Cyber Security in the Quantum Era

Petros Wallden

Computer Security Guest Lecture

University of Edinburgh

27th November 2017

Outline

- Quantum Computers: Is it a threat to Cyber Security?
- Why should we act now?

Outline

- Quantum Computers: Is it a threat to Cyber Security?
- Why should we act now?
- What is "Quantum Security"
- Addressing Quantum Adversaries
- Quantum-enhancement of Security

Outline

- Quantum Computers: Is it a threat to Cyber Security?
- Why should we act now?
- What is "Quantum Security"
- Addressing Quantum Adversaries
- Quantum-enhancement of Security
- Misconceptions
- Recent Technical Advances
- Our Research in this Landscape

Quantum Computers

- Quantum Physics is a very successful theory
- Quantum Physics has many counter-intuitive properties
- Size of transistors in microchip are approaching quantum scale

Quantum Computers

- Quantum Physics is a very successful theory
- Quantum Physics has many counter-intuitive properties
- Size of transistors in microchip are approaching quantum scale

Main Question

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

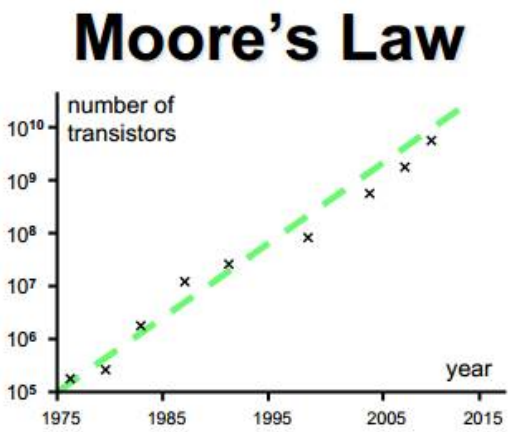
Quantum Computers

- Quantum Physics is a very successful theory
- Quantum Physics has many counter-intuitive properties
- Size of transistors in microchip are approaching quantum scale

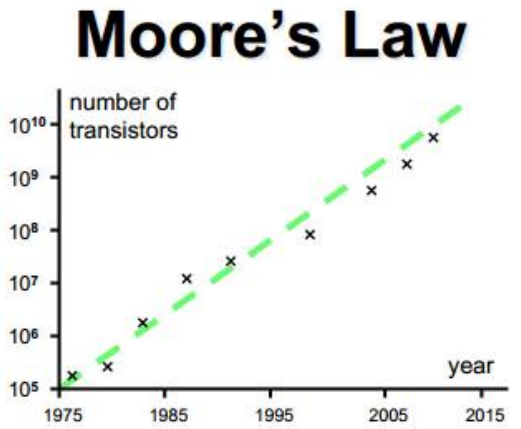
Main Question

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

- Q: What computational power would a QC have?
- A: Greater than classical probabilistic $\mathrm{BPP} \subseteq \mathrm{BQP}$
- Q: Is it possible to built such computing device?
- A: Yes! No fundamental reason stopping us (engineering)


Moore's Law
number of transistors
10^{10}
10^{9}
10^{8}
10^{7}
10^{6}
10^{5}
year
1975
1985
1995
2005
2015

Quantum Computers



Bit	**Qubit**
Takes values either 0 or 1	Can behave as being simultaneously 0 and 1: $\alpha \|0\rangle + \beta \|1\rangle$
Measurement reveals value	Measurement disturbs
Can be copied	*Cannot* be copied
Strings are described w.r.t. single bits (local)	Strings cannot be described w.r.t. single qubits (non-local)
Behave probabilistically	"Complex probabilities"

Quantum Computers: Is it a serious threat?

- Quantum Computers can solve efficiently **factoring** and **discrete log** (Factoring, RSAP, Discrete Log, DHP)
- Intractable problems (classical hardness guarantees security)
  $\Rightarrow$ Tractable problems (for Quantum Computers)

Quantum Computers: Is it a serious threat?

- Quantum Computers can solve efficiently **factoring** and **discrete log** (Factoring, RSAP, Discrete Log, DHP)
- Intractable problems (classical hardness guarantees security) $\Rightarrow$ Tractable problems (for Quantum Computers)

Take-home message

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

Quantum Computers: Is it a serious threat?

- Quantum Computers can solve efficiently **factoring** and **discrete log** (Factoring, RSAP, Discrete Log, DHP)
- Intractable problems (classical hardness guarantees security) $\Rightarrow$ Tractable problems (for Quantum Computers)

Take-home message

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

- Known since 1990's
- Requires unprecedented control of quantum systems

Why act now?

- Huge recent initiative in Quantum Technologies
  Companies: IBM, Google, Microsoft, Intel, Atos, D-Wave, Rigetti, Alibaba, etc
  Governments: UK (£270 million EPSRC), EU (€1 billion Flagship), etc
  Developments in Quantum Technologies are accelerating and the prospect of practical QT is becoming real

Why act now?

- Huge recent initiative in Quantum Technologies
  Companies: IBM, Google, Microsoft, Intel, Atos, D-Wave, Rigetti, Alibaba, etc
  Governments: UK (£270 million EPSRC), EU (€1 billion Flagship), etc
  Developments in Quantum Technologies are accelerating and the prospect of practical QT is becoming real
- Security can be broken **retrospectively**

Why act now?

- Huge recent initiative in Quantum Technologies
  Companies: IBM, Google, Microsoft, Intel, Atos, D-Wave, Rigetti, Alibaba, etc
  Governments: UK (£270 million EPSRC), EU (€1 billion Flagship), etc
  Developments in Quantum Technologies are accelerating and the prospect of practical QT is becoming real
- Security can be broken **retrospectively**
- **Years** (possibly decades), are needed to develop/replace all protocols with "quantum-safe" protocols

Why act now?

- Huge recent initiative in Quantum Technologies
  Companies: IBM, Google, Microsoft, Intel, Atos, D-Wave, Rigetti, Alibaba, etc
  Governments: UK (£270 million EPSRC), EU (€1 billion Flagship), etc
  Developments in Quantum Technologies are accelerating and the prospect of practical QT is becoming real
- Security can be broken **retrospectively**
- **Years** (possibly decades), are needed to develop/replace all protocols with "quantum-safe" protocols

Take-home message

There is a serious medium-time threat that scalable quantum computers will become available. Counter-actions should start now.

Investments in Quantum Computing

Alibaba is spending $15 billion on researching quantum computing, AI, and more

The e-commerce giant looks overseas for R&D to move beyond its roots

NATURE | NEWS

Europe's billion-euro quantum project takes shape

Scientists offer more detail on flagship programme to harness quantum effects in devices.

Elizabeth Gibney

03 May 2017

December 4, 2013 8:59 pm

Autumn Statement 2013: Quantum technology to get £270m boost

What is "Quantum Security"?

Quantum Security:

All aspects affecting secure communications and computations due to the development of **quantum technologies**

What is "Quantum Security"?

Quantum Security:

All aspects affecting secure communications and computations due to the development of **quantum technologies**

- **Negative**: Deal with vulnerabilities due to adversaries holding quantum computers or other quantum devices
- **Positive**: Enhance security, as honest parties can use quantum devices to achieve tasks impossible with classical means

What is "Quantum Security"?

Quantum Security:

All aspects affecting secure communications and computations due to the development of **quantum technologies**

- **Negative**: Deal with vulnerabilities due to adversaries holding quantum computers or other quantum devices
- **Positive**: Enhance security, as honest parties can use quantum devices to achieve tasks impossible with classical means

Most known representatives

1. Lattice-based crypto. Change classical protocols to defend against QC
2. Quantum-key-distribution (QKD). Quantumness used positively to enable KD with information theoretic security

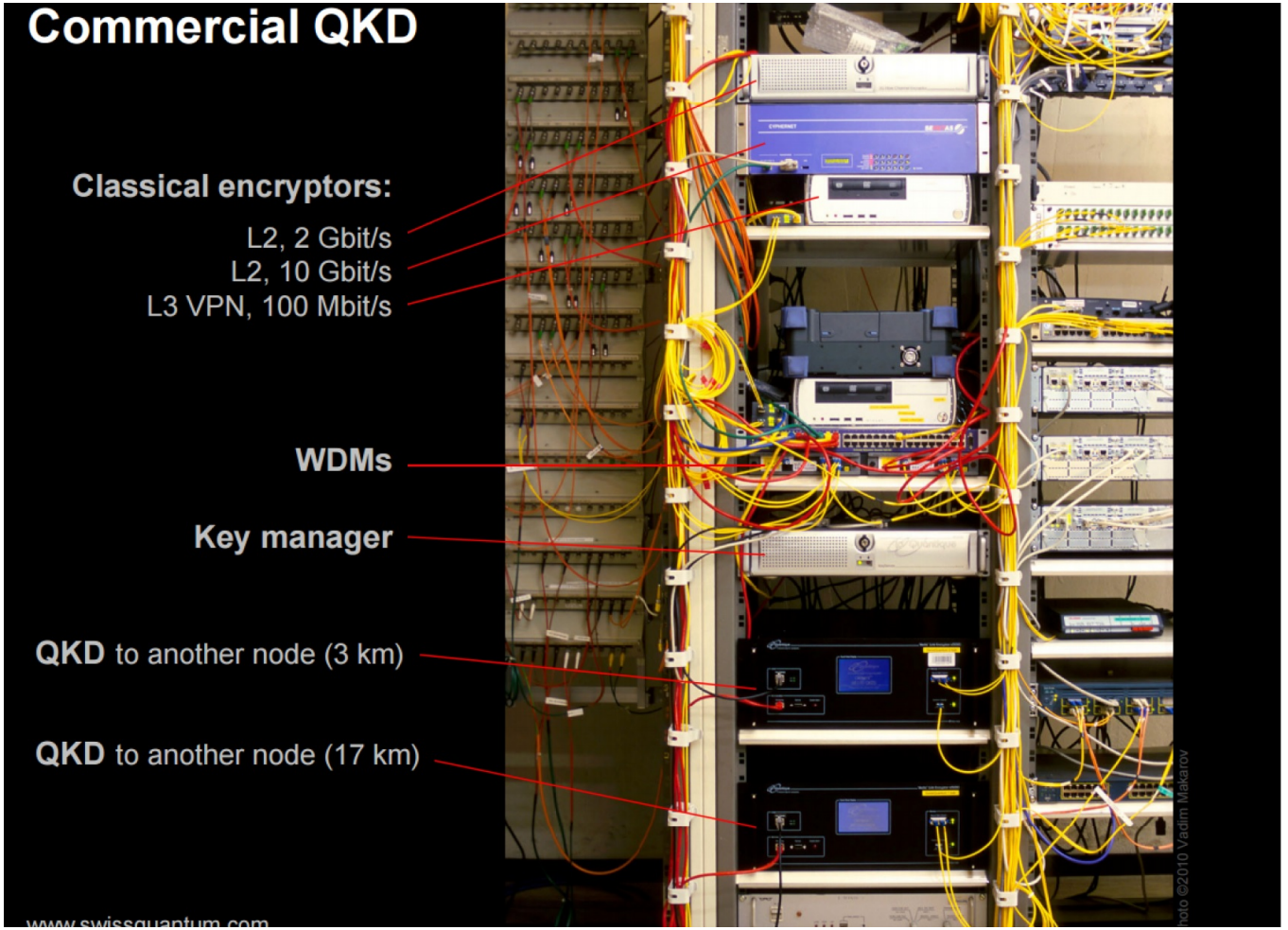
Field is **much wider** and the focus should be to go **beyond** these

Quantum Key Distribution

- Can distribute key unconditionally secure
- Use for one-time-pad $\Rightarrow$ unconditionally secure encryption
- Charles Bennett and Gilles Brassard 1984 (first protocol)

1. Alice sends sequence of qubits to Bob
2. Unknown quantum states:
   (i) **cannot be distinguished** with certainty,
   (ii) **cannot be copied**
3. Any action by Eve can be detected w.h.p. (observation disturbs the system)
4. Alice - Bob, can **estimate information Eve has** on their string
5. If below a threshold, use classical techniques $\Rightarrow$ a **secret key**

Quantum Key Distribution



Quantum Key Distribution

A quantum hacker, exactly as you would imagine him:

(Prof. Vadim Makarov from University of Waterloo)

Addressing Quantum Adversaries

1. **Information Theoretic Security**: Cannot break with any computational power

Addressing Quantum Adversaries

1. **Information Theoretic Security**: Cannot break with any computational power
2. **Post-quantum Security**: Security against computationally-bounded *quantum* adversaries
    - QC-hard problem
    - Valid reduction to hardness of problem
    - Quantum-compatible security definitions

Addressing Quantum Adversaries

1. **Information Theoretic Security**: Cannot break with any computational power
2. **Post-quantum Security**: Security against computationally-bounded *quantum* adversaries
   - QC-hard problem
   - Valid reduction to hardness of problem
   - Quantum-compatible security definitions
3. **Side-channel Attacks**:
   - Quantum Hacking (attack physical implementations)
   - Fundamental quantum non-locality defends against these

Quantum-Enhanced Security

1. **Simple quantum devices for info-theoretic security:** Possible with current technology (QKD, QRNG, etc)

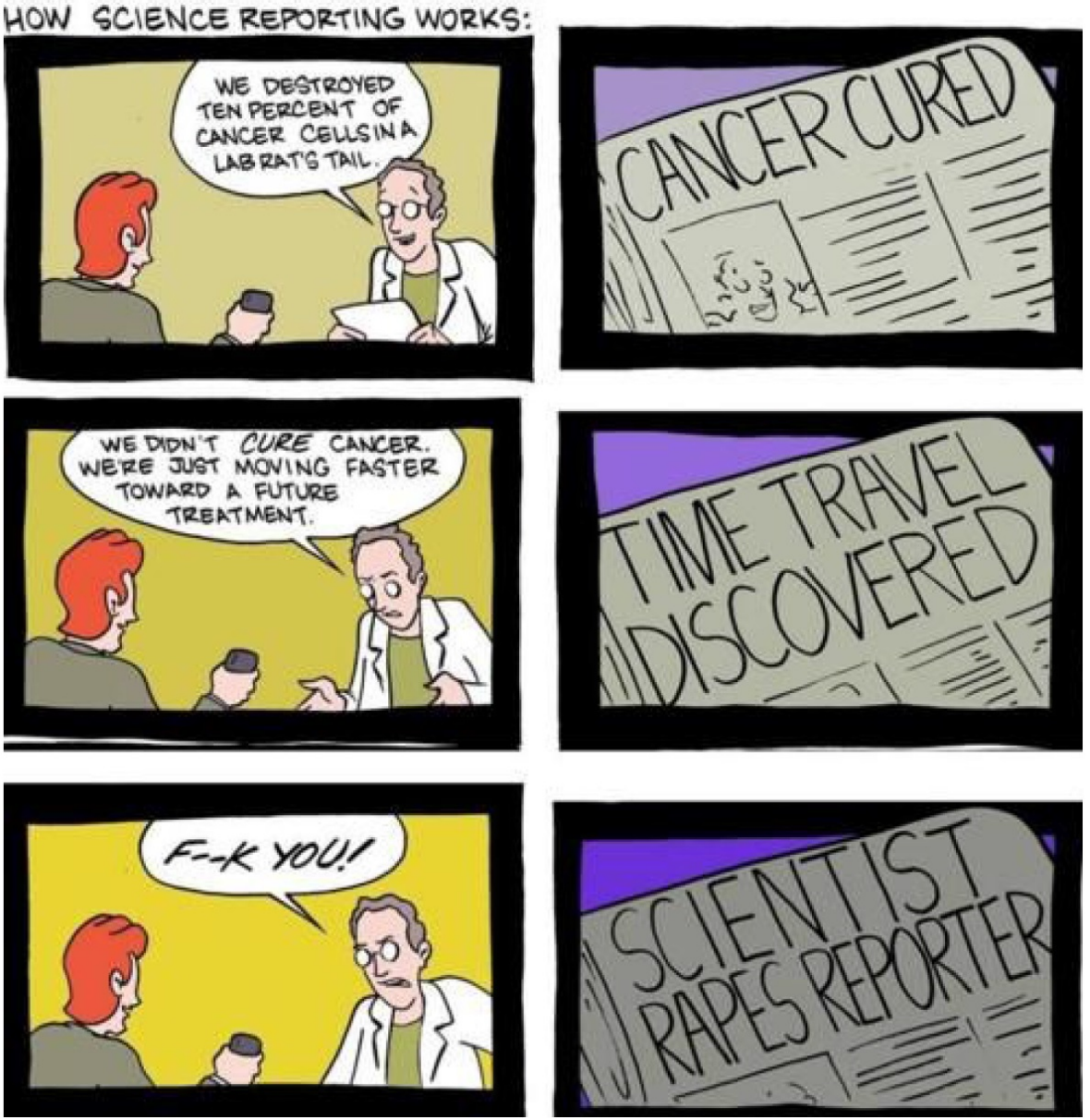
Quantum-Enhanced Security

1. **Simple quantum devices for info-theoretic security:** Possible with current technology (QKD, QRNG, etc)
2. **Enhance efficiency/security of involved classical protocols:** Important classical applications that can be improved with current or close technology (e-voting, SMPC, blockchain, etc)

Quantum-Enhanced Security

1. **Simple quantum devices for info-theoretic security:** Possible with current technology (QKD, QRNG, etc)
2. **Enhance efficiency/security of involved classical protocols:** Important classical applications that can be improved with current or close technology (e-voting, SMPC, blockchain, etc)
3. **Secure use of new quantum computing devices:** QC give new computational power.
   - Few central QC $\Rightarrow$ Need for a secure delegated service
   - Security for protocols involving quantum information (encryption of quant. info., authentication, SMP**Q**C, etc)

Not all hype is based on facts!



Power of Quantum Computation

Myth 1

Quantum Computers are much faster in performing operations than Classical Computers

Reality

Quantum computers are *not* faster. Speed-up is obtained because quantum theory allows algorithms/operations impossible for classical computers.

Power of Quantum Computation

Myth 2

Quantum Computers simultaneously perform all branches of a (probabilistic) computation and can find accepting paths instantly

Reality

QC span the space of possibilities in a peculiar way (behave as complex probabilities). However, at the end of the computation the result is obtained by a single read-out/measurement and "unrealised" paths do not contribute.

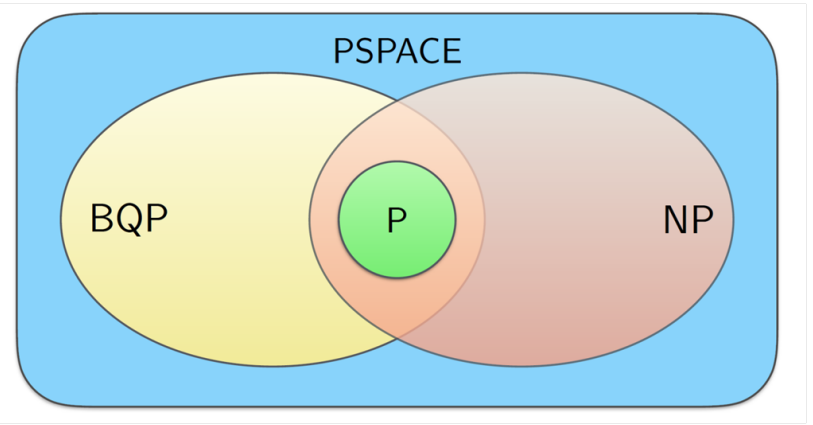
Power of Quantum Computation

Myth 3

Quantum Computers can efficiently solve NP-complete problems (such as Travelling Salesman Problem)

Reality

NP is believed to not be contained in BQP. QC may (and does) provide polynomial or constant speed-up in many problems outside BQP (e.g. quadratic search speed-up).



What it takes to be Quantum-Safe

Myth 4

Using problems that are hard for a quantum computer (outside BQP) suffices to make a crypto protocol secure against any quantum attack

Reality

This is **necessary but not sufficient** condition. Attackers could use their quantum-technologies in any part (not only as a black-box to solve the hard problem). Need (i) **reduction to hardness** to remain valid under the presence of quantum adversaries (e.g. rewinding cannot be used) and (ii) need **security definitions** to account for quantum abilities (e.g. known plaintext or ciphertext attacks should allow for chosen texts being in superposition)

Quantum Computation

Developments in all architectures: Superconducting (leads), ion-traps, cold-atoms, photonic.

Hybrid matter-photon $\Rightarrow$ for applications involving both QComms and Quantum Computing

- *Classical Simulation Limit*: 50-ish qubits [IBM new technique: record 56 qubits]
- *Quantum Advantage (Supremacy)*: Problem (any) that practical QC can solve but not classical computers
- *Size of existing quantum computers*: Is approaching 50 qubits **universal** QC [Google within a year]
- *What about breaking RSA?* Requires O(1000) fault-tolerant qubits at universal QC [possibly in 10 years]

Recent Technical Advances

IBM Simulates a 56-Qubit Machine

By Charles Q. Choi
Posted 30 Oct 2017 | 18:00 GMT

Image: IBM Research

Google's New Chip Is a Stepping Stone to Quantum Computing Supremacy

The search giant plans to reach a milestone in computing history before the year is out.

by Tom Simonite April 21, 2017

ohn Martinis has given himself just a few months to reach a milestone in the history of computing.

Intel Accelerates Its Quantum Computing Efforts With 17-Qubit Chip

By Samuel K. Moore
Posted 10 Oct 2017 | 17:00 GMT

Microsoft Cloud Mobility Productivity

Quantum Team Technology Resources

Empowering the quantum revolutio

Recent Technical Advances

THE QUANTUM COMPUTER FACTORY THAT'S TAKING ON GOOGLE AND IBM

Inside the clean room at Rigetti Computing's Fab-1 facility in Fremont, California.
RIGETTI COMPUTING

Atos Quantum

A real collective, human and technological adventure that opens up to us

To develop technologies and solutions for quantum computing, as well as for quantum safe cyber security products

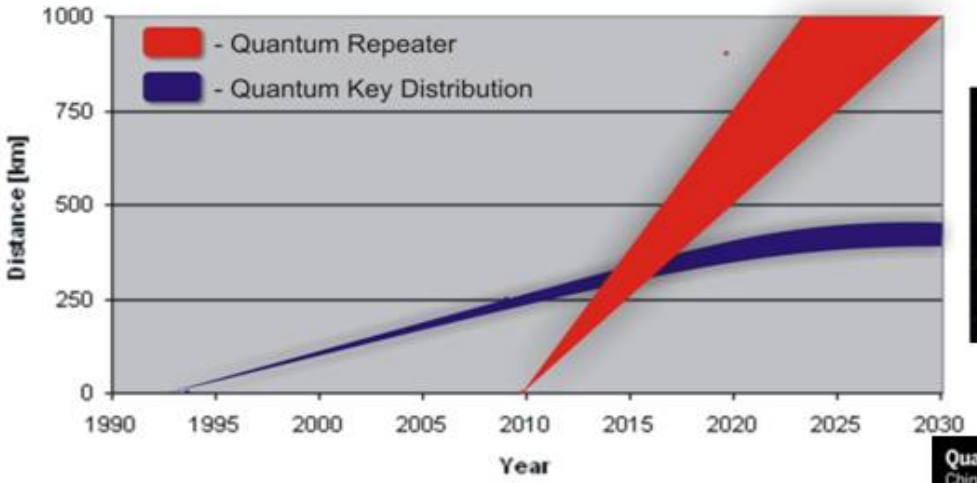
An experimental computer made by a Canadian company has proved its ability to solve increasingly complex mathematical problems. But is it quantum mechanics? (D-Wave Systems)

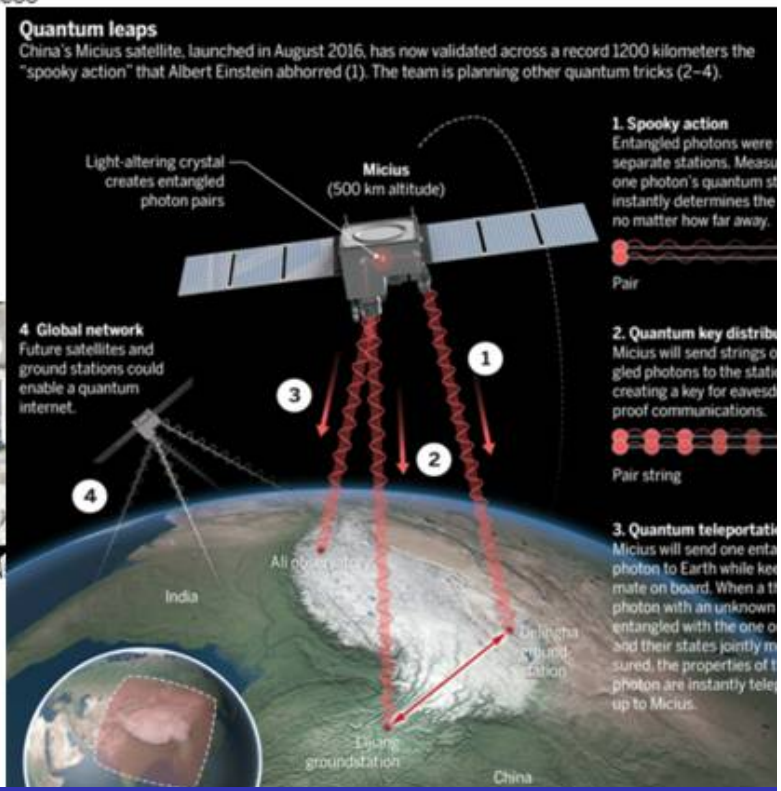
Quantum Communication (QKD)

Developments in all directions: fibre optics, free-space, satellite, continuous variables, discrete variables, time encoding.

- Repeaters (long-distance QKD)
- Loophole-free Bell tests
- **Satellite QKD** (China)
- Metropolitan networks
- Quantum hacking and counter-measures

Recent Technical Advances





Our Recent Research in this Landscape

1. **Security of Classical Protocols:**
   - Develop toolkit of crypto techniques to be used in the presence of quantum adversaries: Quantum Cut-and-Choose [KMW2017]
   - Explore superposition attacks in classical and hybrid protocols

Our Recent Research in this Landscape

1. **Security of Classical Protocols:**
   - Develop toolkit of crypto techniques to be used in the presence of quantum adversaries: Quantum Cut-and-Choose [KMW2017]
   - Explore superposition attacks in classical and hybrid protocols
2. **Quantum-enhancement:** Recent research programme on using quantum verification/certification in hybrid classical-quantum protocols for enhancing classical multiparty functionalities (e-voting, SMPC, blockchain, etc)

Our Recent Research in this Landscape

1. **Security of Classical Protocols:**
   - Develop toolkit of crypto techniques to be used in the presence of quantum adversaries: Quantum Cut-and-Choose [KMW2017]
   - Explore superposition attacks in classical and hybrid protocols
2. **Quantum-enhancement:** Recent research programme on using quantum verification/certification in hybrid classical-quantum protocols for enhancing classical multiparty functionalities (e-voting, SMPC, blockchain, etc)
3. **Quantum Computation Enabled:** Cryptography for quantum information (encryption, authentication, SMPQC, etc). Most important application: Quantum Cloud

The Quantum Cloud

Task

Clients wanting to (securely) delegate their quantum computation to the cloud!

IBM cloud: 16 qubits (more than top-universities labs)

The Quantum Cloud

Task

Clients wanting to (securely) delegate their quantum computation to the cloud!

IBM cloud: 16 qubits (more than top-universities labs)

Our recent most important results:

- Fully classical-client (computationally-secure) blind quantum computation [CCWK2017]

The Quantum Cloud

Task

Clients wanting to (securely) delegate their quantum computation to the cloud!

IBM cloud: 16 qubits (more than top-universities labs)

Our recent most important results:

- Fully classical-client (computationally-secure) blind quantum computation [CCWK2017]
- Non-interacting practical blind QC (QFHE) with minimal quantum client [WHGCK2017]

The Quantum Cloud

Task

Clients wanting to (securely) delegate their quantum computation to the cloud!

IBM cloud: 16 qubits (more than top-universities labs)

Our recent most important results:

- Fully classical-client (computationally-secure) blind quantum computation [CCWK2017]
- Non-interacting practical blind QC (QFHE) with minimal quantum client [WHGCK2017]
- Efficient verifiable and blind QC (overhead down to linear from quadratic) [KW2017a]

Summary

- Quantum computers will break existing cryptography
- Progress towards building quantum computers has been made
- It is necessary to address this threat (2 solutions)
  - Change classical protocols to make them hard for quantum computers
  - Use quantumness to achieve unconditional security
- Can use quantum technologies for enhancing performance and security
  - Classical quantumly-enhanced protocols
  - Use securely quantum computers (Quantum Cloud)

Thanks for your attention!!