Cryptography in a quantum world

Petros Wallden

School of Informatics, University of Edinburgh

25th October 2016

Outline

- What is quantum computation
- Why should we care if quantum computers are constructed? (a crypto view)
- Should we worry?
- Two directions for solving this issue
- An unconditionally secure protocol: Quantum key distribution

What is quantum computation?

- Quantum physics is one of the most successful theories (in terms of theory, accuracy of predictions and applications).
- Quantum systems have strange properties that classical everyday objects do not have. Is probably one of the (conceptually) least understood theories.

Central Question

Can we built a computer using as basic information elements quantum systems, and will this give us extra power?

- Could in principle attempt to construct a computer that basic elements instead of bits are quantum systems (qubits) that behave in this strange way.
- What power would such a machine have? Would it be equally, more or less powerful than normal computers?
- Can we actually built such machines? (What stops us so far is theoretical limitations, practical challenges or both ?)

Quantum Vs Classical Bits

Bit	**Qubit**
Takes values either 0 or 1	Can behave as being simultaneously 0 and 1: $\alpha \left\|0\right\rangle + \beta \left\|1\right\rangle$
Measurement reveals the value of the bit	Measurement disturbs the system
Can be copied	Cannot be copied
String of bits are described in terms of single bits (local)	String of qubits can have properties that cannot be described in terms of single qubits (non-local)
	Qubits behave as waves and "interfere" with each other

Note: Quantum computers are not faster (in terms of operations per second) BUT use the strange quantum properties and can perform algorithms/operations that are not possible with a classical computer.

Why should we care?

Quantum Computation

- Physics simulations
- Breaking cryptography?
- Machine learning
- Data mining
- Distributed computation
- Advances in classical computation
- And more...

Quantum Cryptography

- Key distribution
- Secure authentication
- Digital signatures
- Secure computation
- Quantum money
- Advances in classical cryptography
- And more...

"*For me, the single most important application of a quantum computer is disproving the people who said it's impossible. The rest is just icing on the cake*"

Scott Aaronson

Why should we care?

- There exists algorithm for a quantum computer, that efficiently solves factoring and discrete log (Shor's algorithm).
- Actually all the intractable problems given in Lecture 12 (Factoring, RSAP, Discrete Log, DHP) become tractable with quantum computers!
- Most, currently used, cryptographic protocols are based on the assumption that these problems are hard.
- Quantum computers can solve efficiently (class BQP) a larger class of problems than classical computers. BQP is less explored and so our belief on the hardness of problems for quantum computers is not so well founded.

Take-home message

If a scalable quantum computer is built, most of current cryptography breaks (from emails, bank transactions to national security secrets)!

Should we worry?

- There is no theoretical reason that rules out quantum computers
- State of Art:
  - **2001** Shor's algorithm factors 15 on 7 qubits
  - **2011** Shor's algorithm factors 21
  - **2012** Universal quantum computation on 2 fault tolerant qubits
  - **2014-2015** Qubits and gates in silicon chips
  - **2015** D-Wave 2X, 1000 qubits, optimization problems, no fault tolerance
  - **2016** IBM, universal quantum computation on 5 fault tolerant qubits (publicly available)
  - **2020** NQIT, Q20:20, fault tolerant (20 qubits), scalable
- However (1) current implementations are (in principle) scalable, (2) there is a recent initiative with major funding from governments (U.K., EU, USA, Canada, Australia, China, etc) and leading companies (Google, IBM, etc) worldwide.

Should we worry?

News story

Quantum technologies: a new era for the UK

IS QUANTUM COMPUTING SET FOR AN INVESTMENT BOOM?

September 3, 2015 Timothy Prickett Morgan

Intel (INTC) Stock Gains on Quantum Computing Investment

By Amanda Gomez 09/03/15 - 03:14 PM EDT

The CIA and Jeff Bezos Bet on Quantum Computing

With funding from the Amazon founder and the CIA's investment arm, the Canadian company D-Wave is gaining momentum for its revolutionary approach to computing.

Why's IBM Investing $3 Billion In Quantum Computing & Synth Brains? Trillion Dollar Humanoid Market

Sep 3, 2015 | 26 Likes | 11 Comments

A new strategy to guide ... markets over the next 20 years.

It aims to create a coherent government ... technology community that gives the UK a ...

TECH

Intel to Invest $50 Million in Quantum Computers

... joining effort to solve problems beyond reach of today's hardware

community and is published by Innovate UK and the Engineering and Physical Sciences Research Council.

... million investment in the UK National ... Statement, to be

NSA working on quantum computer to break any encryption

The spy agency is reportedly in a race to build its own quantum ... mother of all decryption machines.

UNSW to receive AU$10m from CommBank for quantum computing

Should we worry?

€1 Billion Quantum Project planned for 2018

23rd May 2016

The European Commission has announced plans to launch a €1 billion project to boost a raft of quantum technologies; from secure communication networks to ultra-precise gravity sensors and clocks.

The initiative, to launch in 2018, will be similar in size, timescale and ambition to two existing projects; the decade-long Graphene Flagship and the Human Brain Project.

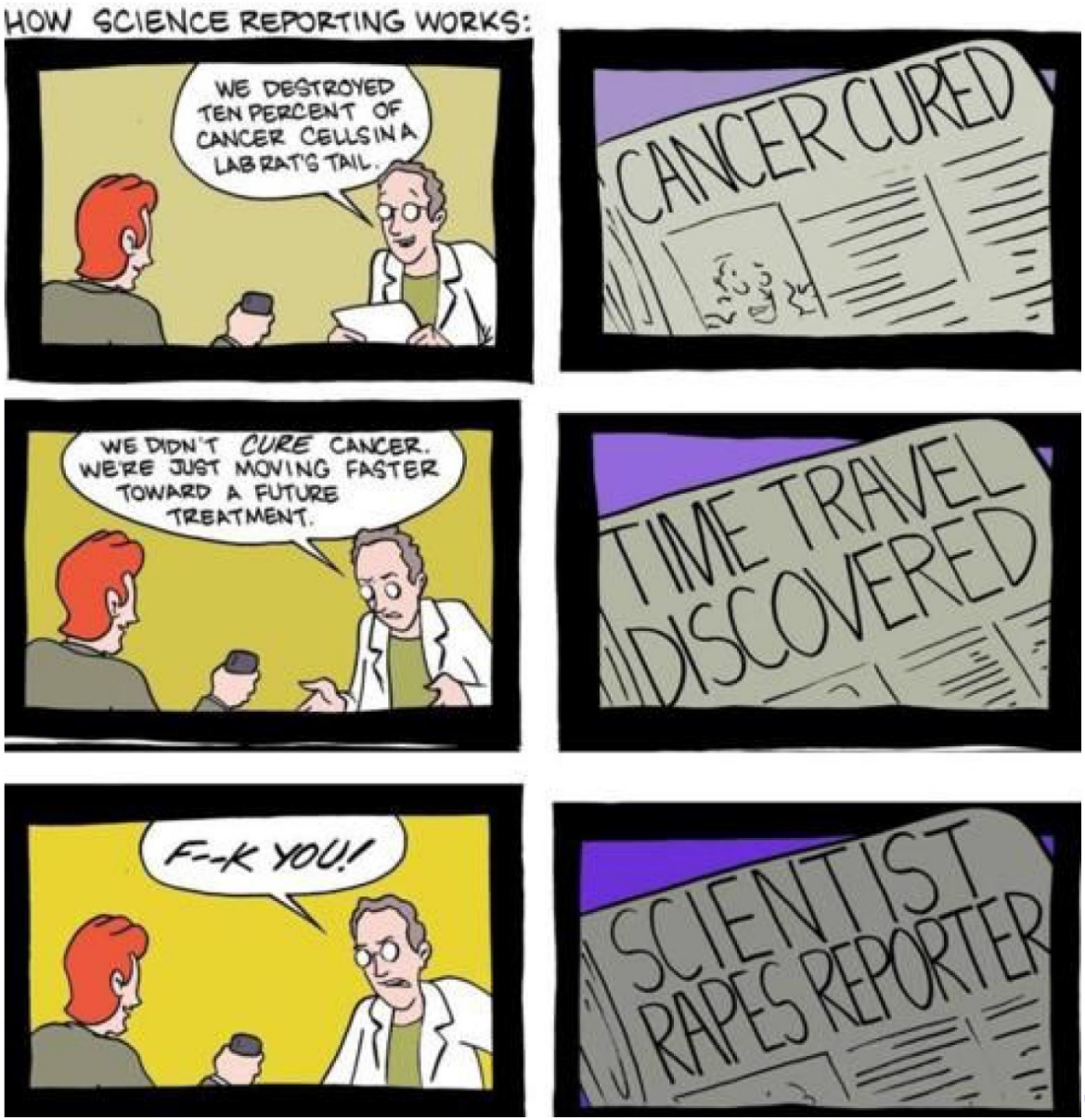
The commission is likely to have a "substantial role" in funding the flagship, according to Tommaso Calarco, who leads the Integrated Quantum Science and Technology Centre at the Universities of Ulm and Stuttgart in Germany. Calarco co-author of the Quantum Manifesto insists "Countries around the world are investing in these technologies. Without such an initiative, Europe risks becoming a second-tier player. The time is really now or never."

Quantum Buzz

High-profile US companies are already investing in quantum computing and Chinese scientists are nearing the completion of a 2,000-kilometre long quantum-communication link — the longest in the world — to send information securely between Beijing and Shanghai.

Should we worry?

- Not all hype is based on facts



Should we worry?

- We should be careful when reading news

NASA, Google reveal quantum computing leap that leaves traditional PCs in the dust

In an experiment, a quantum computer outperformed a con tional machine by 100 million times.

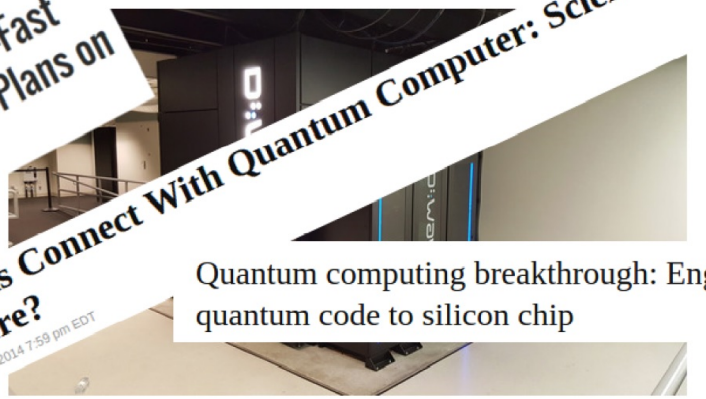
Why Your Brain Is A Quantum Computer

Posted: 05/06/2010 5:12 am EDT | Updated: 05/25/2011 3:45 pm EDT

Lockheed Martin Has Crazy-Fast Quantum Computers And Plans on Actually Using Them

Human-Alien Hybrids Connect With Quantum Computer: Science Fiction Or The Future?

Posted: 06/10/2014 7:29 pm EDT | Updated: 06/10/2014 7:59 pm EDT



Quantum computing breakthrough: Engineers manage to write quantum code to silicon chip

Quantum computers have failed. So now for the science

Why Google's new quantum computer could launch an artificial intelligence arms race

Google's Quantum Computer May Point People to God

Should we worry?

Take-home message

There is a serious medium-time threat that scalable quantum computers will become available.

- No need to panic
- Need to plan NOW how to make communications secure against adversaries that have a quantum computer or that have quantum technological abilities.

Solution 1: Post-quantum cryptography

- Construct crypto protocols that their security is based on the hardness of problems that are hard even for a quantum computer.
- Example of such problems are the "lattice-based" cryptography. However the belief that those problems are indeed hard for quantum computer is not as well founded as in the classical algorithms.

In short, it is difficult to base all protocols on these problems, is not certain that they are quantum-hard and there is always the possibility that some computation model could break this at some point (e.g. using new "quantum gravity" physics).

Solution 1: Post-quantum cryptography

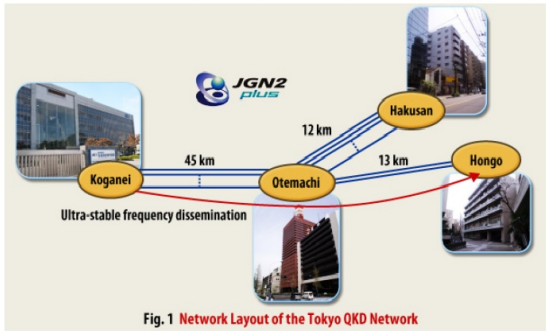
- A quantum adversary can:
  (a) just use his quantum computer to solve a problem in the protocol or
  (b) use his/her quantumness to perform more involved attacks at other steps of the protocol (i.e. reduction of security to the hard problem may not hold).
  Post-quantum need to take into account both issues!
- In involved protocols (e.g. zero knowledge proofs), proof technique may need to be modified (e.g. copying is impossible).

Solution 2: Use quantumness against itself!

- Use quantum properties (no-cloning, measurements disturbs the state, monogamy of entanglement, non-locality, etc) to achieve higher level of security ("unconditional" security)
- This does not rely on computational hardness and thus will be secure against adversaries having a quantum computer (or even an arbitrarily powerful computer).
- Main (and most developed) example: Quantum Key Distribution (QKD).
- Can exploit quantumness to achieve an even more exciting level of security (device-independent cryptography). In this case, the parties do not even trust their own devices!
- This is not a fiction as it is much easier to implement than a quantum computer. E.g. was used in actual elections in Switzerland in 2007.

Solution 2: Use quantumness against itself!

- Quantum Key Distribution (QKD)
- Unconditionally secure
- 1Mbps over 20km
- 12.7Kbps over 307km
- SwissQuantum (2009-2011)
- Tokyo (2010)



Solution 2: Use quantumness against itself!

- QKD backbone
- To be completed 2016
- QuantumCTek
- Commercial and government use

- QKD network
- To be completed
- Battelle and ID Quantique
- Commercial and government use

Solution 2: Use quantumness against itself!

Quantum-Safe Crypto

IDQ is the world leader in QUANTUM KEY GENERATION, QUANTUM KEY DISTRIBUTION and NETWORK ENCRYPTION

SWISS QUANTUM

HOME > QUANTUM-SAFE CRYPTO

Quantum-Safe Crypto

ID Quantique provides high-performance network encryption solutions for the protection of data in transit. IDQ's encryption platform can encrypt high throughput traffic up to 100Gbps on local and storage area networks for data back-up and recovery, as well as on fully meshed global WAN networks for international operations.

IDQ uses state-of-the-art algorithms and highly secure quantum key generation and quantum key distribution (quantum cryptography), ensuring that the solutions are "quantum-safe" for the long-term protection of sensitive data into and beyond the quantum era.

CENTAURIS CN8000
MULTI-LINK, MULTI-PROTOCOL 100G DATA CENTER ENCRYPTION

CENTAURIS LINK ENCRYPTORS
HIGH PERFORMANCE ETHERNET & FIBRE CHANNEL ENCRYPTION

ARCIS
MPLS AND CLOUD ENCRYPTION

CERBERIS
QUANTUM KEY DISTRIBUTION SERVER

Contact

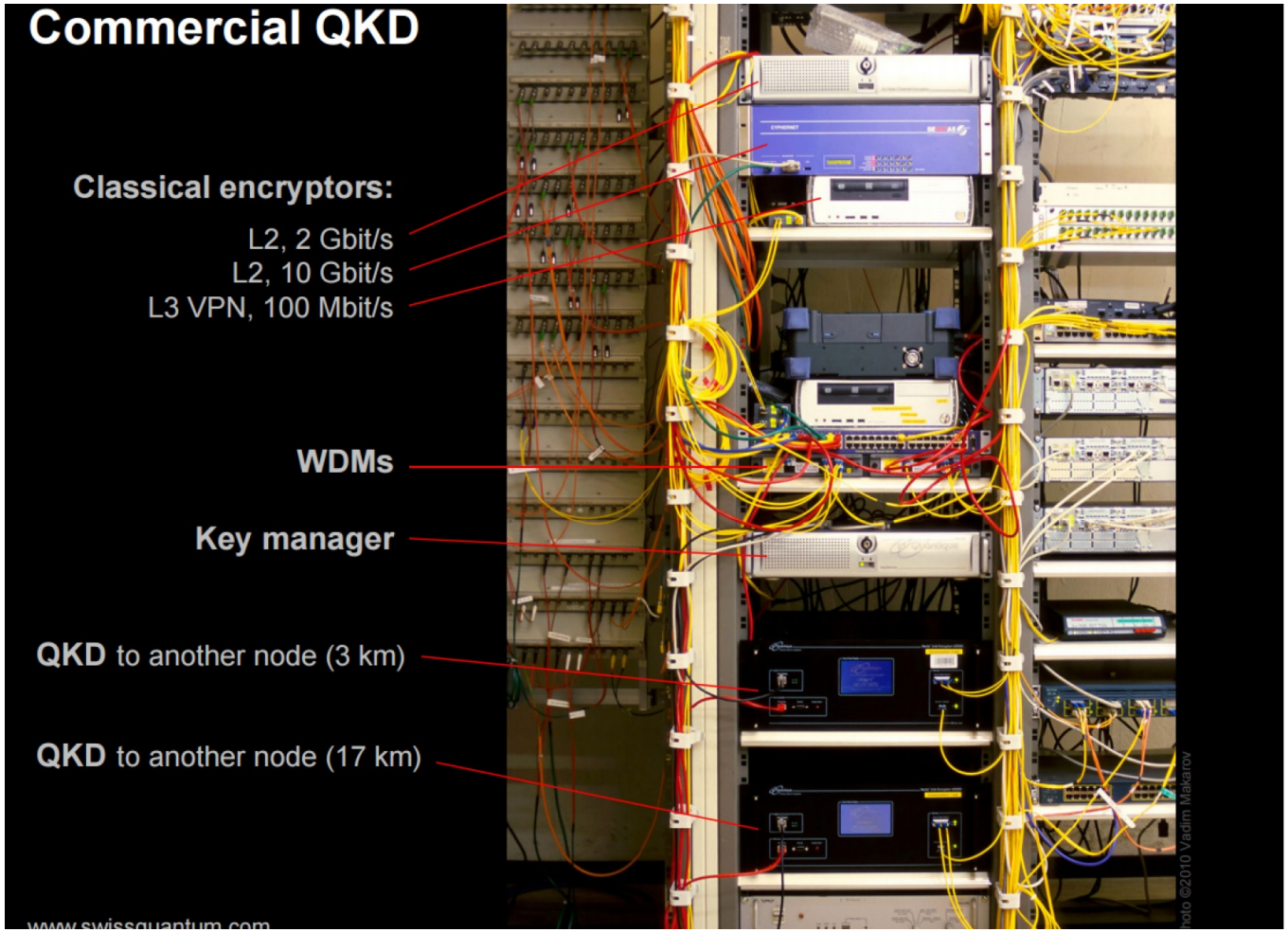
TEL: +41 22 301 83 71
EMAIL: info@idquantique.com

Name
Company
Email
Phone

ARRANGE A CALL BACK

RESOURCE CENTRE

Solution 2: Use quantumness against itself!



Quantum Key Distribution

- Charles Bennett and Gilles Brassard in 1984 gave the first QKD protocol
- Followed "quantum money" paper (Stephen Wiesner)
- Set of states $\{|H\rangle, |+\rangle, |V\rangle, |-\rangle\}$
  $|\pm\rangle = \frac{1}{\sqrt{2}}(|H\rangle \pm |V\rangle)$
- Alice encodes the classical bit 0 with either $|H\rangle$ or $|+\rangle$ and the classical bit 1 with either $|V\rangle$ or $|-\rangle$
- Alice sends a string qubits corresponding to an equal length string of classical bits
  E.g. $|H\rangle |+\rangle |-\rangle |H\rangle |V\rangle$ corresponding to the string 00101
- Bob randomly chooses either the basis $x_0 = \{|H\rangle, |V\rangle\}$ or the basis $x_1 = \{|+\rangle, |-\rangle\}$ and makes a measurement. He records the (classical) outcome $\{0, 1\}$ and the basis $\{x_0, x_1\}$ he measured
- Bob announces the basis x_i he measured (NOT the outcome)
- Alice responds for which qubits Bob measured at the correct basis
- Alice and Bob discard all the qubits that Bob measured in the wrong basis

Quantum Key Distribution

- For the remaining qubits, if no eavesdropping has occurred and no noise (ideal case), Alice and Bob should agree 100%. This is called the **raw key**
- They choose a small fraction (e.g. 10%) of the bits and check if they have any disagreements
  This phase, where Alice and Bob find what fraction of mismatches they have, is called **Parameter Estimation** (PE) phase
- The qubits that are used in the PE phase are also discarded ("sacrifice" some part of the string to establish what correlation Alice has with Bob)
- The remaining bits (after discarding positions that Bob measured at the wrong basis and those that were used at the PE phase) will be used for distilling a secret key
- In the ideal case (no noise), the latter is exactly the secret key that Alice and Bob share
- Neither Alice nor Bob can decide what key they will share by the end. Therefore QKD *generates* a secret key rather than distributes.

Quantum Key Distribution

- Example:

Key	0	0	1	1	0
Encoding (Alice)	$\|H\rangle$	$\|+\rangle$	$\|-\rangle$	$\|V\rangle$	$\|+\rangle$
Measurement (Bob)	x_0	x_0X	x_1	x_1X	x_0X
Outcome	$\|H\rangle$	$\|V\rangle$	$\|-\rangle$	$\|-\rangle$	$\|V\rangle$
Key Obtained	0	$1X$	1	$1X$	$1X$

- Eve cannot copy the states (quantum no-cloning)
- Eve cannot measure the qubit without disturbing it! Any attempt to obtain information increases the number of errors in the PE phase
- In general Alice, Bob and Eve have strings X, Y, W. If X is more correlated with Y than with W, then there is a way to distil a perfectly secret identical string
- The above correlations can be bound from the observed errors in PE.

Quantum Key Distribution

- There exist other attacks, that try to exploit the imperfections of the implementations. Active research in improving security! And an image of a quantum hacker, exactly as you would imagine him:

(Prof. Vadim Makarov from University of Waterloo)

Conclusion

- Quantum computers would break existing cryptography
- Progress towards building quantum computers has been made
- Is necessary to address this threat
- Either change classical protocols to make them hard for quantum computers
- Or use quantumness to have higher level of security: Quantum key distribution