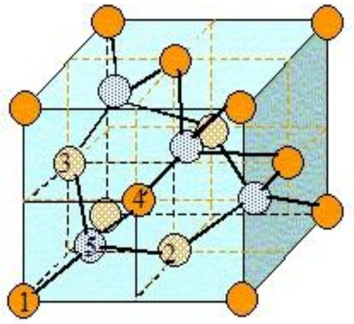
Modeling, Simulation and Visualization for quantum computing : Atos Quantum

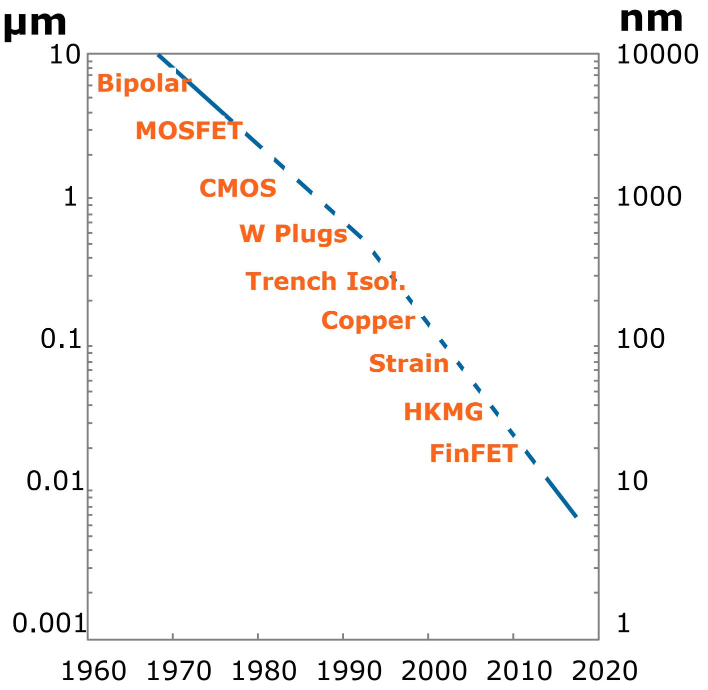
CSD&M 2019 – 13 December 2019

Philippe Duluc,
Atos CTO Big Data & Security
Distinguished Expert – Atos Scientific Community

Atos

The computing disruption





- Moore's law declining: 0,3 nm between 2 atoms in Silicon crystal, chip fabrication process < 10 nm
- obligation for Atos to find new directions in order to provide accelerations required by customers

Atos

The cybersecurity disruption

TODAY/PAST (pre-quantum)

- classical factorization record for **RSA768** in 2010. Two years of computing on several hundreds machines to factorize this :

1230186684530117755130494958384962720772853569595334792197322452151726400507263657518745202199786469389956474942774063845925192557326303453731548268507917026122142913461670429214311602221240479274737794080665351419597459856902143413

=

3347807169895689878604416984821269081770479498371376856891243138898288379387800228761471165253174308773781446799948 9

×

3674604366679959042824463379962795263227915816434308764267603228381573966651127923337341714339681027009279873630891 7

- comp[**RSA1024**] = comp[**RSA768**] * 10^{37}

This exponential complexity is the keystone of RSA crypto algorithm (and almost all asymmetric algos)

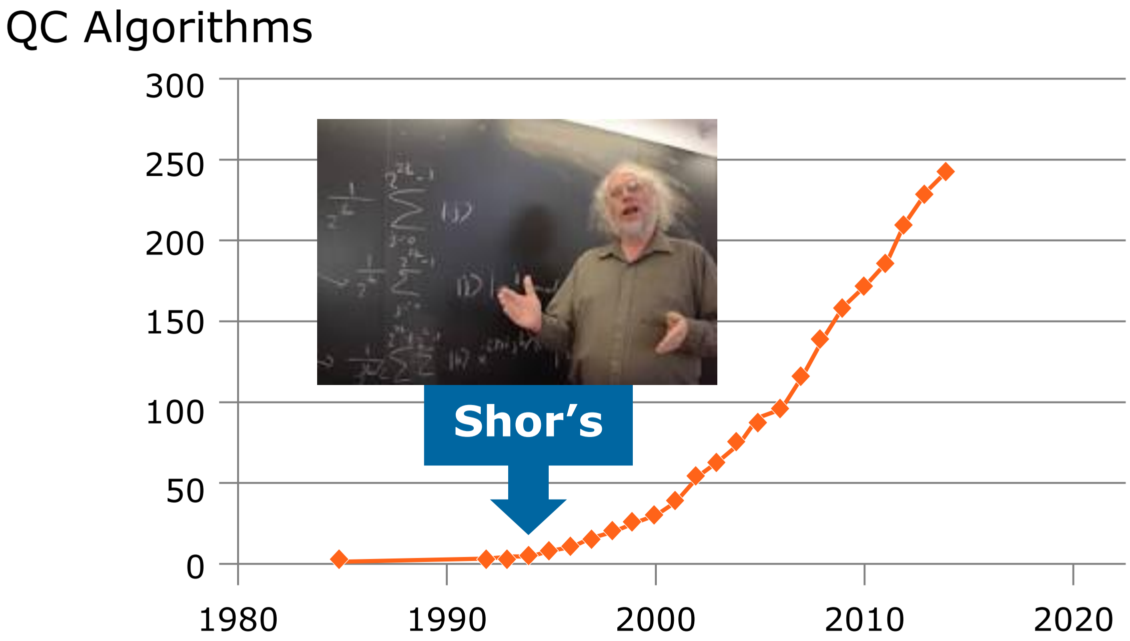
TOMORROW (post-quantum)

- Shor Algorithm: polynomial time
- RSA-768 : almost instantaneous by using a quantum computer with several thousands logical Qubits
- comp[**RSA1024**] = comp[**RSA768**] * 2,4

Critical risk (very high impact, low prob.) for IT security everywhere

Atos

Algorithmic innovation has launched the Quantum Big Race



math.nist.gov/quantum/zoo

Atos

Atos Quantum : a long-term strategic R&D investment of disruptive innovation, set up in 2016

- Atos worldwide leader in supercomputing and European leader in cybersecurity

Quantum Computing will affect sooner and later Atos supercomputing customers and cybersecurity customers

- **Business rationale**
  - **strategic move to keep business leading positions**
  - **aiming mid-term RoI**
  - **in close touch with customers**

Atos

Atos Quantum Program

Atos QLM
Atos Quantum Learning Machine

Focus on quantum software, agnostic in quantum hardware: commercialization (since 2017) of **Atos QLM** which is an appliance making easy to develop quantum algorithms (programing, optimising and testing via emulation up to 41 qubits), free distribution (since 2019) of **myQLM** software

Atos Quantum Accelerator

R&D program with hardware partners: to deliver in 2023 a **NISQ accelerator** (50 to 100 physical qubits) for hybrid supercomputing and driven by **Atos QLM**

Atos Quantum-safe security

Aligned with NIST call for post-quantum standards: preparing the cryptographies and hardware security modules, resistant to quantum attacks

Quantum simulation

- Single qubit: superposition of two states
  - represented by a complex state vector
  - needs 2x2 floating points (64 bits)

$$|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$$

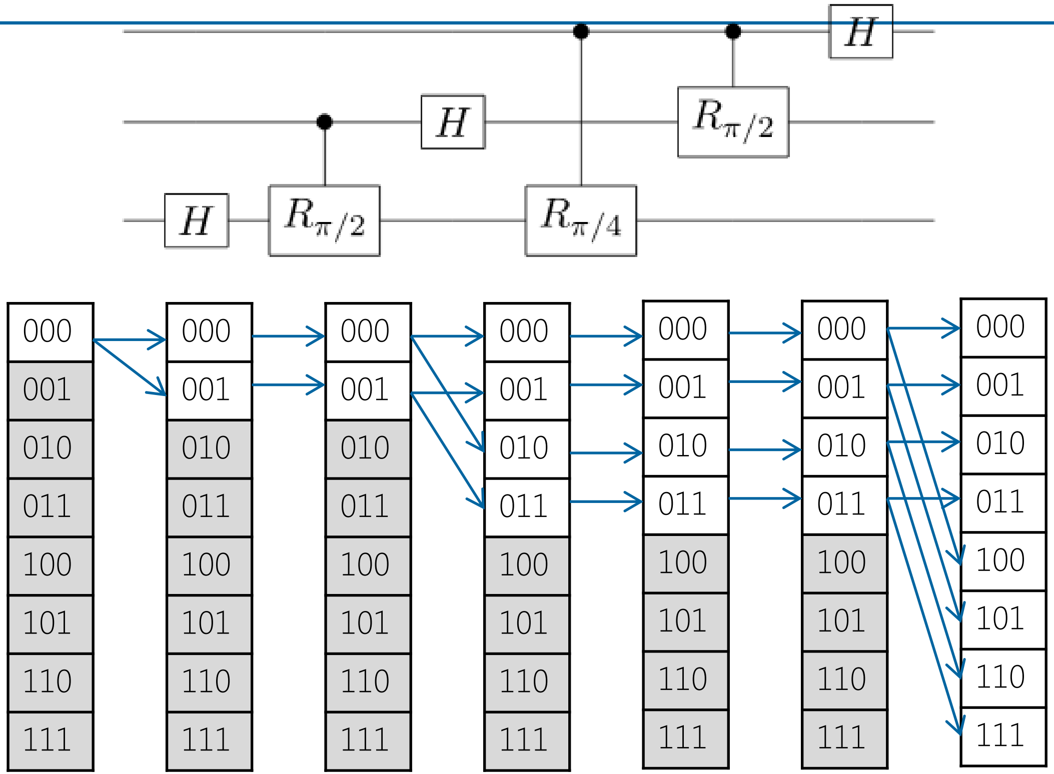
- System of n entangled (and superposed) qubits:
  - complex Hilbert space, 2^n eigenstates (no separation)
  - 2^{n+2} floating points (64 bits) to describe a whole state vector

$$|\Psi\rangle = \sum_{i=0}^{2^n-1} \alpha_i|i\rangle$$

- Quantum gate is represented by a complex matrix (2*2 for 1-qubit, 4*4 for 2-qubits, etc.)
- Quantum gate operations are simulated by matrix-vector product
- Quantum measurement: we can only observe one of all the possible binary states at any given time (one of eigenvalues). **Measurement destroys the quantum superposition**
- In simulation, we could have direct access to the whole state vector (all the values of $\alpha_i' s$) at the expense of huge memory consumption. **Impossible in real life.**

Atos

Quantum simulation (continued)



Up to 8 threads can be used in this simple example.
Shaded parts are vector components which are never explored during simulation.

Atos QLM customers

Hartree Centre
Science & Technology Facilities Council

- commercial success in a new market
- huge interest immediately after announcement in July 2017
  - for education (universities)
  - for research (research centers, university labs)
  - for HPC ecosystems (post Moore's law)
  - for industry (first contracts)

SURF SARA

Argonne NATIONAL LABORATORY

OAK RIDGE National Laboratory

BAYER

fh OBERÖSTERREICH UNIVERSITY OF APPLIED SCIENCES UPPER AUSTRIA

UNIVERSITÉ DE REIMS CHAMPAGNE-ARDENNE

cea

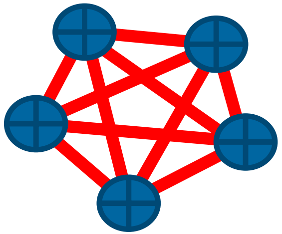
ccrt

JÜLICH FORSCHUNGSZENTRUM

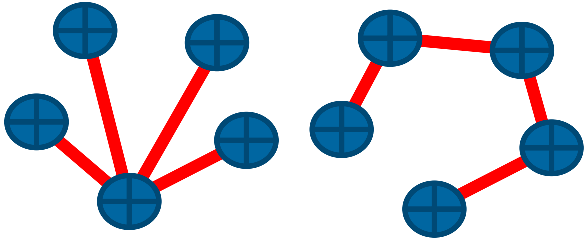
TOTAL

From linear simulation to realistic simulation

- leading hardware technologies for qubits-based circuits:
  - trapped ions qubits
  - superconducting qubits
  - semiconducting qubits



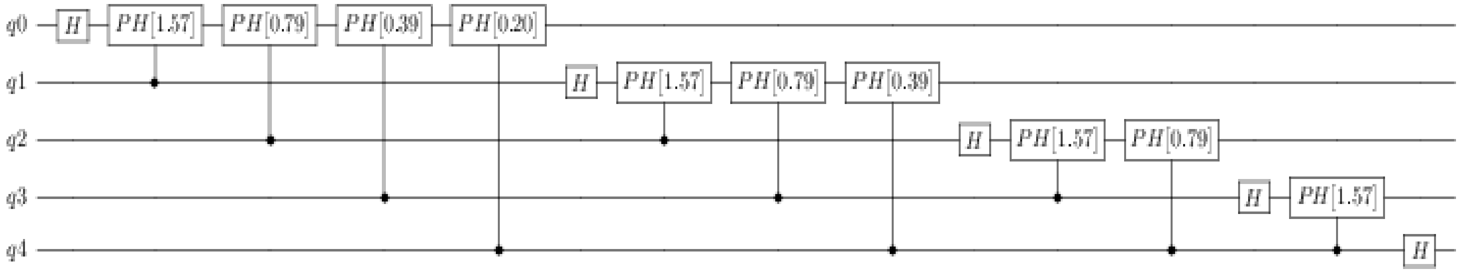
- performances of algorithms are **HW dependent**:
  1. qubit topology, connectivity, gate limitation
  2. stability, quantum noise (decoherence)
  3. speed, shallowness, idling time

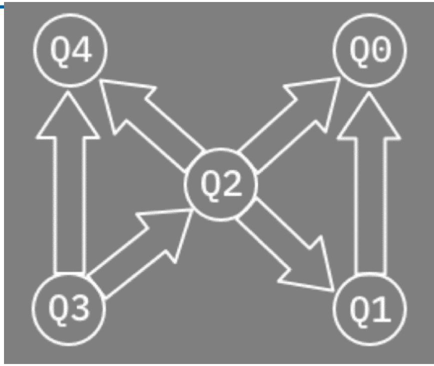


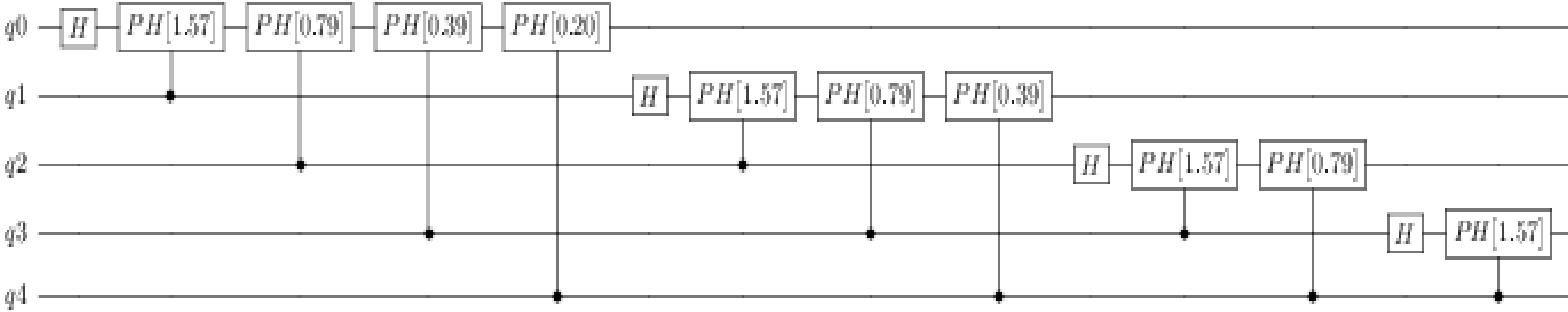
- **Atos QLM** integrates hardware constraints
  - powerful compiler and optimizers
  - testing more realistic (integrating noise models and topology)
  - true performance over present and future accelerators

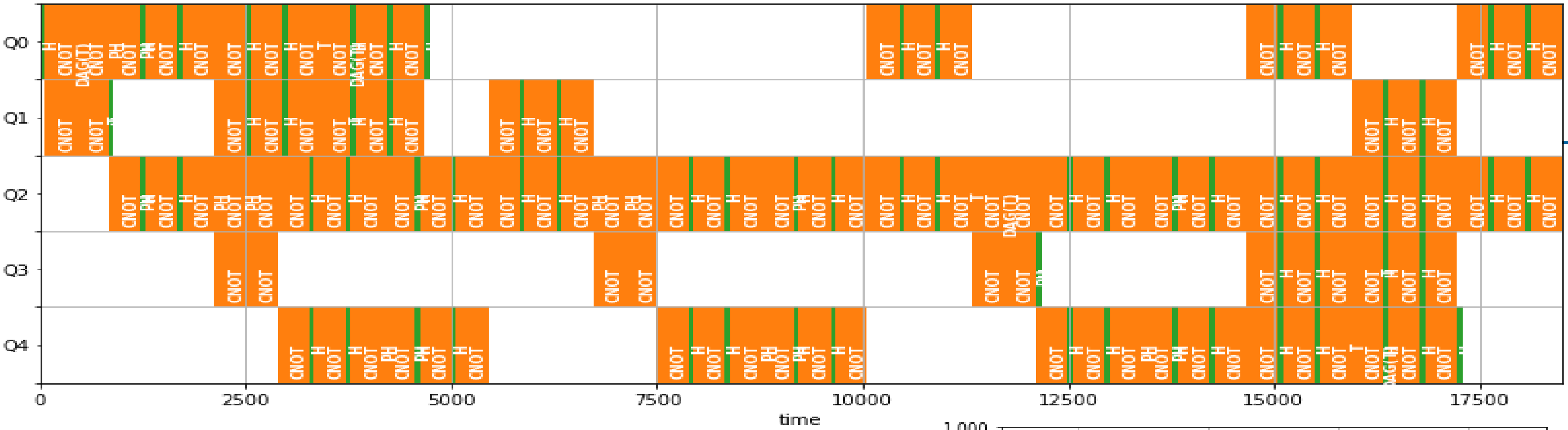
Atos

Optimizing fidelity with QLM

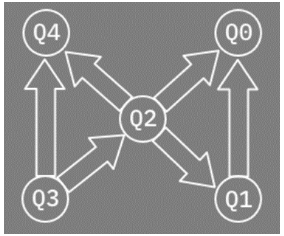




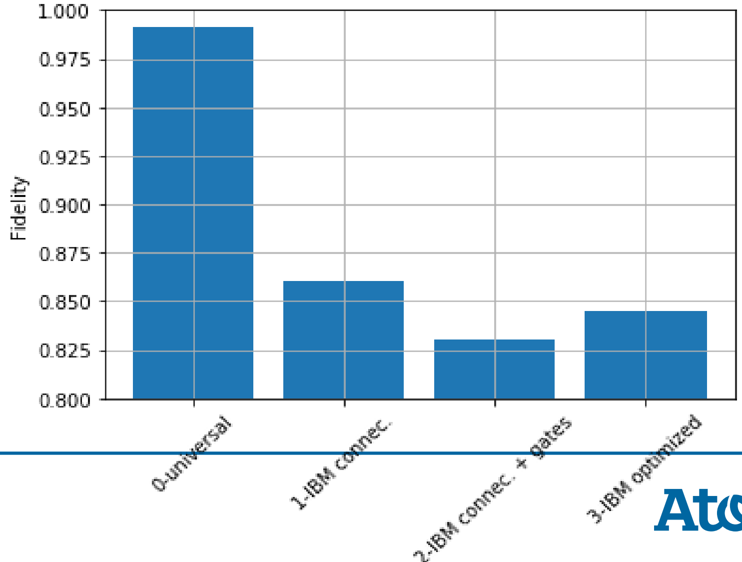




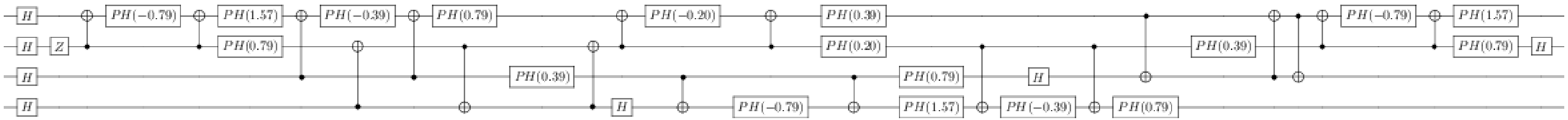
Visualization of Quantum circuit



Connectivity constraints
& gate limitations
increase circuit length
& require QLM optimizations



Optimizing idling time with QLM



qft4

Minimize overall idling time