Quantum Computers vs. Computers Security

JP Aumasson / @veorq — Kudelski Security

DEF CON 23 LAS VEGAS

Schrodinger equation

Uncertainty principle

Entanglement

Hilbert spaces

Nobody understands this stuff, and you don't need it to understand quantum computing

Wave functions

EPR pairs

Unitary matrices

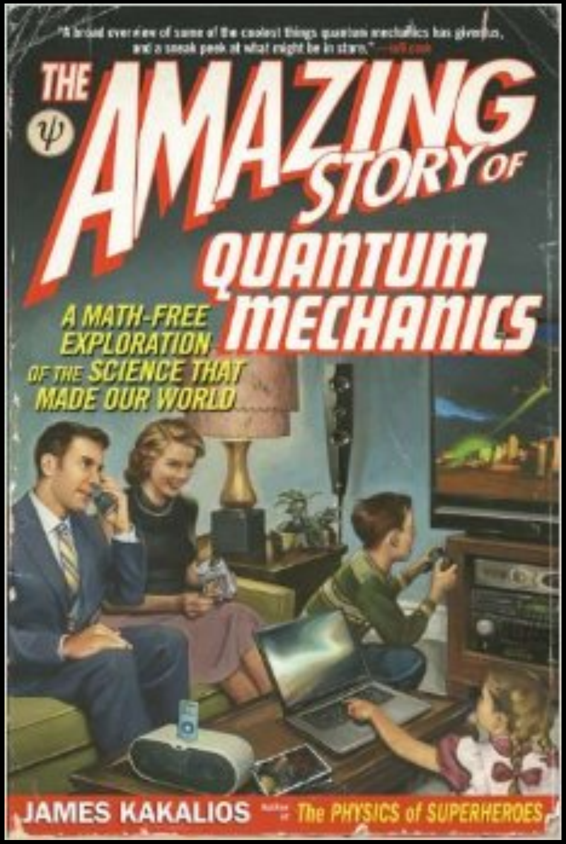
Tensor products

Bell states

Agenda

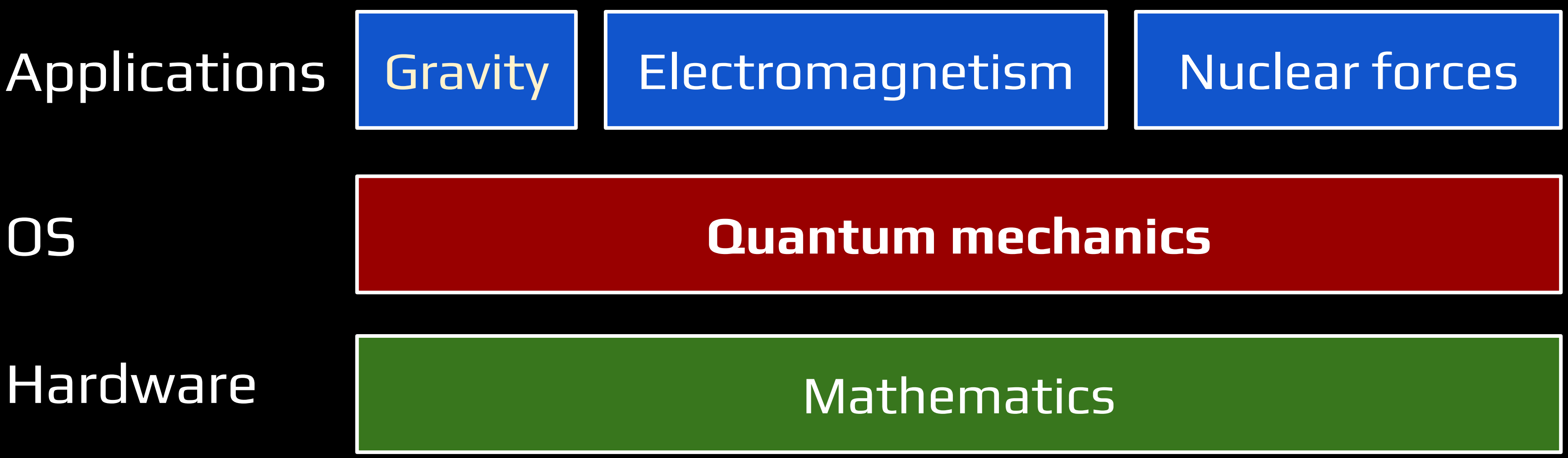
1. QC 101
2. In practice
3. Breaking crypto
4. Post-quantum crypto
5. Quantum key distribution
6. Quantum copy protection
7. Quantum machine learning
8. Conclusions

1. QC 101


THE AMAZING STORY OF QUANTUM MECHANICS
A MATH-FREE EXPLORATION OF THE SCIENCE THAT MADE OUR WORLD
JAMES KAKALIOS
The PHYSICS of SUPERHEROES

Quantum mechanics

Nature's OS



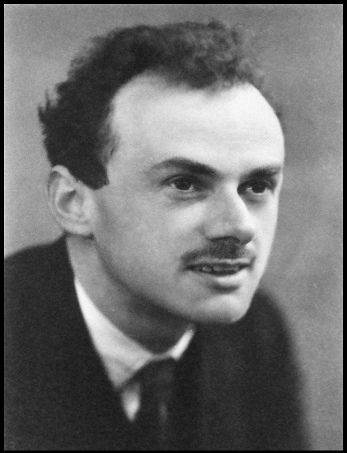
Quantum mechanics — cont.

Particles in the universe behave **randomly**

Their probabilities can be **negative**

"Negative energies and probabilities should not be considered as nonsense. They are well-defined concepts mathematically, like a negative of money."

—Paul Dirac, 1942



Quantum bit (qubit)

$$\alpha\,|0\rangle + \beta\,|1\rangle$$

measure

0 with prob. $|\alpha|^2$

1 with prob. $|\beta|^2$

Stays 0 or 1 forever!

Quantum byte

$$\alpha_{0x00}\,|0x00\rangle + \ldots + \alpha_{0xfe}\,|0xfe\rangle + \alpha_{0xff}\,|0xff\rangle$$

The α’s are called **amplitudes**

Generalizes to 32- or 64-bit quantum words

Quantum computer

Set of **quantum registers**

Qubits/qubytes/quwords

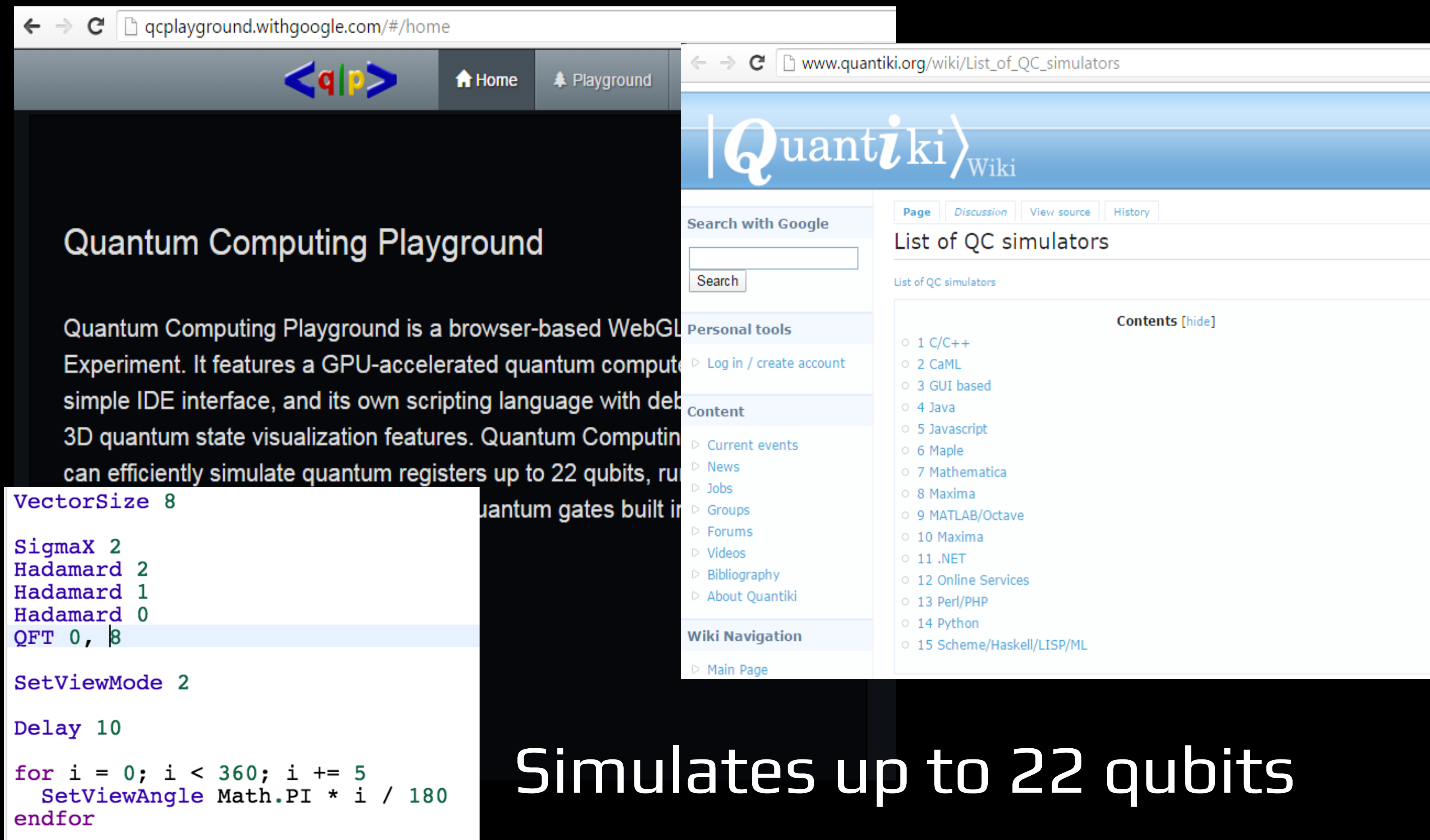
Quantum assembly instructions

Modify probabilities with matrix multiplications

A program usually ends with a **measurement**

Can’t be simulate classically!

Quantum computer simulators



Simulates up to 22 qubits

The killer app

Simulating Physics with Computers

Richard P. Feynman

Department of Physics, California Institute of Technology, Pasadena, California 91107

Received May 7, 1981

Impossible with a classical computer

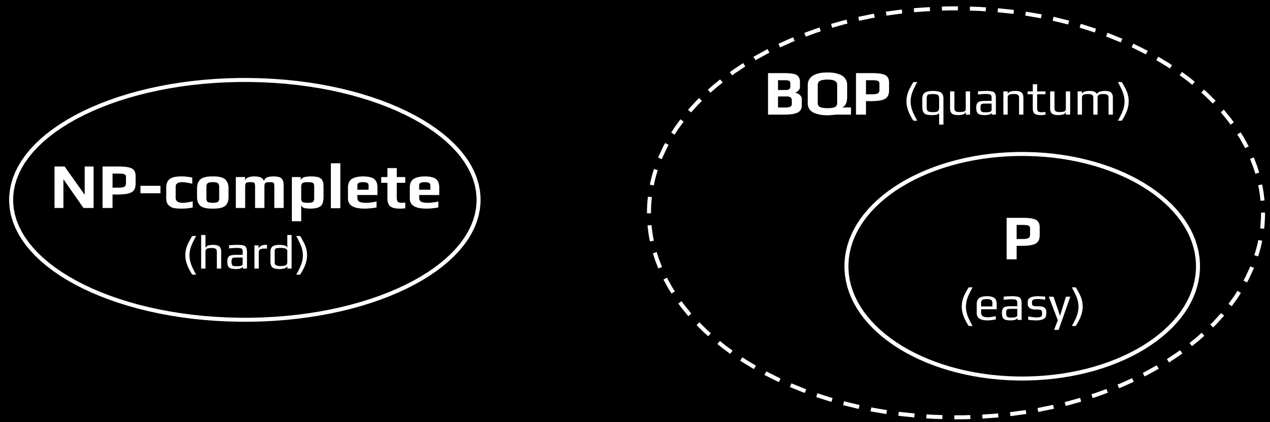
Possible with a quantum computer!

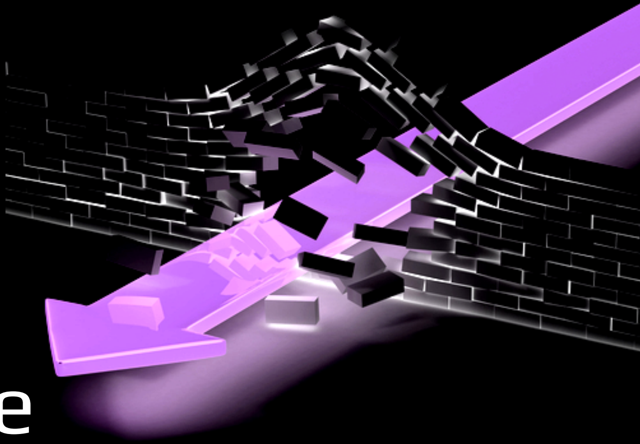
QC vs. hard problems

Ever heard about **NP-complete** problems?

- Solution hard to find, but easy to verify
- SAT, scheduling, Candy Crush, etc.

QC **does not** solve NP-complete problems!





Quantum speedup

Making the impossible possible

Example: **factoring integers**

- Hard classically (exponential-ish)
- Easy with a quantum computer!

Obvious application: **breaking RSA!**

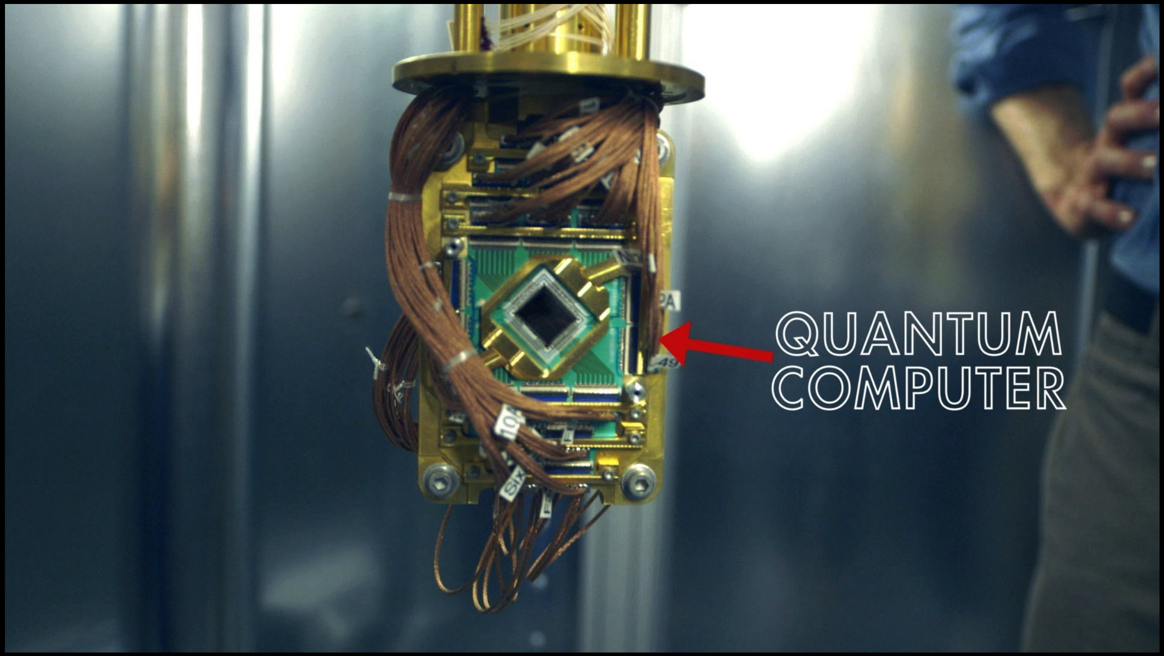
Quantum parallelism

QC kind of encode all values simultaneously

But they **do not** “try every answer in parallel”

You can only **observe one** result, not all

2. In practice



Factoring experiments

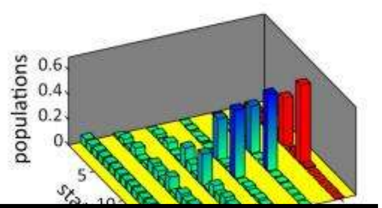
The quantum speed-up poster child

QUANTUM PROCESSOR CALCULATES THAT 15 = 3X5 (WITH ALMOST 50% ACCURACY!)

By Rebecca Boyle Posted August 20, 2012

143 is largest number yet to be factored by a quantum algorithm

April 11, 2012 by Lisa Zyga feature



Quantum factorization of 56153 with only 4 qubits

Nikesh S. Dattani,[1,2,*] *Nathaniel Bryans*[3,†]

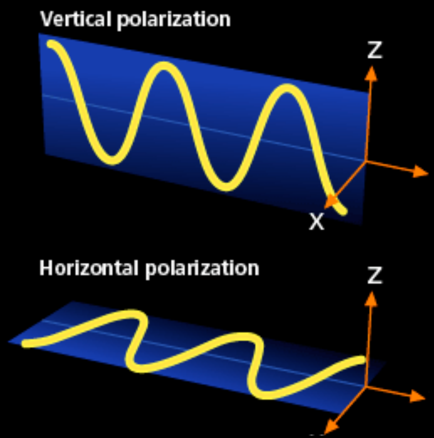
[1] Quantum Chemistry Laboratory, Kyoto University, 606-8502, Kyoto, Japan, [2] Physical & Theoretical Chemistry Laboratory, Oxford University, OX1 3QZ, Oxford, UK, [3] University of Calgary, T2N 4N1, Calgary, Canada. [*] dattani.nike@gmail.com,

Only for numbers with special patterns

Building quantum computers

Qubits obtained from **physical phenomena**

- Photons
- Molecules
- Superconducting



Many challenges:

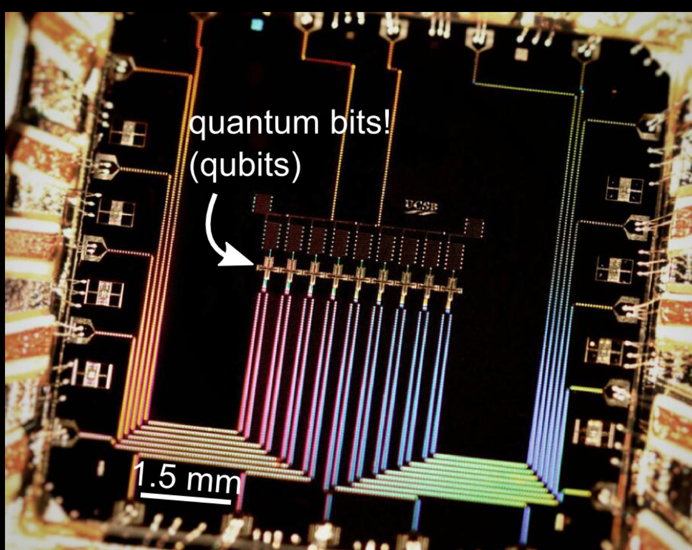
- Qubits mixed up with the environment
- Cooling systems to a low temperature
- Scaling to a useful number of qubits

Recent result (2015)

Stable 9-qubit system

“suppression of environment-induced errors”

“quantum non-demolition parity measurements”



State preservation by repetitive error detection in a superconducting quantum circuit

J. Kelly, R. Barends, A. G. Fowler, A. Megrant, E. Jeffrey, T. C. White, D. Sank, J. Y. Mutus, B. Campbell, Yu Chen, Z. Chen, B. Chiaro, A. Dunsworth, I.-C. Hoi, C. Neill, P. J. J. O’Malley, C. Quintana, P. Roushan, A. Vainsencher, J. Wenner, A. N. Cleland & John M. Martinis

Affiliations | Contributions | Corresponding authors

Nature **519**, 66–69 (05 March 2015) | doi:10.1038/nature14270

3. Breaking crypto

TL;DR: We're doomed

RSA: broken

Diffie-Hellman: broken

Elliptic curves: broken

El Gamal: broken

RSA

Based on the hardness of **factoring**

Knowing **N** = **pq**, look for **p** and **q**

Hard on a classical computer (probably)

BUT **easy on a quantum computer!**

Discrete logarithms

Problem behind **Diffie-Hellman, ECC**

Knowing **g** and $\mathbf{g}^{y}$, look for **y**

Hard on a classical computer (probably)
BUT **easy on a quantum computer!**

What about symmetric ciphers?

Grover algorithm FTW!

AES-128 security

- Classical: 128-bit
- Quantum: **64-bit**

Upgrade to 256-bit keys for 128-bit security

4. Post-quantum crypto

Post-quantum crypto

Alternatives to RSA, Diffie-Hellman, ECC

- Seem resistant to QC

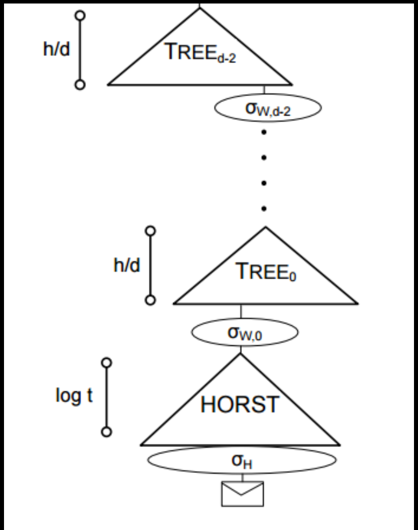
http://pqcrypto.org/

Hash-based signatures

Problem: inverting **hash functions**

SPHINCS signatures http://sphincs.cr.yp.to/

- 41 KB signatures
- 1 KB public and private keys
- Slow (100s signatures/sec)



Multivariate signatures

Problem: solve complex systems of equations

$0 = X_1X_2X_3 + X_1X_3 + X_2X_4$

$1 = X_1X_3X_4 + X_2X_3X_4$

$0 = X_1X_3 + X_2X_3$

Many schemes have been broken :-/

QC vs signatures and encryption

Minor impact on **signatures**

- Just issue new post-quantum signatures

Encryption compromised anyway

- Old ciphertexts could be decrypted

Code-based crypto

Problem: decoding **error-correcting codes**

Schemes: McEliece (1979), Niederreiter (1986)

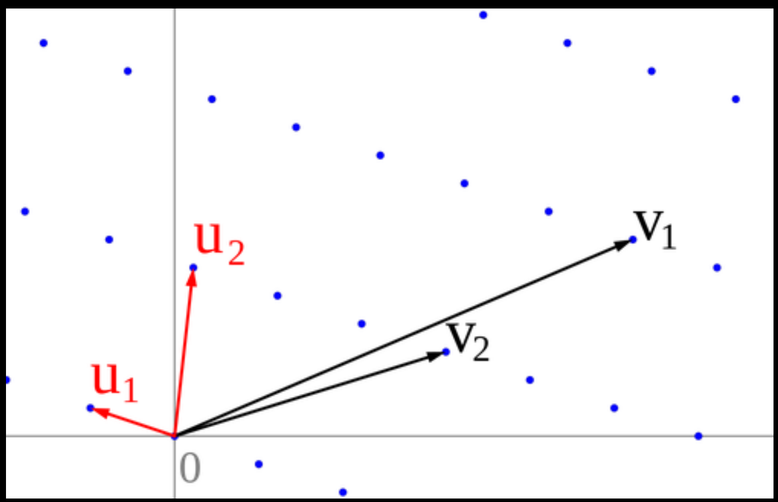
Limitations:

- Large keys (a few KB+)
- Fewer optimized implementations

Lattice-based crypto

Encryption and signature schemes

Learning-with-errors: learn a simple function given results with random noise



5. Quantum key distribution

Quantum key distribution (QKD)

Establish a **shared key** between 2 parties

- “Quantum Diffie-Hellman”
- Not quantum computing, strictly speaking

“Security based on the laws of physics”

- Eavesdropping will cause errors
- Keys are truly random

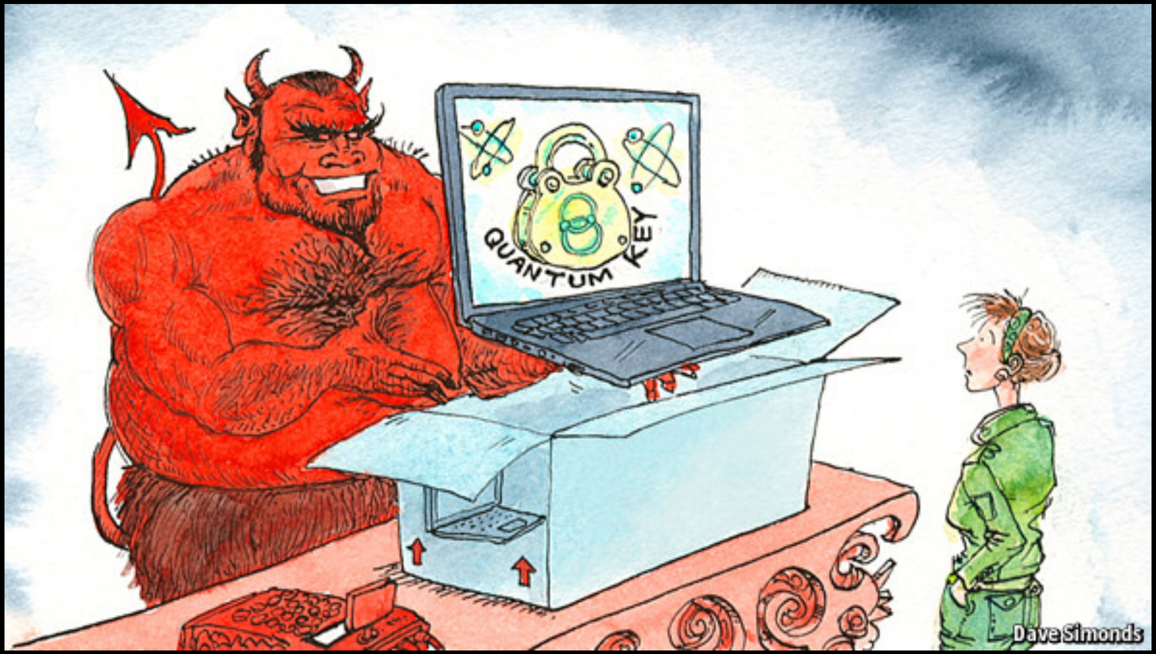
BB84

First QKD protocol, not really quantum

Alice's random bit	0	1	1	0	1	0	0	1
Alice's random sending basis	+	+	X	+	X	X	X	+
Photon polarization Alice sends	↑	→	↘	↑	↘	↗	↗	→
Bob's random measuring basis	+	X	X	X	+	X	+	+
Photon polarization Bob measures	↑	↗	↘	↗	→	↗	→	→

Caveats

Like any security system, it's complicated



Security

Quantum cryptography is secure… except when it's not

Researchers close one security hole in quantum key distribution, but seem to …

Eventually relies on **classical crypto**

- Typically with frequent key changes

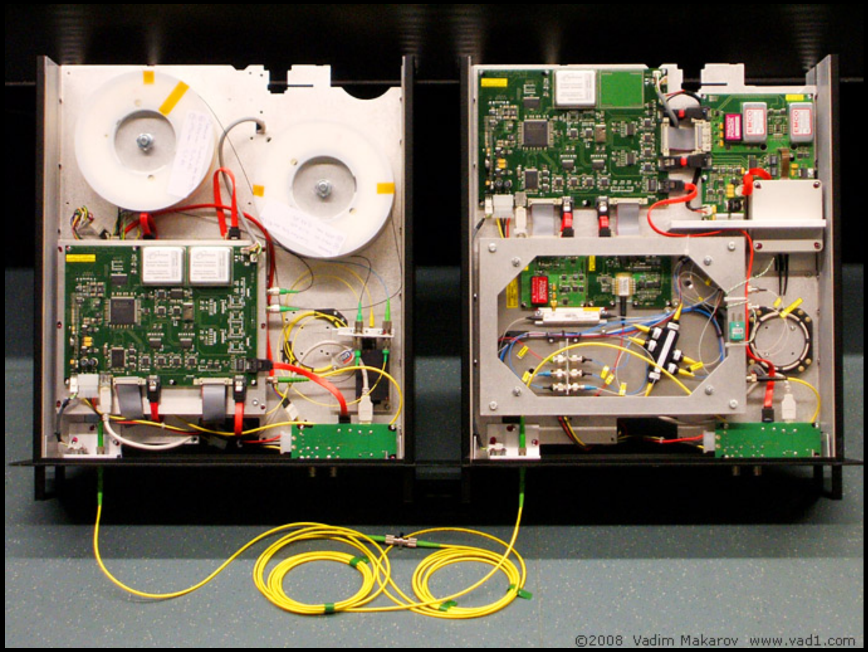
QKD **implementations** have been attacked

"Quantum hacking"

Deployment

Dedicated optical fiber links

Point-to-point, limited distance (< 100 km)

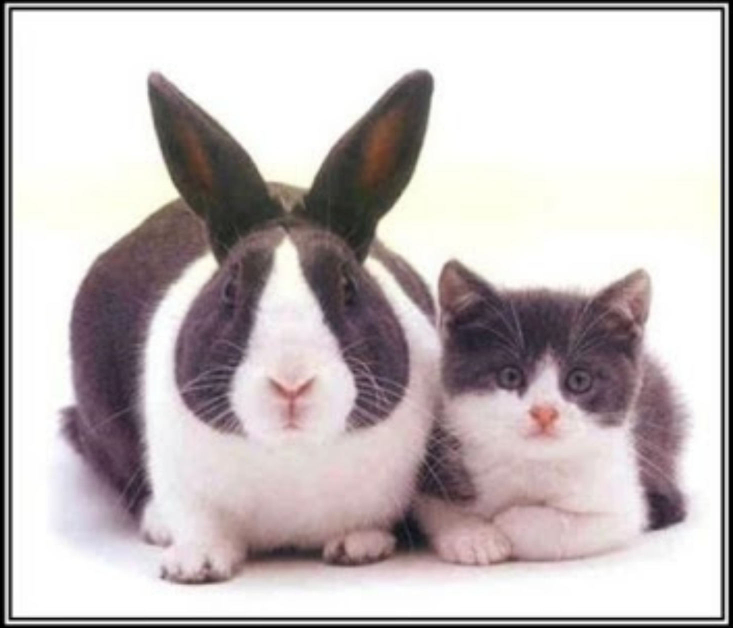


6. Quantum copy protection

Quantum copy protection

Idea: leverage the **no-cloning principle**

'cos you can't know everything about a qubit



CLONING

Results may vary

Quantum cash

Impossible to counterfeit, **cos' physics** (1969)

- Qubits with some secret encoding
- Only the bank can authenticate bills
- Decentralized using (classical) pubkey crypto

Quantum software protection

Using quantum techniques

- "Obfuscate" the functionality
- Make copies impossible

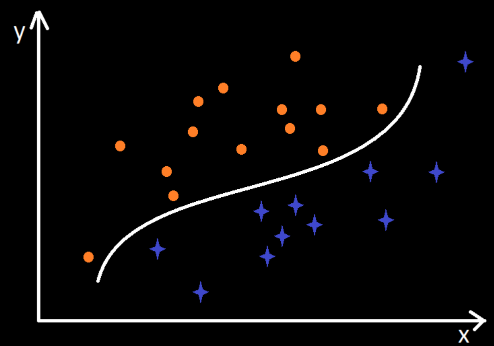
```
verify(pwd) {
   return pwd == "p4s5w0rD"
} # we want to hide the password (or anything related: hash...)
```

1. Turn `verify()` into a list of qubits
2. Verification: apply a transform that depends on `pwd`, then measure the qubits

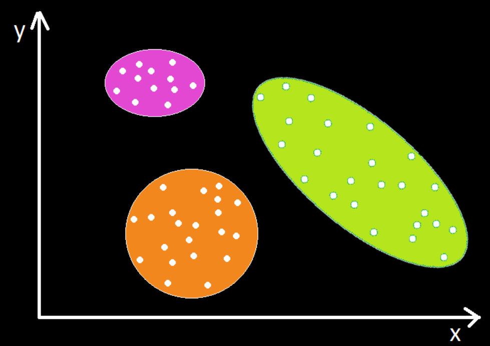
7. Quantum machine learning

Machine learning

“Science of getting computers to act without being explicitly programmed” —Andrew Ng



Supervised



Unsupervised

Successful for spam filtering, fraud detection, OCR, recommendation systems

ML and security: no silver bullet

Intrusion detection (network, endpoint)

- Problem of false positives’ cost
- Many abnormal patterns that aren’t attacks

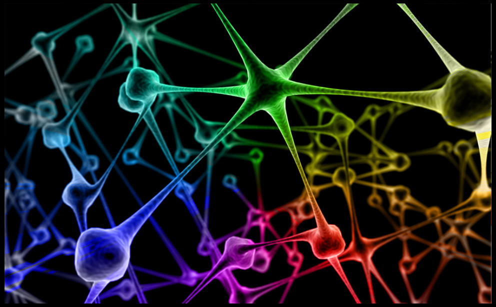
Vendors give neither

- Details on the techniques used, nor
- Effectiveness figures or measurements

Quantum machine learning

"Port" of basic ML techniques to QC, like

- k-means clustering
- Neural networks



Many use **Grover** for a **square-root speedup**

Potential exponential speedup, but...

Quantum RAM (QRAM)

Awesome concept

- Addresses given in superposition
- Read values retrieved in superposition

Many QML algorithms need QRAM

But it'd be extremely **complicated to build**

8. Conclusions

Quantum computers su**

ARE NOT superfaster computers

WOULD NOT solve NP-hard problems

MAY NEVER BE BUILT anyway

MAXIMUMPC Best of the Best Build a PC Features Reviews How-Tos

MIT Scientist Offers $100k Prize To Anyone Able To Prove Quantum Computing Is Useless

Brad Chacos Feb 7, 2012

Quantum computers are awesome

Would BREAK ALL CRYPTO deployed (pubkey)

Give new meaning and power to COMPUTING

May teach us a lot about NATURE

Thank you!