

# Quantum computers

## Threat and promise

J Avron

June 4, 2023

# Overview

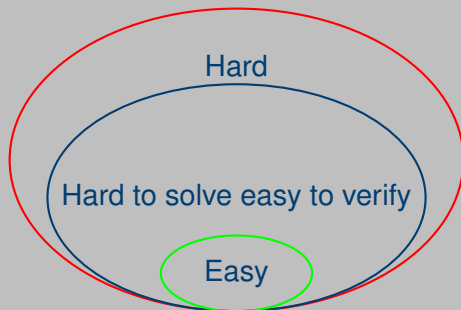
- 1 What's the problem with cyber security?
- 2 Quantum computers: The threat
- 3 The quantum promise
- 4 The word view of QM
- 5 A biblical perspective



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

Not guaranteed by math or physics

Rests on belief



# Factoring

Hard to solve easy to verify

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



# RSA: Standard cyber security tool

The image shows a Windows Certificate dialog box in the foreground, displaying details for a certificate. The 'General' tab is active, showing the following information:

Field	Value
Signature hash algorithm	sha256
Issuer	DigiCert SHA2 Secure Server ...
Valid from	Tuesday, August 14, 2018 02:...
Valid to	Wednesday, October 30, 201...
Subject	online.leumi-card.co.il, IT, Leu...
Public key	RSA (2048 Bits)
Public key parameters	05 00
Authority Key Identifier	KeyID:a0f80611e823161d52f2

Below the table, a hexadecimal representation of the public key is shown:

```

30 82 01 0a 02 82 01 01 00 86 c4 82 3a c3
60 2f a6 63 8d 9d af 46 94 72 07 86 e7 cd
e9 13 a4 d4 66 12 f2 76 38 99 52 94 62 ae
c4 d5 c8 77 34 0f 24 c9 e2 fa 13 e2 02 d4
29 a7 76 64 72 cc b3 b4 99 6e a4 30 53 dc
ea 25 e5 4f 1f cb f7 9c 25 ba 35 f1 07 5d
31 87 dc 26 a9 da 8c 31 ee 72 cf 41 1a 92
be 5b ba 44 13 3a 7b 28 a6 76 77 db 13 b9
b3 5d c3 27 80 c9 52 28 d4 47 8c b4 39 82
  
```

Buttons at the bottom of the dialog include 'Edit Properties...', 'Copy to File...', and 'OK'.

In the background, a web browser window is visible, showing a page from the University of Haifa (האוניברסיטה הפתוחה). The page title is 'עסקאות בטיחות' (Security Transactions). The browser's address bar shows a URL with 'utm\_source=DapapEmail'. The page content includes a search bar, a login button, and a list of transactions.

# 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 copied

Quantum money



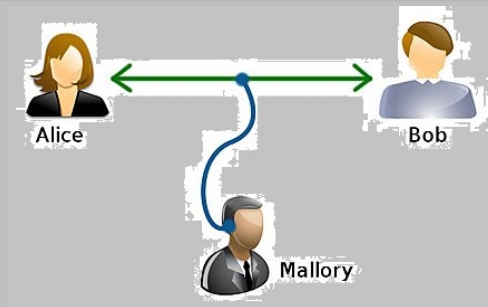
Stephen Wiesner 1942-2021

# Secure Quantum communication

Security guaranteed by physics

## The uncertainty principle

If information is leaked the quantum system changed

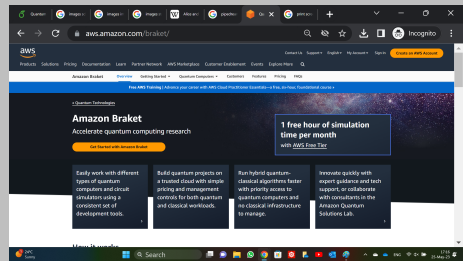


Alice and Bob can tell if there is an eavesdropper



# Current status

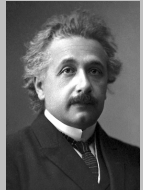
- Quantum communication (QKD):  
Market of enthusiasts
- Quantum cloud computing  
Small and unreliable computers:  
Market of enthusiasts  
Maybe useful for chemistry
- Large quantum computers:  
Don't exist yet
- Post quantum crypto:



# 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*

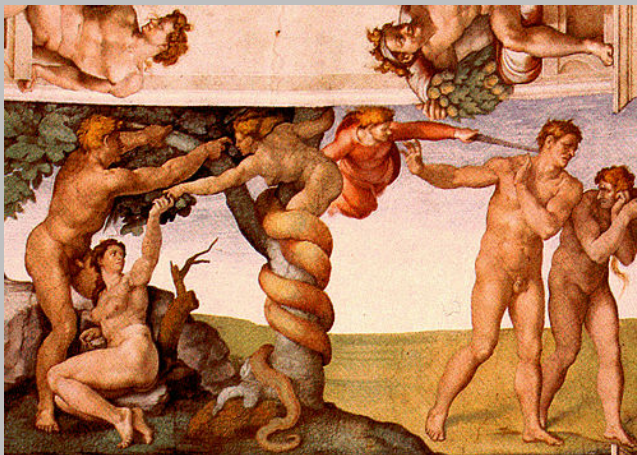
(Received March 25, 1935)

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



וַיִּמְעַץ הַדֵּעַת טוֹב וְרָע לֹא תֹאכַל מִמֶּנּוּ כִּי בַיּוֹם אֲכָלְכֶם מִמֶּנּוּ מוֹת תָּמוּת.