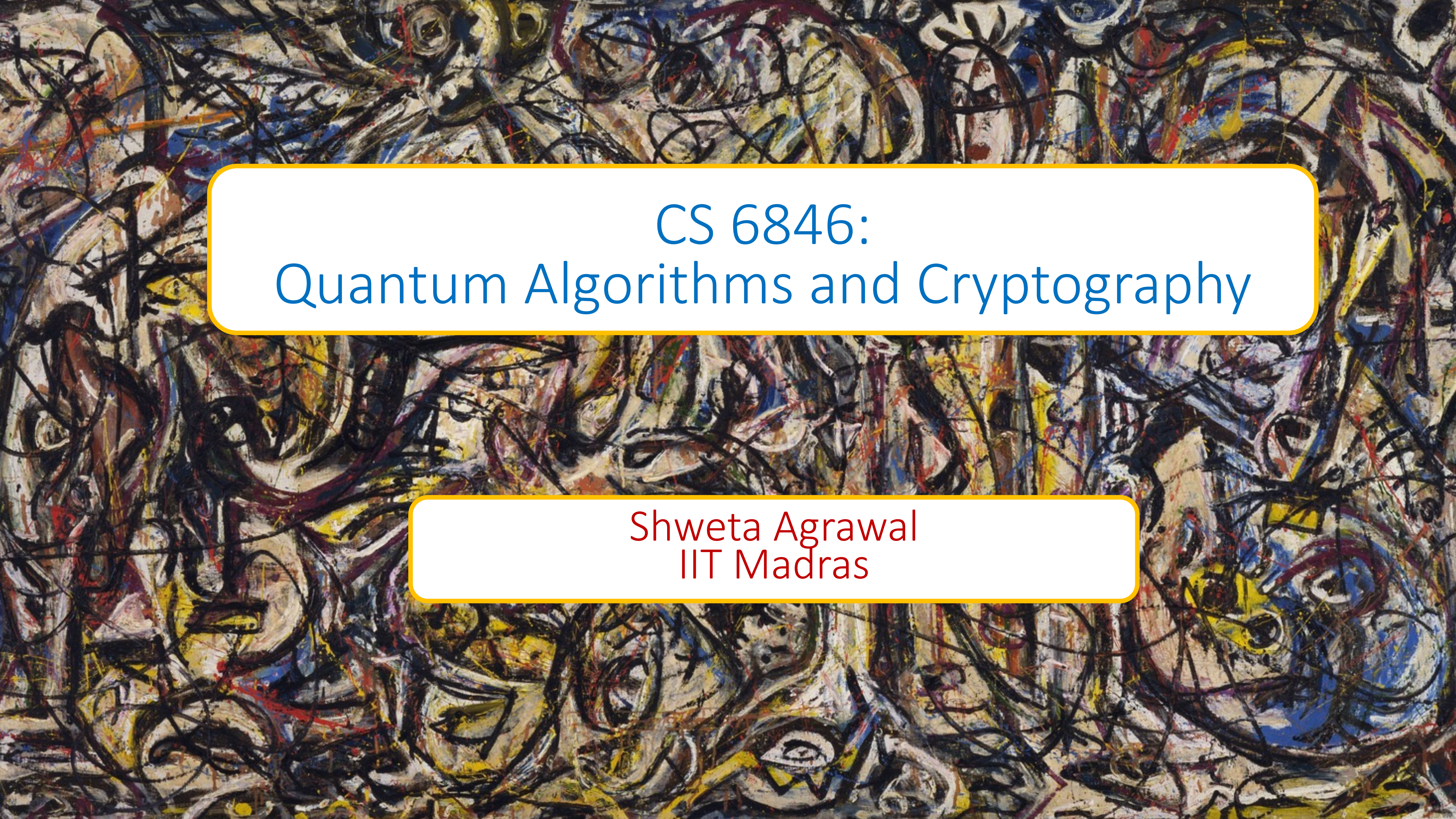
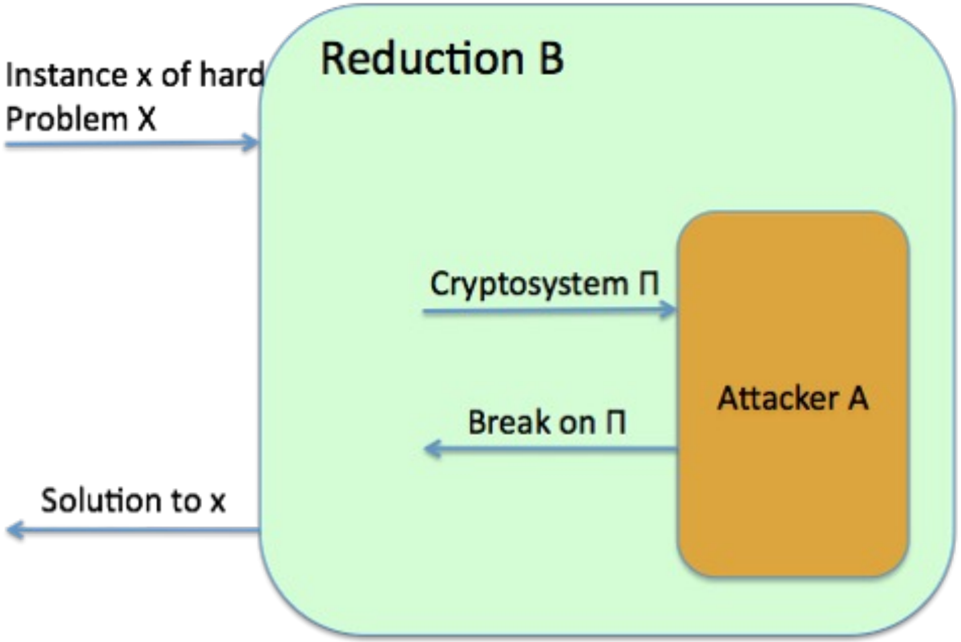


CS 6846: Quantum Algorithms and Cryptography

Shweta Agrawal
IIT Madras

Cryptography

Cryptography guarantees that breaking a cryptosystem is at least as hard as solving some difficult mathematical problem.



Difficult for who?

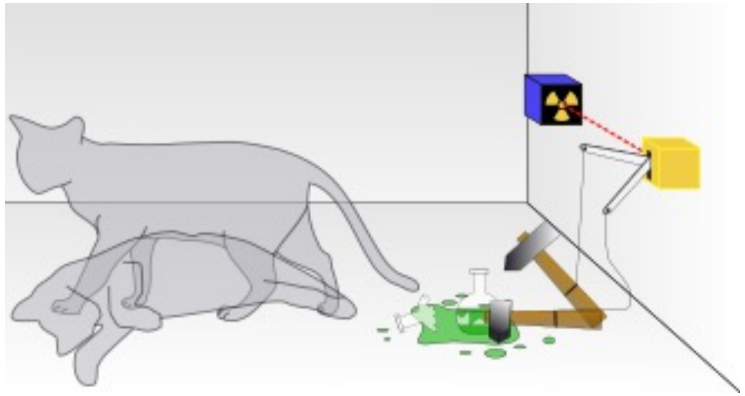
The Cryptographic Adversary

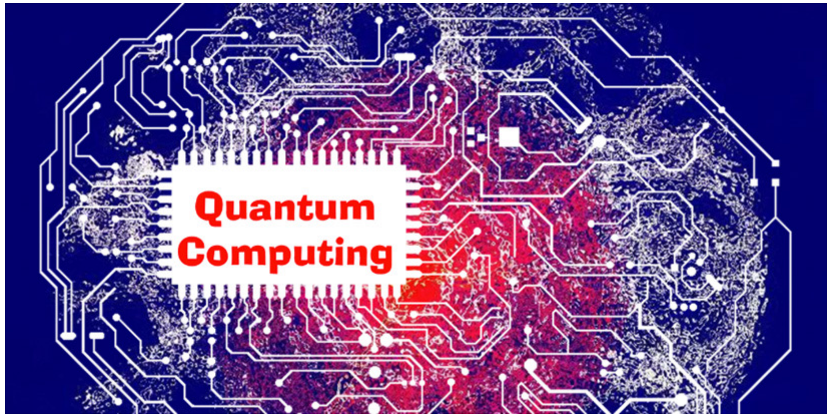
- Adversary in cryptography normally modeled by a classical computer.
- Typical guarantee is that unless the adversary can solve hard problem, attack takes more than age of universe (in CPU cycles)
- Robust to type of computer (mobile/laptop/supercomputer)
- What if the attacker is quantum?

Quantum Computers

Fundamentally New Paradigm of Computing!

- Computers that use laws of quantum rather than classical physics
- May allow exponential speedups
- Most current day cryptography relies on hardness of factoring, discrete log: **broken** if quantum computers are realized

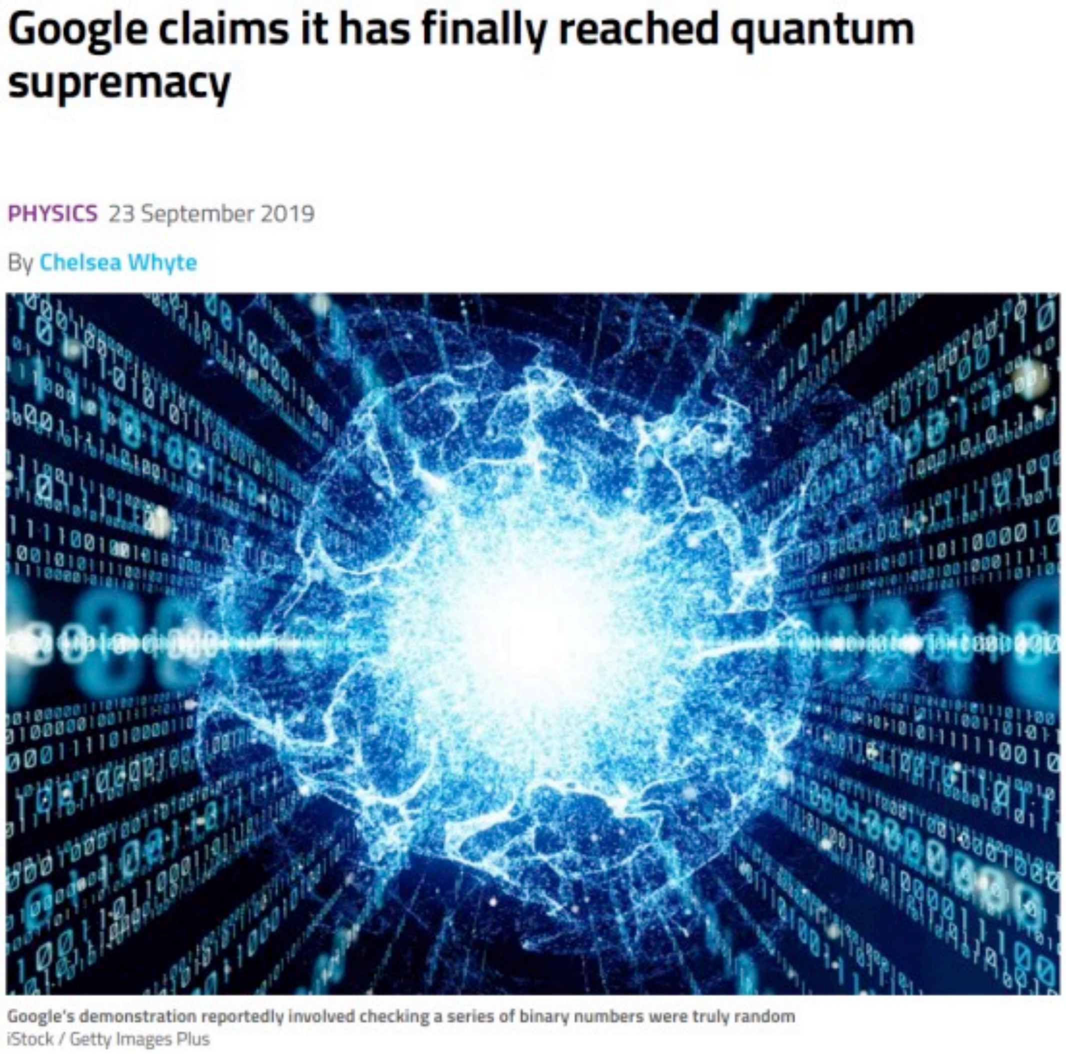




Is this threat real?

In short: YES!

- National Institute of Standards and Technology (NIST), initiated a process to solicit, evaluate, and standardize quantum-resistant public-key crypto
- Significant global research effort



Google claims it has finally reached quantum supremacy

PHYSICS 23 September 2019

By Chelsea Whyte

Google's demonstration reportedly involved checking a series of binary numbers were truly random
iStock / Getty Images Plus

In this course

- Foundations of Quantum Computation:
  - Mathematical Model for Quantum Mechanics, Quantum gates and quantum computing, quantum algorithms, Grover's algorithm, Shor's algorithm.
- Lattice Based Cryptography:
  - Public key encryption, Signatures, Classical Fully Homomorphic encryption
- Topics in Quantum Cryptography:
  - Quantum Random Oracle Model, Quantum Rewinding, Quantum Fully Homomorphic encryption

Foundations of Quantum Computation

- Church-Turing Thesis
  - Any reasonable model of computation can be simulated using a Turing Machine.

- Extended or strong Church-Turing Thesis
  - Any reasonable model of computation can be simulated efficiently using a Turing Machine.
  - Upto polynomial reductions
  - Read Wiki page

What about quantum mechanical processes? Can they be simulated efficiently by Turing Machines?

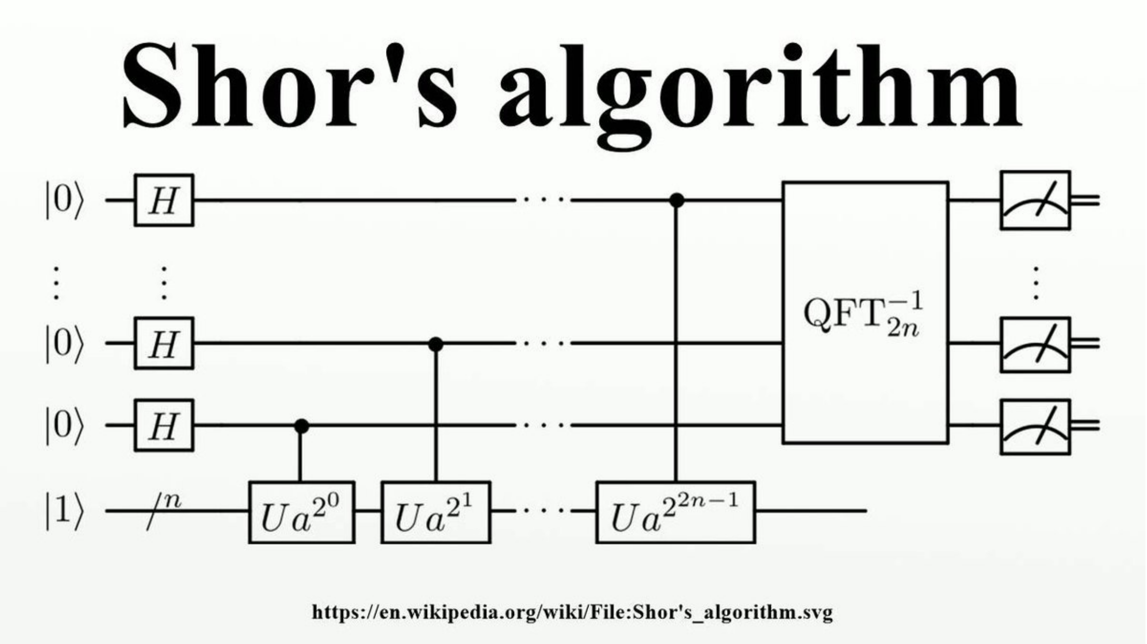
Foundations of Quantum Computation

What about quantum mechanical processes? Can they be simulated efficiently by Turing Machines?

- There are examples where this is not known.
- There are efficient quantum algorithms that perform tasks that do not have (known) efficient classical algorithms.
    - These efficient quantum algorithms break modern day cryptography
    - Factoring, discrete log, bilinear maps
- Thus, quantum computation may be a potential counterexample to the extended Church-Turing Thesis.

Foundations of Quantum Computation

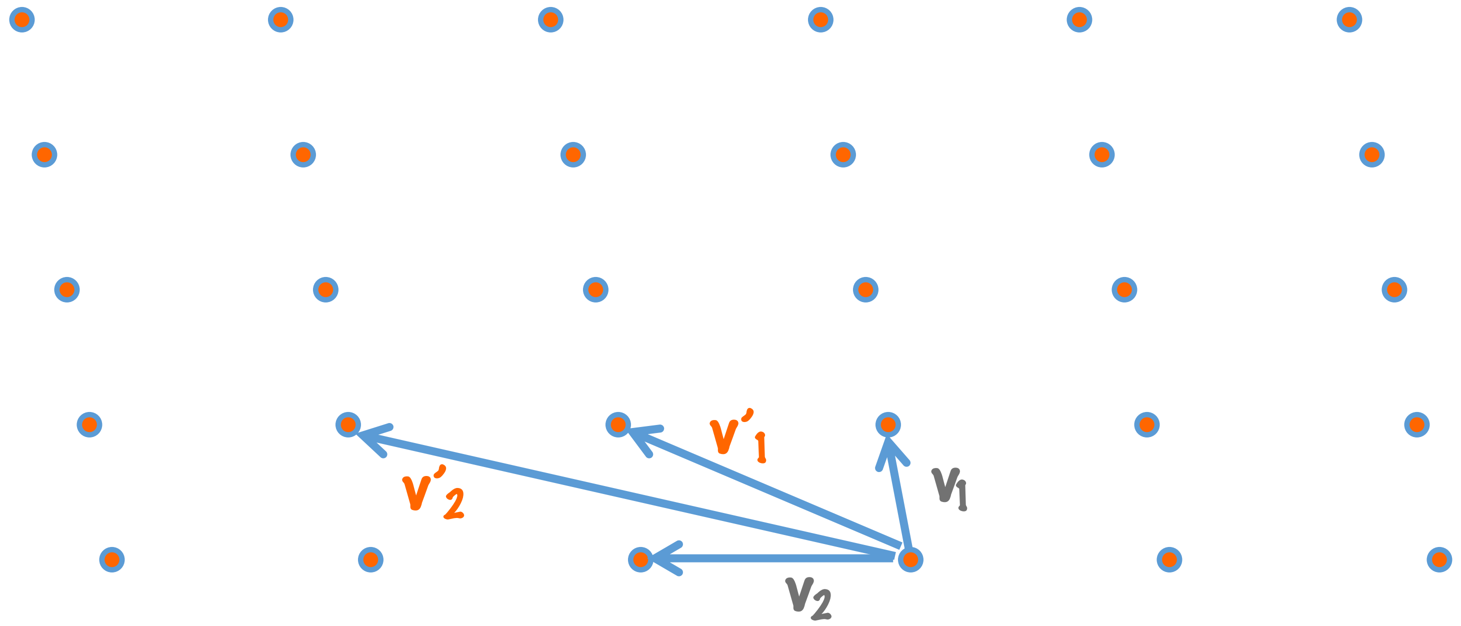
- We will study a mathematical model for representing quantum computation
- Quantum circuits, quantum gates, quantum algorithms
- Speedups over classical algorithms
- Culminate with Shor’s algorithm which breaks RSA, DLOG etc


Shor's algorithm

https://en.wikipedia.org/wiki/File:Shor's_algorithm.svg

Lattice Based Cryptography

- Base hardness on mathematical problems for which quantum computers offer no advantage
- Most promising: problems in high dimensional lattices.

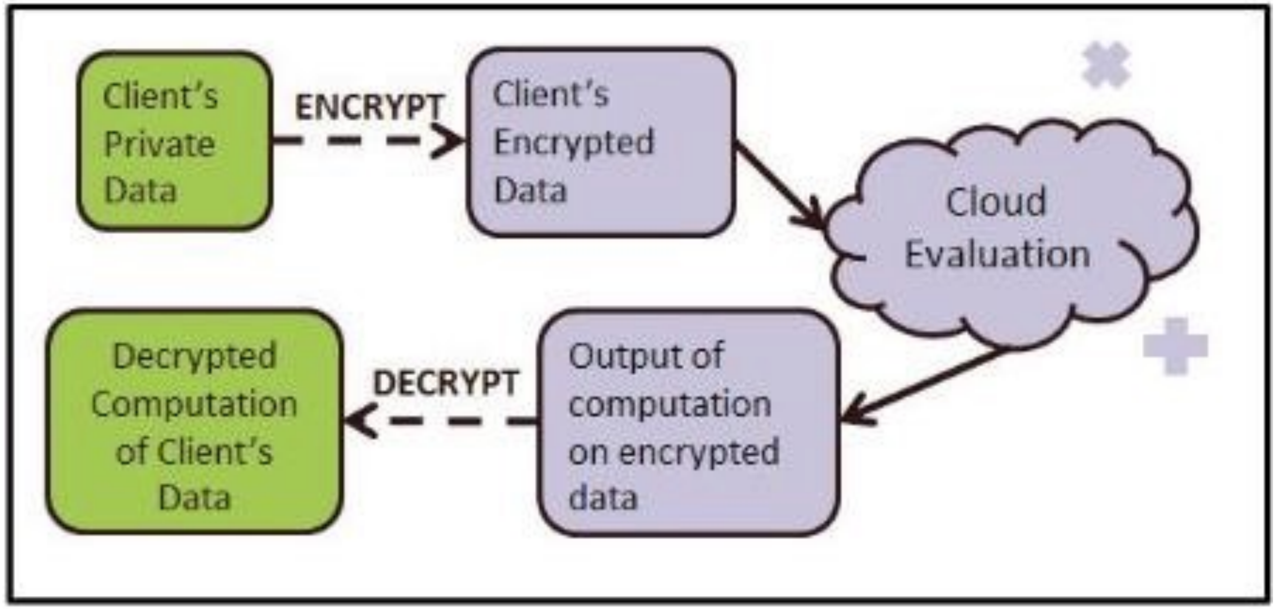


Discrete subgroup in R^n

Hard: Shortest Vector Problem

Lattice Based Cryptography

- What useful cryptography can we do from lattices?
- Turns out – a lot!
- Best example: fully homomorphic encryption



Client's Private Data

ENCRYPT

Client's Encrypted Data

Cloud Evaluation

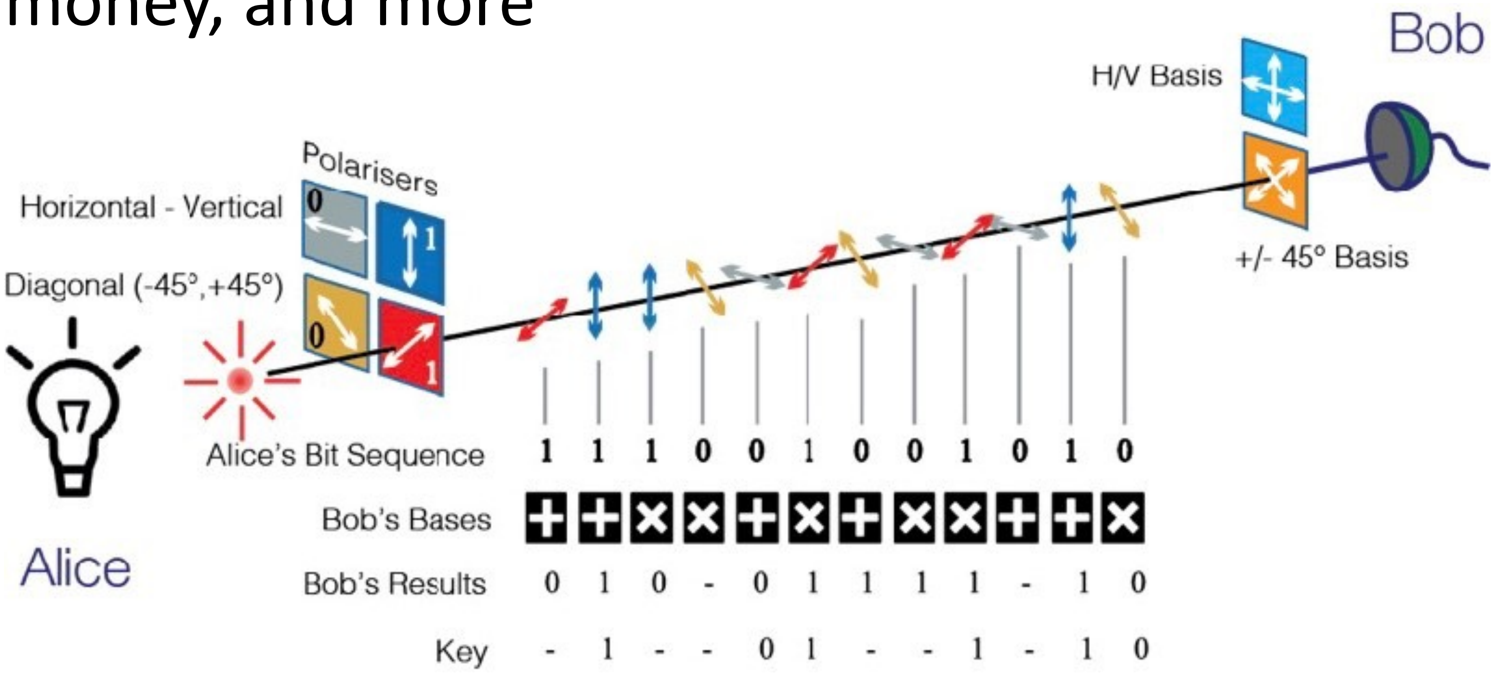
Output of computation on encrypted data

DECRYPT

Decrypted Computation of Client's Data

Topics in Quantum Cryptography

- Quantum Random Oracle Model, Quantum Rewinding
- Quantum Fully Homomorphic Encryption
- Protocols using quantum physics, such as quantum key distribution, quantum money, and more



Alice's Bit Sequence	1	1	1	0	0	1	0	0	1	0	1	0
Bob's Bases	+	+	×	×	+	×	+	×	×	+	+	×
Bob's Results	0	1	0	-	0	1	1	1	1	-	1	0
Key	-	1	-	-	0	1	-	-	1	-	1	0

Image Reference: Quantum Flagship, qt.eu

Resources

- Main Reference: UIUC and Princeton lecture notes on Quantum Cryptography
- Other lecture notes from the internet (see webpage)
- No text book required
- Questions?

Requirements

- Class Participation: 10%
- Scribe notes (beyond class material): 10%
- Project and class presentation : 50%
- Assignments : 30%

Collaboration is encouraged but you must write up solutions on your own. You must also write the names of all the people you discussed the problem with. In case you find material that will help you in solving some problems, you should mention the source in your writeup. Class participation will also be taken into account when assigning grades.

I expect all students to behave according to the highest ethical standards. Any cheating or dishonesty of any nature will result in disciplinary action.

Other Admin

- Schedule Change: Choose alternate times for Wed and Fri.
- Mailing list
- Teaching Assistants: Anshu Yadav, Anuja Modi
- Questions?