Engineering Quantum Computing at Politecnico di Torino

from technological modelling to industrial software applications

Bartolomeo Montrucchio, Mariagrazia Graziano,
Olivier Terzo

Quantum Computing and High Performance Computing

CINECA Casalecchio di Reno, Bologna, 19 December 2019

POLITECNICO DI TORINO

LINKS
LEADING INNOVATION & KNOWLEDGE FOR SOCIETY

The PoliTO team on Quantum Computing



DET+DISAT

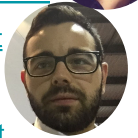
mariagrazia.graziano@polito.it

giovanna.turvani@polito.it

giovanni_cirillo@polito.it








DAUIN

bartolomeo.montrucchio@polito.it

filippo.gandino@polito.it

mohammad.ghazivakili@polito.it

edoardo.giusto@polito.it

antonio.lioy@polito.it

ignazio.pedone@polito.it




LINKS

olivier.terzo@linksfoundation.com

andrea.scarabosio@linksfoundation.com

alberto.scionti@linksfoundation.com

carmine.damico@linksfoundation.com

TECHNOLOGY

APPLICATIONS

Hardware for Quantum Computing

- Many technologies (superconductors, trapped ions, molecules, *etc.*) have been proposed as candidate for the implementation of a quantum computer.
- They can significantly differ in terms of:
  - temperature;
  - magnetostatic fields;
  - bandwidth of EM signals employed for the implementation of quantum gates;
  - non-ideality (*e.g.* decoherence and relaxation) timescales;
  - native gates;
  - fabrication and maintenance costs.
- A system capable of evaluating the quality of a quantum circuit/algorithm on different quantum computers, taking always into account their pros and cons, is required.

TECHNOLOGY

POLITECNICO DI TORINO

LINKS
LEADING INNOVATION & KNOWLEDGE FOR SOCIETY

Methodology for comparing quantum technologies

TECHNOLOGY

Given the same circuit/algorithm, technologies can be compared in terms of:

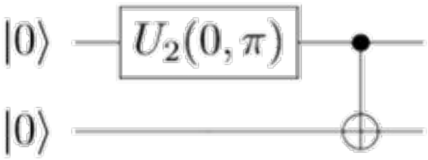
- effects of non-idealities in the execution;
- native quantum gates;
- qubits connectivity;

circuit transpiling

- feasibility of a quantum circuit according to the classical hardware instrumentation required for manipulating qubits (bandwidth, time duration of elementary pulses, amplitude of electromagnetic signals, magnetostatic fields, *etc.*).

Comparison must be simplified by taking into account the main features of each technology

Example: Bell state circuit



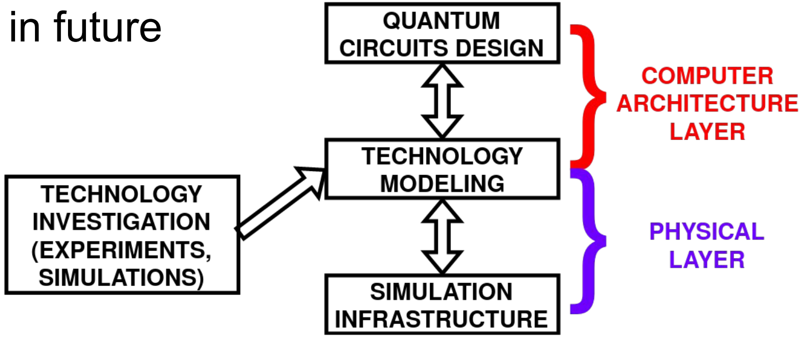
Superconducting qubits

Trapped ions

Methodology for analyzing a QC technology

TECHNOLOGY

- Perspective: development of a software tool for designing and comparing the execution of quantum circuits with different technologies (superconductors, trapped ions, molecules, *etc.*).
- Each technology is described by a simplified model which takes into account its main physical properties, in particular non-idealities, starting from experiments or physical (*e.g. ab-initio*) simulations.
- An optimized simulator for non-ideal quantum circuits is required.
- The integration of this infrastructure into Quantum Computing frameworks as Qiskit is going to be proposed in future



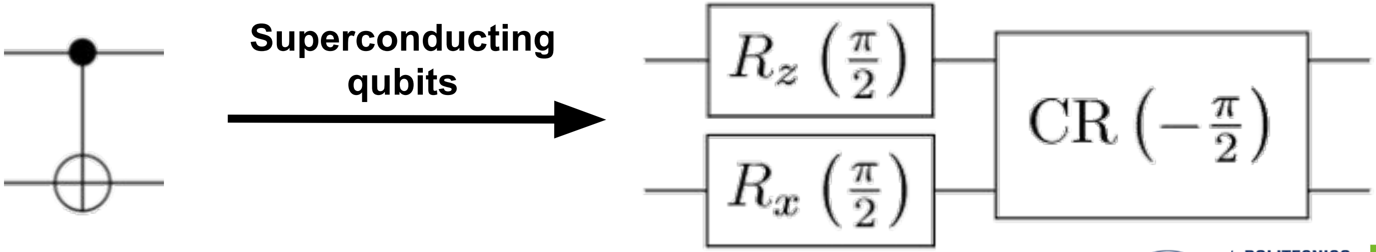
POLITECNICO DI TORINO

LINKS LEADING INNOVATION & KNOWLEDGE FOR SOCIETY

Quantum circuits design

- The simulator is thought for ensuring quantum circuits design with more degrees of freedom:
  - Setting the parameters of each quantum gate according to its physical implementation (core)
  - Using hardware-agnostic gates of a HDL (currently OpenQASM), with automatic derivation of the parameters of *physical gates*
- *Ad-hoc* quantum circuit transpiling strategies according to the exhamined technology can be defined.

TECHNOLOGY



POLITECNICO DI TORINO

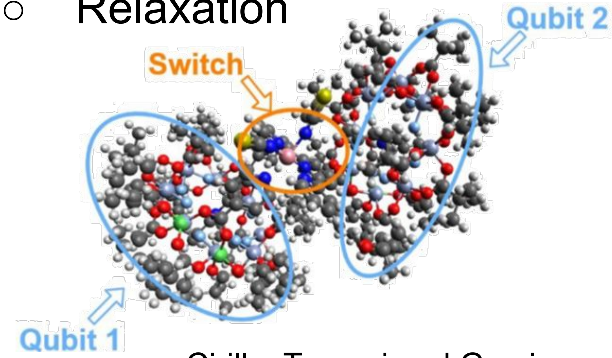
LINKS LEADING INNOVATION & KNOWLEDGE FOR SOCIETY

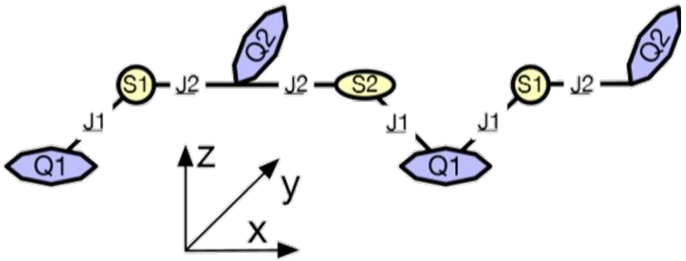
A practical example: Cr_7Ni molecular nanomagnets

Main features:

- Chain of spins exploited for encoding qubits and switches
- Possibility to implement $R_{x,y}(\theta)$ and Controlled-phase gate (universal set of quantum gates)
- Non-idealities:
  - Interaction between adjacent spin qubits
  - Decoherence
  - Relaxation

TECHNOLOGY





Cirillo, Turvani and Graziano, *IEEE Transactions on Nanotechnology*, 18(2019), pp. 1027-1039.

POLITECNICO DI TORINO

LINKS LEADING INNOVATION & KNOWLEDGE FOR SOCIETY

A practical example: Cr_7Ni molecular nanomagnets

1. Build simplified descriptions of qubit and switch evolutions in presence of external EM fields (with the possibility to regulate pulse shape, duration, amplitude, *etc.*) and non-idealities (qubit-qubit interaction, relaxation, decoherence).
2. Define single-qubit and Controlled-phase gates, which are the micro-instructions of the computer architecture, over the simplified models of the system evolution.
3. Define more complex gates based on microinstructions, eventually optimizing with circuit transpiling and virtual-Z gates.
4. Design a quantum circuit/algorithm with low-level routines or in OpenQASM.
5. **Evaluate the results in presence of non-ideality phenomena**.

TECHNOLOGY

```
function singlequbitevolution(...){
      ...
}
function singleswitchevolution(...){
      ...
}
function switchinteractionqubits(...){
      ...
}
```

→

```
qs.rotate(0,pi/2,-pi/2)
qs.rotate(1,pi/2,-pi/2)
qs.controlledphase(0,1,pi)
qs.rotate(1,pi,-3*pi/2)
qs.measure()
```

→

```
OPENQASM 2.0;
include "qelib1.inc";
qreg q[2];
creg c[2];
h q[0];
cx q[0], q[1];
measure q -> c;
```

Applications

- Optimization of Constraint Satisfaction Problems
  - Graph exploration
- Apply QC to IT problems
  - Internet of Things
    - Air Pollution Monitoring sensor networks
  - Process Scheduling
- Investigation on already available Quantum-Proof DLT
- Integration IoT + DLT
  - Food-Chain use case

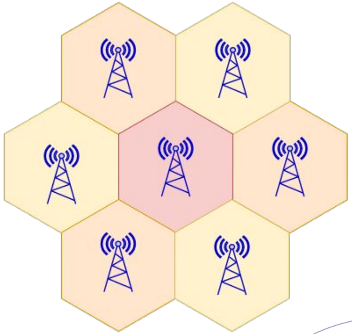
APPLICATIONS

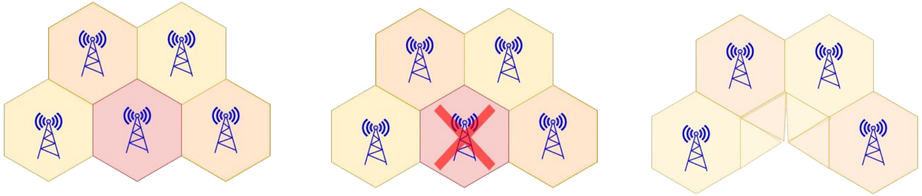
POLITECNICO DI TORINO

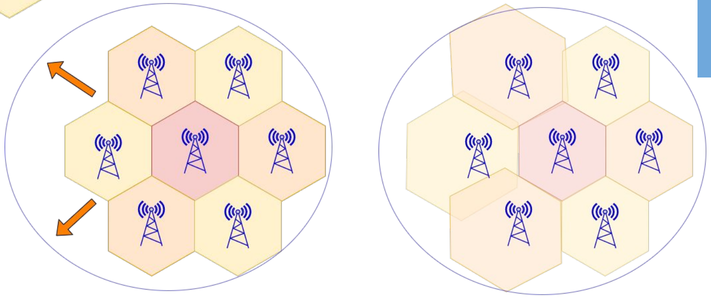
LINKS LEADING INNOVATION & KNOWLEDGE FOR SOCIETY

Collaboration with TIM in Telco Industry

- Optimization of LTE network infrastructures
  - Physical Cell Identifier (PCI) Planning
  - Self-organizing Networks (SON)
    - Configuration
    - Optimization
    - Healing







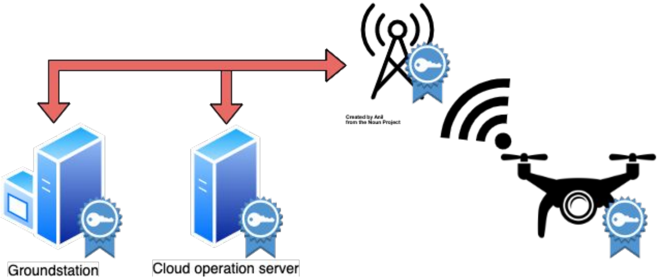
APPLICATIONS

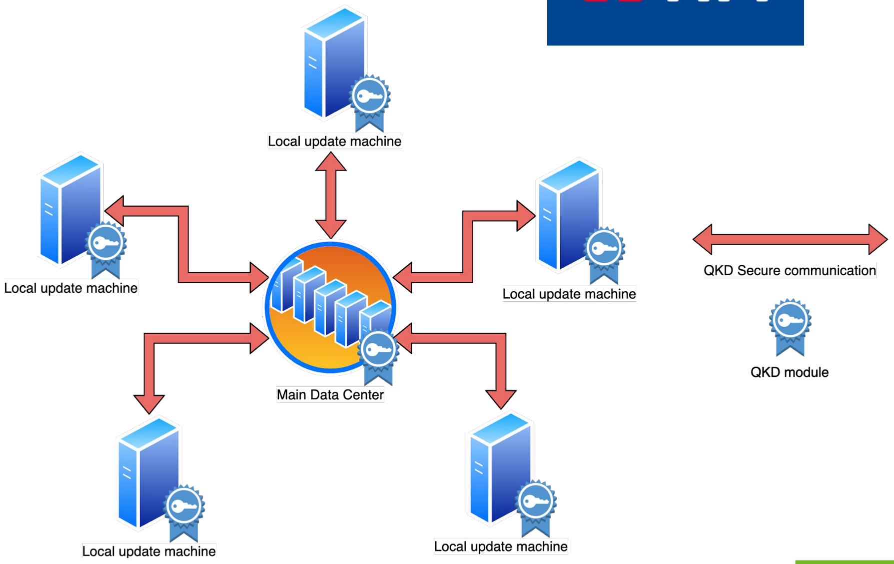
Collaboration with TIM in Telco Industry

- Quantum Key Distribution applications
  - Automotive
  - Drones
  - Computer networks
  - DLT

TIM

APPLICATIONS





POLITECNICO DI TORINO

LINKS
LEADING INNOVATION & KNOWLEDGE FOR SOCIETY

QKD in softwarised networks

- **Quantum key distribution (QKD)**
  - cryptographic method for **random secret keys exchange**
  - based on quantum mechanics effects (e.g. superposition, entanglement)
  - beyond the assumed computational complexity of mathematical problems
  - **quantum-resistant**
  - many protocols have been developed (e.g. **BB84**, E91)
- **QKD applications**
  - key exchange in Network Function Virtualization (NFV) / Software-Defined Network (SDN) scenario
  - using optical networks, optical switches
  - commercial solutions (e.g. ID Quantique ID3100 Clavis)
  - replacing the classic algorithms for key exchange in many protocols:
    - IPsec, IKE (network layer)
    - TLS (transport layer)
    - IEEE 802.1 MACsec (data link layer)
- **QKD standards and helpful frameworks**
  - ETSI GS QKD (https://www.etsi.org/committee/qkd)
  - Qiskit (https://qiskit.org)

APPLICATIONS

Activities on QKD

- **QKD and Virtual Network Security Functions (VNSFs)**
  - are distributed virtual security appliances
  - shall communicate over long distances on distributed infrastructures
  - typically leverage on SDN and VPN protocols
  - orchestration platforms are in place for their management (e.g. OpenStack)
  - QKD support for secure key exchange

- **Analysis of criticalities regarding QKD**
  - BB84 protocol vulnerabilities
    - classical channel required
    - authentication of the parties
  - QKD attacks
    - Time-shift attack (TSA)
    - MITM attack

APPLICATIONS

POLITECNICO DI TORINO

LINKS
LEADING INNOVATION & KNOWLEDGE FOR SOCIETY

Quantum pattern matching for genomic sequencing

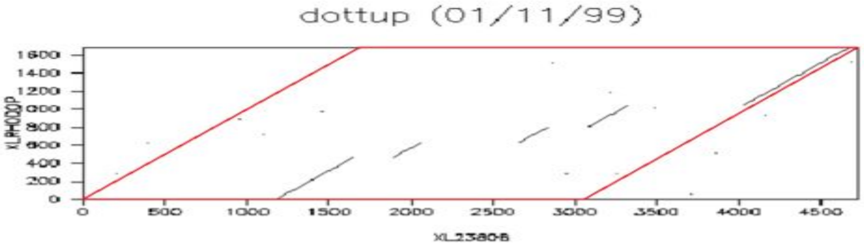
- Modern genomic sequencing requires huge computational resources ⇒ test potential of QC speed-up ($\sqrt{N}$ speed from Grover's algorithm)
- Several QC algorithms have been proposed for this task. Among others 2 top performer (all based on Grover's algorithm):
  - ***Quantum Associative Memory*** (D. Ventura, T. Martinez,Information Sciences 124 (2000) 273-296)
  - ***Quantum pattern recognition*** (Konstantinos Prousalis & Nikos Konofaos, *Scientific Reports*, volume 9, Article number: 7226 (2019)
- Algorithm written with Qiskit, validated against original Quantum Assembly implementation and run on simulator with limited number of qubits (small sequence of reference encoded genome from HIV virus)

APPLICATIONS

POLITECNICO DI TORINO

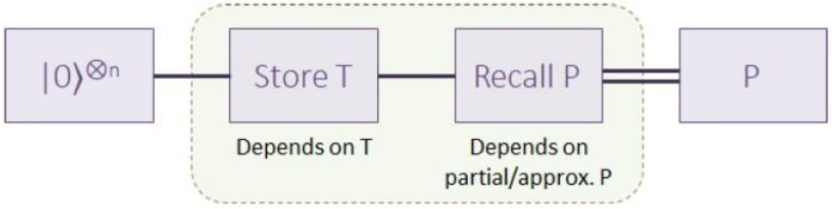
LINKS
LEADING INNOVATION & KNOWLEDGE FOR SOCIETY

Quantum Pattern Recognition



- Recurrence dot matrix between two genomic sequences (having 1 where the corresponding characters matches and 0 otherwise).
- The algorithm initializes the quantum register as a superposition between all the diagonals from the recurrence dot matrix together with their corresponding indices.
- After initialization, we can search for binary search patterns (that we can interpret as “matching bit maps”) inside this quantum database.

Quantum Associative Memory



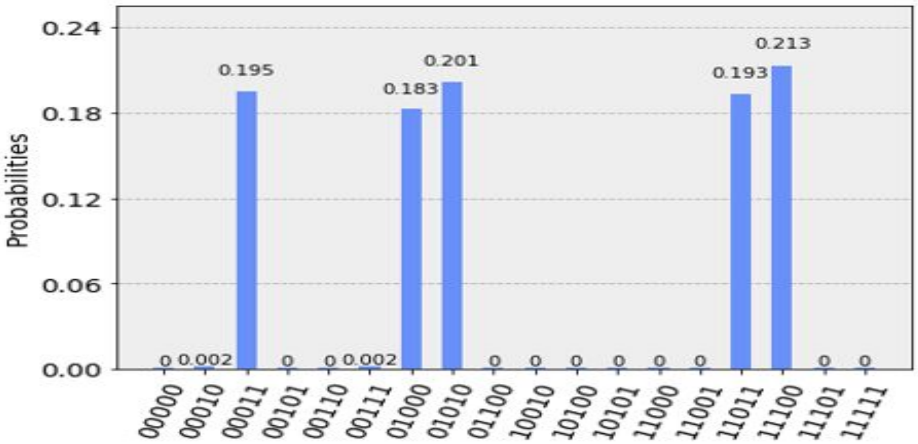
- Its goal is to find and complete a search pattern containing wildcard characters (i.e. *?*) inside a reference genome.
- The quantum register will be initialized as a superposition of all the possible sub-sequences from reference genome of length *m* (where *m* is the size of the chosen search pattern), together with their indices.

POLITECNICO DI TORINO

LINKS
LEADING INNOVATION & KNOWLEDGE FOR SOCIETY

APPLICATIONS

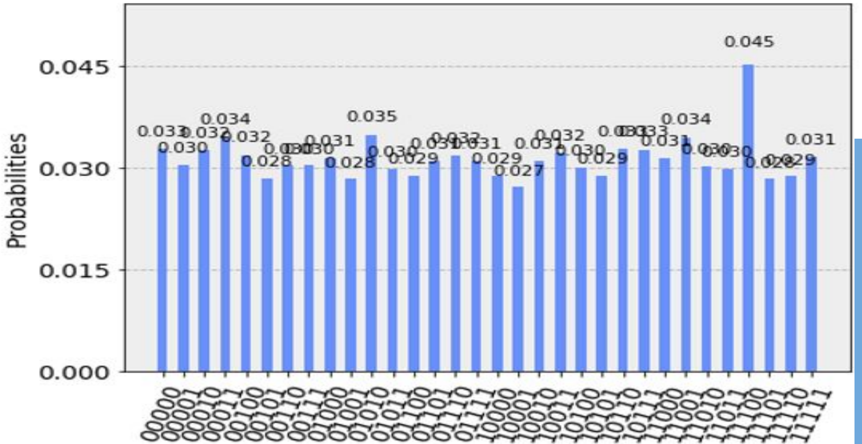
Quantum Pattern Recognition



Reference: TGGAAGGGCTAATTCACTCCCAAAGAAGACAA
Search patterns: *111*, *110*, *011*, *101*.

- Total qubits=18, circuit depth=164673
- Very accurate results but too large circuit depth for practical application on present QC

Quantum Associative Memory



Reference: 32200222130033101311100020020100
Search patterns: *203*

- Total qubits=19, circuit depth=7049
- It works, it is relatively “light” but is not robust against real-world QC with noise

POLITECNICO DI TORINO

LINKS
LEADING INNOVATION & KNOWLEDGE FOR SOCIETY

Education: courses on QC at PoliTO

- *Nano & Quantum Computing* (Graduate course)
  - Held by Prof. Mariagrazia Graziano since 2018-2019 A.Y.
    - Quantum hardware
- *Quantum Computing* (Graduate course)
  - Held by Proff. Bartolomeo Montrucchio and Anna Filomena Carbone since 2018-2019 A.Y.
    - Quantum algorithms
- *Introduction to Quantum Information and Quantum Computation* (undergrad.)
  - Held by Proff. Anna Filomena Carbone and Bartolomeo Montrucchio since 2019-2020 A.Y.
    - Overview of quantum information and computation, hints about hardware

EDUCATION

Laboratory sessions coherent with the contents of each course:

- Qiskit
- D-Wave

Education, Dissemination and Advocating

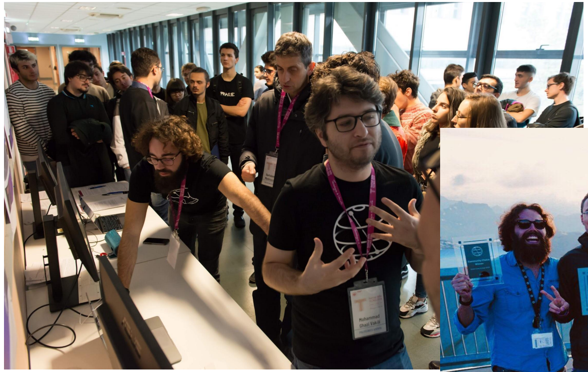
EDUCATION

DET

- 1 Ph.D. Thesis under development, 6 M.Sc. theses on various topics (technology and circuits)

DAUIN + LINKS

- 1 M.Sc. thesis on quantum algorithms



Festival della Tecnologia
PoliTo 2019

Qiskit Camp Europe 2019
Community Choice Award

POLITECNICO DI TORINO

LINKS
LEADING INNOVATION & KNOWLEDGE FOR SOCIETY

Thank you for your attention

Backup

Education: M.Sc. theses

DET (Prof. Mariagrazia Graziano)

- G.A. Cirillo, “A quantum computation model for molecular nanomagnets”, April 2018
- M. Simoni, thesis on molecular QC with expected completion in March 2020
- Four theses on quantum annealing, modeling of technologies different from molecular ones and quantum circuits design, under development

DAUIN (Prof. Bartolomeo Montrucchio) + LINKS

- R. Palmieri: “Implementation and testing of current quantum pattern matching algorithms applied to genomic sequencing”

EDUCATION