SERMA
SAFETY & SECURITY

Quantum Computing

What does really mean for Security people?

Who I am

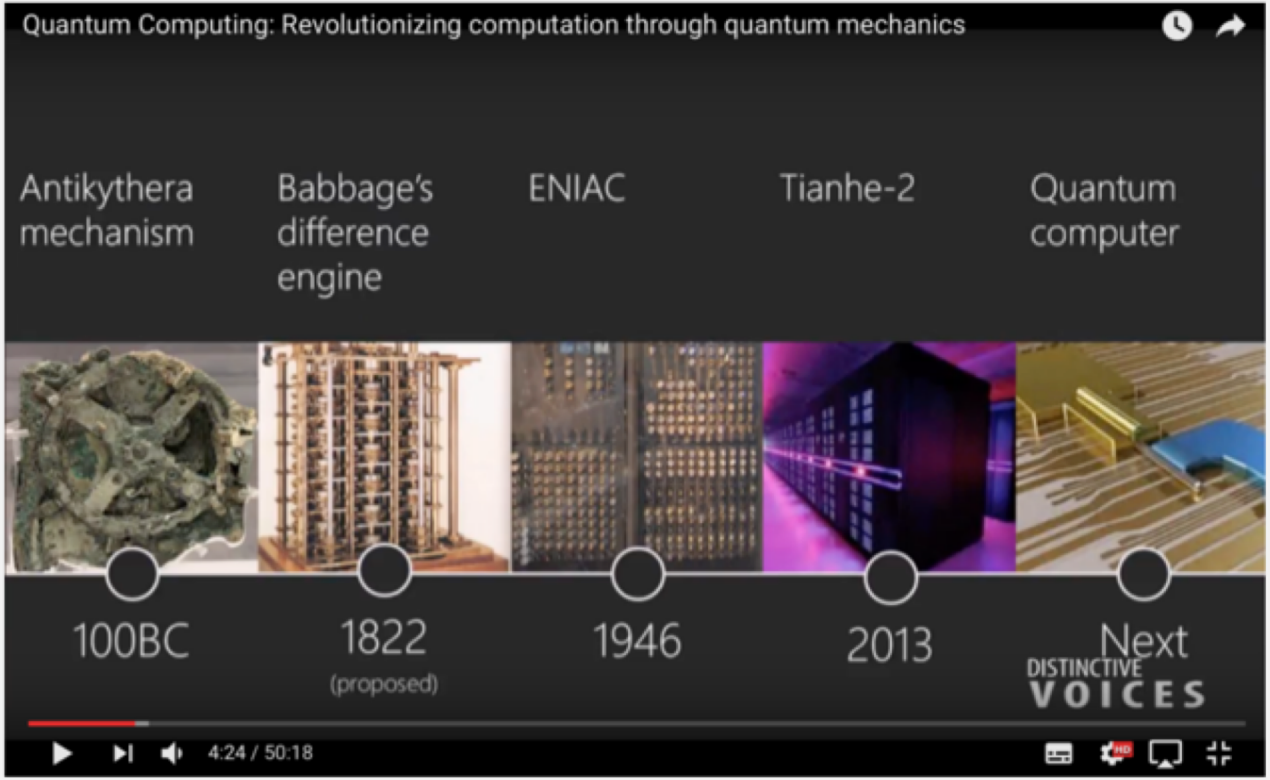
- More than 25 years of experience in Cybersecurity
- “So called” Expert in IT and IoT security
- Former manager of the application security of a Fortune 50 company
- (Old?)Engineer in electronics and computing
- Speaker & trainer (BlackHat, HITB, Tedx…)
- Head of offensiv & defensic R&D inside S3
- Hardsploit project, Quantum computing, DIY Bio Hacking and more...

Back to our subject

- Quantum Computing ?
- My vision : How to hack the entire IT industry with one particles behavior
- Our agenda for this talk : The journey of a security guy in quantum computing world … without any PhD

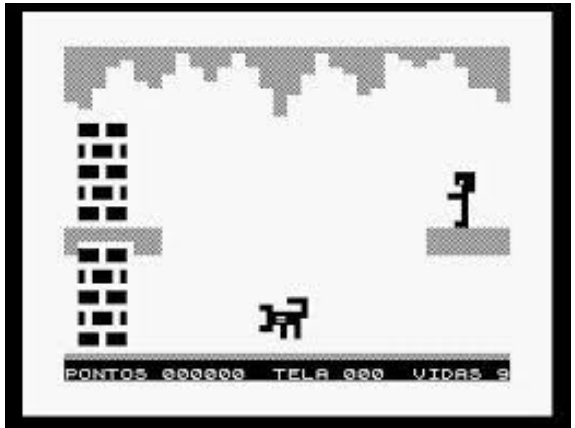
Computing history in 1 slide

- Trust me : Computing's Hardware have already change over the age !



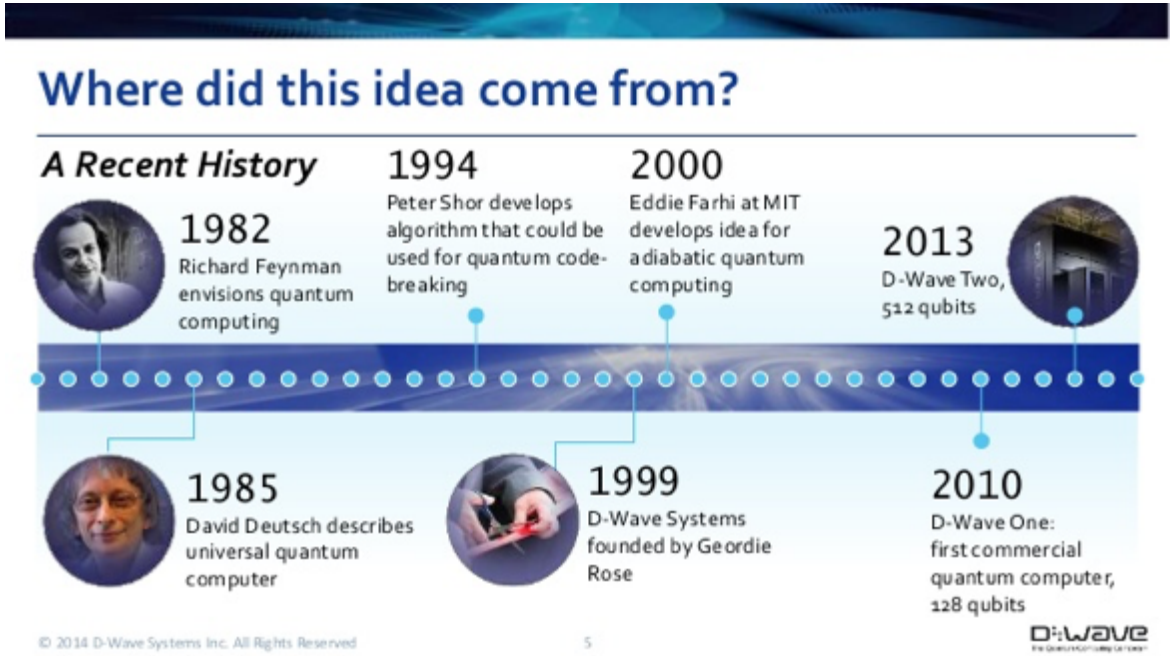
Computer hardware already evolved in past!

- Some People would seem to not accept that there could be a evolution of hardware that supports our « computing” needs… They could be (really) wrong !
- May be it will be Quantum computing, maybe DNA based computing or something else.
- But Computing’s hardware could change over the age.

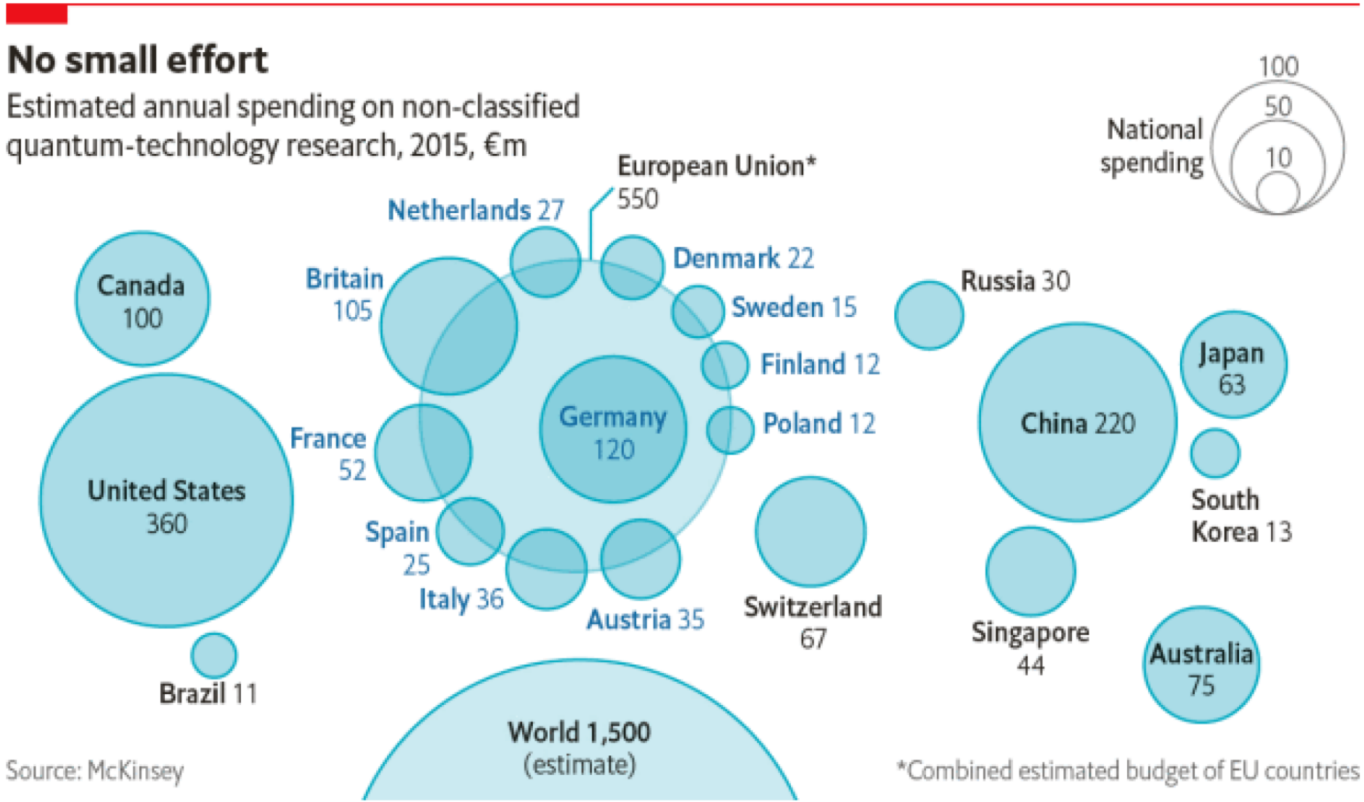


What is Quantum Computing?

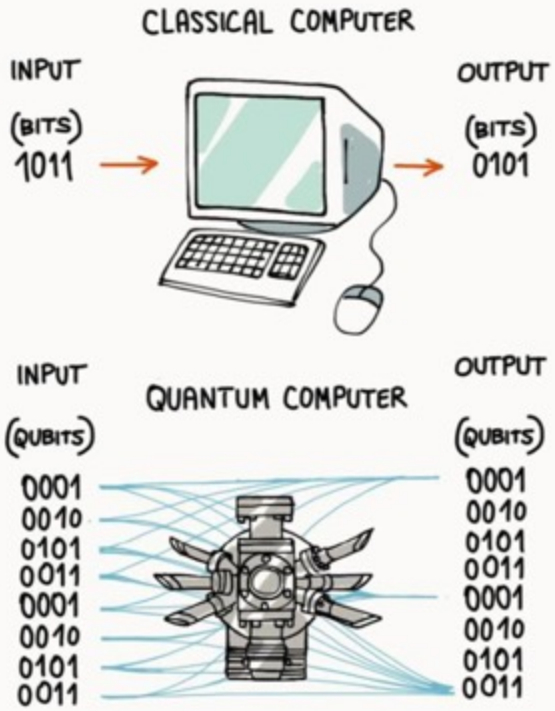
- A Quantum computer is a machine that performs calculations bases on the laws of Quantum Mechanics



Investments in the domain are huge



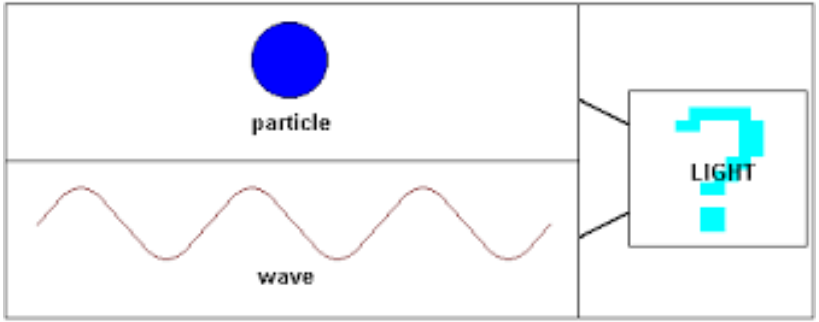
Quantum Computing?



- A QUANTUM SYSTEM REPLACES CLASSICAL BITS WITH QUANTUM QUBITS
- QUBITS FOLLOW THE SUPERPOSITION PRINCIPLE AND CAN EXIST AS "0" AND "1" AT THE SAME TIME
- USING QUBITS INSTEAD OF BITS, WITH A SINGLE INPUT ONE COULD PROCESS ALL THE POSSIBLE COMBINATIONS OF "0" AND "1"'S IN A STRING AT THE SAME TIME
- QUANTUM ALGORITMS USING THIS ABILITY COULD SOLVE CERTAIN TYPES OF PROBLEMS MUCH, MUCH FASTER THAN ANY CLASSICAL COMPUTER

WTF : 1 and 0 @ the same time !?

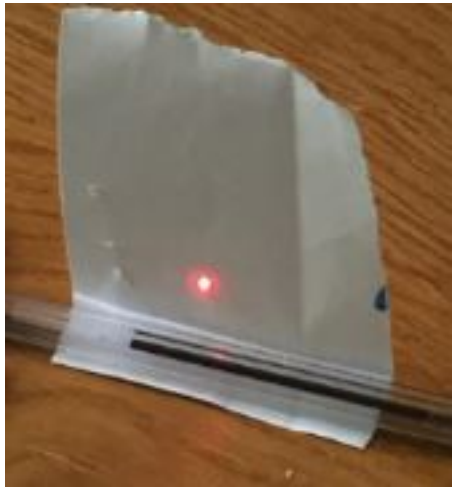
- How it's possible?
- Duality of wave and particule behavior
- **Everythings, @ atomic level** could behave as a Wave and a particle?



How to imagine the wave-particle duality.

Wave & Particles behavior experiments (1/3)

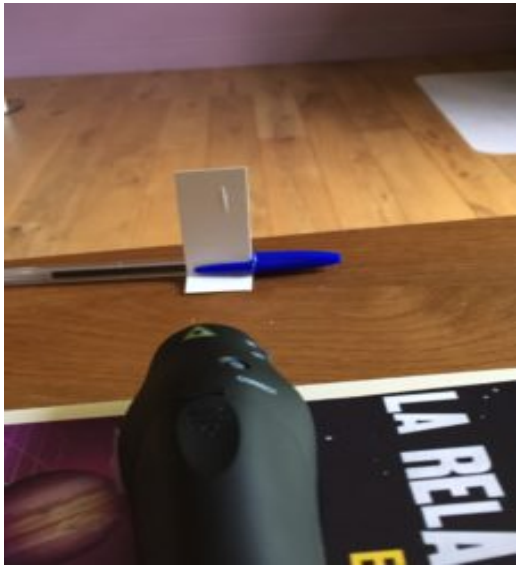
- As a ~~IT security consultant~~ / hacker, how to check That ?
- Make , @ home, a double slit experiment ….But with hacker style ☺



- Step 1 : use a laser point against a wall
  - You see a spot !
  - (photon = particule behaviour)

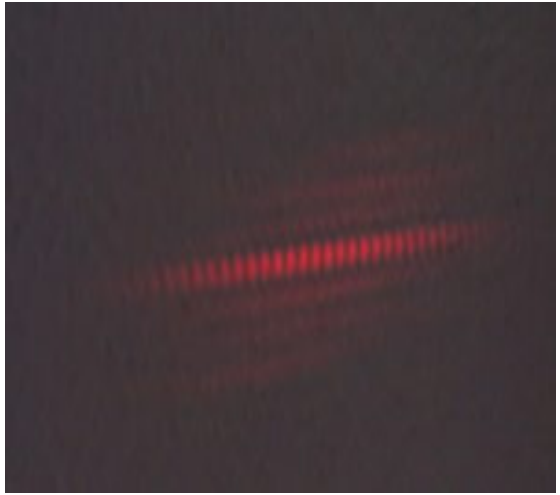
Wave & Particles behavior experiments (2/3)

- Step 2 : send the (same!) laser beam through a double slit



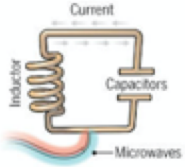
Wave & Particles behavior experiments (3/3)

- Step 2 : You will see an interférence pattern (witch is a wave existance proof)
- Photons behave at the same time as a particules (step 1) and as a wave (Step2) …
- and this help some guys to design hardware qubit to make a quantum computer : a powerfull new tool for computing !



Many ways to create the Hardware of Qubits

Superconducting loops



A resistance-free current oscillates back and forth around a circuit loop. An injected microwave signal excites the current into super-position states.

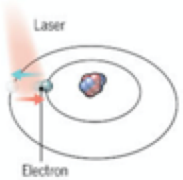
Longevity (seconds)	**0.00005**
Logic success rate	**99.4%**
Number entangled	**9**

Company support
Google, IBM, Quantum Circuits

Pros
Fast working. Build on existing semiconductor industry.

Cons
Collapse easily and must be kept cold.

Trapped ions



Electrically charged atoms, or ions, have quantum energies that depend on the location of electrons. Tuned lasers cool and trap the ions, and put them in super-position states.

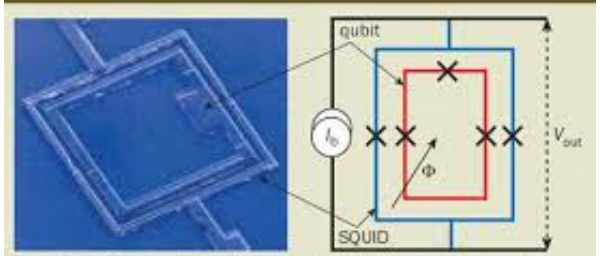
Longevity (seconds)	**>1000**
Logic success rate	**99.9%**
Number entangled	**14**

Company support
ionQ

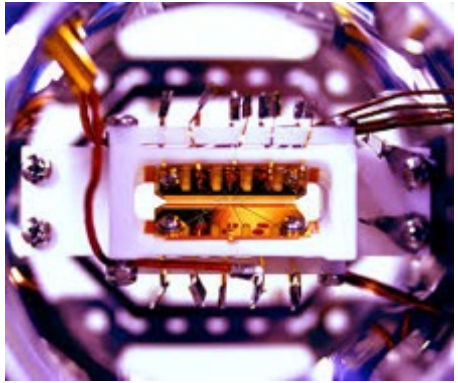
Pros
Very stable. Highest achieved gate fidelities.

Cons
Slow operation. Many lasers are needed.

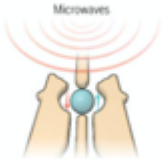
3 Making measurements on a flux qubit



A scanning electron micrograph (left) and circuit diagram of a flux qubit at Delft. The current circulating in the qubit (shown in red) is measured using a superconducting quantum interference device (SQUID). This device, which is shown in blue, is a loop that contains two more Josephson junctions.



Silicon quantum dots



These "artificial atoms" are made by adding an electron to a small piece of pure silicon. Microwaves control the electron's quantum state.

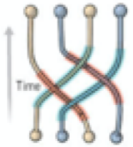
Longevity (seconds)	**0.03**
Logic success rate	**~99%**
Number entangled	**2**

Company support
Intel

Pros
Stable. Build on existing semiconductor industry.

Cons
Only a few entangled. Must be kept cold.

Topological qubits



Quasiparticles can be seen in the behavior of electrons channeled through semi-conductor structures. Their braided paths can encode quantum information.

Longevity (seconds)	**N/A**
Logic success rate	**N/A**
Number entangled	**N/A**

Company support
Microsoft, Bell Labs

Pros
Greatly reduce errors.

Cons
Existence not yet confirmed.

More Qubit = More Exponential computing power

50 qubits

Processing power a quantum computer would need to be able to outperform today's fastest supercomputers

INNOVATION THROUGH **QUANTUM SUPREMACY**

Quantum Computers: They are coming…

QUANTUM SUPREMACY

The IBM Q Lab. Image: IBM Research/Flickr

IBM Just Made a 17 Qubit Quantum Processor, Its Most Powerful One Yet

Meredith Rutland Bauer

MIT Technology Review

Log in / Create an account Search

Topics+ The Download Magazine Events More+ Subscribe

Intelligent Machines

IBM Raises the Bar with a 50-Qubit Quantum Computer

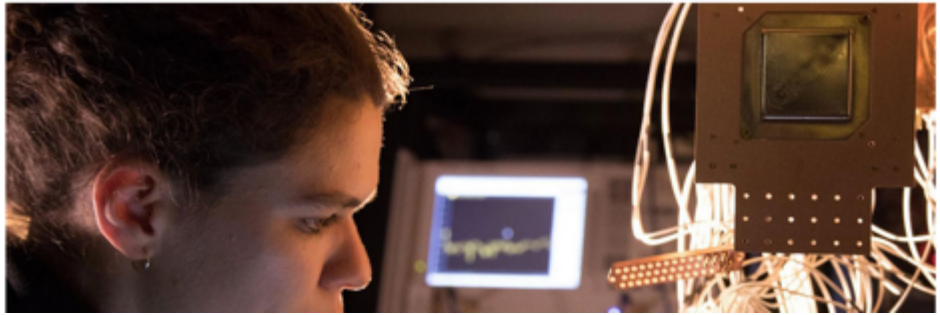
e built the most sophisticated quantum
naling progress toward a powerful new
g information.

vember 10, 2017

Home | News | Physics | Technology

DAILY NEWS 6 March 2018

Google's 72-qubit chip is the largest yet



Application?

Quantum supremacy: a snapshot of applications

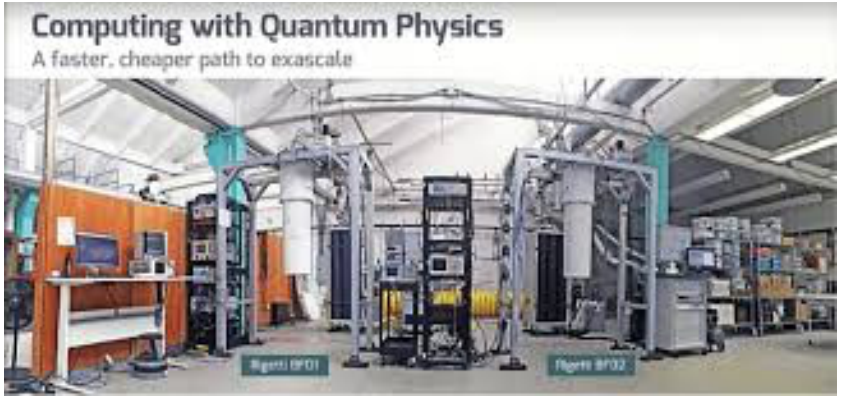
ESTABLISHED

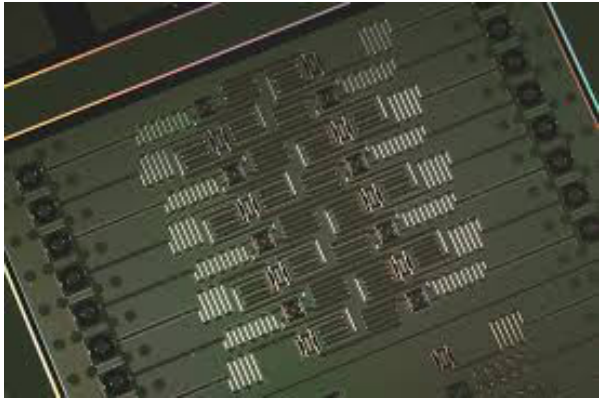
- Chemistry
- Materials science
- Precision measurement
- Cryptography

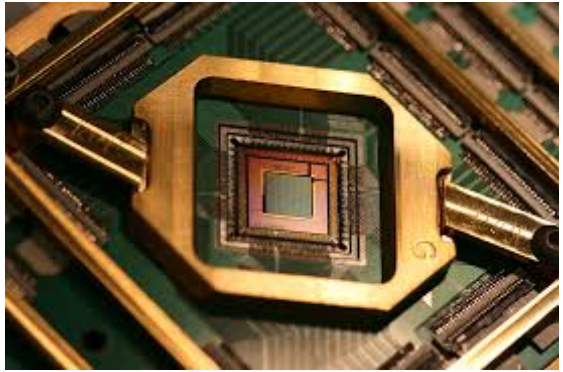
EMERGING

- Optimization
- Big data
- Machine learning
- Climate modelling

Quantum Computers & Processors: actual Form factor?







Quantum Computers :
New way of programming

SERMA
SAFETY & SECURITY

What does the code of a quantum computer program look like?

- New type of programming (weird one)
- and completly new way of designing any algorithm (Disconnecting your « classical brain » for a « quantum brain » is hard …trust me !)
- Juste one example: In Quantum bit world, cloning (=make a simple copy of the value) of a Qbit is not possible (decoherence of quantum state !)

New programming IDE, new logical gate to understand…

Programming a QC in real life !

-> Demo 101

https://quantumexperience.ng.bluemix.net/qx

SERMA
SAFETY & SECURITY

Quantum Computers: a threat for security ?

SERMA
SAFETY & SECURITY

Juste 1 threat example

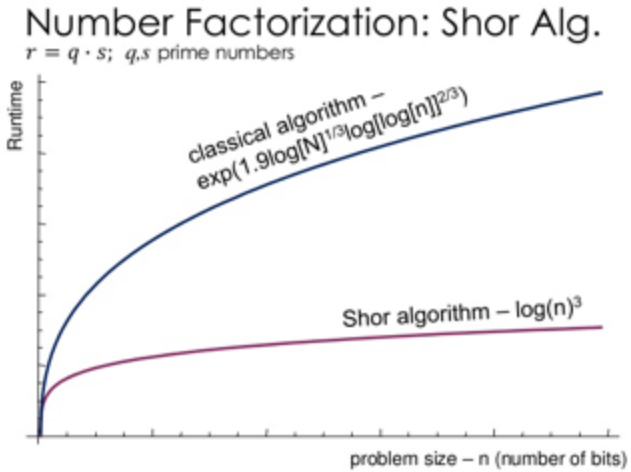
- Among other things… Classical Crypto defense issue on the rise !

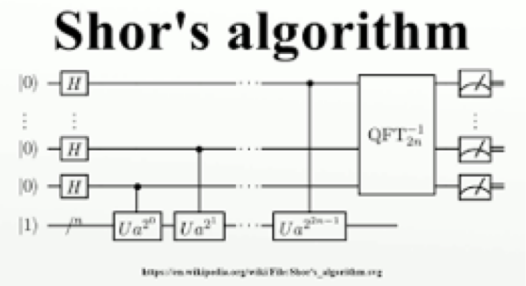
How Secure Will Our Current Cryptography Be When Full Scale Quantum Computing Arrives?

Algorithm	Key Length	Security level (Conventional Computer)	Security level (Quantum Computer)
RSA-1024	1024 bits	80 bits	~0 bits
RSA-2048	2048 bits	112 bits	~0 bits
ECC-256	256 bits	128 bits	~0 bits
ECC-384	384 bits	192 bits	~0 bits
AES-128	128 bits	128 bits	64 bits
AES-256	256 bits	256 bits	128 bits

UNIVERSITY OF WATERLOO | IQC Institute for Quantum Computing

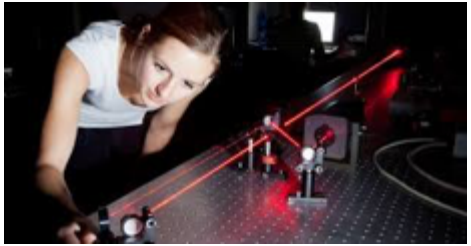
Why ? -> Shor's algorithm





Quantum mecanic could improve our defenses…

- But Quantum mecanics could also help improving
- the security defense



- Quantum Cryptography or QKD
- Quantum Key Distribution

Cryptography comparaison

Quantum Safe Cryptography Comparison

'Post-quantum' cryptography

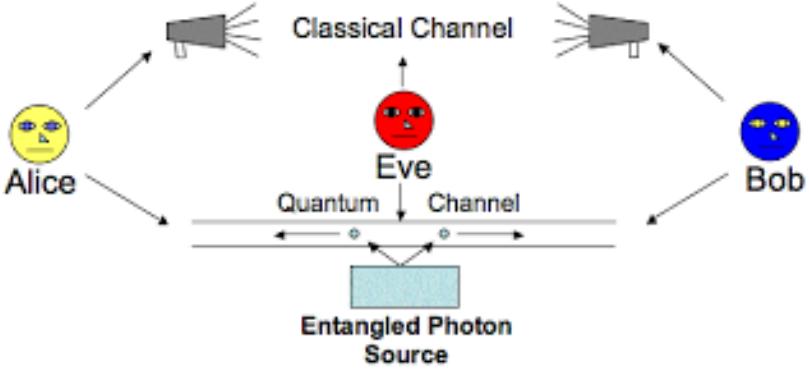
- Security relies on the hardness of certain computational problems
- Vulnerable to advances in cryptoanalysis and computing power
- No security proof

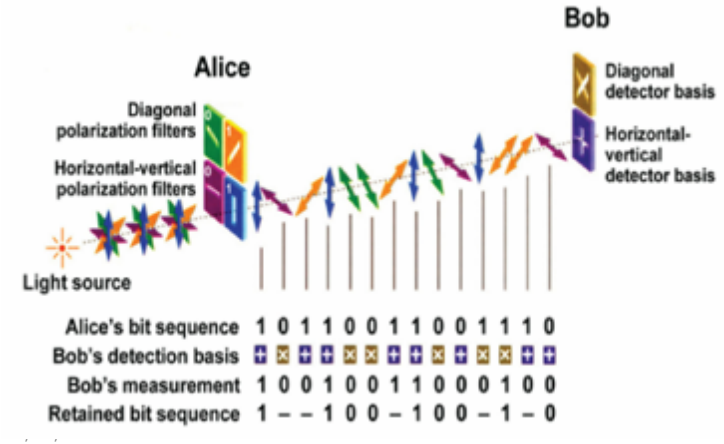
Quantum cryptography

- ✓ Security is based on some quantum property
- ✓ Typically no computational assumptions and therefore secure against quantum attacks
- ✓ Conceptual security guaranteed by quantum physics

What option delivers better security in practice?

BB84 protocol will save the world... Or not

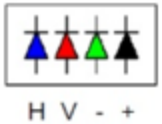


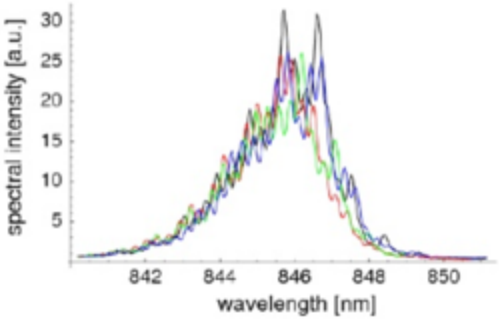


How to attack this?

- Spectral attack
  - Each polarization state can be created using its own laser photo diode
  - For Eve, instead of measuring the polzarization (**thus altering the photon state**), she can just use spectral analysis to recover the information:

C.K.,P. Zarda, M. Halder, H. Weinfurter





Conclusion

- Quantum Computing is a bit a « disruptive » subject for Security world
- Impacts of this new technology reminds me the result of CyberGrand Challenge where IA code surpass main reverse engineering specialist or pentesters to find and correct vulnerability
- But as usual, This techno will be use for good and evil (be prepared)

QA ?

- Questions?
- We are hiring … a lot ! ;-)
- Good hacking for all CTF teams
- Contact : @meallainyann / y.allain AT serma.com