Quantum computers

Threat and promise

J Avron

June 4, 2023

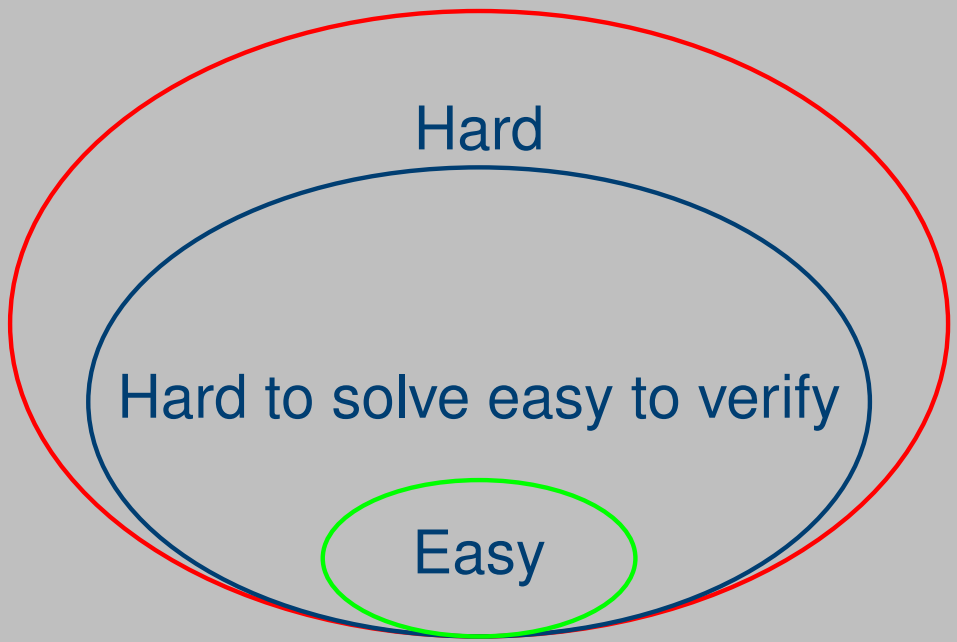
Overview

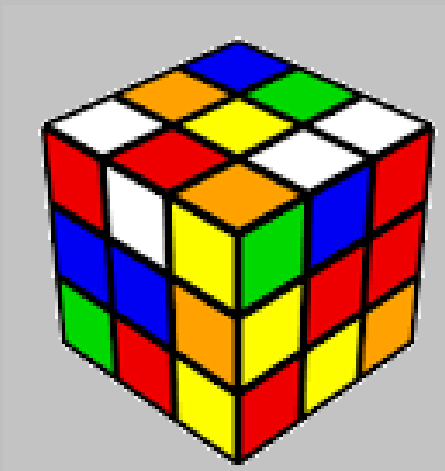
1. What's the problem with cyber security?
2. Quantum computers: The threat
3. The quantum promise
4. The word view of QM
5. A biblical perspective

What's the problem with (classical) cyber security?

Not guaranteed by math or physics

Rests on belief



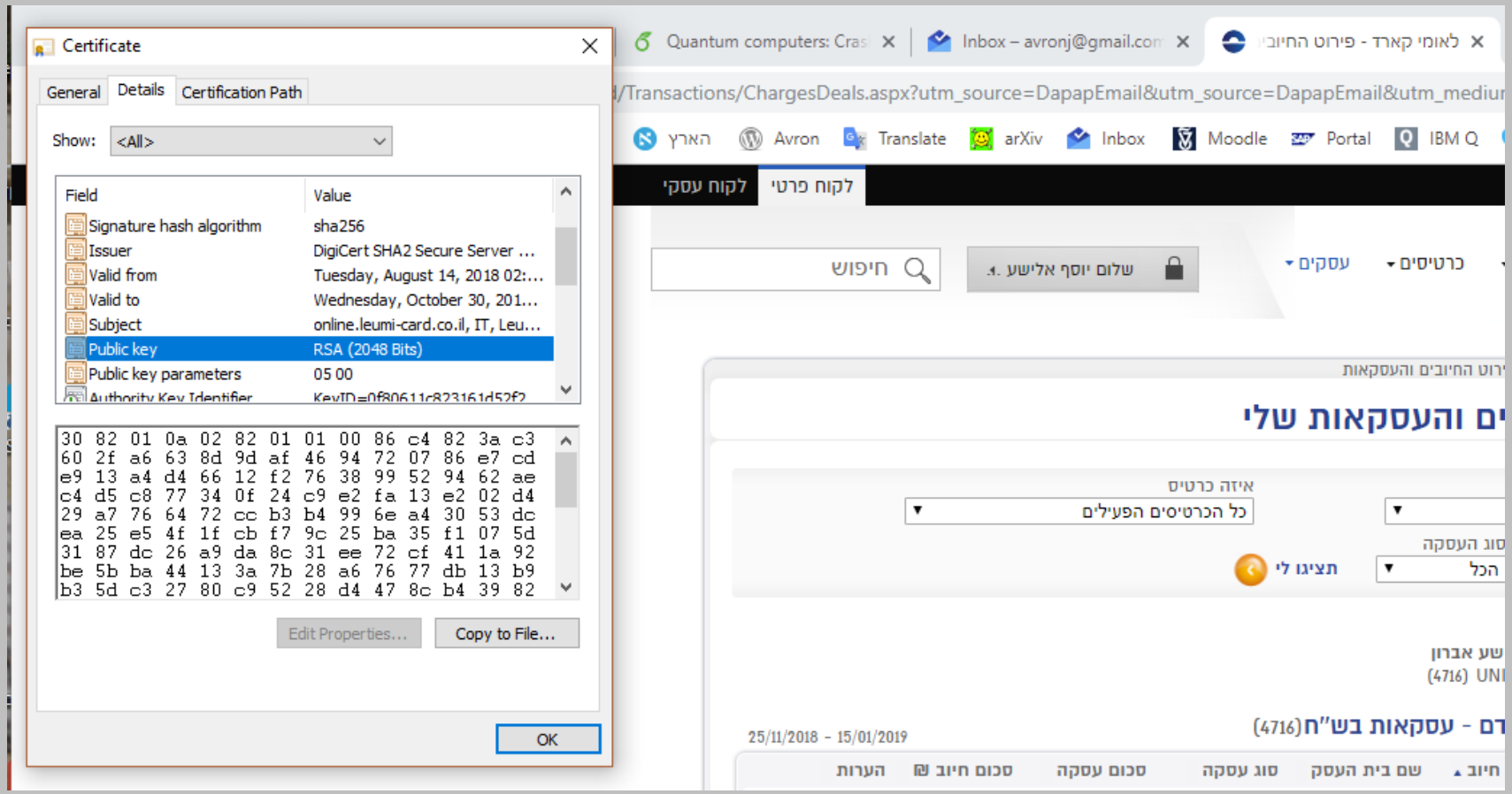


Factoring

Hard to solve easy to verify

- $19043 = 137 \times 139$
- $137, 139 \in \textit{Primes}$
- Hard to solve
- Easy to verify

RSA: Standard cyber security tool



Shor algorithm 1994

The future ain't what it used to be–Yogi Berra

- Factoring easy for quantum computers
- Large quantum computers do not exist yet
- When large quantum computers be available?

10 years, 20 years, never

Secret records today may be unsafe tomorrow

The quantum promise

No-cloning

- Unknown quantum state:
  Output of quantum computer running an unknown program

No-cloning

An unknown quantum state can't be copies

Quantum money

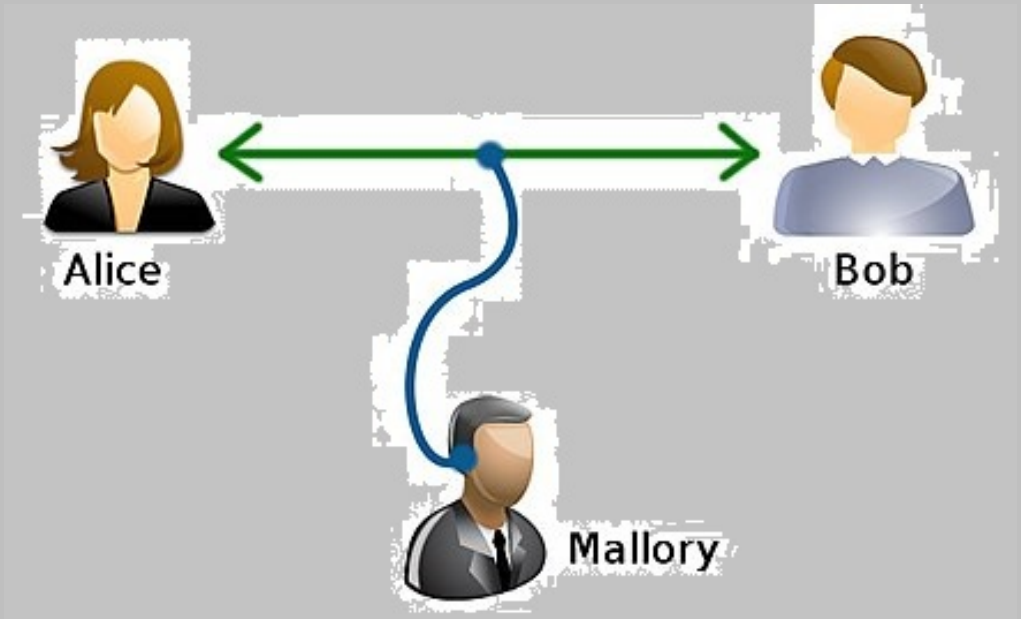
Stephen Wiesner 1942-2021

Secure Quantum communication

Security guaranteed by physics

The uncertainty principle

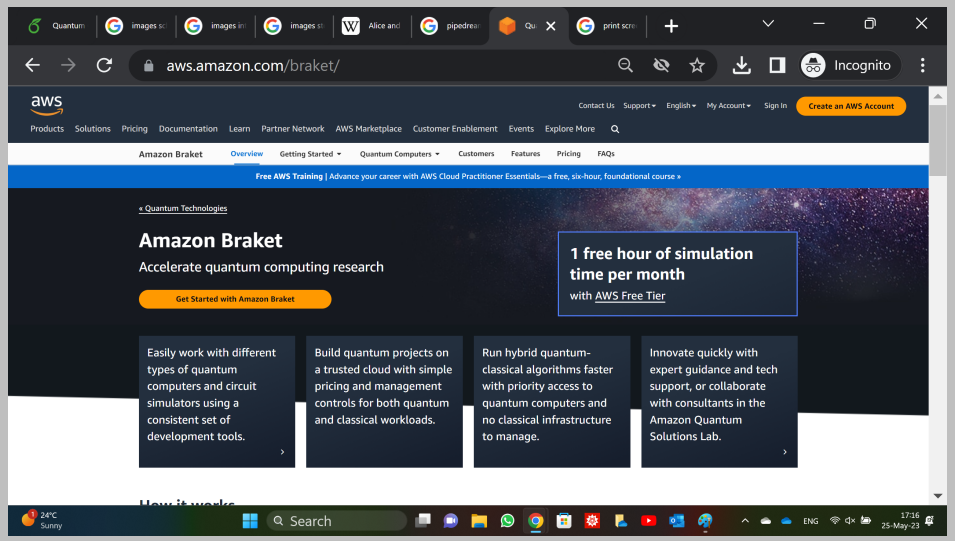
If information is leaked the quantum system changed



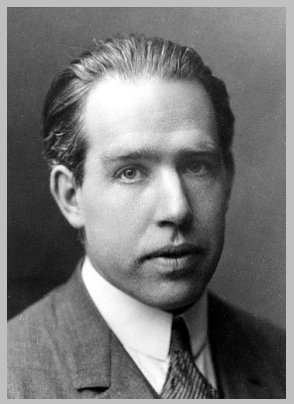
Alice and Bob can tell if there is an eavesdropper

Current status

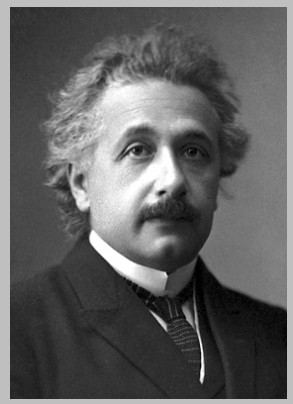
- Quantum communication (QKD):
  - Market of enthusiasts
- Quantum cloud computing
  - Small and unreliable computers:
  - Market of enthusiasts
  - Maybe useful for chemistry
- Large quantum computers:
  - Don't exist yet
- Post quantum crypto:



The meaning of Quantum state



- Physics is about what nature is
- A quantum state is about what is possible



MAY 15, 1935 PHYSICAL REVIEW VOLUME 47

Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?

A. EINSTEIN, B. PODOLSKY AND N. ROSEN, *Institute for Advanced Study, Princeton, New Jersey*

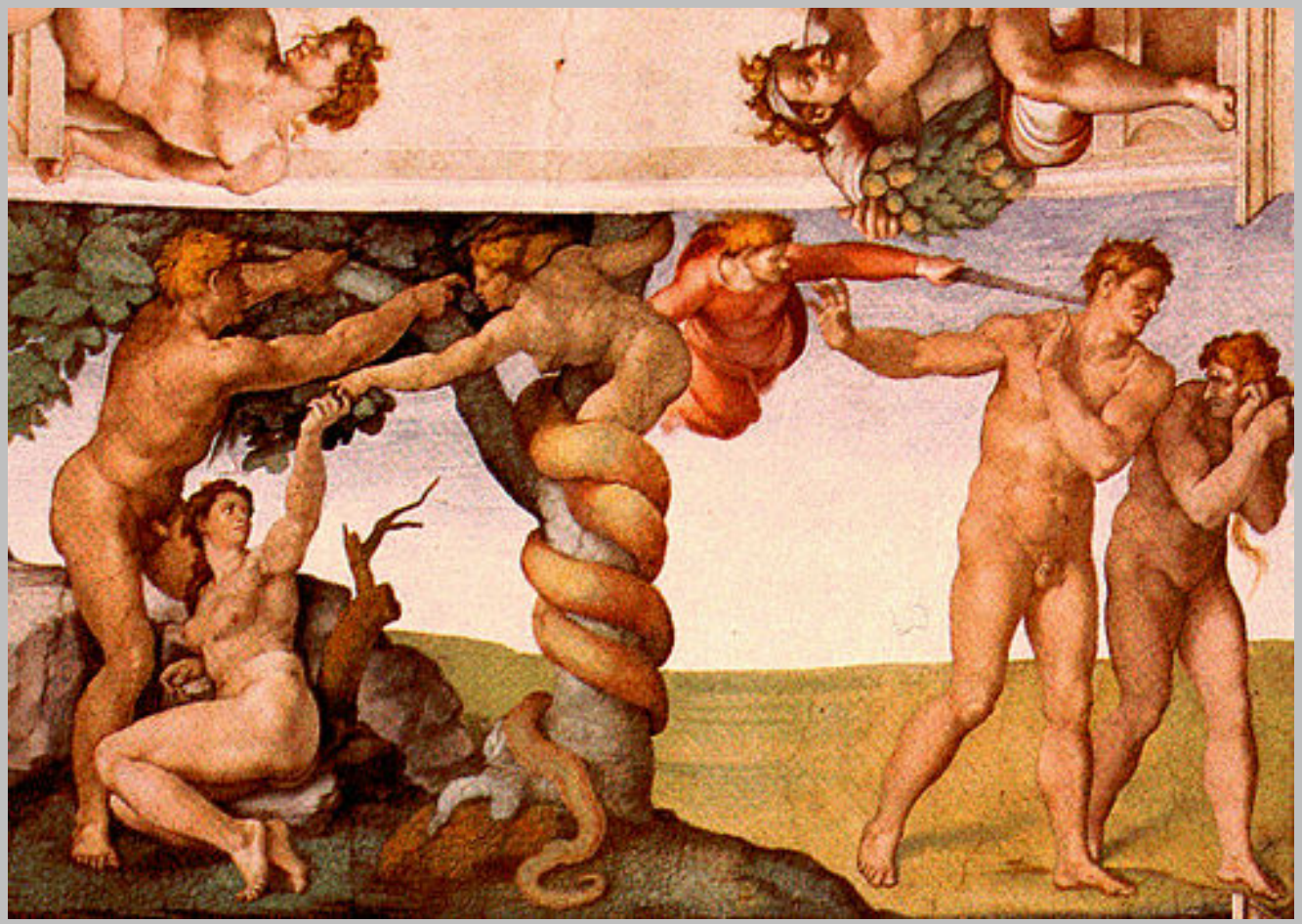
(Received March 25, 1935)

In a complete theory there is an element corresponding to each element of reality. A sufficient condition for the reality of a physical quantity is the possibility of predicting it with certainty, without disturbing the system. In

quantum mechanics is not complete or (2) these two quantities cannot have simultaneous reality. Consideration of the problem of making predictions concerning a system on the basis of measurements made on another system that

A biblical perspective

...and the tree of the knowledge of good and evil



וּמֵעֵ֣ץ הַדַּ֔עַת טֹ֖וב וָרָ֑ע לֹ֣א תֹאכַ֗ל מִמֶּ֛נּוּ כִּ֥י בְיֹ֛ום אֲכָלְךָ֖ מִמֶּ֥נּוּ מֹ֖ות תָּמֻֽות