QUANTUM COMPUTING & CRYPTO: HYPE VS. REALITY

ABHISHEK PARAKH
UNIVERSITY OF NEBRASKA AT OMAHA

QUANTUM COMPUTING: I CAN SUM IT UP IN ONE SLIDE

Pure Magic!

SERIOUSLY: HOW DOES IT WORK?

- That's simple: Even Justin Trudeau knows it!
- It works by harnessing the quantum phenomenon where
  - Particles can be in multiple states at the same time
  - Multiple *places* at the same time
  - "Looking" at (reading the state) will change the state
  - Nothing is really under control – including the states and read-outs
  - No one knows if a quantum algorithm when run will give the correct output (probabilistic)
  - But it works

LET’S TRY THIS AGAIN: HOW DOES IT WORK?

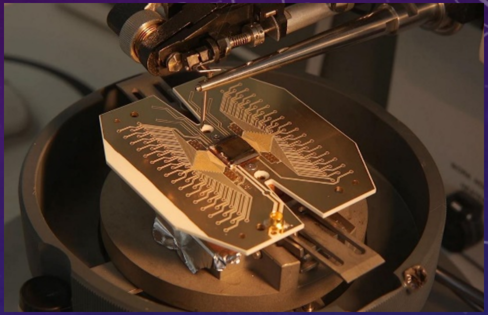
Honestly, no one really “understands” QM!

HOW CAN SCIENTISTS ACCEPT SUCH A THING?

- That’s the toughest part – most engineers/scientists cannot accept not understanding the underlying systems that they are working with
  - So most don’t care for quantum computing and that’s perfectly fine!
- The smart ones, however, avoid asking the tough questions
  - It is how it is – tell me how can I make money off of this!

LET'S GET TO IT THEN

- Quantum computing: analogue computing based on principles of quantum mechanics



- Quantum cryptography: uses photons as quantum particles to achieve secure key distribution over insecure public channels

- Contrary to common thinking, these are completely different from each other
    - Hardly anything common between them in terms of implementation/technology used
    - Quantum computing is in its early stages
    - Quantum cryptography is mature enough - buy off-the-shelf

QUANTUM COMPUTING NEWS IN LAST WEEK

- China’s new quantum computing device built inside a diamond
  - Factor 35 into 5 and 7
- Computerworld: It’s time to decide how quantum computing will help your business
  - Planning must start right now: 5-10 years away
- Phys.org: New materials bring quantum computing closer to reality
- Trendintech.com: Quantum computers sound great but who will program them
- Singularityhub.com: Quantum computing demands a whole new kind of programmer
- Wired.com: The bizarre quantum test that could keep your data secure
- Trendintech.com: Europe takes quantum computing to the next level with this billion euro project

LET'S FIRST TALK ABOUT QUANTUM COMPUTING

- Quantum mechanics was born in early 20th century
  - An attempt to make sense of experimental observations
  - Most famous is the Young's double slit experiment – one particle appears to be in multiple places at the same time
  - Einstein famously disliked quantum mechanics
  - In an attempt to prove it wrong, he published the famous paper on EPR pairs
    - Also known as Entangled particles
    - Two particles separated by infinite amount of distance can be entangled – a interaction with one will instantaneously change the other
    - Goes against theory of relativity: nothing can travel faster than speed of light
- Max Born, Heisenberg, Pauli: coined the term quantum mechanics circa 1924
- Schrodinger, Dirac, etc.
- Quantum computing: The idea mainly originated in 1980s paper by Feynman

TIMELINE (INTERSPERSED WITH CRYPTO)

- Quantum cryptography arguably started around 1970s
- 1970: Stephen Wiesner tried to publish a paper on unclonable electronic money
- 1973: Bennett provided a model for reversible Turing machine
- 1980-82: Paul Benioff developed the quantum Turing machine that does not dissipate any energy
- 1982: Feynman said we should build a quantum computer
- 1982: No-cloning theorem introduced
- 1984: Bennett and Brassard developed the first quantum cryptography protocol that provides unconditional security
- 1985: Deutsch gave a model for universal quantum computer

TIMELINE CONTINUED

- 1993: Quantum teleportation introduced
- 1992 (Bang!): Deutsch introduced the first quantum algorithm that is faster than classical algorithms
- 1994: Shor introduced a factoring algorithm that would destroy modern public-key cryptography
- 1995: Shor developed a 9-qubit quantum error correcting code
- 1996: Quantum search algorithm by Grover
- New decision algorithms and Quantum Artificial Intelligence
- Immense progress in the area of quantum information theory

QUANTUM COMPUTING: WHAT MADE IF FAMOUS

- Factorization in log n steps rather than $n^{1/2}$ steps [Shor]

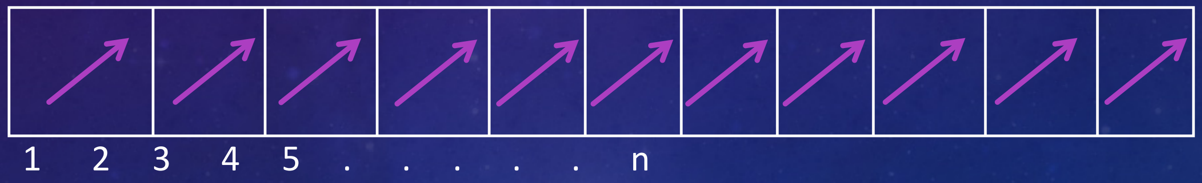
- Database search in $n^{1/2}$ rather than n steps [Grover]

QUANTUM PRIMITIVES

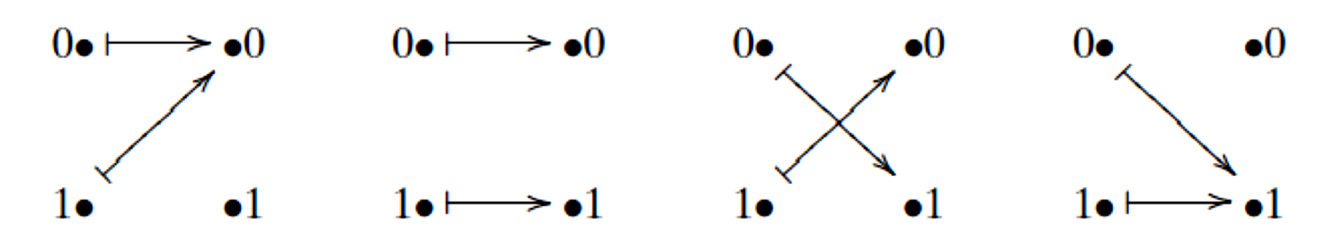
- Superposition
- Collapse upon measurement
- Deterministic evolution (*Schrödinger equation*)
- No cloning of an unknown state
- Counter-intuitive behavior of objects
- New quantum information science

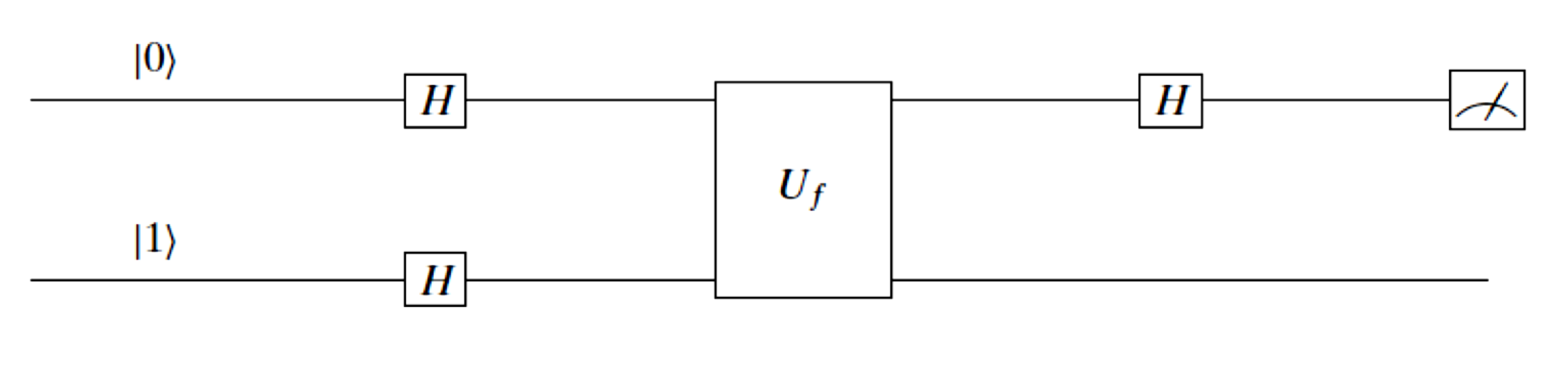
WHAT MAKES QUANTUM COMPUTERS SO POWERFUL: QUANTUM REGISTER IN SUPERPOSITION

Each cell has a qubit. Number of states is 2^n

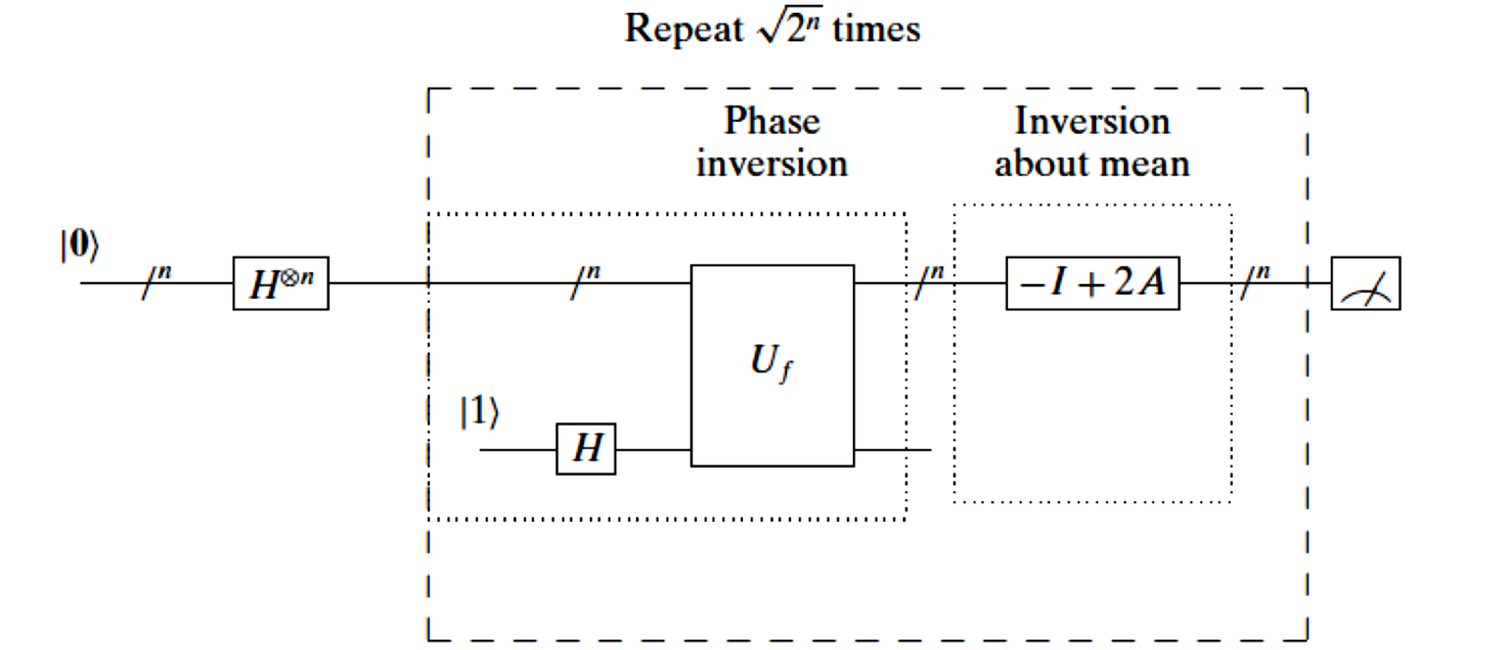


DEUTSCH'S ALGORITHM

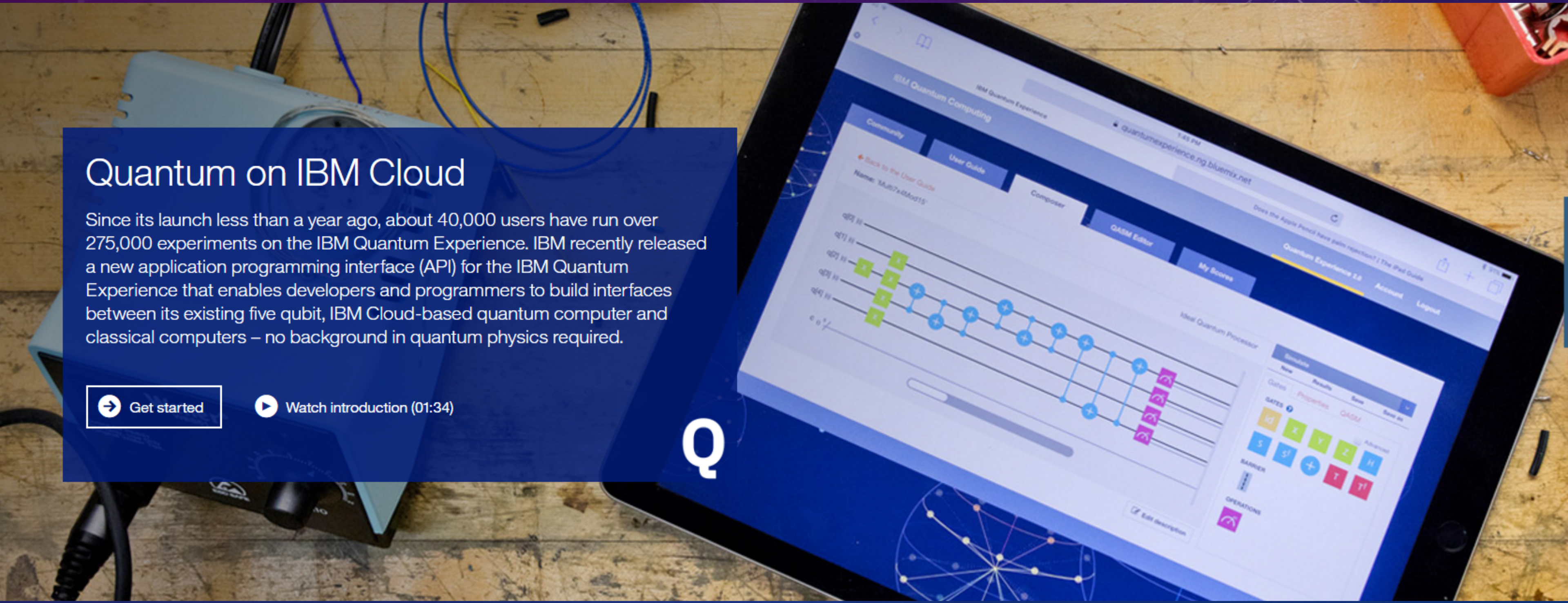




GROVER'S SEARCH ALGORITHM: UNSORTED DATABASE



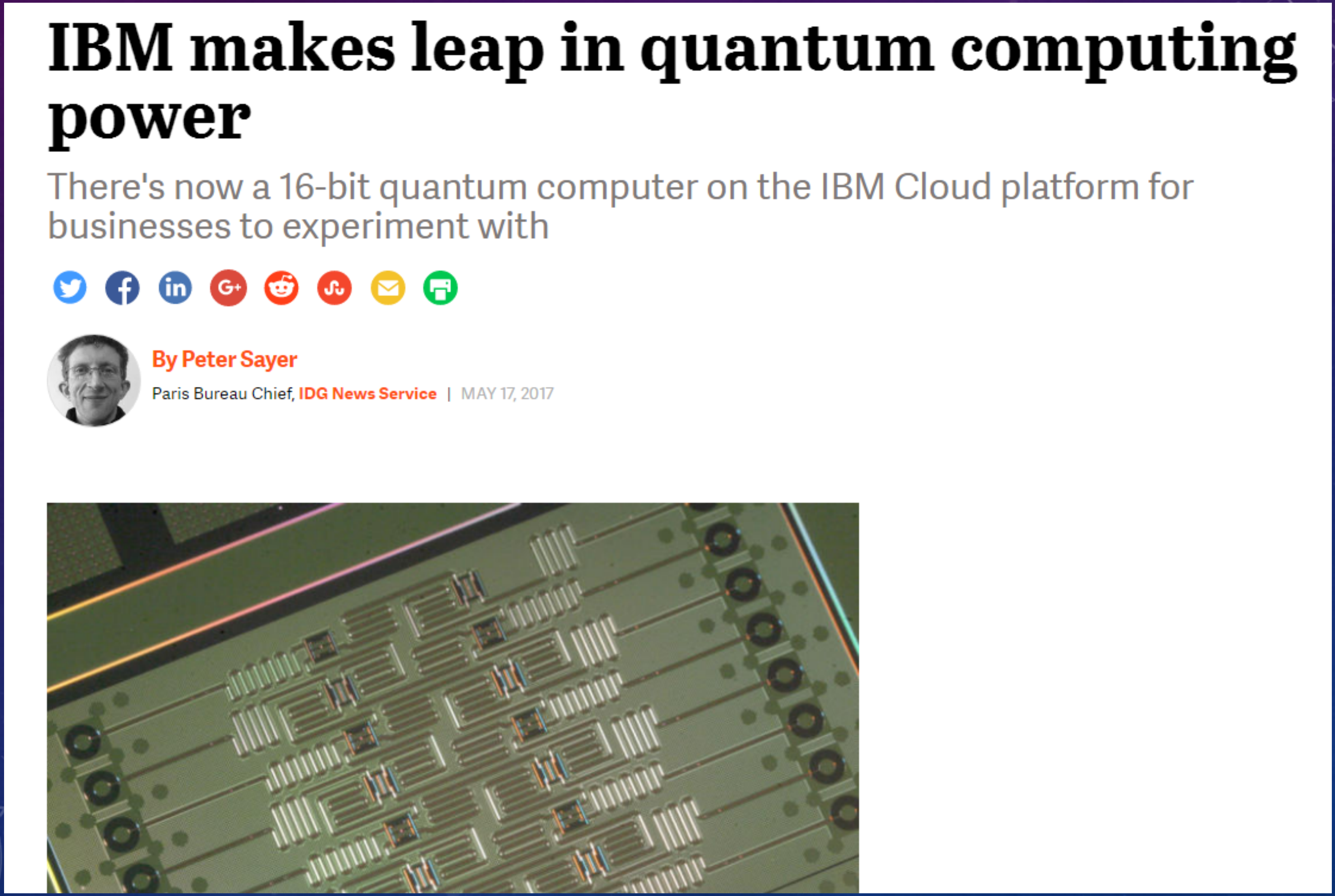
IBM QUANTUM COMPUTER: A 5-QUBIT COMPUTER



Quantum on IBM Cloud

Since its launch less than a year ago, about 40,000 users have run over 275,000 experiments on the IBM Quantum Experience. IBM recently released a new application programming interface (API) for the IBM Quantum Experience that enables developers and programmers to build interfaces between its existing five qubit, IBM Cloud-based quantum computer and classical computers – no background in quantum physics required.

BREAKING NEWS: THIS MORNING
IS THIS MOORE’S LAW IN EXPONENTIAL FORM?



IBM makes leap in quantum computing power

There's now a 16-bit quantum computer on the IBM Cloud platform for businesses to experiment with

By Peter Sayer

Paris Bureau Chief, IDG News Service | MAY 17, 2017

OTHER COMPANIES

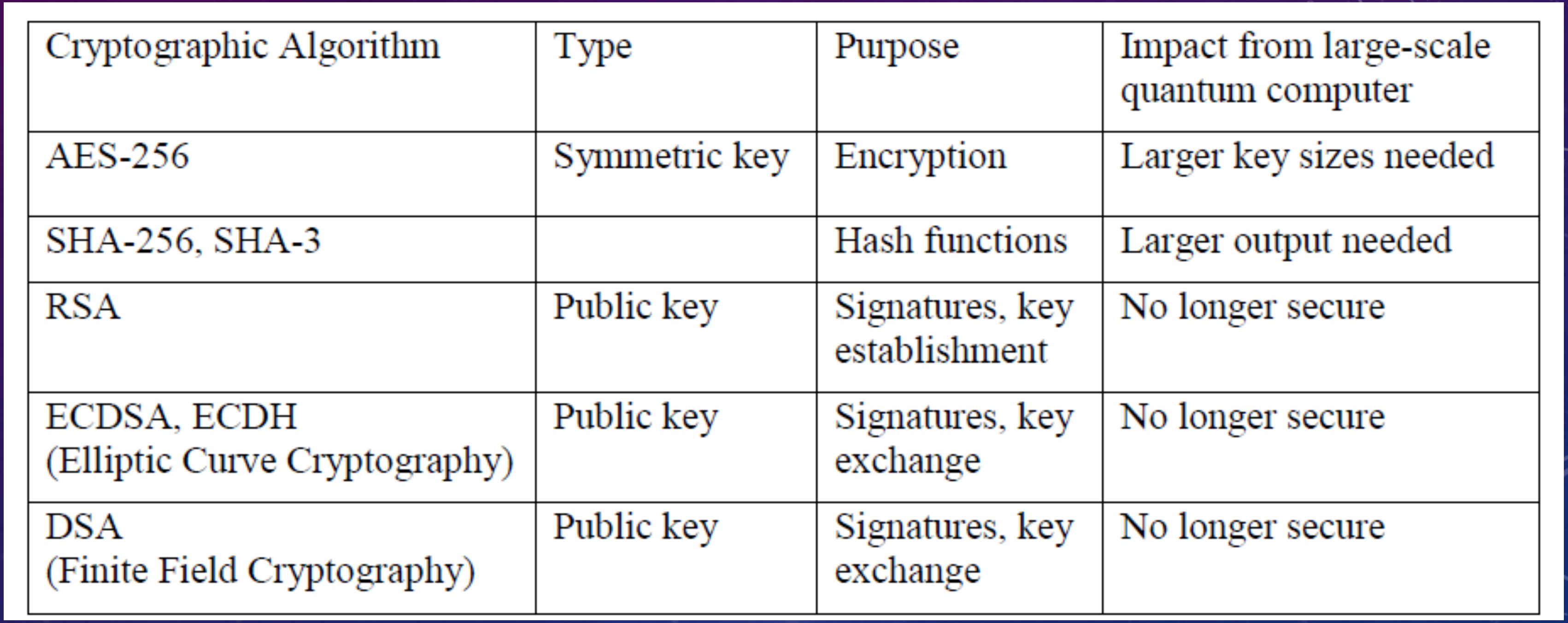
- Google's quantum computer: https://www.technologyreview.com/s/544421/googles-quantum-dream-machine/
  - Google's project estimates that Martinis's group can make a quantum annealer with 100 qubits as soon as 2017 – haven't heard anything yet

- https://en.wikipedia.org/wiki/List_of_Companies_involved_in_Quantum_Computing_or_Communication

DWAVE: WHAT APPLICATIONS IS IT CURRENTLY BEING USED FOR?

- Good to break widely used crypto (potentially)
- Modeling quantum mechanical processes: behavior of atoms/particles
- Optimization problems (D-Wave)
- Radiotherapy optimization
- Protein Folding
- Water Network Optimization
- Machine learning
- Object Detection
- Labeling News Stories
- Video Compression
- Monte-Carlo Simulation

QUANTUM COMPUTING IMPACT ON CRYPTOGRAPHY



Cryptographic Algorithm	Type	Purpose	Impact from large-scale quantum computer
AES-256	Symmetric key	Encryption	Larger key sizes needed
SHA-256, SHA-3		Hash functions	Larger output needed
RSA	Public key	Signatures, key establishment	No longer secure
ECDSA, ECDH (Elliptic Curve Cryptography)	Public key	Signatures, key exchange	No longer secure
DSA (Finite Field Cryptography)	Public key	Signatures, key exchange	No longer secure

NIST Timeline:

Fall 2016 – formal Call for Proposals

Nov 2017 – Deadline for submissions

3-5 years – Analysis Phase

2 years later – Draft standards ready

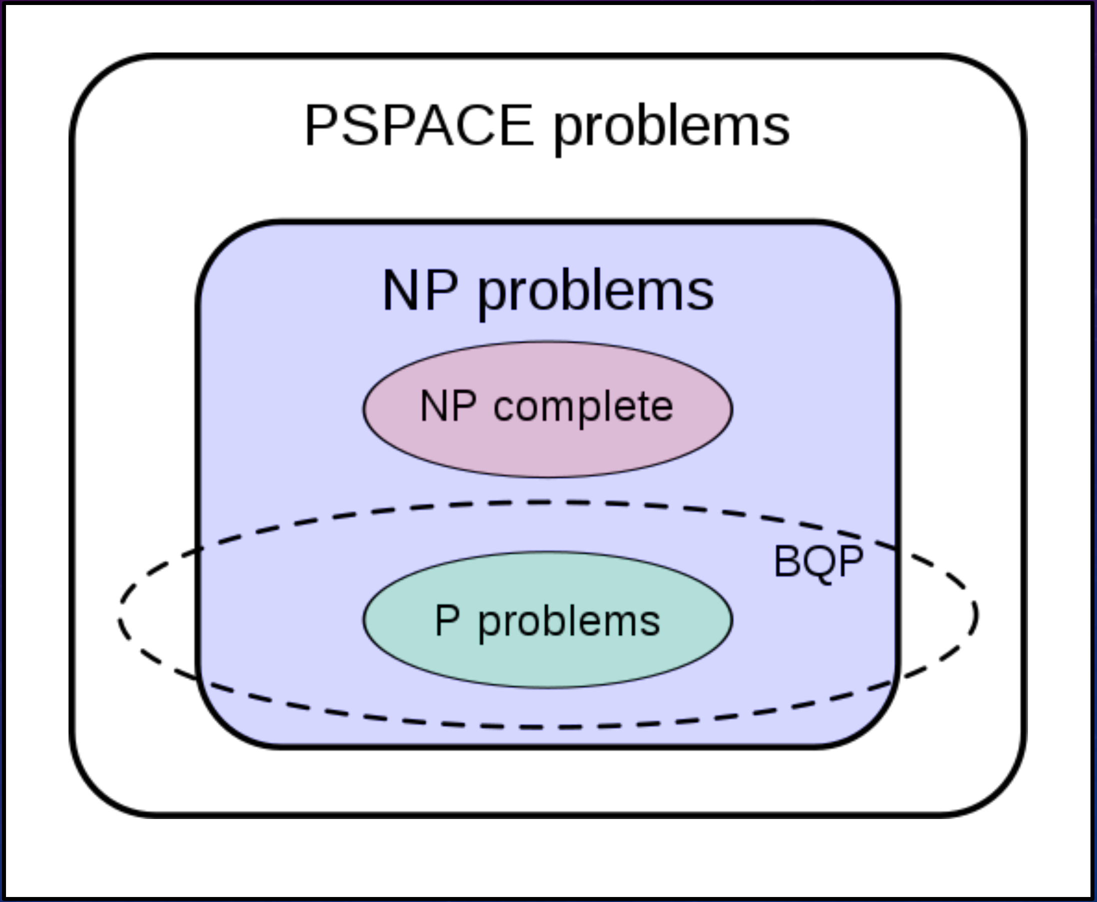
CRYPTOGRAPHY IN A QUANTUM WORLD

- Quantum Cryptography – we'll discuss this next
- Classical Cryptography believed to be resistant to Quantum Attacks
  - Lattice-based crypto
  - Multivariate polynomials based crypto
  - Hash-based crypto
  - Error-correction code based crypto
  - Supersingular elliptic curve isogeny crypto
  - Several other candidates…

WHICH ONE SHOULD WE ADOPT?

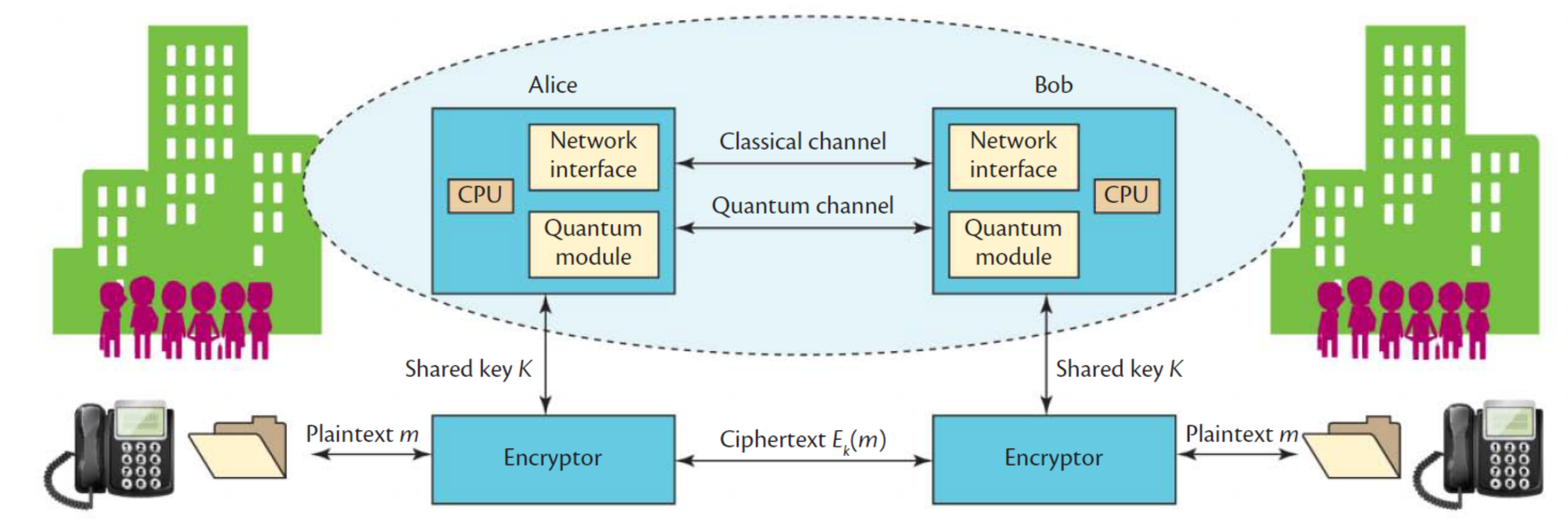
- NIST is playing it safe
  - There are already classical systems deployed and hence does not want to take the leap to quantum crypto
  - New classical algorithm don’t have security proofs either
  - There may be another quantum computing algorithm discovered tomorrow that may break them
  - For us unfortunately – it is what it is
- Once there are quantum computers, it is natural to phase out classical cryptographic algorithms
  - Maybe this will become a fall back

QUANTUM COMPUTING: AT PRESENT NO ONE KNOWS HOW POWERFUL THEY ARE



QUANTUM CRYPTOGRAPHY

- Replace public key encryption systems
  - Therefore provides a way to exchange encryption keys



QUANTUM CRYPTOGRAPHY: OTHER APPLICATIONS

- Quantum random number generator
- Quantum secret sharing: key management
- Semi quantum communication: one side quantum other classical
- Quantum teleportation
- Secure direct communication
- Position based quantum cryptography
- Superdense coding

THERE IS A LOT THAT QUANTUM CRYPTO CANNOT DO

- What it does, it does with perfect secrecy but there is a lot that it cannot do

- Bit commitment protocols (online gambling)
- Secure multiparty computations
  - No homomorphic encryption
- Cannot work over large distances
- Does not solve the authentication problem

PHYSICAL IMPLEMENTATIONS

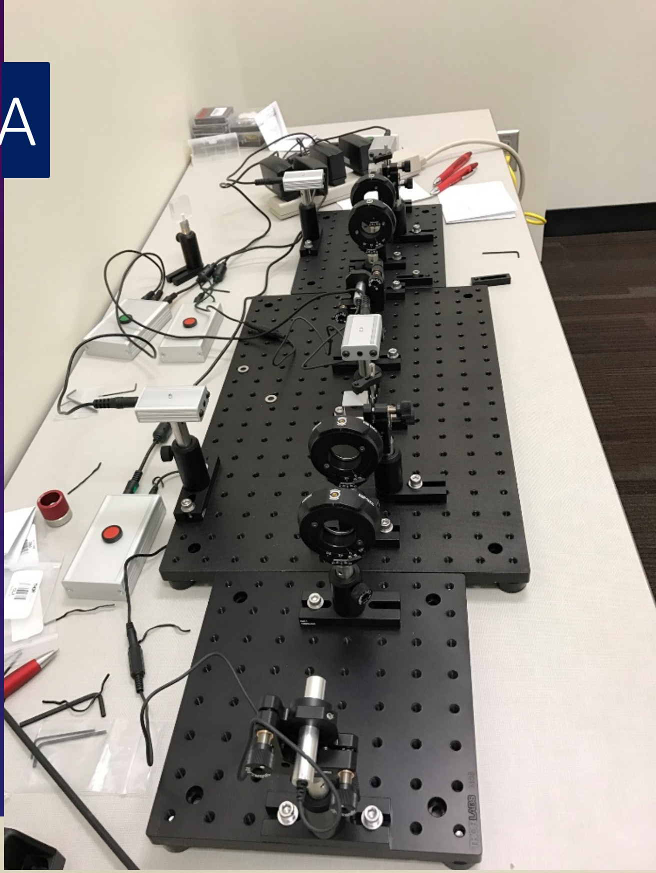
- Difficult to manufacture single photon emitters and detectors
  - As a result, several implementation based attacks exist on QKD systems

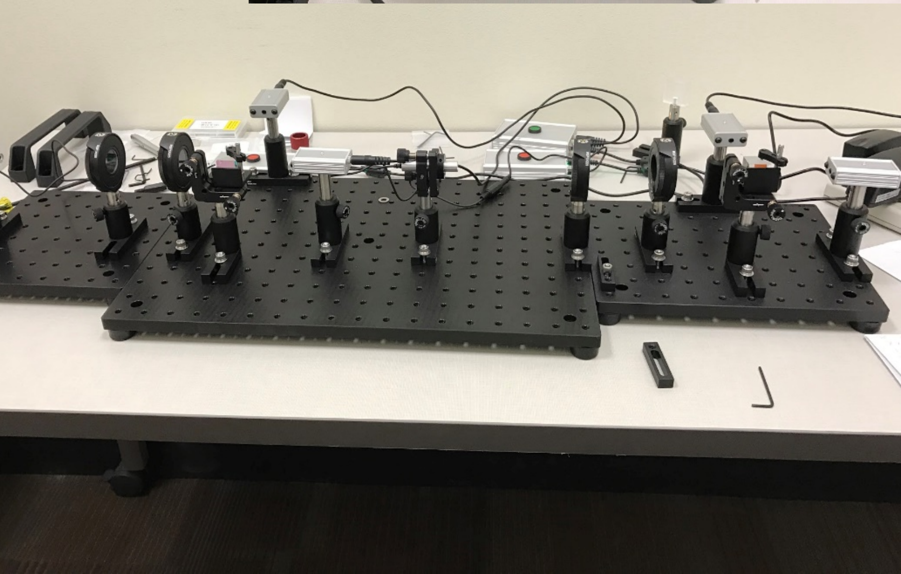
- Number of newer protocols fix these issues:
  - Decoy state protocol
  - Device-independent cryptography

QUANTUM PROGRAMMING LANGUAGES

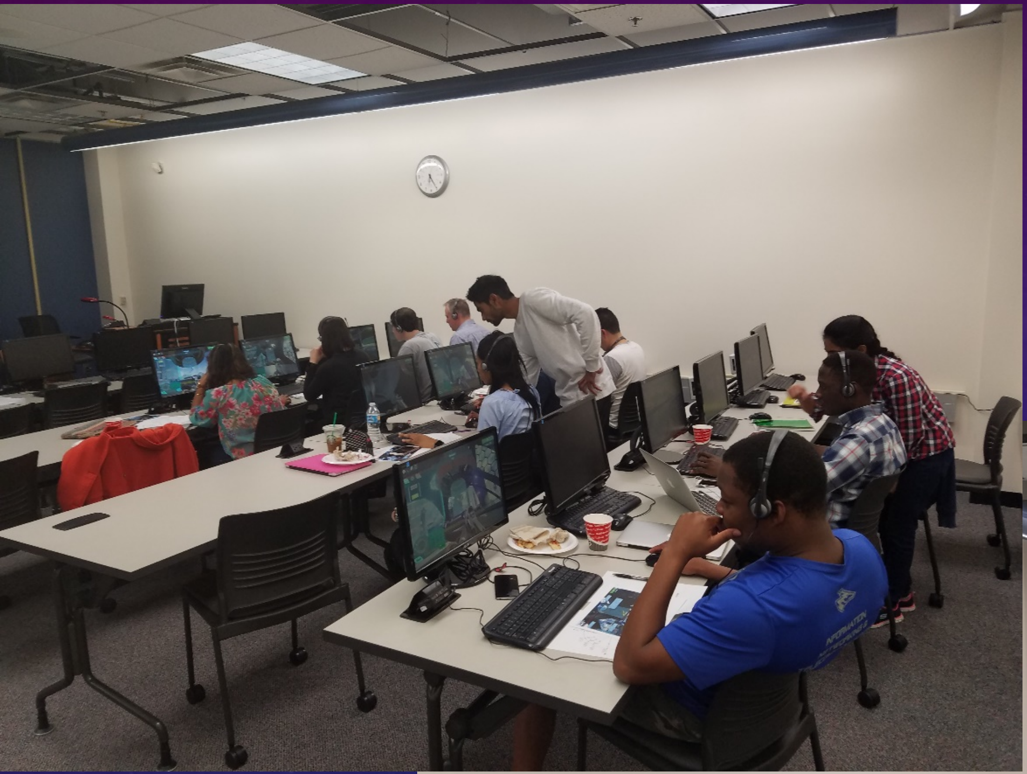
- Race to be The programming language for quantum computers
- Wikipedia has a reasonably good article
- Quantiki.org is a quantum Wikipedia and has great amounts of detail

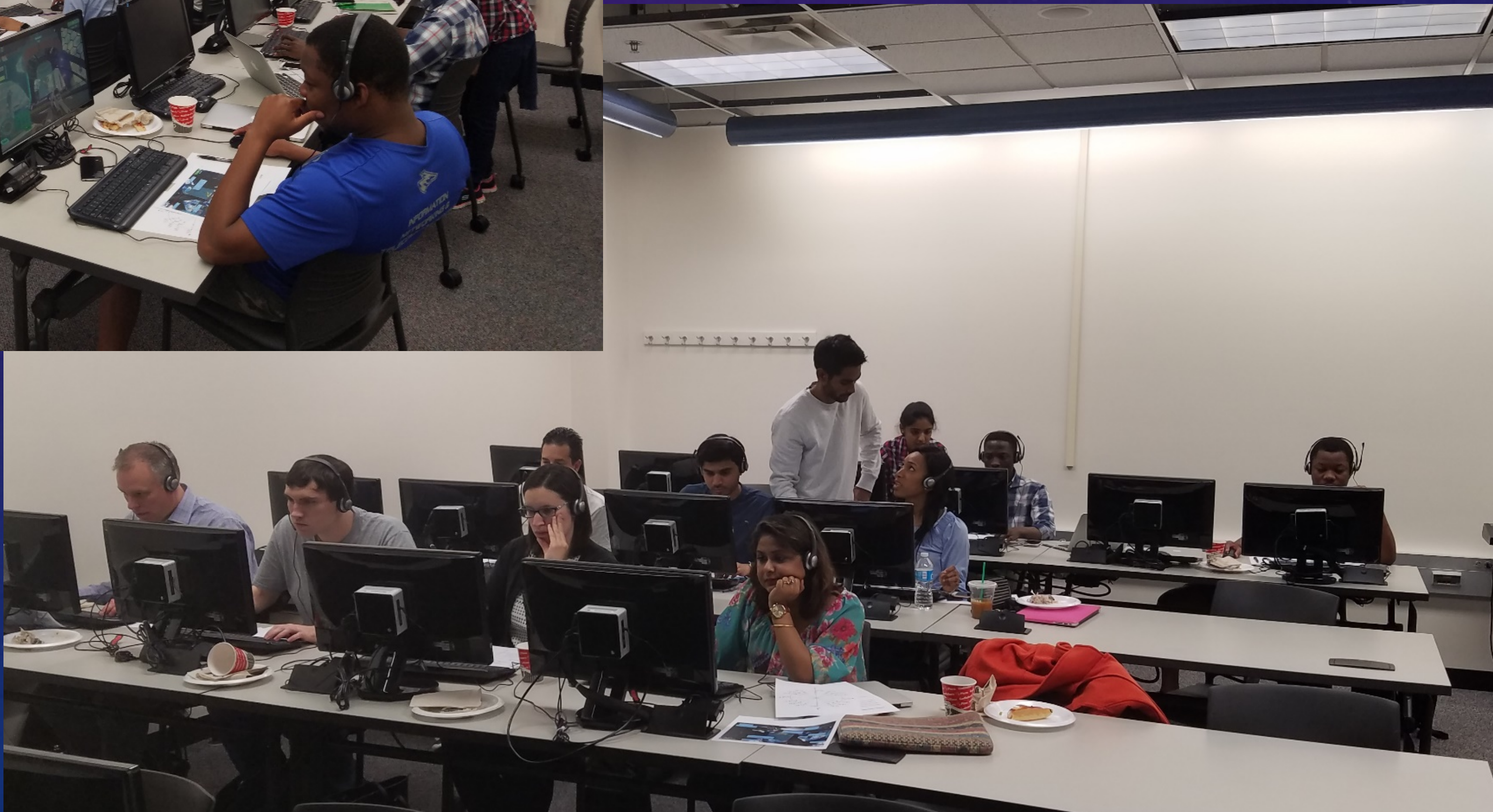
QKD AT UNIVERSITY OF NEBRASKA OMAHA





QUASIM: A QUANTUM GAME BEING BUILT AT UNO: NSF FUNDED





THANK YOU!

- Words of Great Charles Bennett – A Founder of quantum information theory: https://www.youtube.com/watch?v=9q-qoeqVVD0

- *Talk* to your kids about quantum theory before it's too late: https://imgur.com/gallery/Ftilh