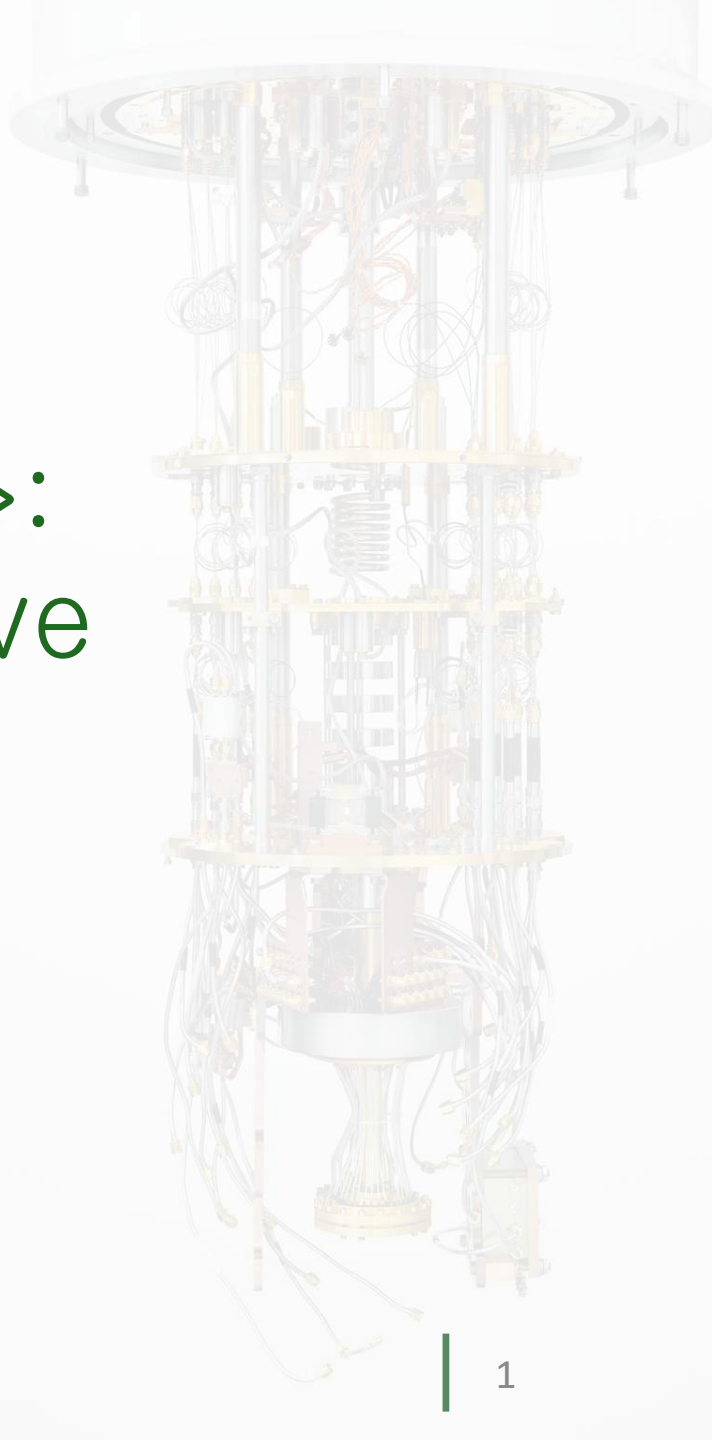
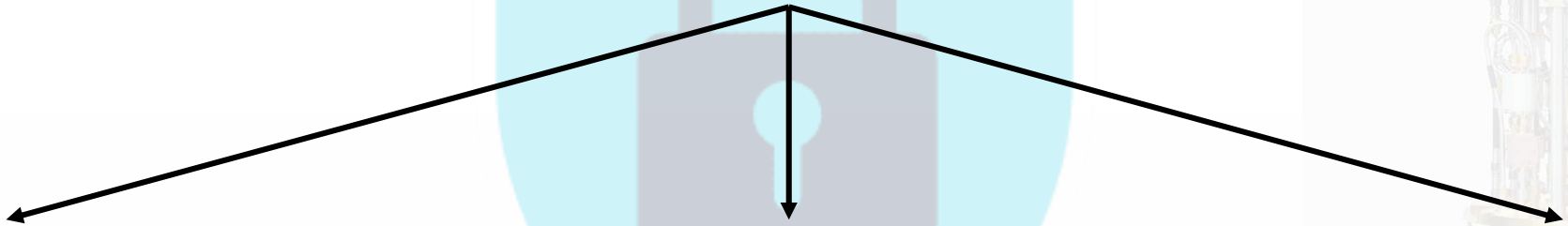
From Classical to <Quantum|Computing>: Cybersecurity Perspective



Muhamad Felemban
Director, IRC for Intelligent Secure Systems
Assistant Professor, Computer Engineering Dept.
Assistant Professor, Computer Science Dept.
KFUPM

Computational security

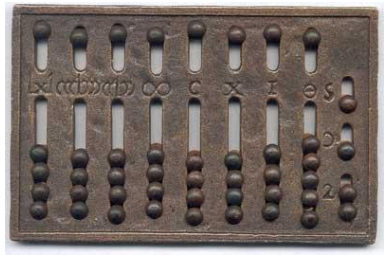
A cryptography scheme can be said to be computationally secure if it cannot be cracked in 'reasonable time’

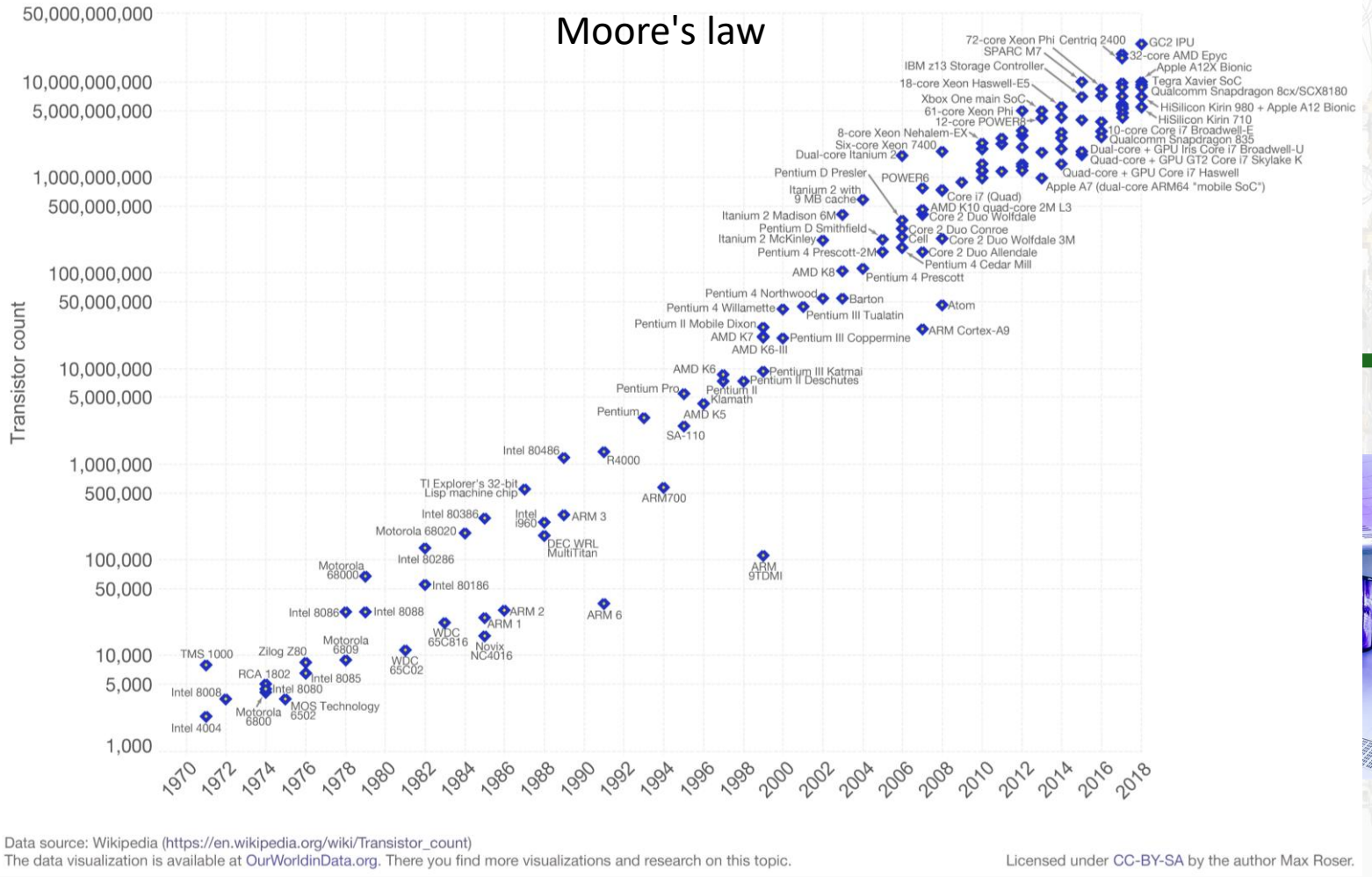


6955049856859924881463626247592788039715
3549410739391320974684455051368768161

This was believed to be a computationally hard problem that might take years to crack

History of computing





Data source: Wikipedia (https://en.wikipedia.org/wiki/Transistor_count)
The data visualization is available at OurWorldinData.org. There you find more visualizations and research on this topic.

Licensed under CC-BY-SA by the author Max Roser.

Can we think of another computing paradigm?

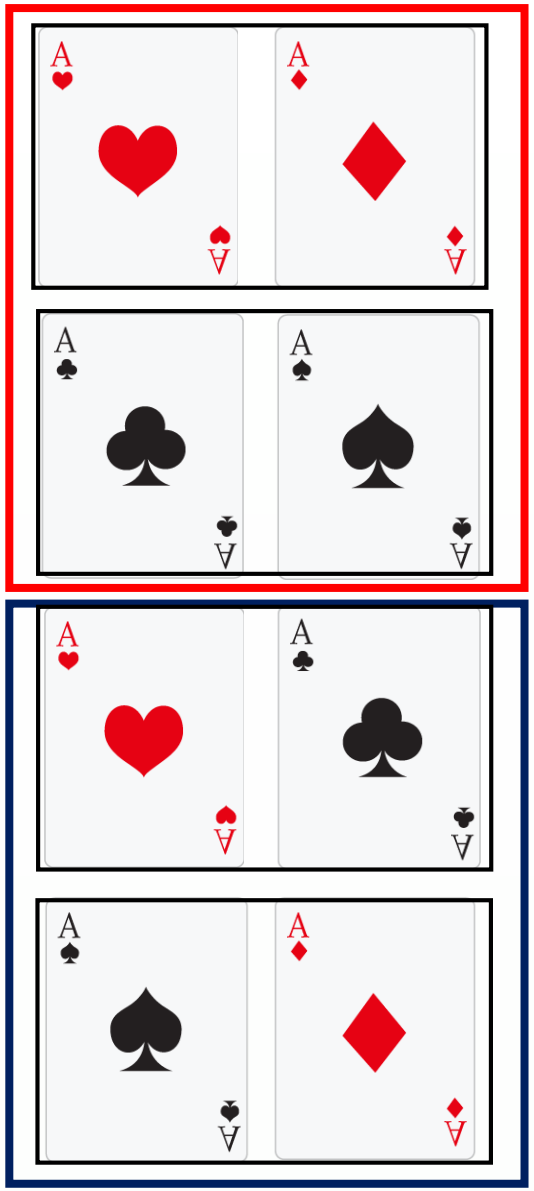
Simulating Physics with Computers - 1982

"The first question is, What kind of computer are we going to use to simulate physics? ….

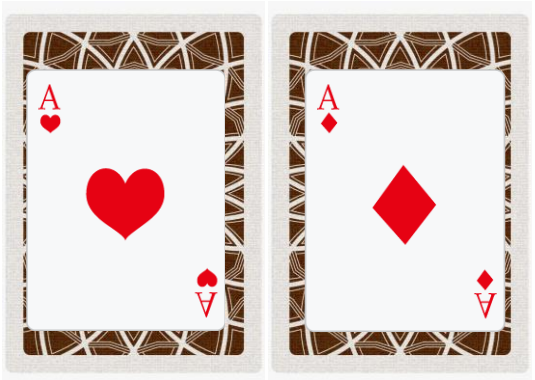
Can physics be simulated by a universal computer? "

Quantum Computing

What can it do?



How many draws?



Classically, we need

$\sim 2^n$

In general

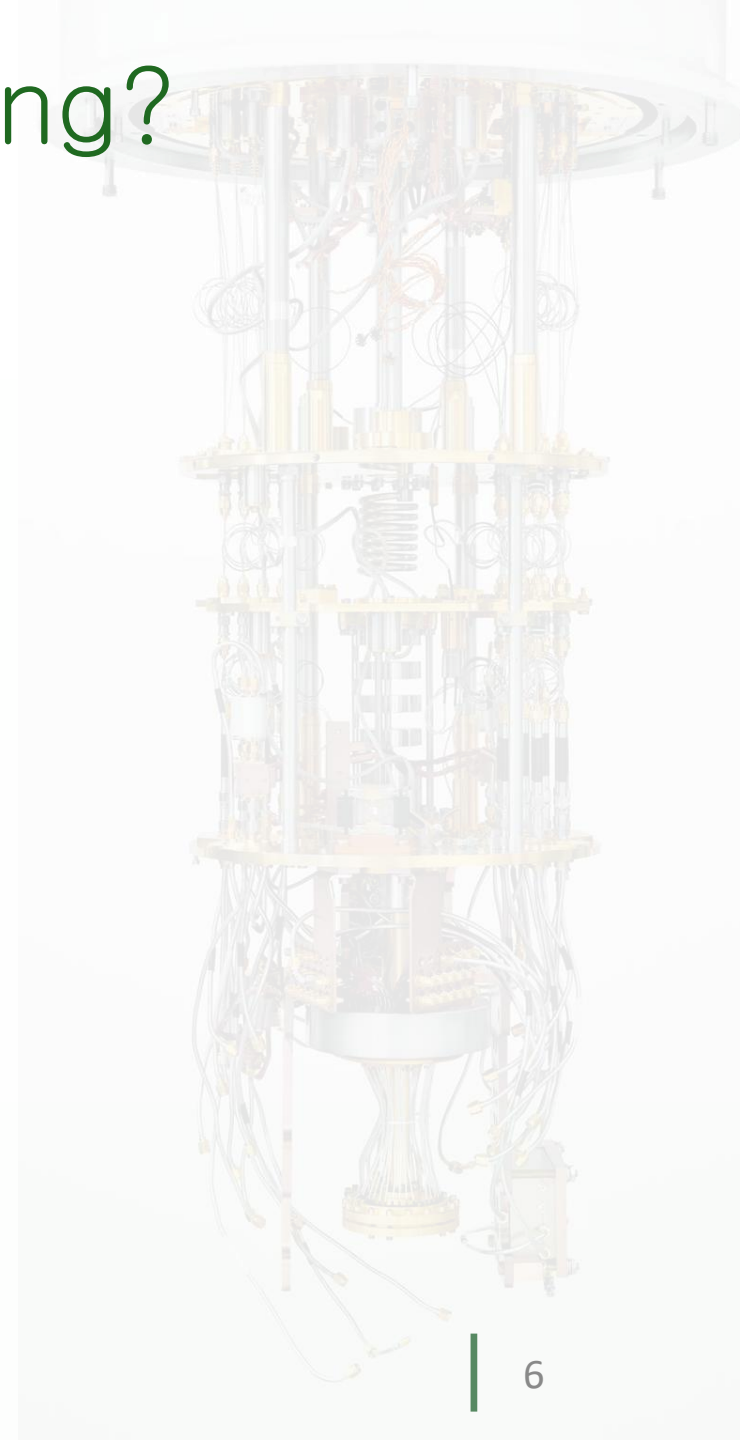
→

Using quantum computing

1

Deutsch's algorithm - 1985

Four postulates



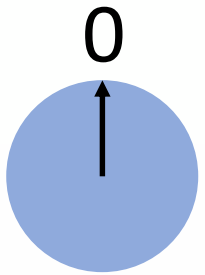
First postulate

Superposition

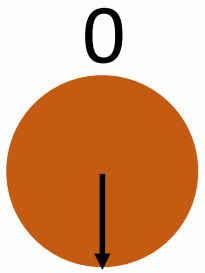
Bit

0

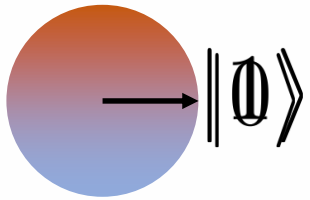
1



$|0\rangle$



$|1\rangle$

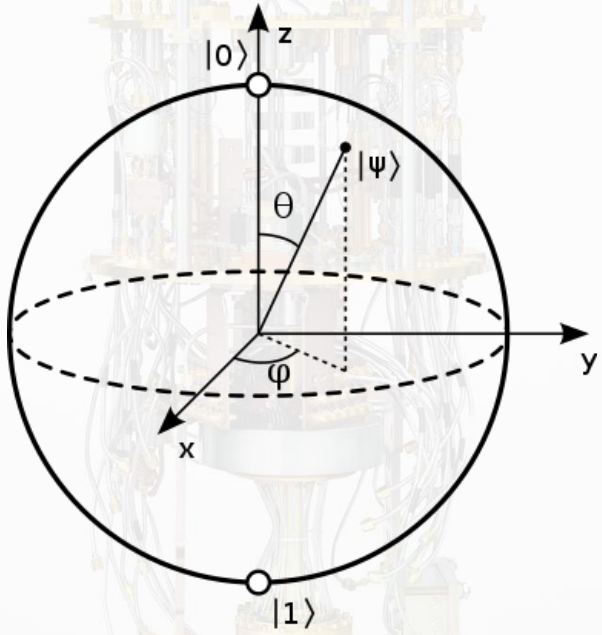


$|0\rangle + |1\rangle$

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

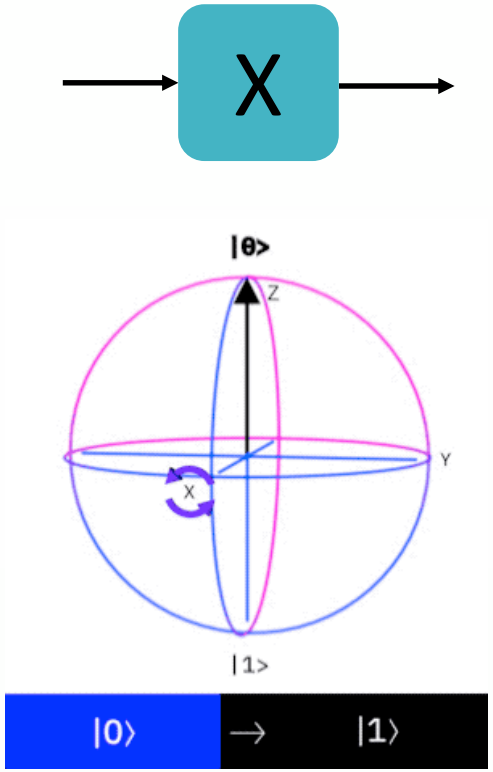
$$|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

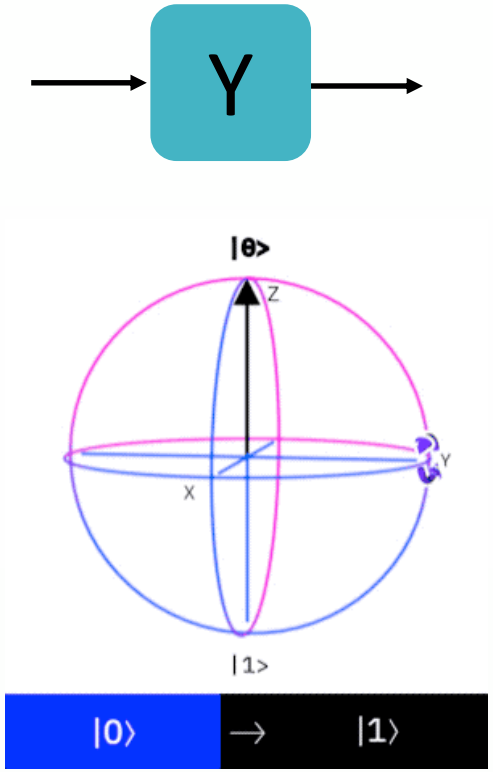
Block sphere

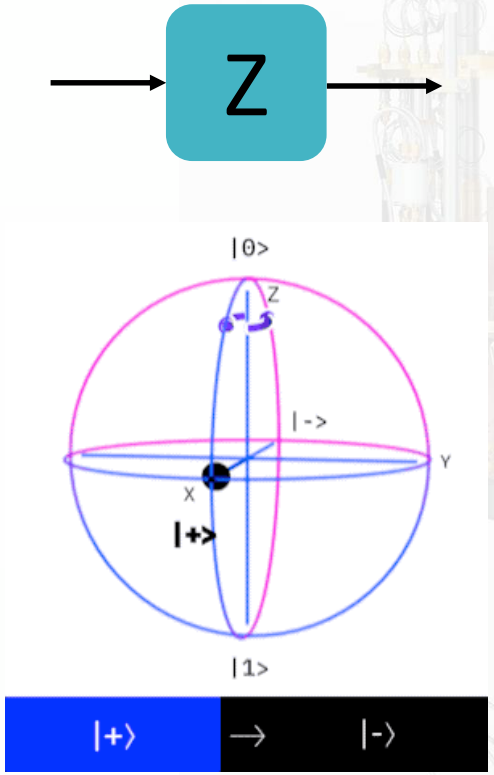


Second postulate

Qubit Evolution

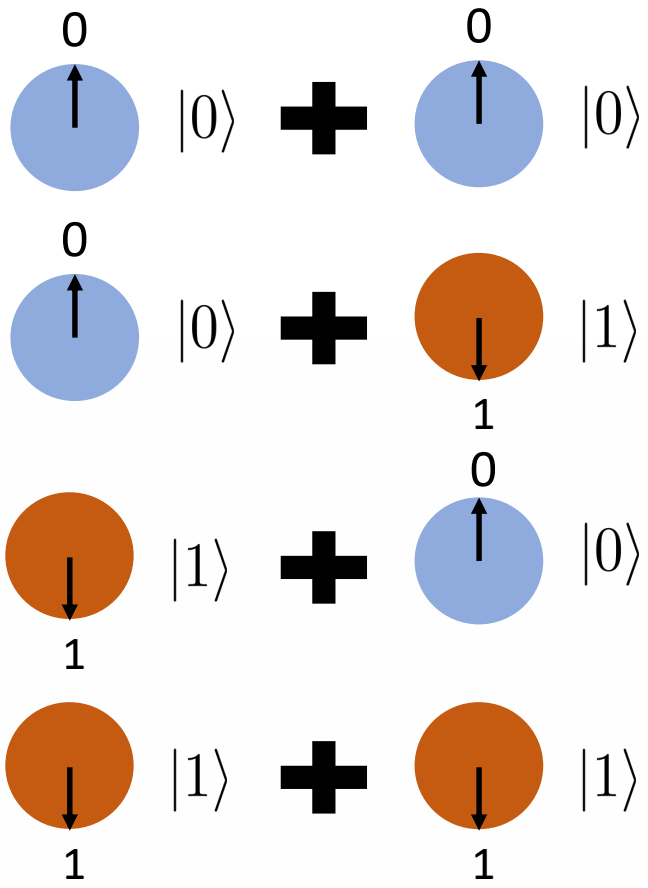


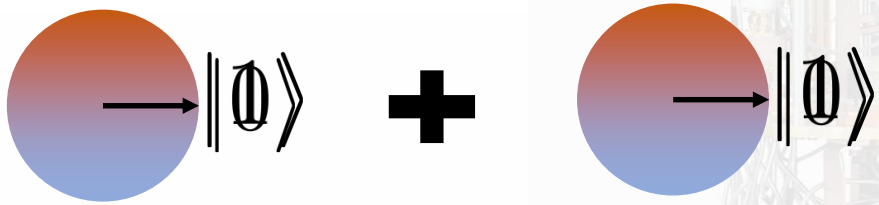




Quantum parallelism

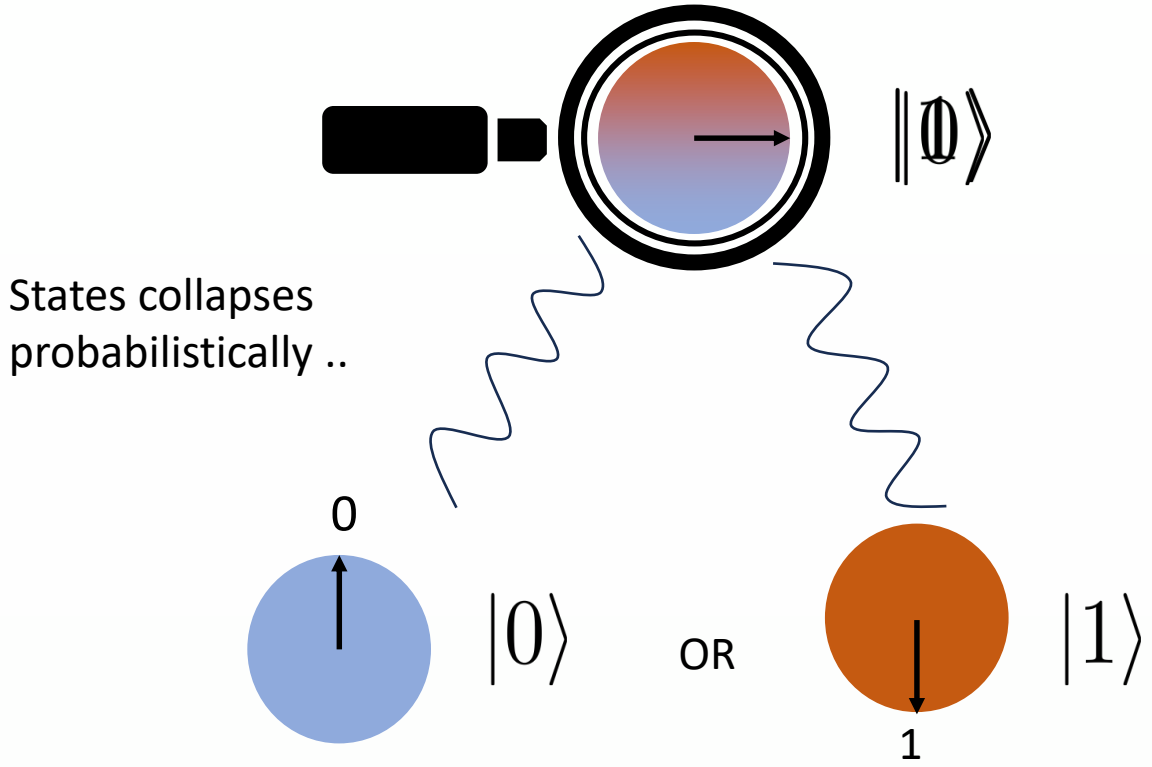
We can “ADD” two qubits





Third postulate

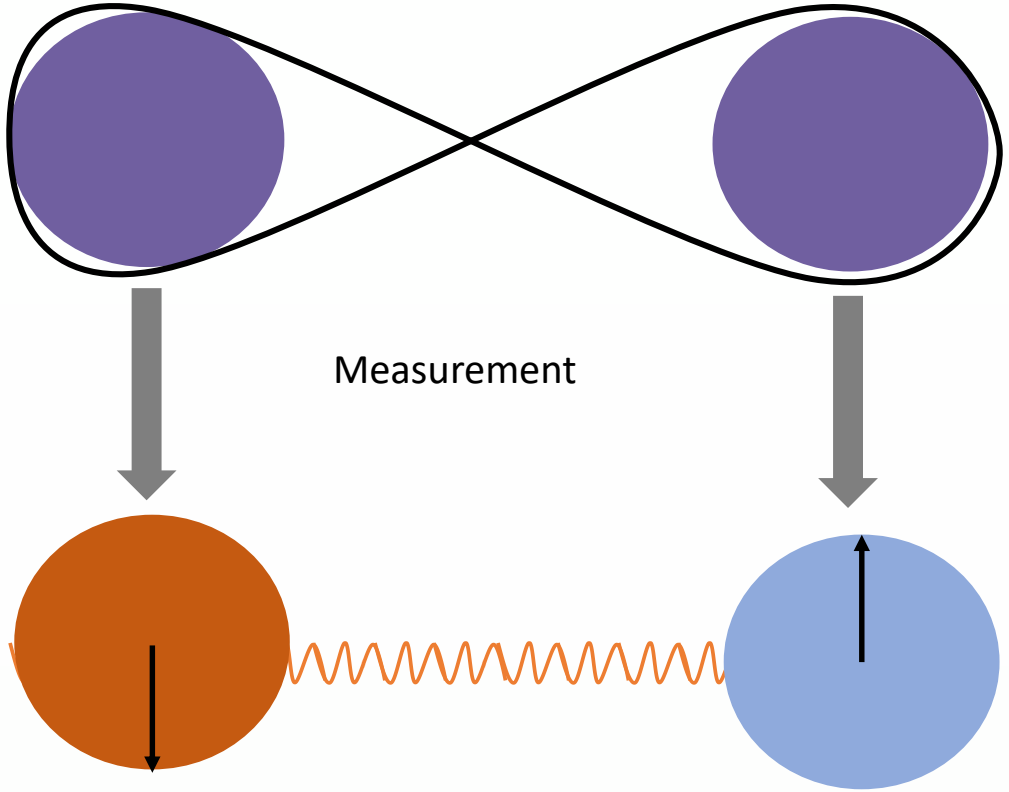
Measurement



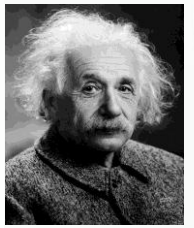
No-cloning theorem

Fourth postulate

Entanglement



Spooky actions at a distance…



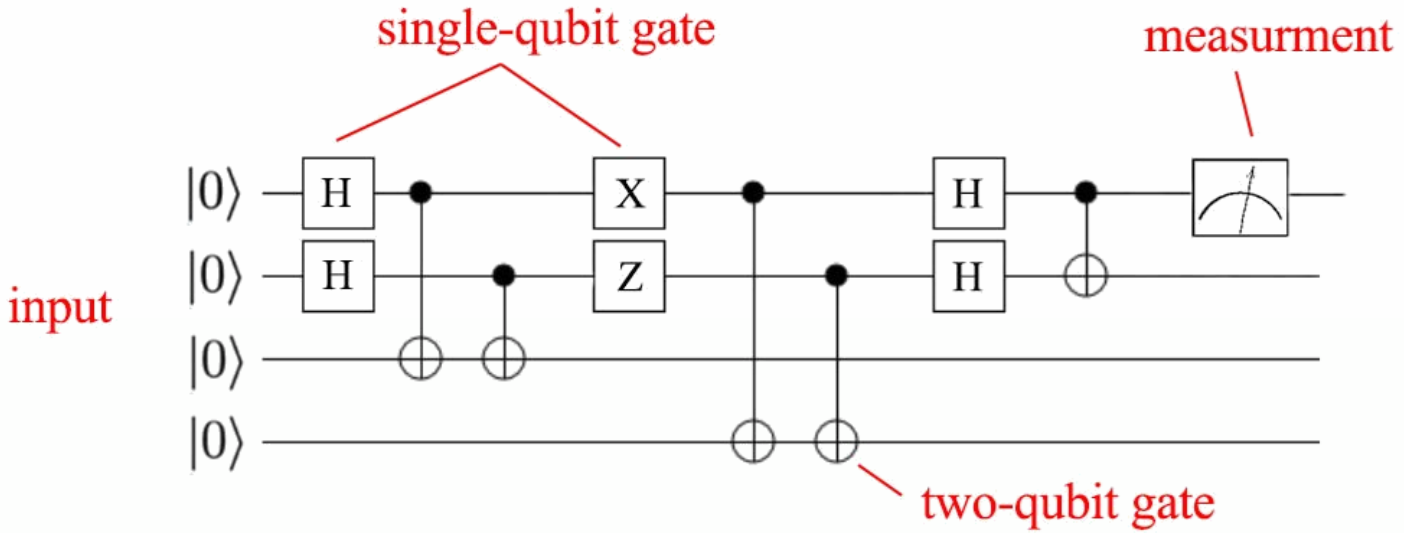
Full-fledged quantum computers

A quantum computer consists of multiple qubits

$$|\psi_0\psi_1\rangle = \alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle \qquad \alpha, \beta, \gamma, \delta \in \boldsymbol{C}$$

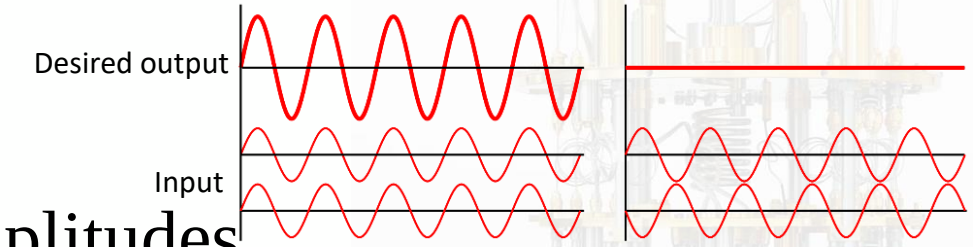
$$|\alpha|^2 + |\beta|^2 + |\gamma|^2 + |\delta|^2 = 1$$

Can apply quantum gates to a subset of qubits in a multi-qubit state



Secret sauce of quantum algorithms

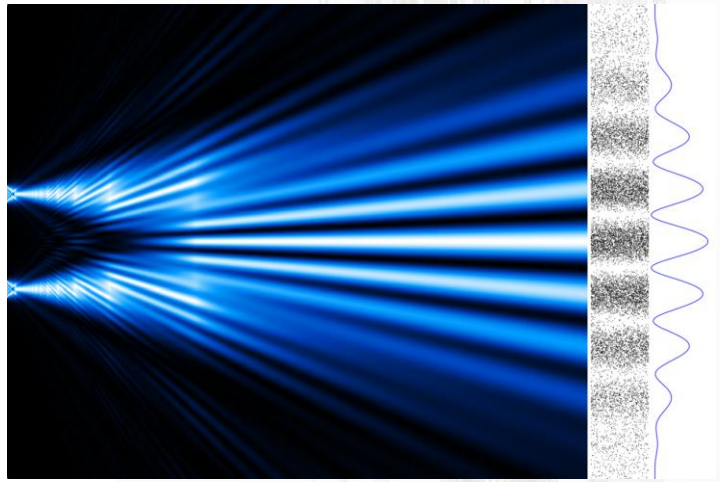
- **Warning:** a quantum computer does *not* simply "try out all solutions in parallel"



- The magic comes from allowing complex (or even just negative real) superposition amplitudes

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

- Can *carefully* choreograph computations so that wrong answers "cancel" out their amplitudes, while correct answers "combine" to produce the desired output (**quantum interference**)



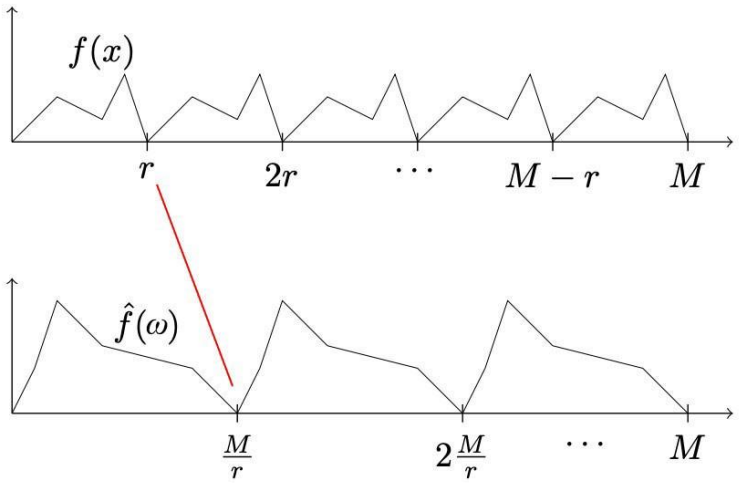
Using interference in integer factoring: order-finding

$2, 4, 8, 16, 32, 64, 128, 256, 512, 1024, \ldots$

$2, 4, 8, 1, 2, 4, 8, 1, 2, 4, 8, 1, 2 \ldots$ mod 15

$2, 4, 8, 16, 11, 1, 2, 4, 8, 16, 11, 1, 2 \ldots$ mod 21

these sequences are periodic



Quantum Fourier Transform

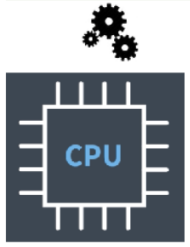
Shor's algorithm

Problem: Given a large integer N (typically several hundred digits long), factorize N as a product of primes.

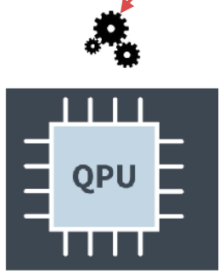
Steps :

1. Pick a random number a < N.
2. Compute gcd(a,n).
3. If gcd(a, N) ≠ 1,then it is a non-trivial factor of N, then we are done.
4. Otherwise, use the period-finding subroutine (below) to find r, the period of the following function:
$$f(x) = a^x \bmod N$$
5. If r is odd, go back to step 1.
6. If $a^{r/2} = -1 \pmod N$, go back to step 1.

Classical Part

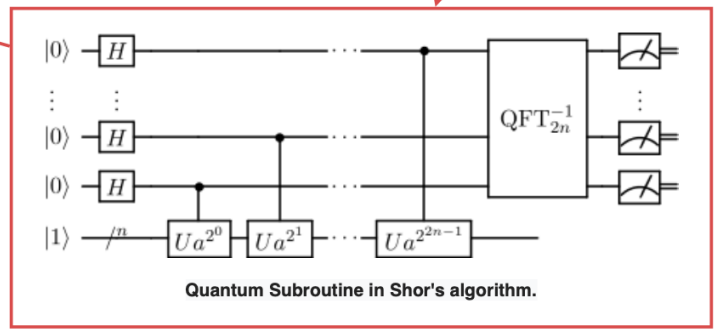


Classical Processor



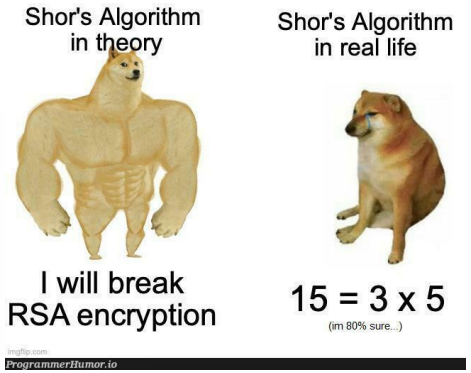
Quantum Processor

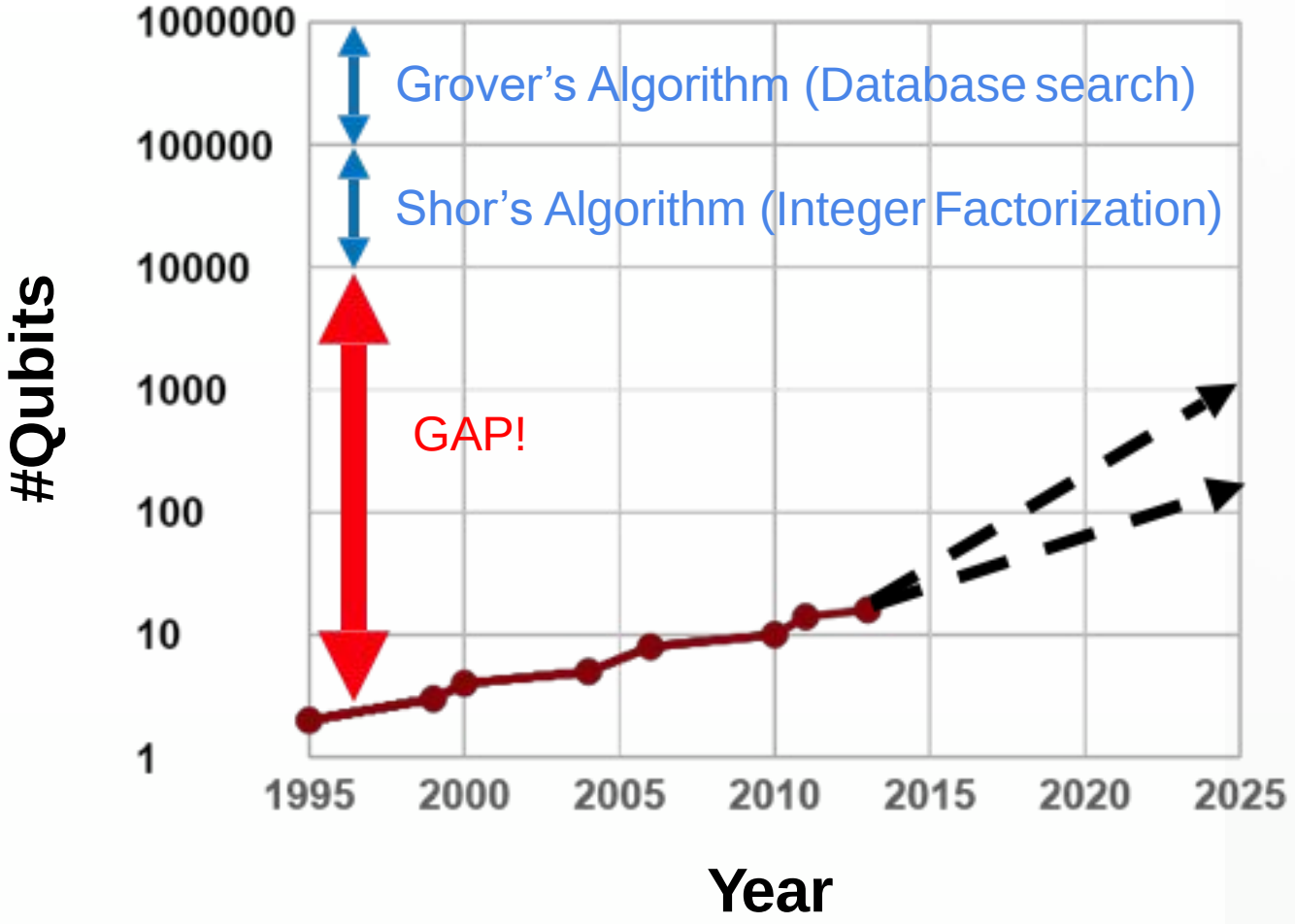
Quantum Part



Quantum Subroutine in Shor's algorithm.

The algorithms to machines gap





Qubits Needed

Qubits Buildable

Post-quantum RSA

Proposal: multi-prime RSA with terabyte keys!

[Submitted on 23 Dec 2022]

Factoring integers with sublinear resources on a superconducting quantum processor

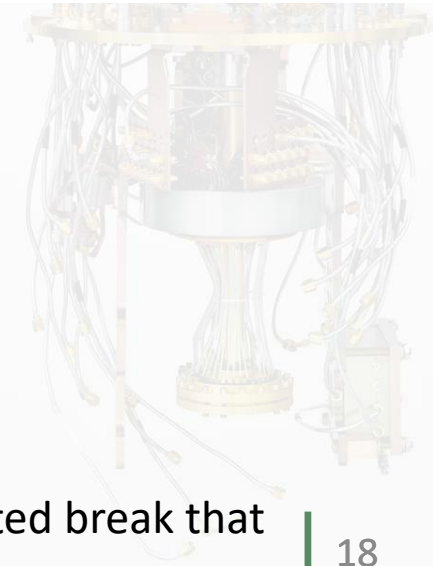
Bao Yan, Ziqi Tan, Shijie Wei, Haocong Jiang, Weilong Wang, Hong Wang, Lan Luo, Qianheng Duan, Yiting Liu, Wenhao Shi, Yangyang Fei, Xiangdong Meng, Yu Han, Zheng Shan, Jiachen Chen, Xuhao Zhu, Chuanyu Zhang, Feitong Jin, Hekang Li, Chao Song, Zhen Wang, Zhi Ma, H. Wang, Gui-Lu Long

Shor's algorithm has seriously challenged information security based on public key cryptosystems. However, to break the widely used RSA-2048 scheme, one needs millions of physical qubits, which is far beyond current technical capabilities. Here, we report a universal quantum algorithm for integer factorization by combining the classical lattice reduction with a quantum approximate optimization algorithm (QAOA). The number of qubits required is O(logN/loglog N), which is sublinear in the bit length of the integer N, making it the most qubit-saving factorization algorithm to date. We demonstrate the algorithm experimentally by factoring integers up to 48 bits with 10 superconducting qubits, the largest integer factored on a quantum device. We estimate that a quantum circuit with 372 physical qubits and a depth of thousands is necessary to challenge RSA-2048 using our algorithm. Our study shows great promise in expediting the application of current noisy quantum computers, and paves the way to factor large integers of realistic cryptographic significance.

"No. Just No." – **Scott Aaronson**

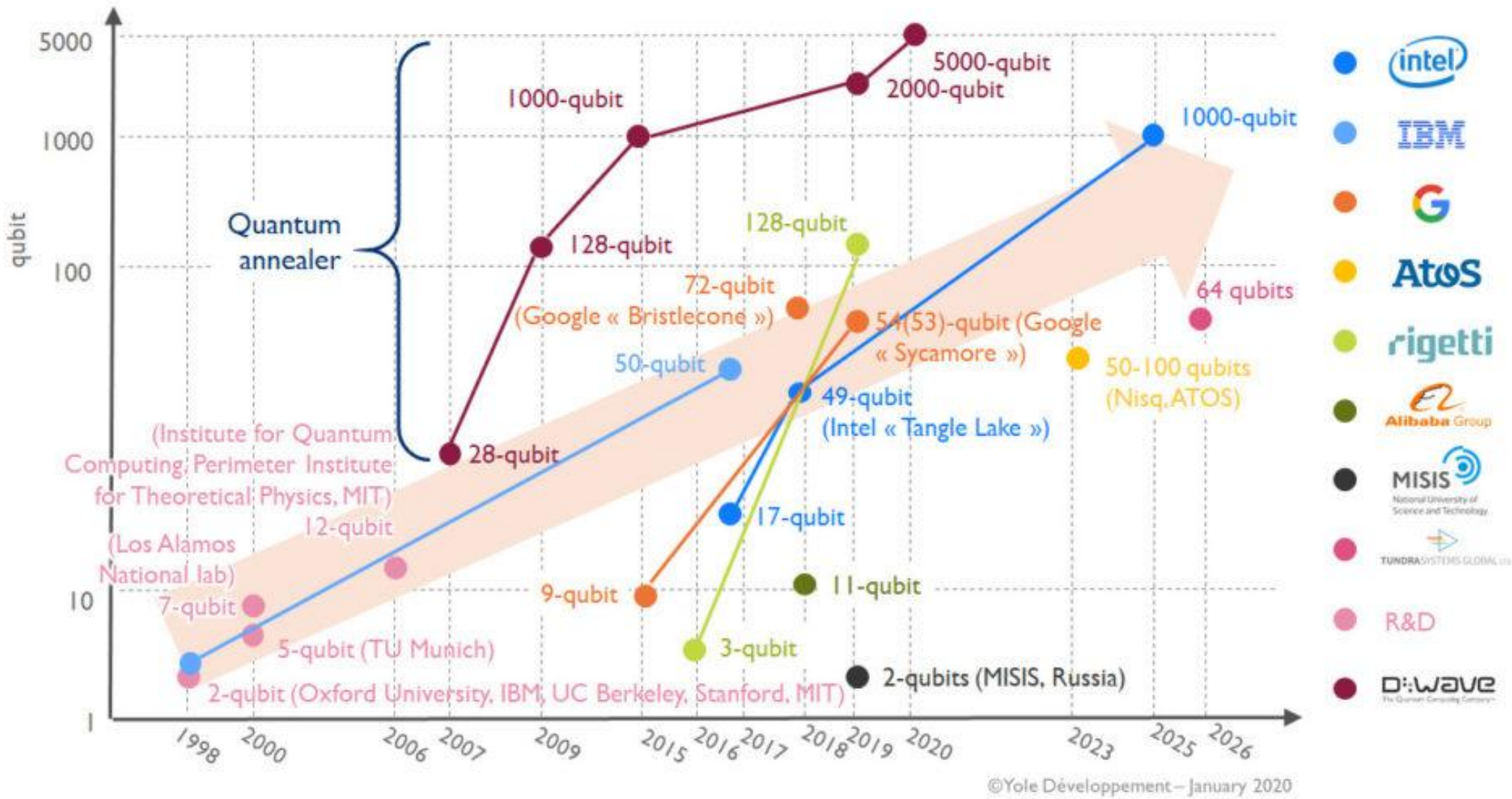
"I am *much* less worried that this technique will work now." – **Bruce Schneier**

" High level answer:
-Don't panic
-Don't procrastinate in your migration to quantum-safe cryptography
-Plan a migration to post-quantum public-key cryptography, and ALSO be prepared for an unexpected break that works" – **Michele Mosce**



Physical qubit roadmap for quantum computer

(Source: Quantum Technologies 2020 report, Yole Développement)



©Yole Développement – January 2020

Post-quantum cryptography (Classical algorithms believed to withstand quantum attacks)

MIT Technology Review

Topics+ Top Stories Maga

re and Tandon Chemical Engineers are beating Breast Cancer

Computing

NSA Says It "Must Act Now" Against the Quantum Computing Threat

The National Security Agency is worried that quantum computers will neutralize our best encryption – but doesn't yet know what to do about that problem.

by Tom Simonite February 3, 2016

NIST releases quantum-resistant cryptography standards -- ACT NOW!

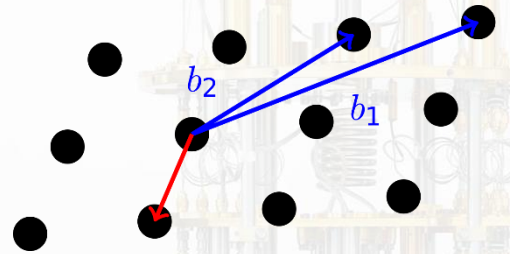
https://pqshield.com/the-new-nist-pqc-standards-are-here/

Lattice-based cryptography

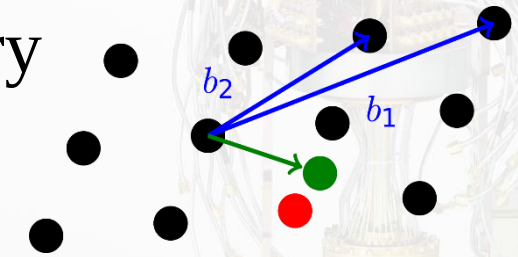
Very versatile computational problems

- Public-key encryption
- Digital signatures
- Hash functions
- Fully homomorphic encryption
- Key exchange

Shortest vector problem



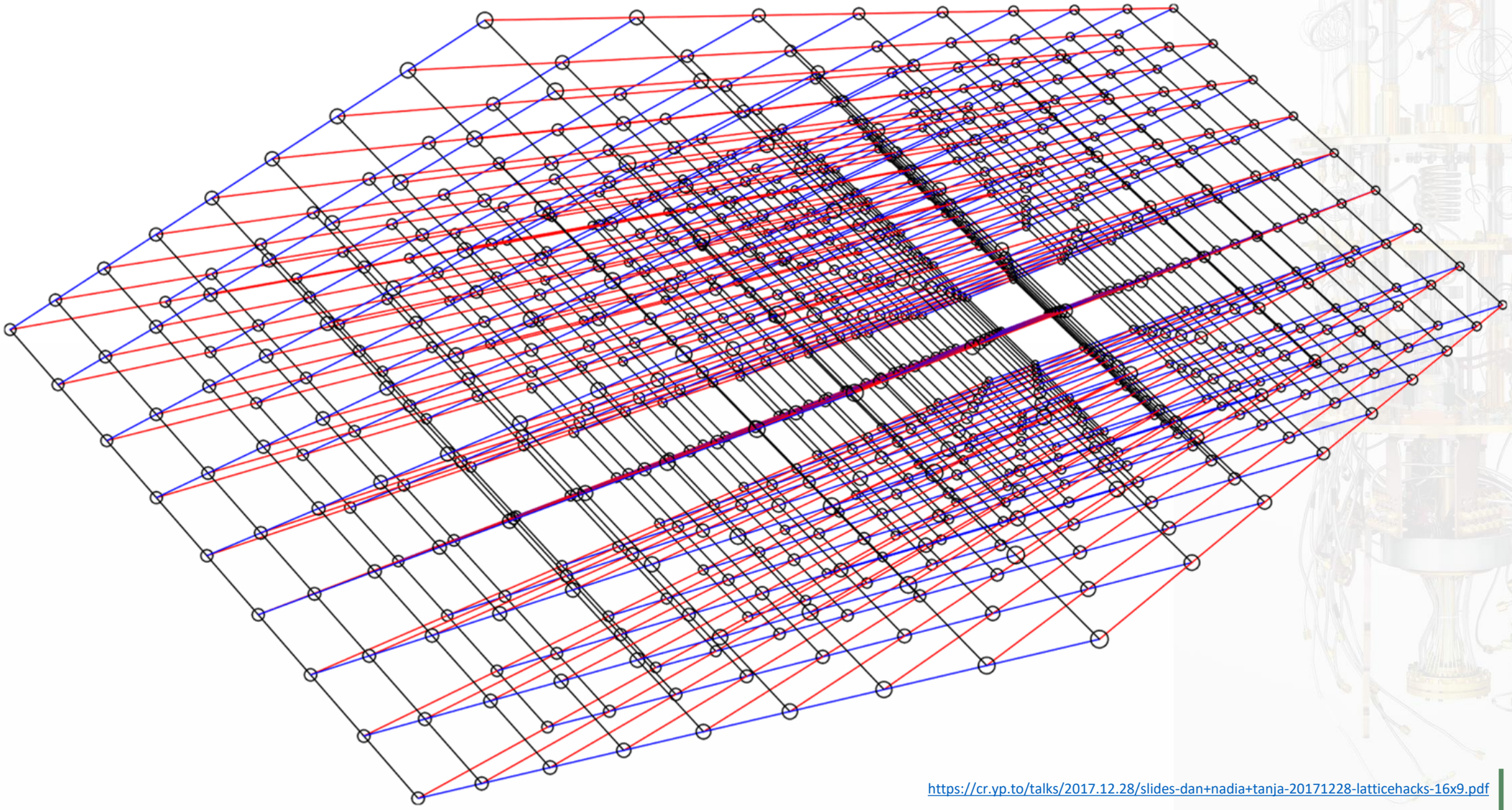
Closest vector problem



Based on hardness of problems in algebraic number theory

- Believed to be hard also for quantum computers

Lattice-based cryptography

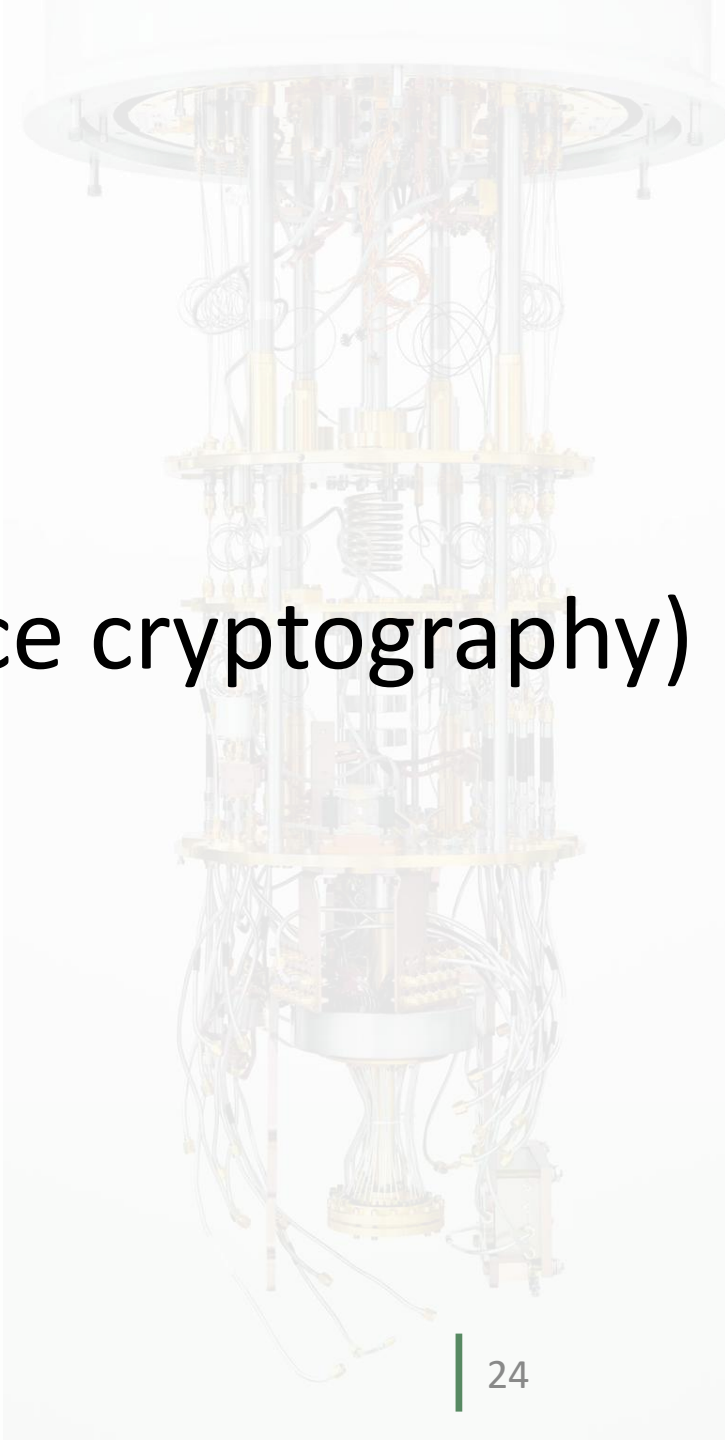


https://cr.yp.to/talks/2017.12.28/slides-dan+nadia+tanja-20171228-latticehacks-16x9.pdf

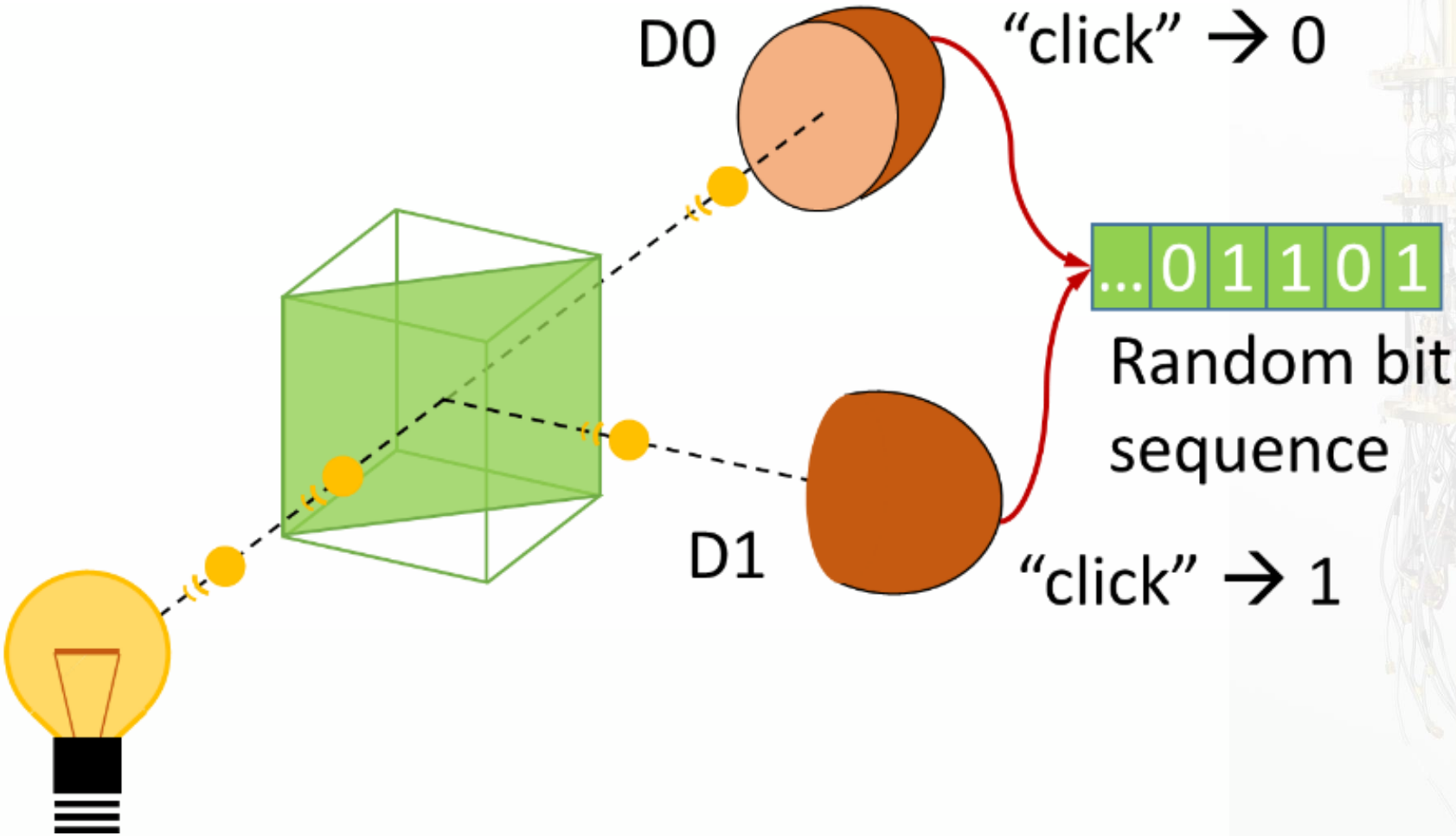
Is that it?

Quantum-Enhanced Cryptography

(Use quantum mechanics to enhance cryptography)



Quantum random number generator



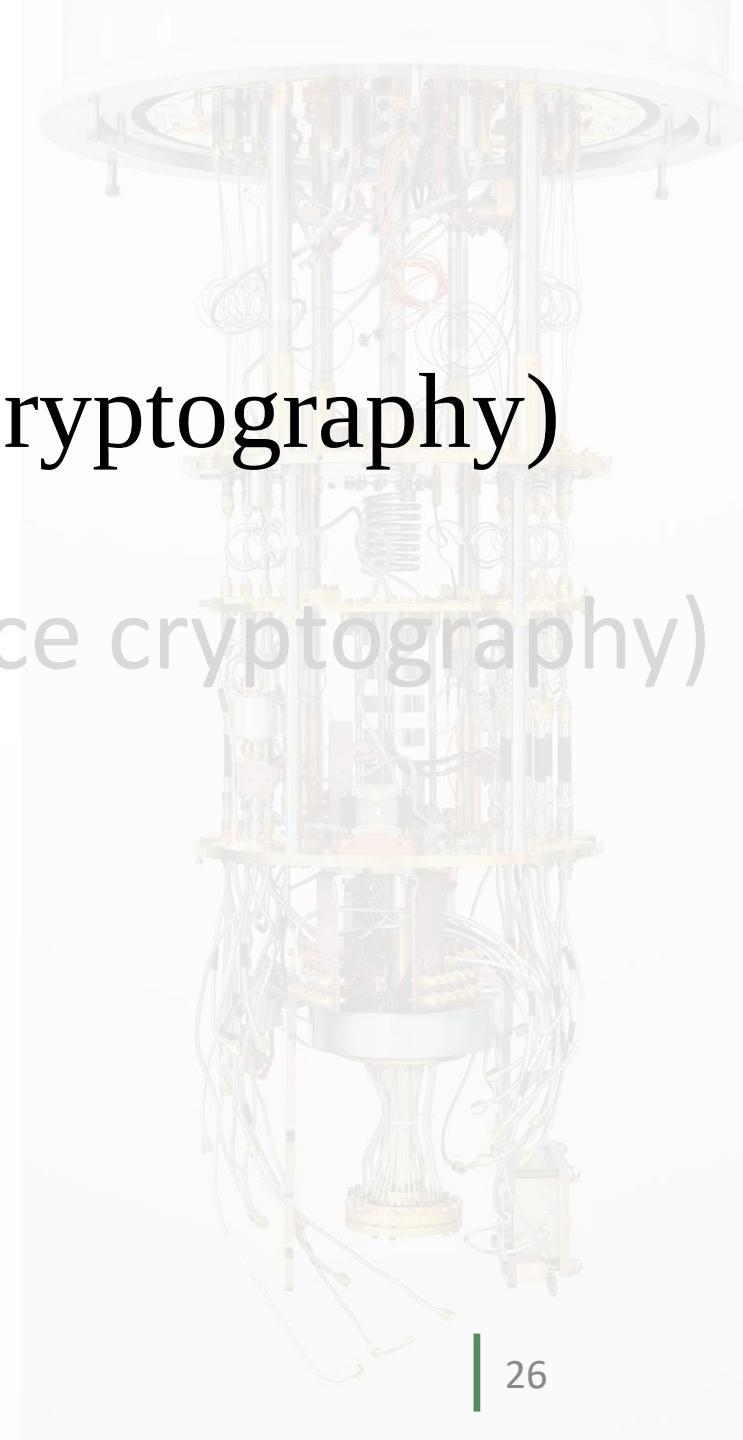
There is more…

Quantum-Enabled Cryptography

(Use quantum mechanics to build cryptography)

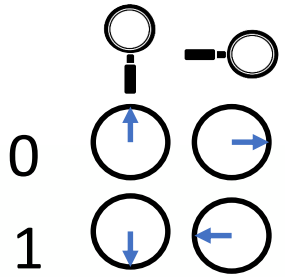
Quantum-Enhanced Cryptography

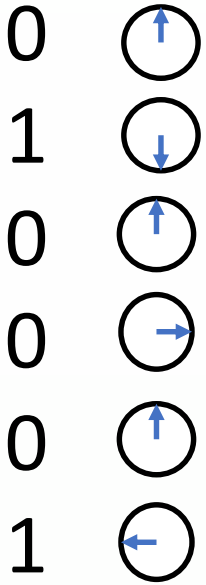
(Use quantum mechanics to enhance cryptography)



Quantum key distribution

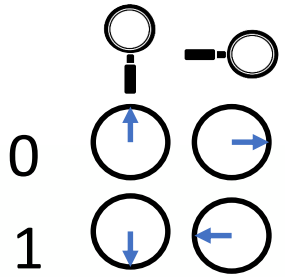
Without Eve

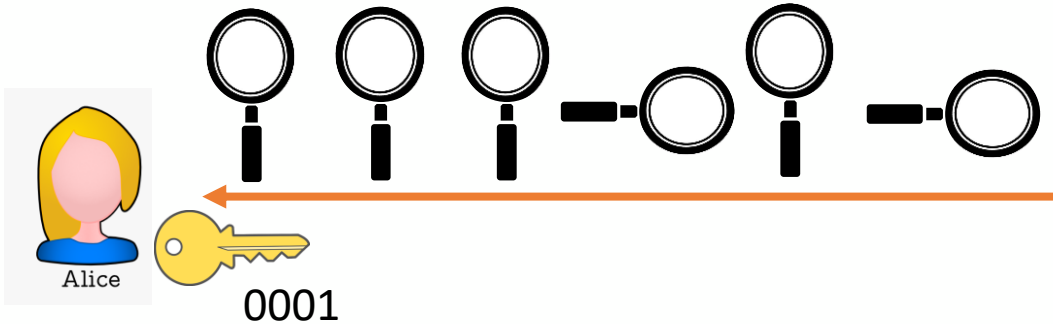


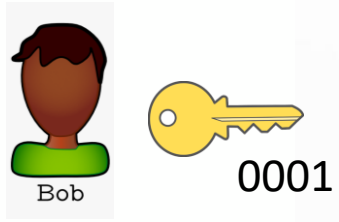


Quantum key distribution

Without Eve







0

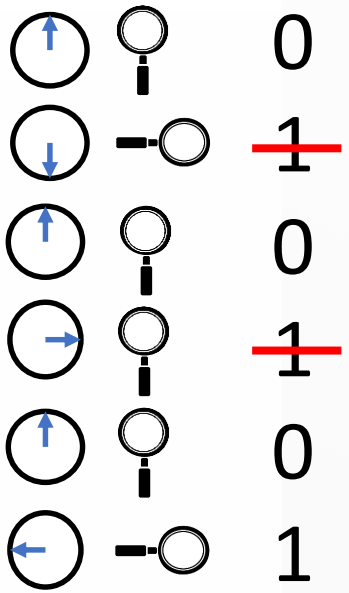
~~1~~

0

~~0~~

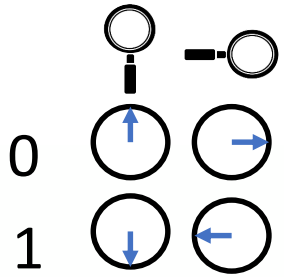
0

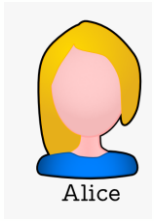
1

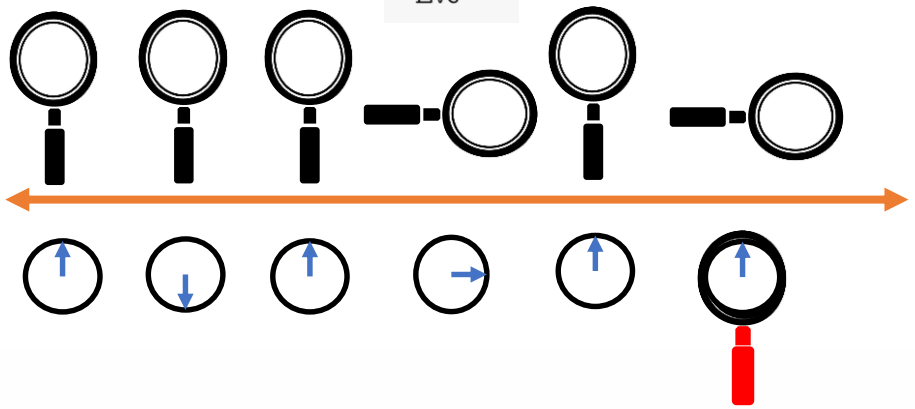


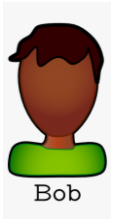
Quantum key distribution

Wih Eve

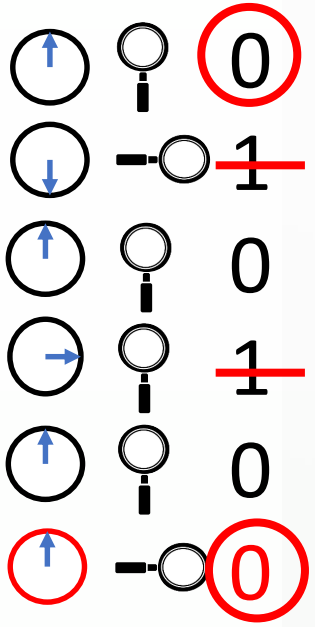








0
1
0
0
0
1



BB84 Protocol

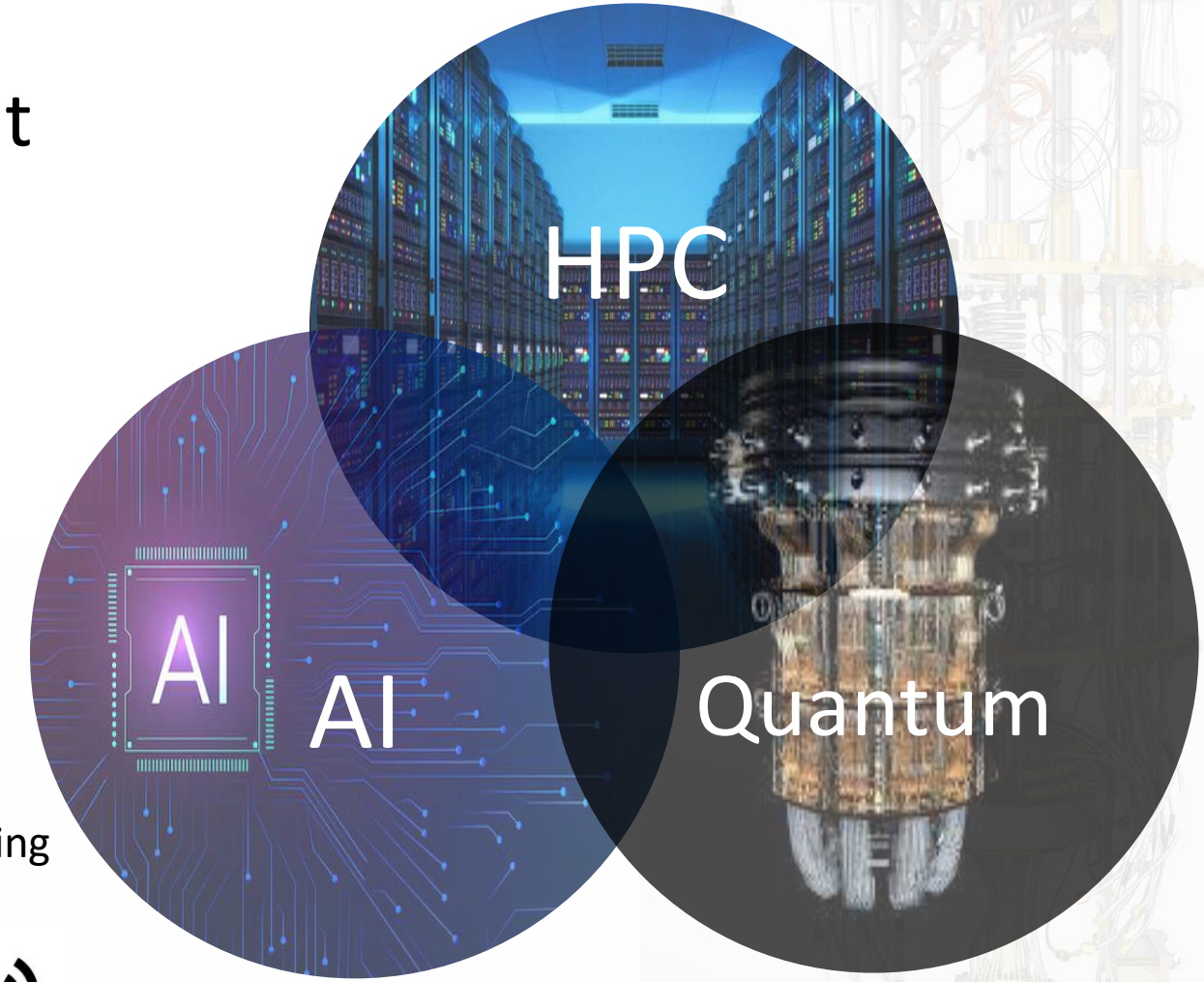
From hope to hype

Solving real-world problems that will impact 100% of humans requires a combination of ..

Technology

~~Quantum Computing~~

Computing Simulation Communication Sensing



Post-Quantum ~~Cryptography~~ Cybersecurity

Thank you

For more information about our research

https://ri.kfupm.edu.sa/ISS

https://faculty.kfupm.edu.sa/COE/mfelemban/

mfelemban@kfupm.edu.sa