Quantum Information

Marco Chiani

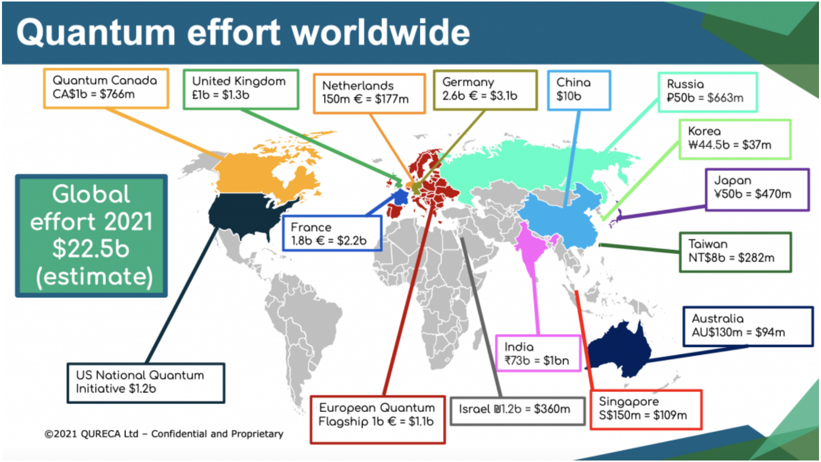
University of Bologna, Italy

Dept. of Electrical, Electronic, and Information Engineering "Guglielmo Marconi"

Aperitivo con AI: there is plenty of WORK at the bottom!
Bologna, February 17, 2021

Summary

- Introduction
- Quantum Mathematical Tools
- Quantum algorithms
- Secure quantum communication


Quantum effort worldwide
Quantum Canada
CA$1b = $766m
United Kingdom
£1b = $1.3b
Netherlands
150m € = $177m
Germany
2.6b € = $3.1b
China
$10b
Russia
₽50b = $663m
Korea
₩44.5b = $37m
Japan
¥50b = $470m
Global effort 2021 $22.5b (estimate)
France
1.8b € = $2.2b
Taiwan
NT$8b = $282m
Australia
AU$130m = $94m
India
₹73b = $1bn
US National Quantum Initiative $1.2b
European Quantum Flagship 1b € = $1.1b
Israel ₪1.2b = $360m
Singapore
S$150m = $109m
©2021 QURECA Ltd – Confidential and Proprietary

- Quantum sensing: use of quantum mechanical phenomena such as entanglement to yield higher statistical precision than purely classical approaches
- Quantum computation: algorithms using quantum mechanical phenomena such as superposition and entanglement
- Quantum communications:
  - to secure communication
  - to move quantum information
  - to improve classical communication

Quantum bits - qubits

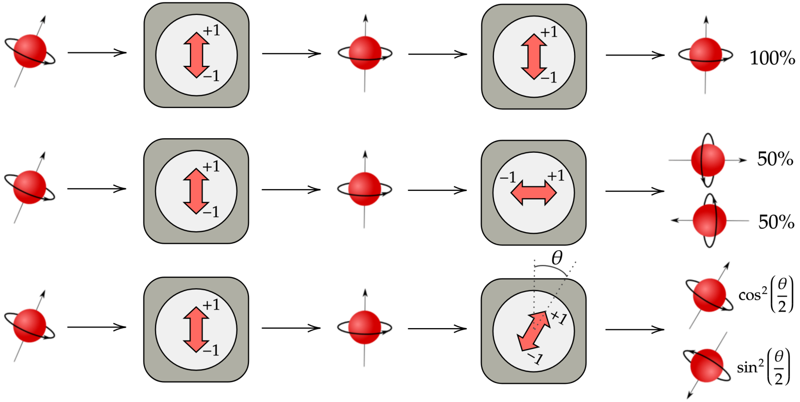
Define "state" of a classical/quantum system

... "state" means whatever information is required about a specific system, in addition to physical laws, in order to predict its behavior in future experiments†

- Classical (macroscopic) example: switch "open" or "closed" $\rightarrow$ state is one classical bit
- Quantum example: spin of an electron. Measured in any direction (Stern-Gerlach), two possible results, "same $(+1)$" or "opposite (-1)", with some probabilities.

To predict its behavior we need a two-dimensional unit norm complex $\mathbb{C}^2$ vector $[\alpha, \beta]^T$ (referred to a specific direction, let's say along z)

† *Fano, Ugo. "Description of states in quantum mechanics by density matrix and operator techniques." Reviews of Modern Physics (1957)*

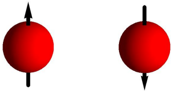


⇒ Measurements are not gentle: after we measure, the state becomes what has been observed (collapses).

⇒ If we know the spin along z, we know nothing about the spin along x.

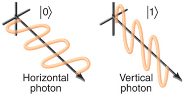
Quantum state: spin of an electron / photon polarization

$$\textit{state } \psi = \begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \alpha \begin{bmatrix} 1 \\ 0 \end{bmatrix} + \beta \begin{bmatrix} 0 \\ 1 \end{bmatrix} \qquad |\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle \qquad (\textit{qubit})$$



"spin up" "spin down"

$$|\psi\rangle = \alpha\,|u\rangle + \beta\,|d\rangle$$



$$|\psi\rangle = \alpha\,|H\rangle + \beta\,|V\rangle$$

The state allows to calculate the probabilities for spin measurements in any possible direction, as well as the behavior in future experiments.

$$\text{P(measuring "up")} = |\alpha|^2$$

$$\alpha, \beta \in \mathbb{C}, \quad |\alpha|^2 + |\beta|^2 = 1$$

$$\text{P(measuring "down")} = |\beta|^2$$

Some examples of qubit physical implementation (incomplete list)

Physical support	**Name**	**Information support**	$\|0\rangle$	$\|1\rangle$
Photon	Polarization encoding	Polarization of light	Horizontal	Vertical
	Number of photons	Fock state	Vacuum	Single photon state
	Time-bin encoding	Time of arrival	Early	Late
Coherent state of light	Squeezed light	Quadrature	Amplitude-squeezed state	Phase-squeezed state
Electrons	Electron Spin	Spin	Up	Down
	Electron number	Charge	No electron	One electron
Nucleus	Nuclear spin addressed through NMR	Spin	Up	Down
Optical lattices	Atomic spin	Spin	Up	Down
Josephson junction	Superconducting charge qubit	Charge	Uncharged superconducting island ($Q = 0$)	Charged superconducting island ($Q = 2e$, one extra Cooper pair)
	Superconducting flux qubit	Current	Clockwise current	Counterclockwise current
	Superconducting phase qubit	Energy	Ground state	First excited state
Singly charged quantum dot pair	Electron localization	Charge	Electron on left dot	Electron on right dot
Quantum dot	Dot spin	Spin	Down	Up
van der Waals heterostructure	Electron localization	Charge	Electron on bottom sheet	Electron on top sheet

from Wikipedia

Quantum computing

Quantum computing: modifying quantum states

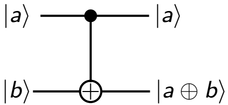
Quantum Mechanics: it is possible to act on physical systems to change states according to linear transformations $\boldsymbol{U}$ s.t. $\boldsymbol{U}^\dagger \boldsymbol{U} = \boldsymbol{I}$ (unitary transformations)

- Single qubit gate example: $\boldsymbol{X} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$

$$|\psi\rangle \;—\boxed{\boldsymbol{X}}—\; \boldsymbol{X}\,|\psi\rangle$$

$$\boldsymbol{X}(\alpha\,|0\rangle + \beta\,|1\rangle) = \alpha\,|1\rangle + \beta\,|0\rangle \qquad \text{“bit flip”}$$

- Two-qubits gate example: controlled-not, CNOT ($a, b \in \{0, 1\}$)



It is possible to realize an arbitrary $\boldsymbol{U}$ by using single-qubit and CNOT elementary gates.

Quantum computing

The state of n qubits is a complex vector with dimension $N = 2^n$.

Example $n = 3$

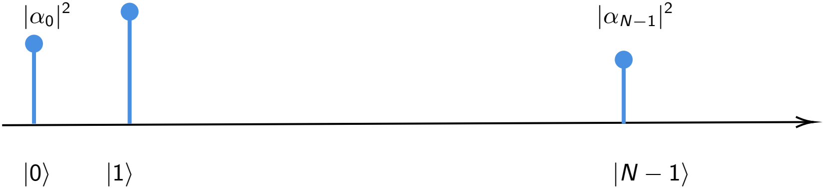
$$\alpha_0 |000\rangle + \alpha_1 |001\rangle + \cdots + \alpha_7 |111\rangle$$

Exponential compression:

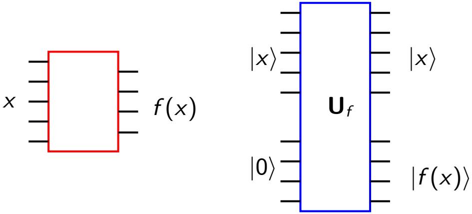
$$40 \text{ qubits} \Rightarrow 2^{40} \simeq 10^{12}$$

However, when we measure we see just one configuration, with prob. $|\alpha_j|^2$.

Example: $|\alpha_7|^2$ is the probability to measure $|111\rangle$



Classical vs. Quantum



Exploiting superposition: input $\sum_x |x\rangle\ |0\rangle \Rightarrow$ output $\sum_x |x\rangle\ |f(x)\rangle$

Main quantum algorithms

- Polynomial-time Algorithms for Prime Factorization and Discrete Logarithms (Shor's algorithm)
- Quantum search, space of N elements. Classical search operations: $O(N)$ Quantum search $O(\sqrt{N})$ (Grover's algorithm)

Polynomial-time Algorithm for Prime Factorization on a Quantum Computer (Shor, 1994)
Ingredients:

- Factorization by order-finding
- Period-finding by Quantum Fourier Transform

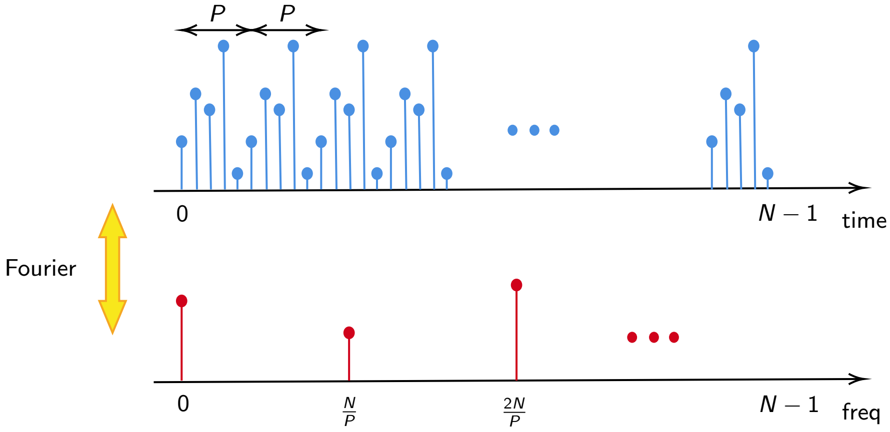
Tools from number theory

- The integer N as a factor in common with $x-1$ if $x^2 \bmod N = 1$ and $x \bmod N \neq \pm 1$
- To find x: generate random y, then find the period of $y^a \bmod N$:

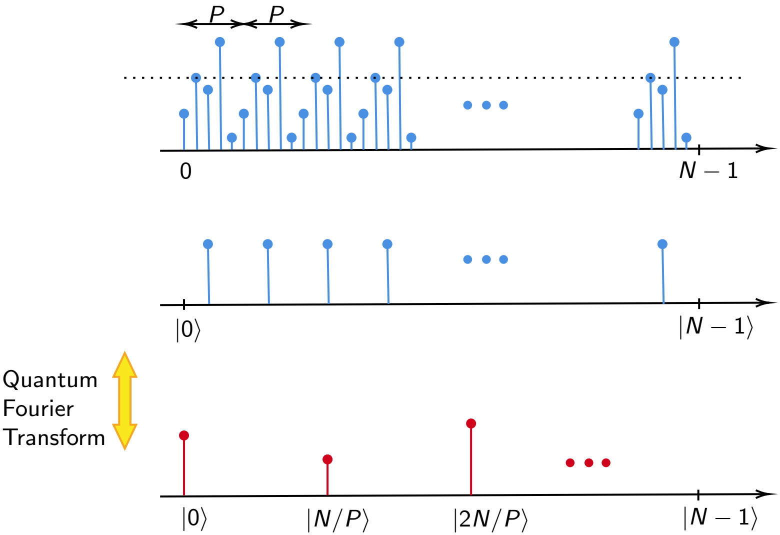
$$y^0 \bmod N, y^1 \bmod N, \ldots$$

$$\text{Factoring} \iff \text{period-finding}$$

(Warning: imprecise statements, just to give the idea)
A function with period P in time has frequency components at frequencies k/P.

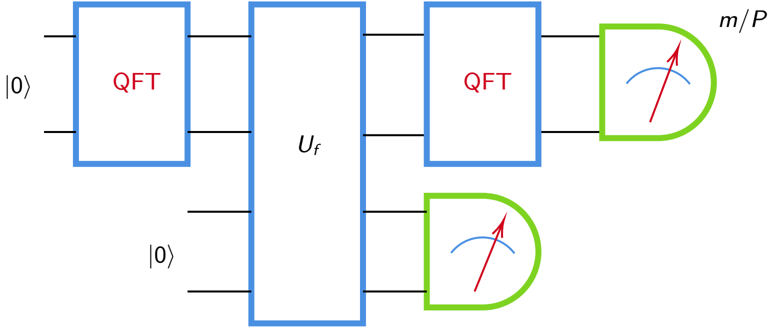


(Warning: imprecise, just to give the idea)



Quantum order-finding, $f(a) = f(a + P)$

(Warning: imprecise, just to give the idea)



Generate the superposition $\sum_x |x\rangle$ by QFT of a Dirac's delta
U_f = unitary, computes $f(a)$ in a register $\Rightarrow$ output $\sum_x |x\rangle\,|f(x)\rangle$
Measure the second register. For example it turns out $f(x) = 12$
Left in the first reg: superposition of all $|x\rangle$ with x giving $f(x) = 12 \Rightarrow$ periodic
Then, Quantum Fourier Transform: the measured frequency is some random multiple of $1/P$
By repeating a couple of times, P can be derived with high probability

Quantum machine learning

The state of n qubits is a complex vector with dimension $N = 2^n$

$$\boldsymbol{x} \in \mathbb{C}^N \iff |x\rangle \text{ of } \log_2 N \text{ qubits}$$

	Classical	Quantum
FFT	$O(N \log N)$	$O((\log N)^2)$
Eigenvect, eigenval of sparse matrices	$O(N^2)$	$O((\log N)^2)$
Matrix inversion	$O(N^3)$	$O((\log N)^3)$

Table: Number of operations for basic linear algebra subroutines

Quantum and AI

- ...
- Quantum deep learning
- Quantum convolutional neural networks
- Quantum principal component analysis
- TensorFlow Quantum
- Quantum neural networks
- ...

Some existing quantum computers

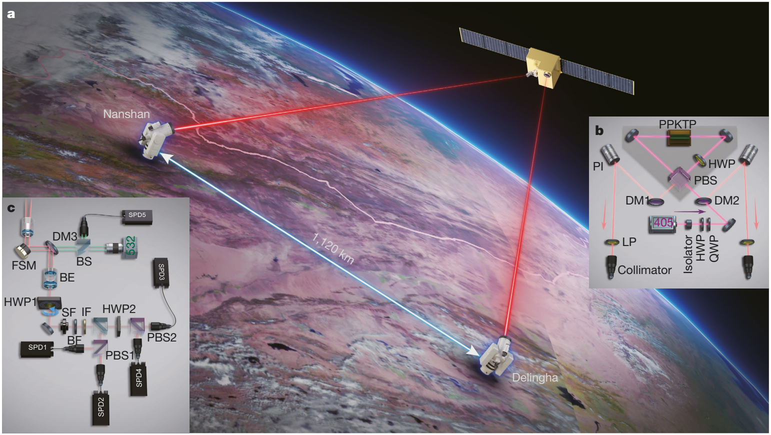
Company	Cloud Access	Technology	Quantum Computer	qubits	SDK/Lang.
IBM	Yes	Superconducting	IBM Q Montreal	27	QisKit/Python
			IBM Q Manhattan	65	QisKit/Python
			IBM Q Santiago	5	QisKit/Python
Rigetti	Through AWS	Superconducting	Aspen-8	32	Amazon Braket/Python
D-Wave	Through AWS	Superconducting, Quant. Annealer*	D-Wave 2000Q	2048*	Amazon Braket/Python
IonQ	Through AWS	Trapped Ion	-	79	Amazon Braket/Python
Google	No	Superconducting	Bristlecone	72	Cirq/Python
			Sycamore	53	Cirq/Python
Honeywell	On-demand	Trapped Ion	System Model HØ	6	-
Xanadu	Yes	Photonic Quantum Computing	-	12	Strawberry Fields/Python
OriginQ	Yes	Superconducting	Wu Yuan	6	QPanda/C++

TABLE 4.1 Literature-Reported Estimates of Quantum Resilience for Current Cryptosystems, under Various Assumptions of Error Rates and Error-Correcting Codes

Cryptosystem	Category	Key Size	Security Parameter	Quantum Algorithm Expected to Defeat Cryptosystem	# Logical Qubits Required	# Physical Qubits Required[a]	Time Required to Break System[b]	Quantum-Resilient Replacement Strategies
AES-GCM[c]	Symmetric encryption	128 192 256	128 192 256	Grover's algorithm	2,953 4,449 6,681	4.61×10^6 1.68×10^7 3.36×10^7	2.61×10^{12} years 1.97×10^{22} years 2.29×10^{32} years	
RSA[d]	Asymmetric encryption	1024 2048 4096	80 112 128	Shor's algorithm	2,050 4,098 8,194	8.05×10^6 8.56×10^6 1.12×10^7	3.58 hours 28.63 hours 229 hours	Move to NIST-selected PQC algorithm when available
ECC Discrete-log problem[e-g]	Asymmetric encryption	256 384 521	128 192 256	Shor's algorithm	2,330 3,484 4,719	8.56×10^6 9.05×10^6 1.13×10^6	10.5 hours 37.67 hours 55 hours	Move to NIST-selected PQC algorithm when available
SHA256[h]	Bitcoin mining	N/A	72	Grover's Algorithm	2,403	2.23×10^6	1.8×10^4 years	
PBKDF2 with 10,000 iterations[i]	Password hashing	N/A	66	Grover's algorithm	2,403	2.23×10^6	2.3×10^7 years	Move away from password-based authentication

Quantum Computing: Progress and Prospects. Washington, DC, USA: Nat. Acad. Press, 2019.

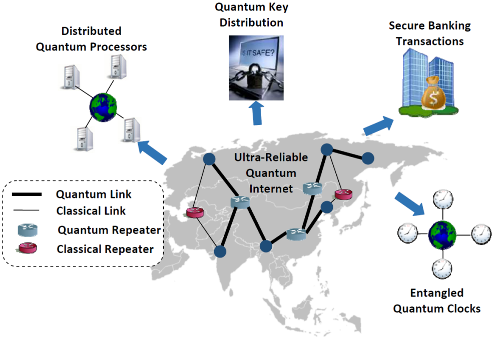
Entanglement-based QKD between two ground stations separated by 1,120 km



Yin, Juan, et al. "Entanglement-based secure quantum cryptography over 1,120 kilometres." Nature (2020).

- To move and process quantum information
- Most important function: generate long distance quantum entanglement
- Applications:

generation of multiparty shared secrets | blind quantum computing
secure private-bid auctions | distributed quantum computing
improved sensing | quantum-enhanced measurement networks



H. J. Kimble, "The quantum internet," Nature, 2008.

Wehner, Elkouss, Hanson, "Quantum internet: A vision for the road ahead," Science, 2018.

Babar, et al. "Duality of Quantum and Classical Error Correction Codes: Design Princip. and Examp", IEEE Comm. Surv. Tutor. 2019.

Mihir, et al. "Routing entanglement in the quantum internet." npj Quantum Information 2019.