Why Quantum Technologies Matter in Critical Infrastructure and IoT

February 2018

ID Quantique. Overview

Founded in 2001

By 4 quantum physicists from the University of Geneva
Today more than 60 people

Geneva, Switzerland - Headquarters
Bristol, UK – Research
Hangzhou, China – Joint Venture

Develops technologies based on quantum physics

Performs R&D, production, professional services, integration, support

Clients : Governments / Banks / Gaming Industry / Universities / IT Security/Energy

IoT : Are we opening Pandora's Box?

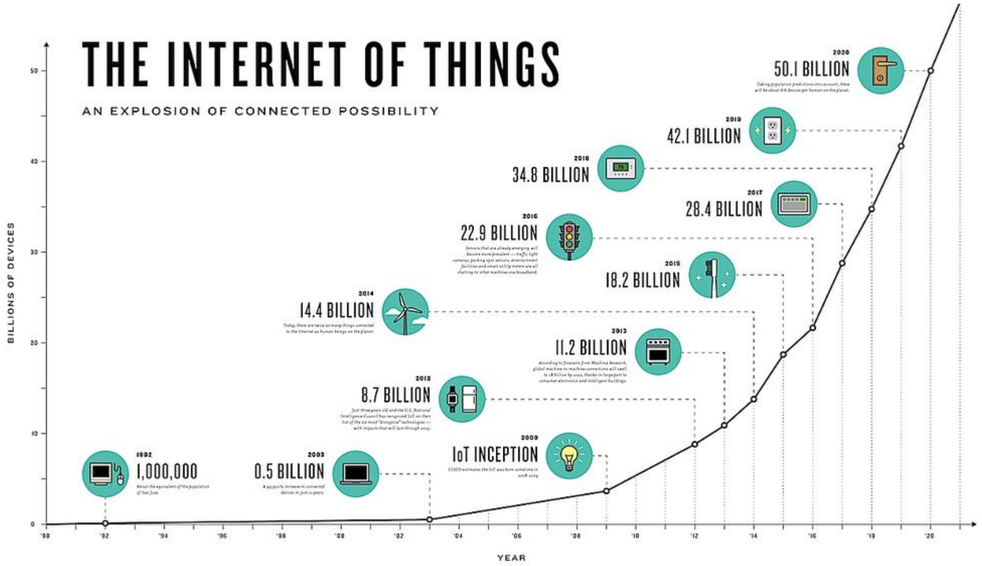
IoT Facts: Rapid Growth

SWISS QUANTUM

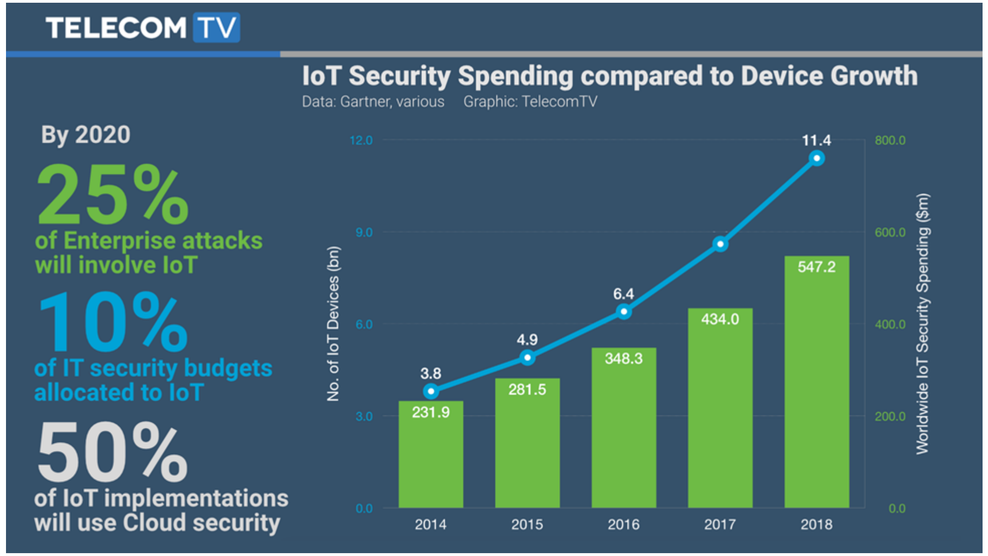
- It is all is connected!

IDQ

IoT Facts: Growth & Security Spendings



https://www.cnccookbook.com/need-know-now-iot-internet-things-cnc-manufacturing/



https://datafloq.com

- 30% of G2000 companies will be using data from digital IoT connected products and assets to improve product innovation success rates and organizational productivity
- The potential cybersecurity and physical safety concerns associated with IoT devices will pressure CIOs at G2000 companies to increase IoT security spending
- Asia/Pacific (excluding Japan) (APeJ) will be the geographic region with the most IoT spending in 2018 – $312 billion

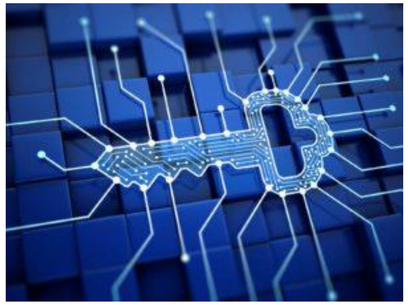
IoT Facts

- Increase in attack vectors!

IoT Risks in Critical Infrastructures

- **Devices and systems in our critical infrastructures become ever more interconnected**
  - Increase in attack vectors
  - Increasingly important to ensure that they have adequate cryptographic protections
- **Rapid technological advancements will also favor new attack vectors**
- **New Quantum technologies will threaten current cryptographic primitives**
- **The interconnected nature of IoT makes the scalability of those vectors unprecedented**

IoT Risks in Critical Infrastructures



⇧ Critical Infrastructure + ⇧ Internet of Things = ⇧ More Risks, so ⇨ ⇧ Cyber Security

Quantum Threats to Today's Cryptography

- Recent breakthroughs in quantum computing have brought about a credible threat to the widely used cryptographic primitives which underpin our infrastructures and networks:
  - Exponential speed-up brought by Quantum computer's weird "superposition state", a quantum bit can be a "0" and "1" at the same time
  - Ultimately, the whole quantum computer can now be in a superposition state, which provides <u>exponential computing power.</u>
  - Threat to public key cryptography, such as RSA, Elliptic Curve Cryptography & Diffie Hellmann
  - Shore's discrete algorithm is much faster than any classical algorithm

Swiss Quantum Skiing and more Cats!

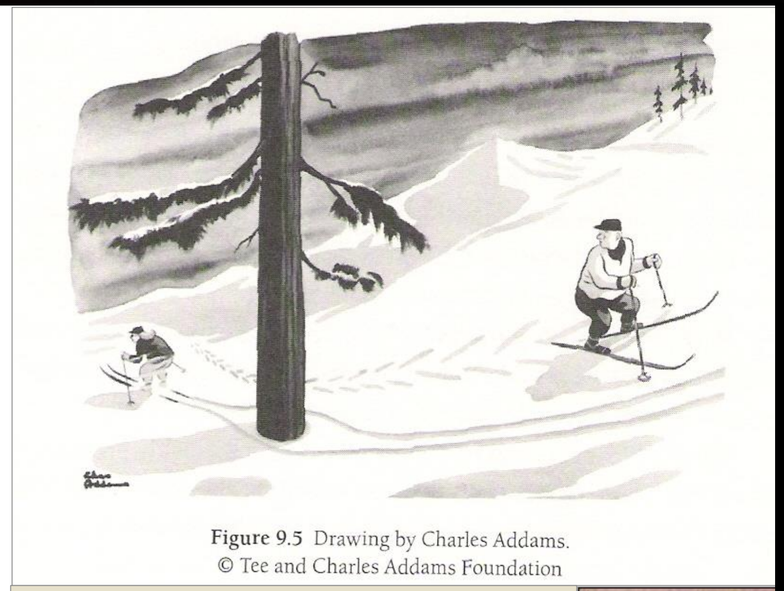
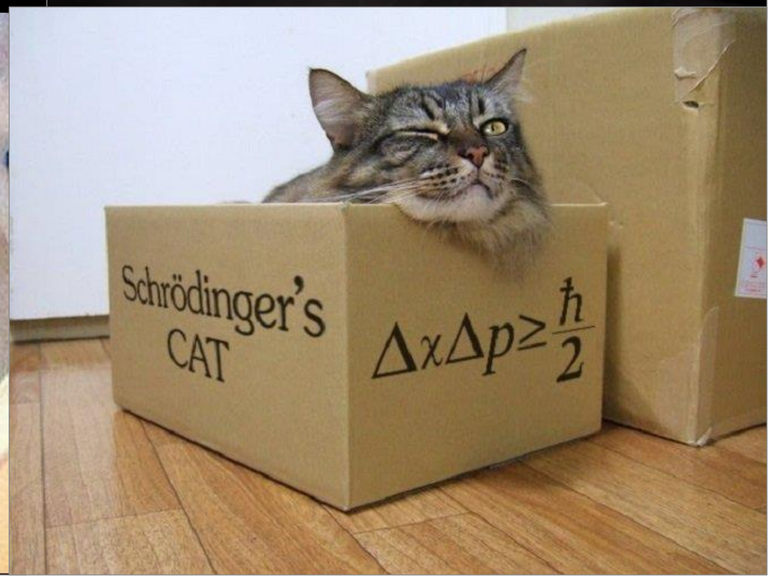
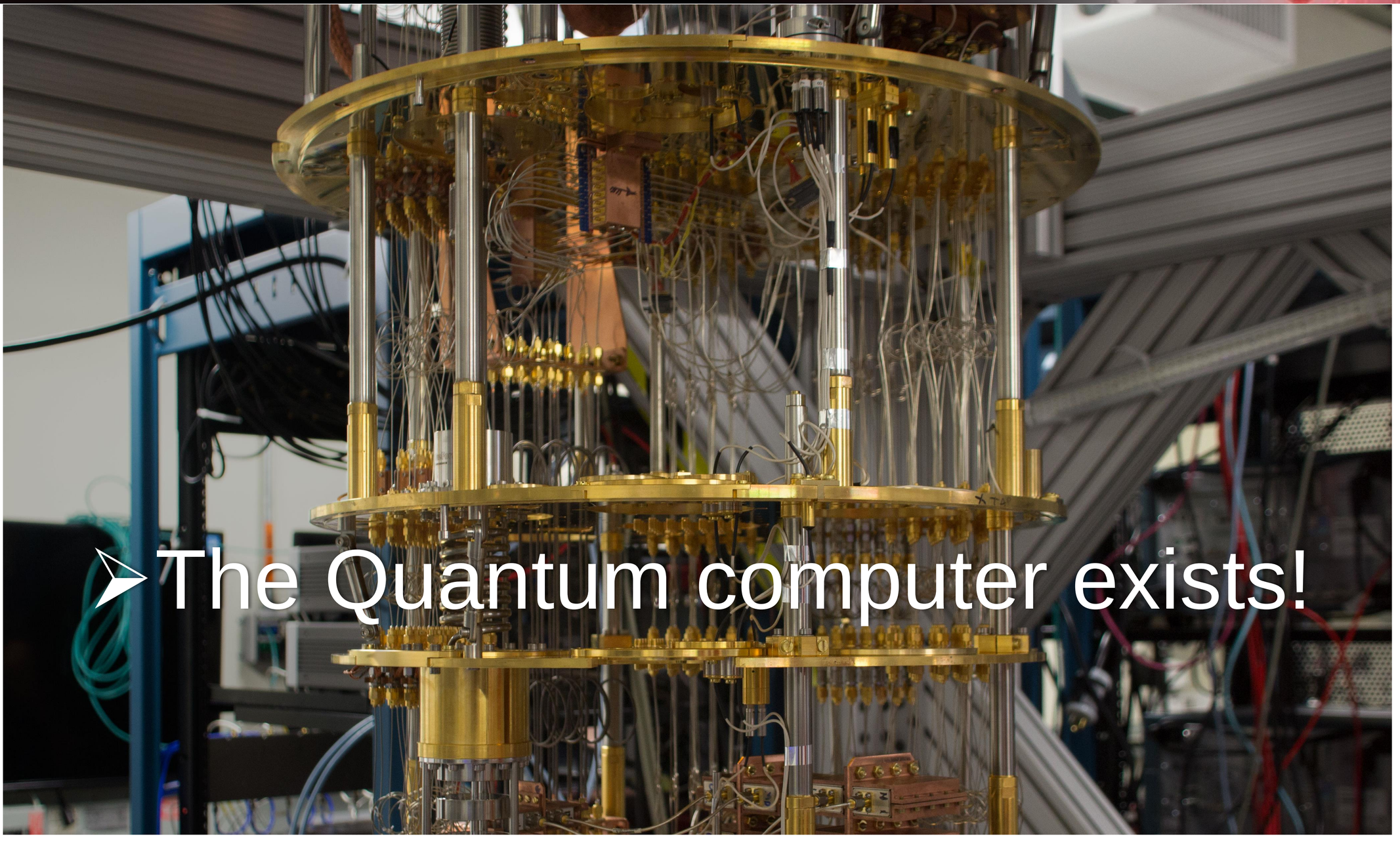


Figure 9.5 Drawing by Charles Addams.
© Tee and Charles Addams Foundation





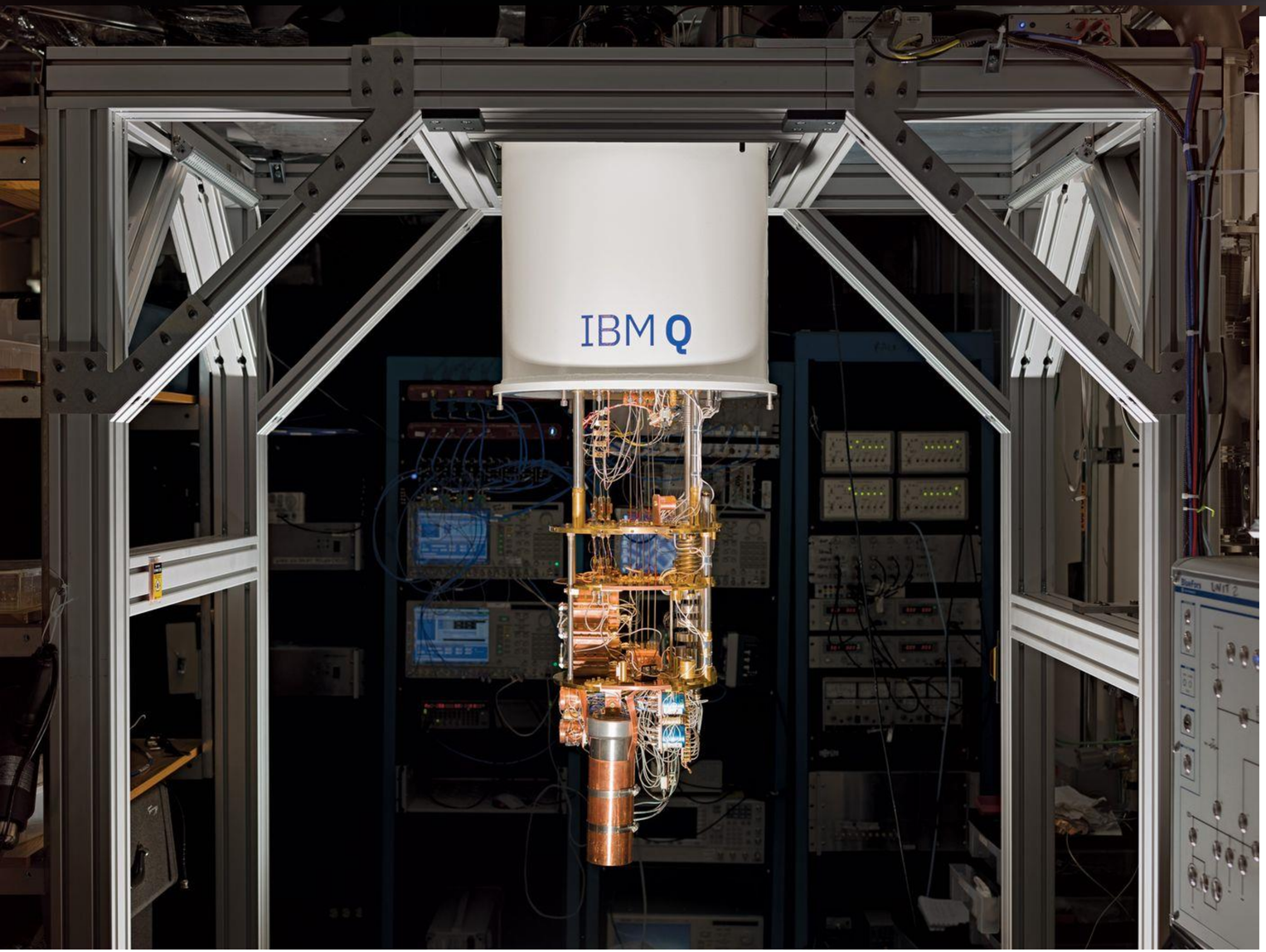
- The Quantum computer exists!

IDQ

The Quantum computer already exists!

IBM has launched the first quantum computing cloud, which allows external users to experiment with a small number of qubits

Big… but mostly cold gas and light!



Google’s target for proving quantum supremacy: (the ability of a quantum computer to resolve certain problems faster than the best available conventional processors) by the end of 2017

Quantum computer can’t run Shore’s Algorithm yet….but it’s only a question of time!

So When??

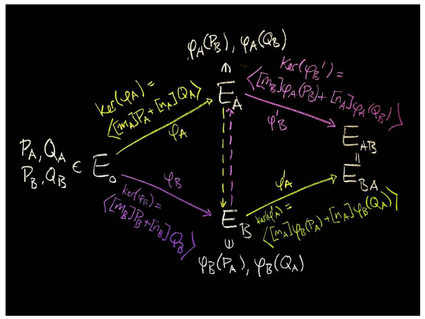
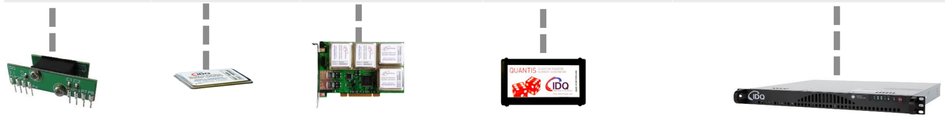
Dr Michele Mosca (Institute for Quantum Computing in Canada & CEO of evolutionQ Inc.) :

- large-scale quantum computing is 10-15 years away,
- 1 in 7 chance of crypto primitives being affected by quantum attacks in 2026
- 1 in 2 chance by 2031

  - May sound a long time away, but given the timescales for developing and deploying many critical infrastructure devices (20y+), it would be prudent to start preparing now!

Protect against Quantum?

New cryptographic techniques have emerged in recent decades that do provide protection against quantum threats = Quantum Safe

Quantum Key Distribution (QKD) (aka Quantum Cryptography) ✓ protection against quantum threats	
New Quantum Resistant algorithms (aka Post Quantum Crypto)	
Quantum Random Number Generators (QRNG) ✓ improving cryptographic key generation	**OEM Components** / **Dedicated Devices** / **Distributed Appliance** Qube – Quantis OEM – Quantis PCIe – Quantis USB – Quantis Appliance Optical cube + software – Stand-alone – Embedded – Easily Removable – For multi-threading environments 

Hardware Protections & Key Generation

- Another aspect fundamental to security is the random number generator (RNG), essential to all crypto operations
  - Generating strong keys, based on true randomness, is the cornerstone of security
  - good keys must be unique, unpredictable and truly random

- Software-based RNGs are not sufficient, as the computer programs they run are purely deterministic and cannot generate true randomness without external entropy sources
  - RNGs should be based on hardware, and the resulting crypto key should also be protected in hardware

Having strong crypto algorithms with weak keys is akin to putting a huge padlock on your front door and then hiding the key under the mat!

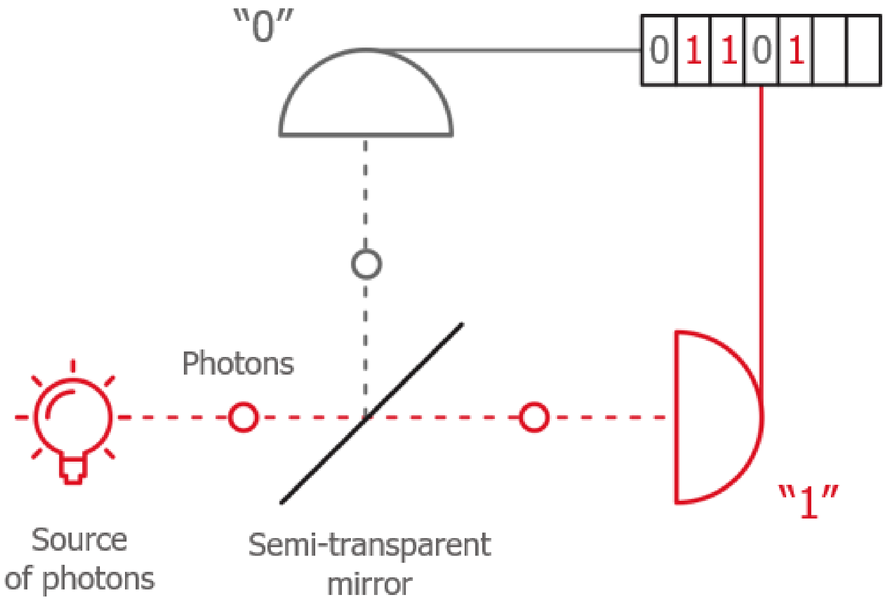
Quantum Physics-based RNGs (QRNG)

Principle :

- Quantum physics describes the particles' behavior
  - Radioactive decay, photon state, etc.…

It is the only theory including randomness

- probabilistic by nature



Advantages :

- Speed : instantaneous and inexhaustible entropy
- Robust process : can't be influenced
- Simplicity : the process can be modeled and theoretically certified as secure

Solution: Iot Specific Risk Mitigation with a QRNG Chip

SWISS QUANTUM

- **Generating strong keys, based on true randomness, will be a cornerstone of IoT security**

Good keys must be unique, unpredictable and truly random. Also resistance to external environmental perturbations is critical.

Get the hardware right now!

- **IDQ / SK telecom QRNG chip**

The world smallest low cost QRNG for security, IoT & critical infrastructure applications

- IoT, SmartGrid, SmartCity, SmartHome, etc
- Computing devices, like mobile phones, tablets, servers, etc
- Seed generation for blockchain
- Artificial Intelligence

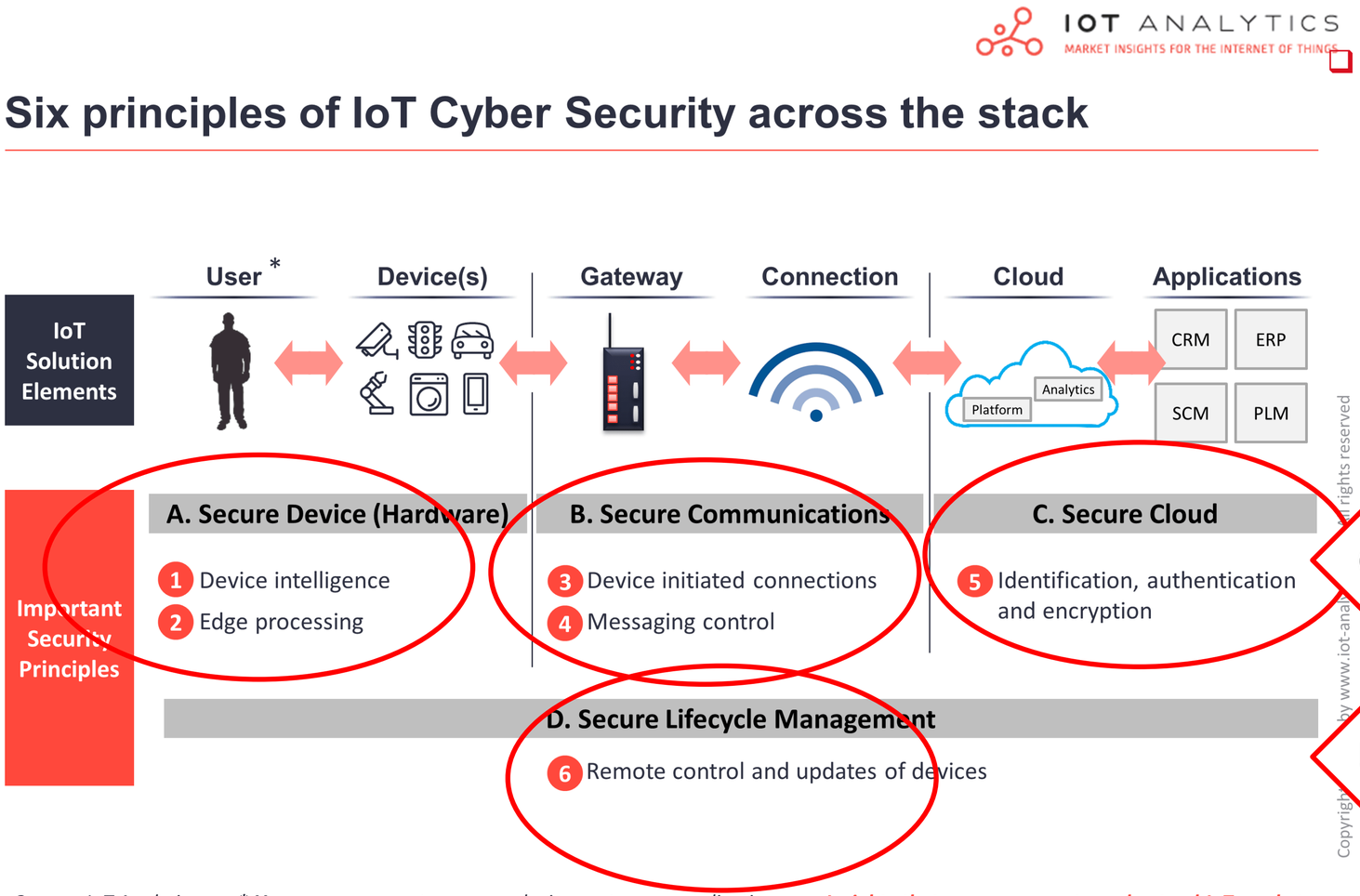
IDQ

Keymile/ ABB Integration – True Number Generator QRNG

First encryption card for mission-critical infrastructure with truly random numbers

- Crypto (confidentiality & authentication) for MPLS data flows
- Extreme requirements: Jitter at Nanosecond level
  Latency at Microsecond level
- -30 to 80°C operations
- Lifetime in the field: up to 40 years
- FPGA crypto capabilities enabling secure future upgrades
- Supports critical infrastructure backbones
- Secures transit of data generated by edge sensors

Recommendations: Iot Specific Risk Mitigation



IoT Crypto Security Requirements (US Department of Homeland Security recommendations)

- ❑ All interactions between devices MUST be mutually **authenticated**
- ❑ All communications between devices SHOULD be **encrypted**
- ❑ When used, cryptographic **keys MUST be protected** (i.e. use of Trusted Platform Module)

QRNG, QKD, Encryption

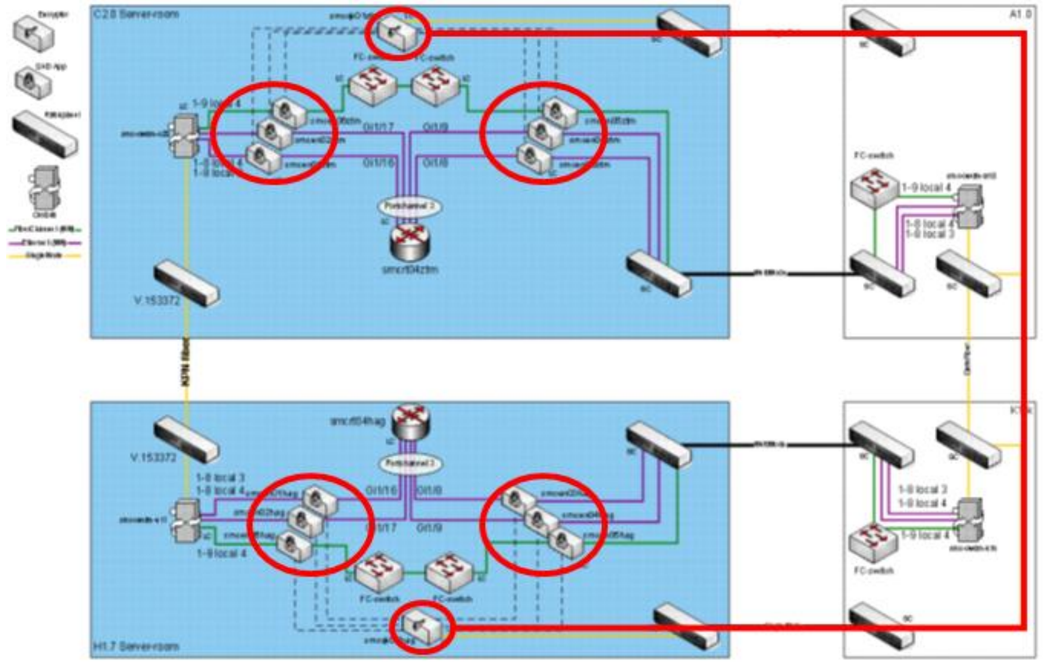
Upgradability & Crypto-agility

Quantum Key Distribution (QKD)

SWISS QUANTUM

Atos SIEMENS

- Wide-scale QKD is already being deployed on transport networks to provide quantum-safe protection to critical infrastructures in countries such as China
- QKD is not yet adapted for edge or hyperconnected networks
- Applications of QKD are currently restricted to specific cases, such as highly critical links between major infrastructure components rather than IoT field deployments



IDQ

Quantum - Resistant Algorithms

- Quantum Resistant Algorithms (also known as Post Quantum Cryptography) refer to cryptographic primitives (such as latticebase or code-based)

- NIST has launched a solicitation and evaluation process with the goal to standardize on one or more quantum resistant public key crypto algorithm. The process will take at least 5 years.

- Not provably secure from a mathematical perspective (unlike QKD), they must be rigorously tested and analysed before being deployed

Iot: Risk Mitigation Now!

- **PREPARE NOW!**
  - **Understand and document the threat models** which might affect your critical infrastructure deployments. Prepare upgrade path for the future
  - **Build a process for continual evaluation** for such threat models
  - **Prepare for the upcoming quantum era** by investigating the impact of quantum technologies upon your devices, systems and deployment = Quantum risk assessment

- **ACT NOW!**
  - **Build crypto agility into your devices**, systems and deployments to ensure an upgrade path in the future
  - Build hardware devices and systems with a view to long term security in the field:
    - ✓ **Spare computing power** able to support upgraded crypto-primitives and run time protection
    - ✓ **Hardware based key generation** for adequate security of cryptographic operations throughout the lifetime of the device, ideally based on quantum photonics for resilience to environmental influences

THANK YOU!

Olivier.Pfeiffer@idquantique.com