

Quantum Computers vs. Computers Security

JP Aumasson / @veorq – Kudelski Security

DEF CON
LAS VEGAS **23**

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

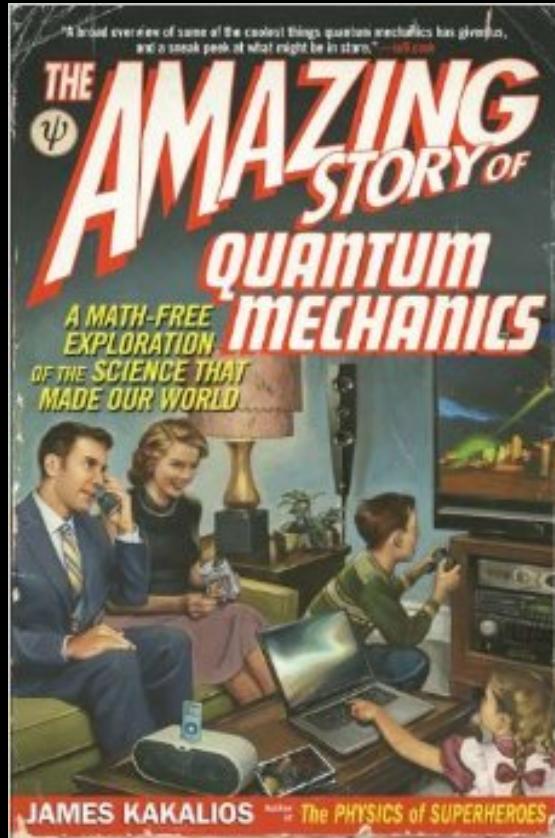
Tensor products

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



Quantum mechanics

Nature's OS

Applications

Gravity

Electromagnetism

Nuclear forces

OS

Quantum mechanics

Hardware

Mathematics

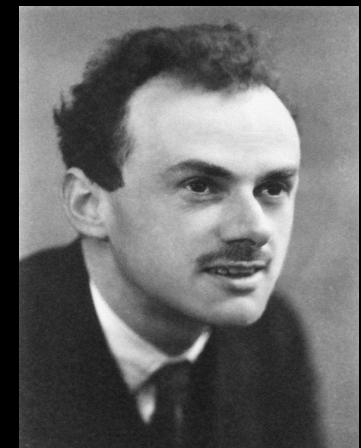
Quantum mechanics – cont.

Particles in the universe behave **randomly**

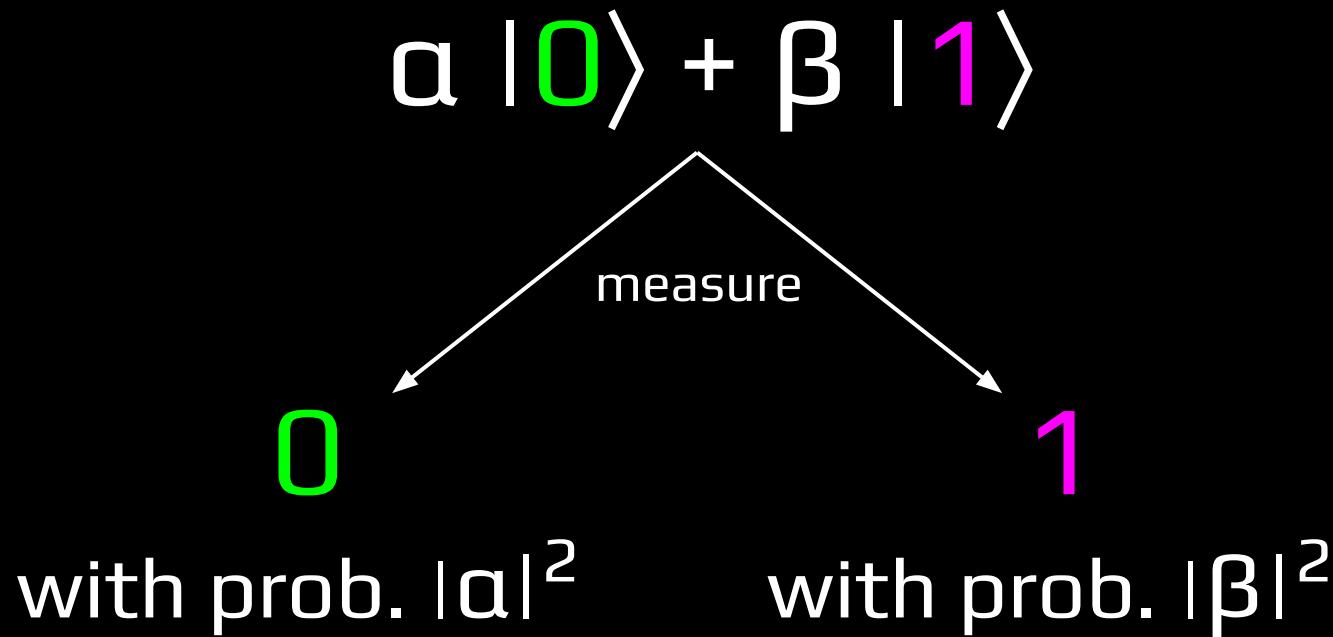
Their probabilities can be **negative**

"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)



Stays 0 or 1 forever!

Quantum byte

$$a_{0x00} |0x00\rangle + \dots + a_{0xfe} |0xfe\rangle + a_{0xff} |0xff\rangle$$

The a 's are called **amplitudes**

Generalizes to 32- or 64-bit quantum words

Quantum computer

Set of **quantum registers**

Qubits/qubties/quwords

Quantum assembly instructions

Modify probabilities with matrix multiplications

A program usually ends with a **measurement**

Can't be simulate classically!

Quantum computer simulators

The image shows a web browser with two tabs open. The left tab displays the 'Quantum Computing Playground' at qcplayground.withgoogle.com. It features a dark background with a navigation bar at the top containing a logo (<qlp>), a 'Home' button, and a 'Playground' button. Below the navigation bar, the title 'Quantum Computing Playground' is displayed. The main content area contains text describing the playground as a browser-based WebGL Experiment, mentioning GPU-accelerated quantum computation, a simple IDE interface, and its own scripting language with debugging features. A code editor window shows some quantum circuit code. The right tab displays the 'List of QC simulators' at www.quantiki.org/wiki/List_of_QC_simulators. The page has a blue header with the Quantiki logo. It includes a search bar, personal tools (log in/create account), content links (Current events, News, Jobs, Groups, Forums, Videos, Bibliography, About Quantiki), and a main content area titled 'List of QC simulators' which lists 15 different QC simulators, each preceded by a numbered circle (1 through 15). A 'Contents [hide]' link is also present.

qcplayground.withgoogle.com/#/home

www.quantiki.org/wiki/List_of_QC_simulators

Quantum Computing Playground

Quantum Computing Playground is a browser-based WebGL Experiment. It features a GPU-accelerated quantum computer, a simple IDE interface, and its own scripting language with debugging features. Quantum Computing Playground can efficiently simulate quantum registers up to 22 qubits, running quantum gates built in C/C++.

```
VectorSize 8
SigmaX 2
Hadamard 2
Hadamard 1
Hadamard 0
QFT 0, 8

SetViewMode 2

Delay 10

for i = 0; i < 360; i += 5
    SetViewAngle Math.PI * i / 180
endfor
```

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

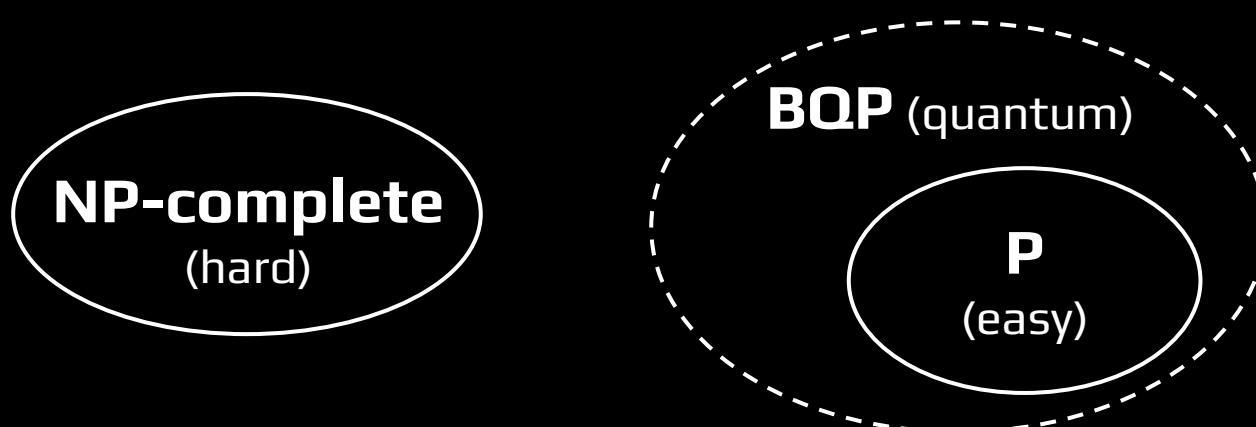
Possible with a quantum computer!

QC vs. hard problems

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

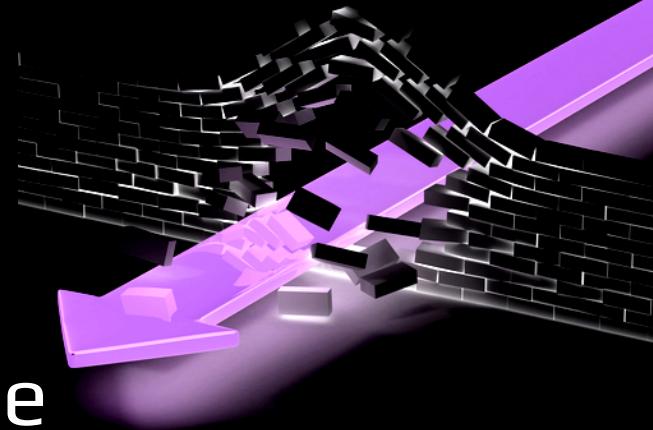
Solution hard to find, but easy to verify
SAT, scheduling, Candy Crush, etc.

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

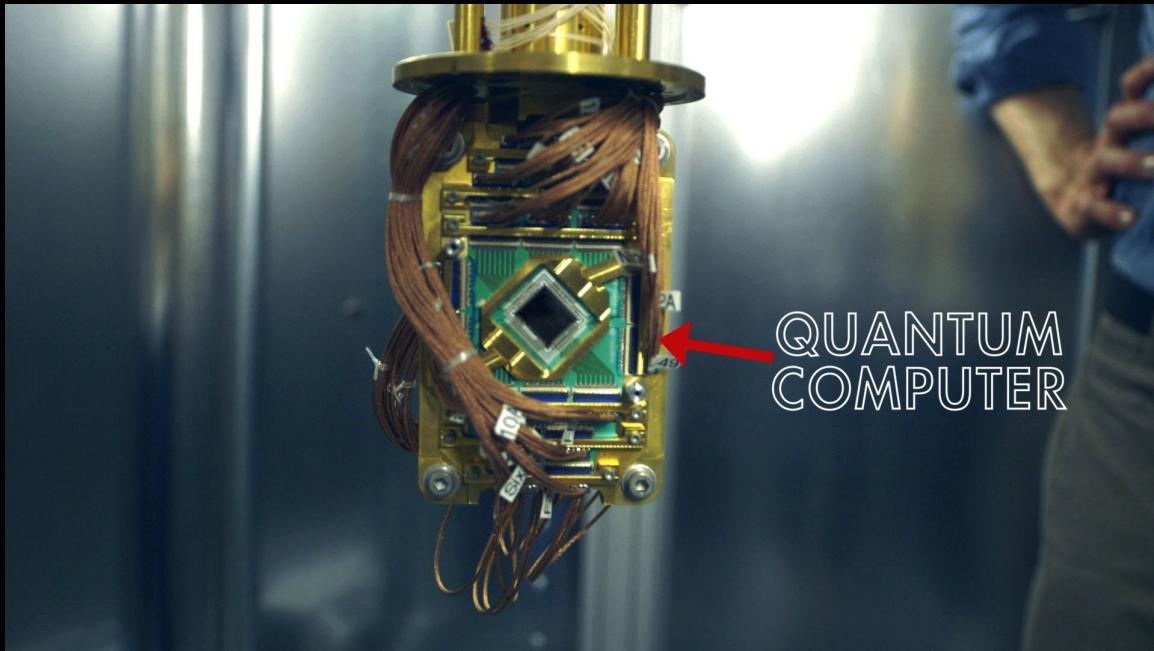
QC kind of encode all values simultaneously

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

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



2. In practice



Factoring experiments

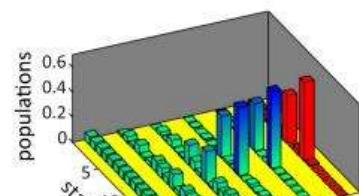
The quantum speed-up poster child

QUANTUM PROCESSOR CALCULATES THAT $15 = 3 \times 5$ (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

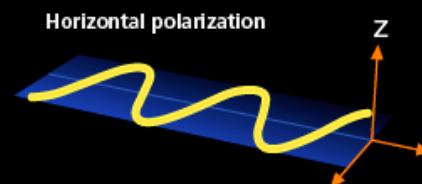
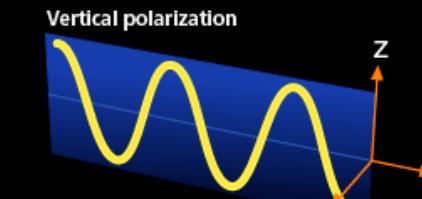
Building quantum computers

Qubits obtained from **physical phenomena**

Photons

Molecules

Superconducting



Many challenges:

Qubits mixed up with the environment

Cooling systems to a low temperature

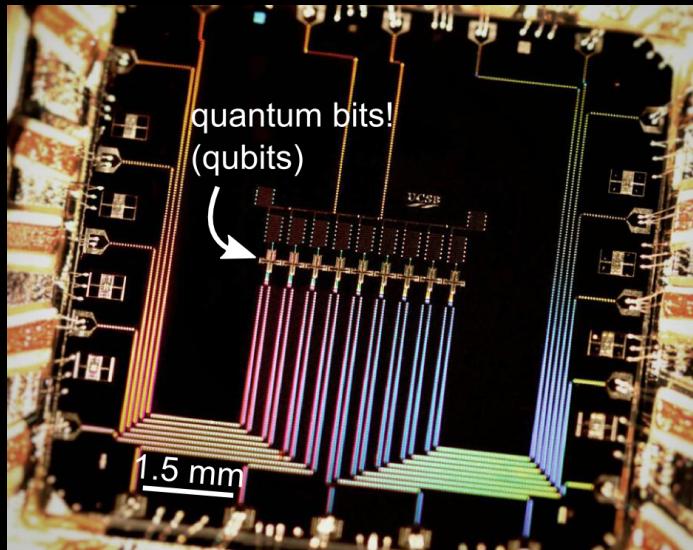
Scaling to a useful number of qubits

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 **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

hope

Post-quantum crypto

Post-quantum crypto

Alternatives to RSA, Diffie-Hellman, ECC

Seem resistant to QC

<http://pqcrypto.org/>

The screenshot shows the NIST Information Technology Laboratory (ITL) website. The main header features the text "The Seventh International Conference on Post-Quantum Cryptography" in large white font, with the subtitle "Fukuoka, Japan, February 24-26, 2016" below it. The background of the header is a blue and purple abstract pattern. The left sidebar contains the NIST logo, the ITL name, and navigation links for "About ITL", "Publications", and "Topics". A breadcrumb navigation bar at the bottom left includes "NIST Home > ITL > Computer Security Division". A large white rectangular box at the bottom contains the text "Workshop on Cybersecurity in a Post-Quantum World".

Hash-based signatures

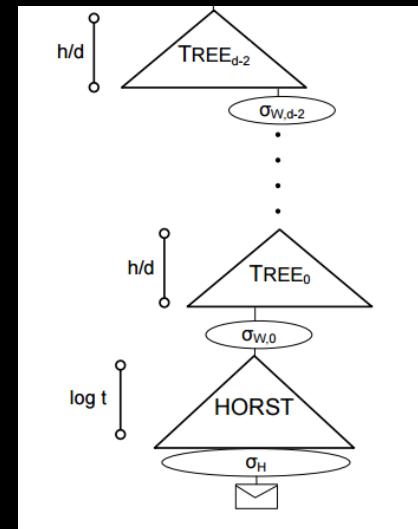
Problem: inverting **hash functions**

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

$$0 = X_1 X_2 X_3 + X_1 X_3 + X_2 X_4$$

$$1 = X_1 X_3 X_4 + X_2 X_3 X_4$$

$$0 = X_1 X_3 + X_2 X_3$$

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:

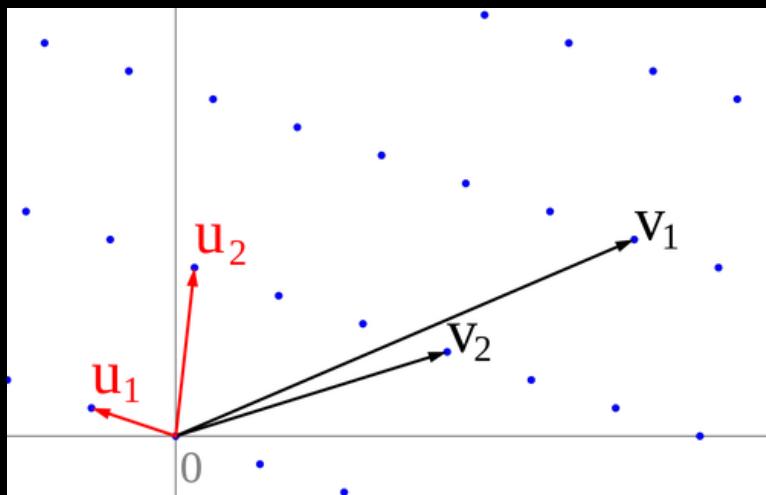
Large keys (a few KB+)

Fewer optimized implementations

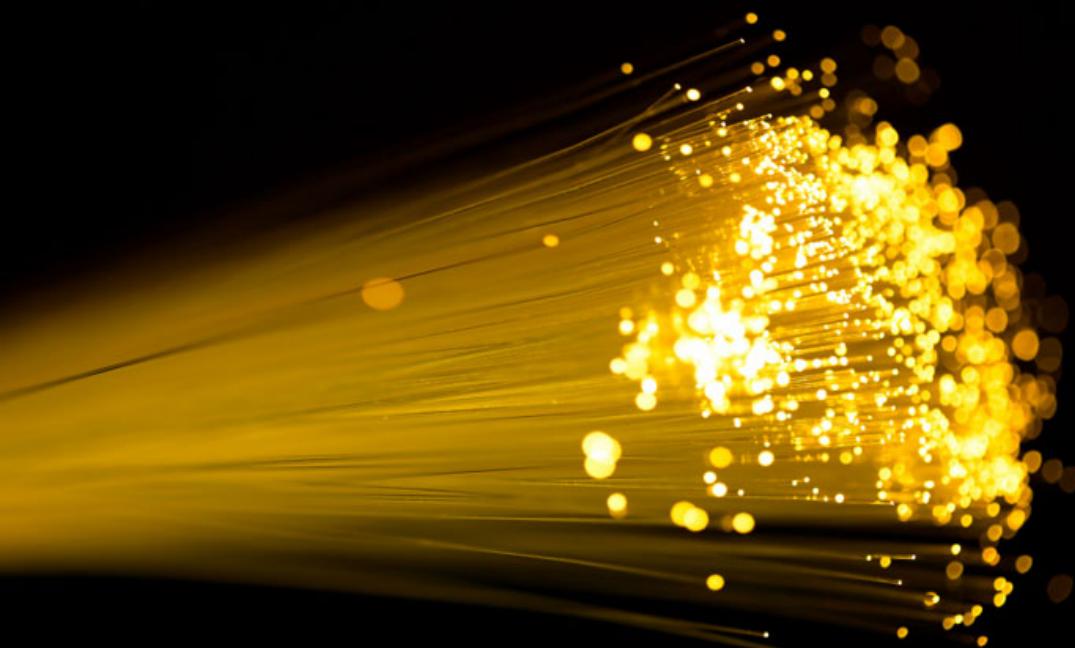
Lattice-based crypto

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

Quantum key distribution

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	↑	↗	↓	↗	→	↗	→	→

Quantum key distribution

Caveats

Like any security system, it's complicated



Quantum key distribution

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"

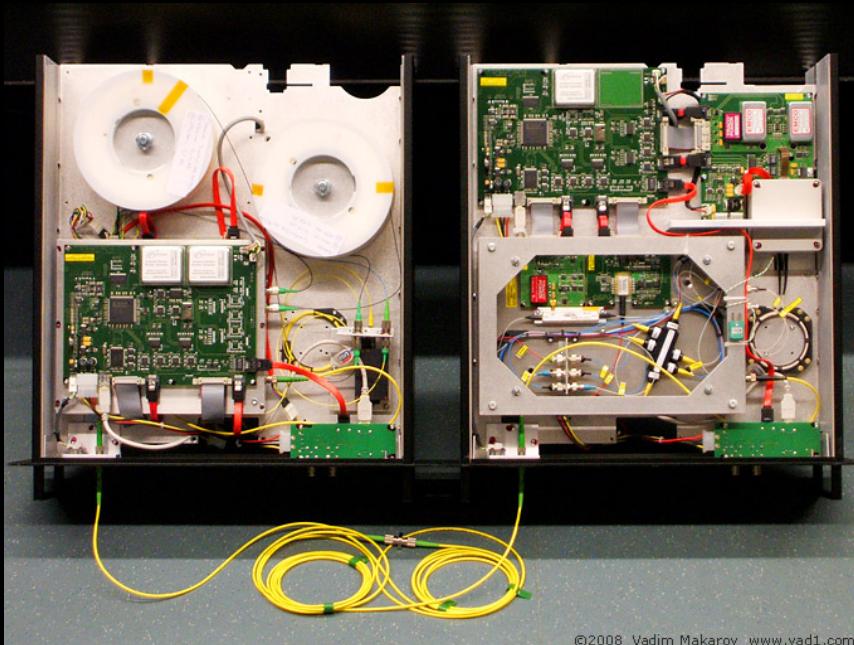


©2010 NTNU Info / Geir Mogen

Deployment

Dedicated optical fiber links

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



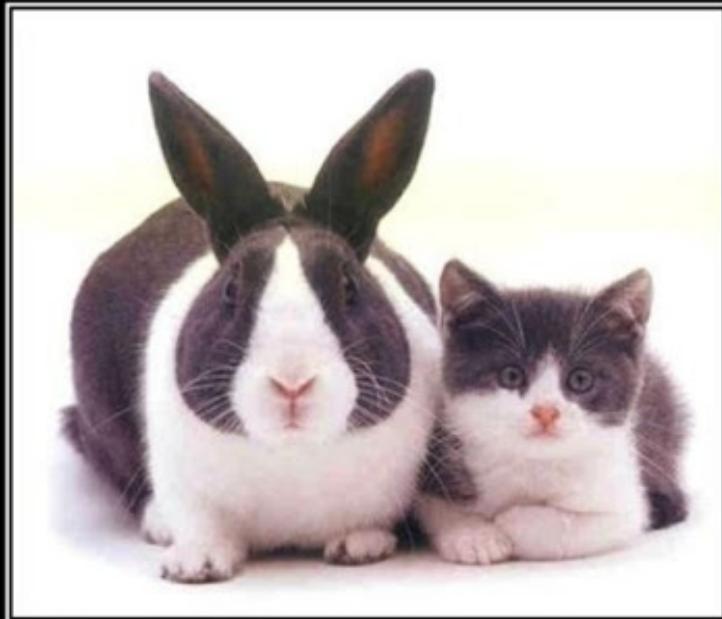
6. Quantum copy protection



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 copy protection

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 copy protection

Quantum software protection

Using quantum techniques

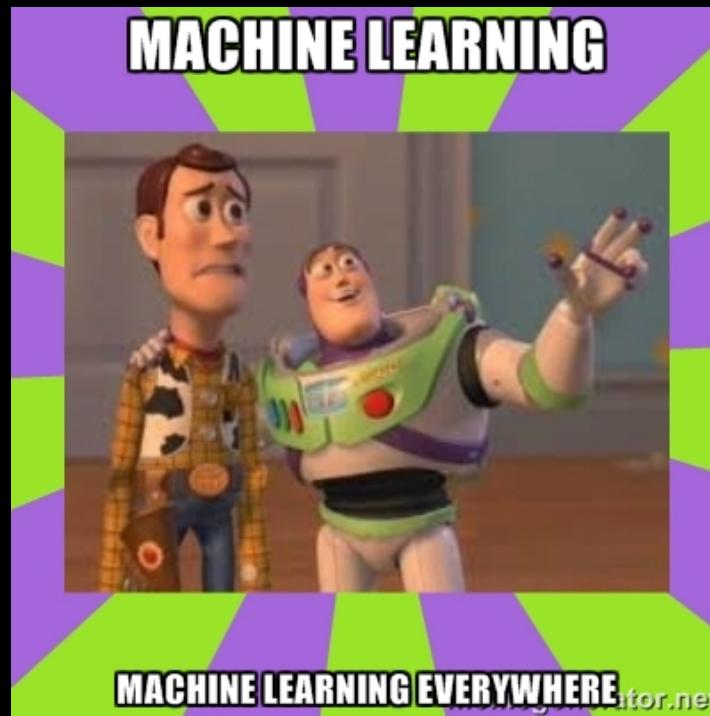
"Obfuscate" the functionality

Make copies impossible

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

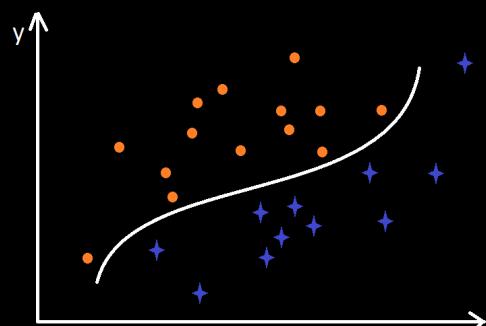
1. Turn `verify()` into a list of qubits
2. Verification: apply a transform that depends on `pwd`, then measure the qubits

7. Quantum machine learning

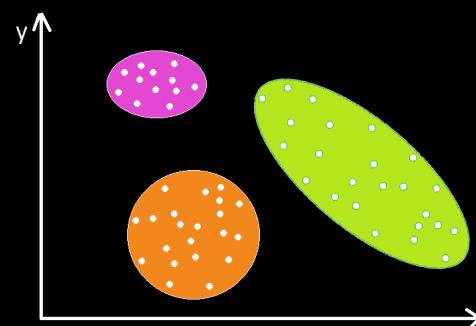


Machine learning

“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

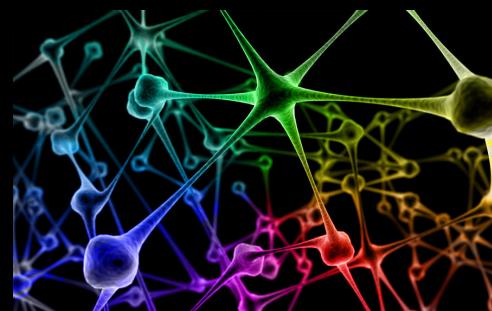
Quantum machine learning

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 superfast computers
WOULD NOT solve NP-hard problems
MAY NEVER BE BUILT anyway



[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!