# An introduction to Quantum Computing and Quantum Random Number Generators

**Giuseppe Vallone**

*email*: vallone@dei.unipd.it


UNIVERSITÀ
DEGLI STUDI
DI PADOVA

DIPARTIMENTO
DI INGEGNERIA
DELL'INFORMAZIONE

INFN and The Future of Scientific Computing - 4 May 2018

# Summary

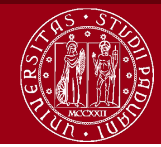

1 Introduction

2 Quantum Computing
- Circuit model
- Alternatives to circuit model
- Implementations

3 Quantum Random Number Generators

4 Conclusions

# Summary



1 Introduction

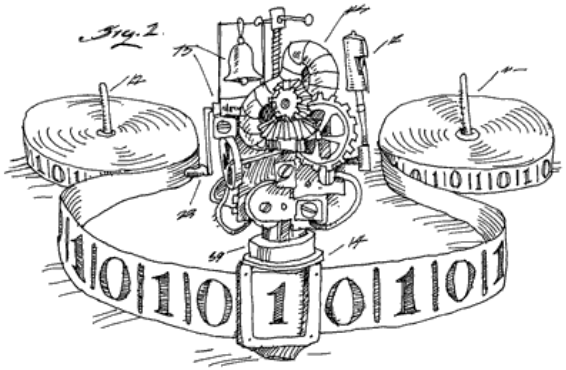
2 Quantum Computing
- Circuit model
- Alternatives to circuit model
- Implementations

3 Quantum Random Number Generators

4 Conclusions

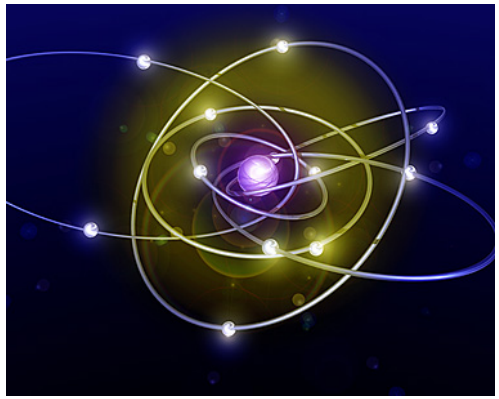
# What is Quantum Information?

Information Theory



$\Leftrightarrow$

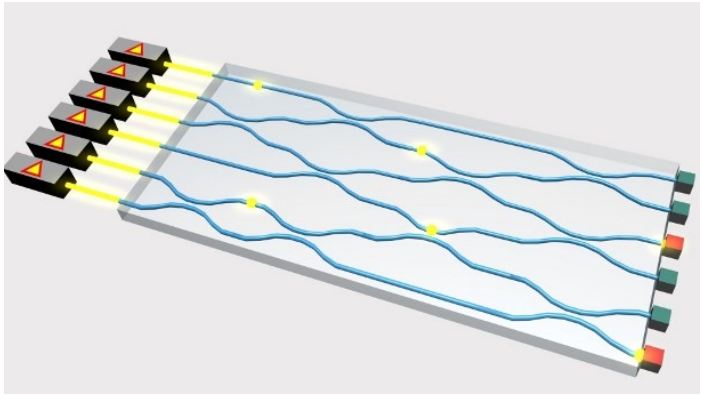
Quantum Mechanics



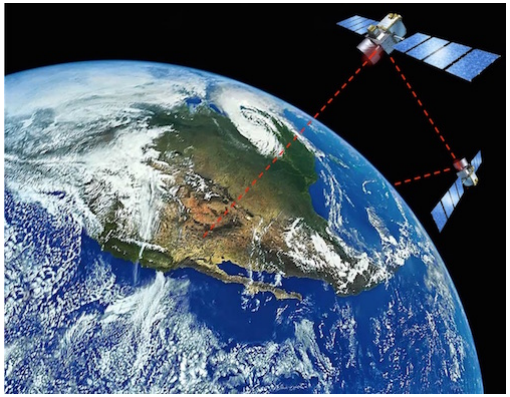
Merging two big XXth century revolutions:
information theory (Shannon, Turing) and Quantum Mechanics.

# Examples of applications

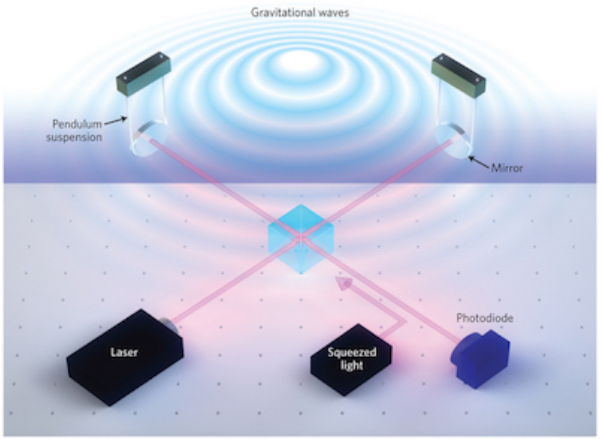
## Quantum computer

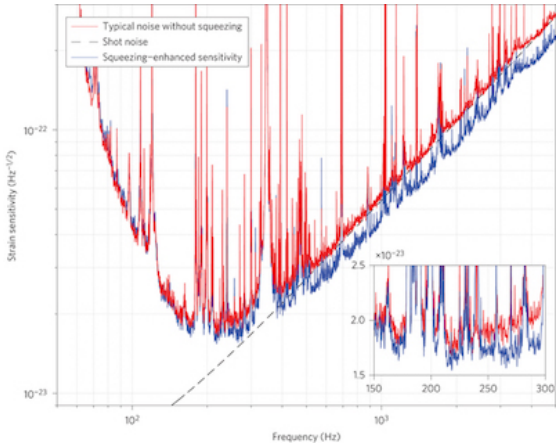


## Quantum cryptography



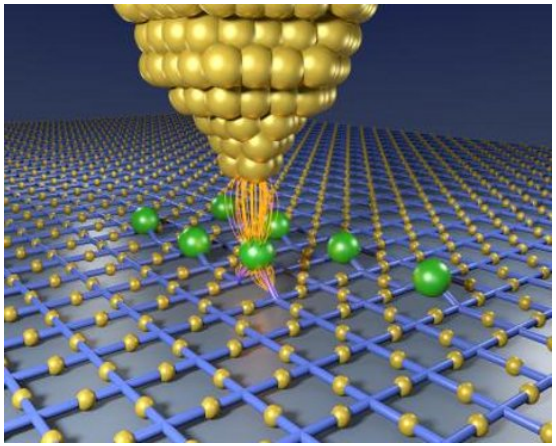
## Quantum metrology



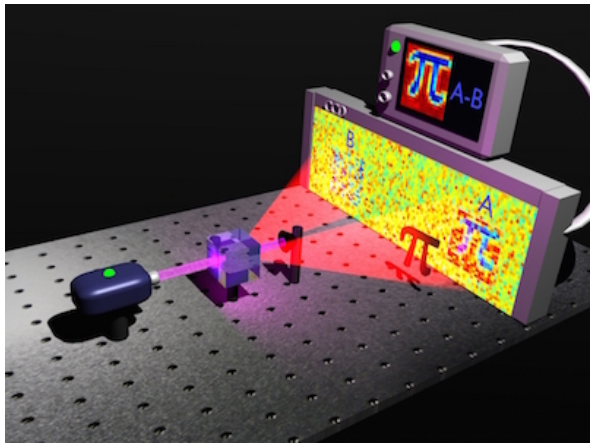



# Examples of applications

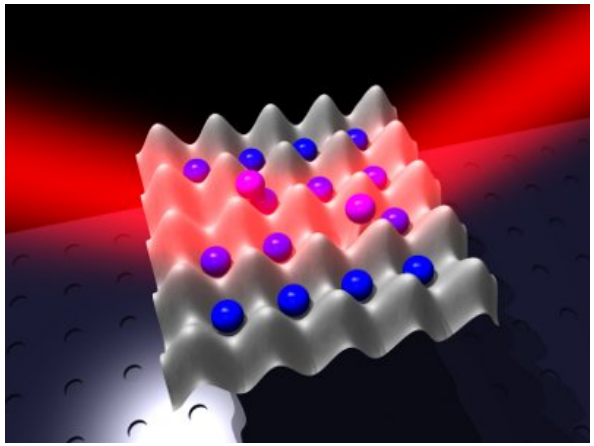
## Quantum sensing



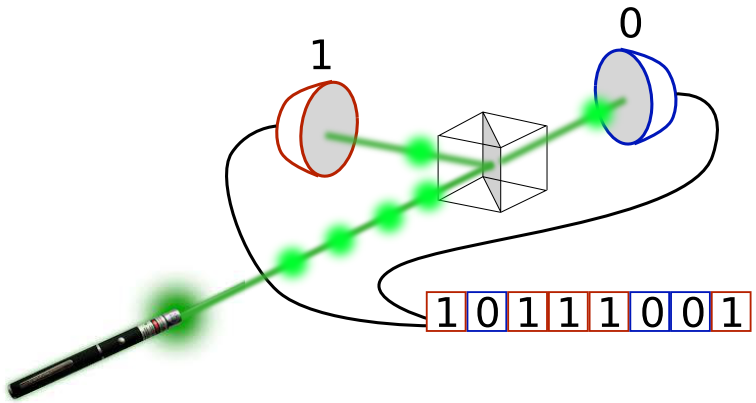
## Quantum imaging




## Quantum simulation



## Quantum random number generation



# But...

...be aware of fake!

# Summary

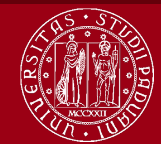
1 Introduction

2 Quantum Computing
- Circuit model
- Alternatives to circuit model
- Implementations

3 Quantum Random Number Generators

4 Conclusions

# Summary



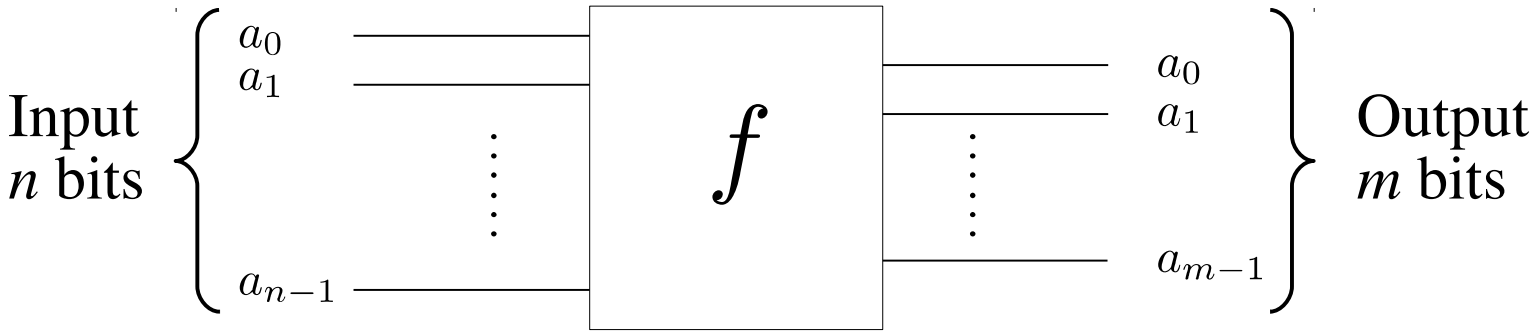
1 Introduction

2 Quantum Computing
- Circuit model
- Alternatives to circuit model
- Implementations

3 Quantum Random Number Generators

4 Conclusions

# One-slide review of classical computation




**Universal gates**: any function

$$f : \{0,1\}^n \to \{0,1\}^m$$

can be built from two elementary gates: NAND and COPY.

# Quantum computer: superposition principle

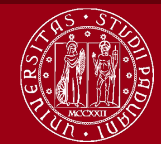
- Quantum mechanics: physical states are represented as vectors $|\psi\rangle$

# Quantum computer: superposition principle

- Quantum mechanics: physical states are represented as vectors $|\psi\rangle$
- Superposition principle: if $|\psi_1\rangle$ and $|\psi_2\rangle$ are physical states, any linear combination is a physical state:

$$|\Psi\rangle = a|\psi_1\rangle + b|\psi_2\rangle \qquad a, b \in \mathbb{C}$$

# Quantum computer: superposition principle



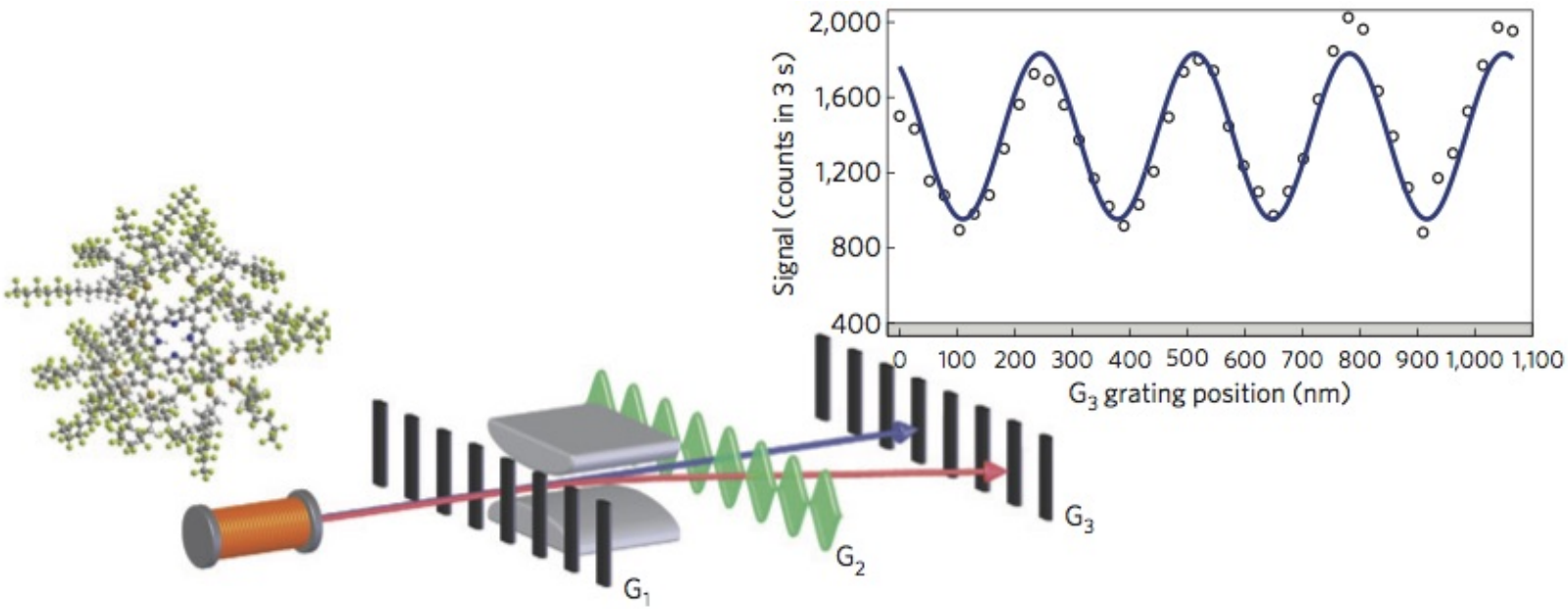
- Quantum mechanics: physical states are represented as vectors $|\psi\rangle$
- Superposition principle: if $|\psi_1\rangle$ and $|\psi_2\rangle$ are physical states, any linear combination is a physical state:

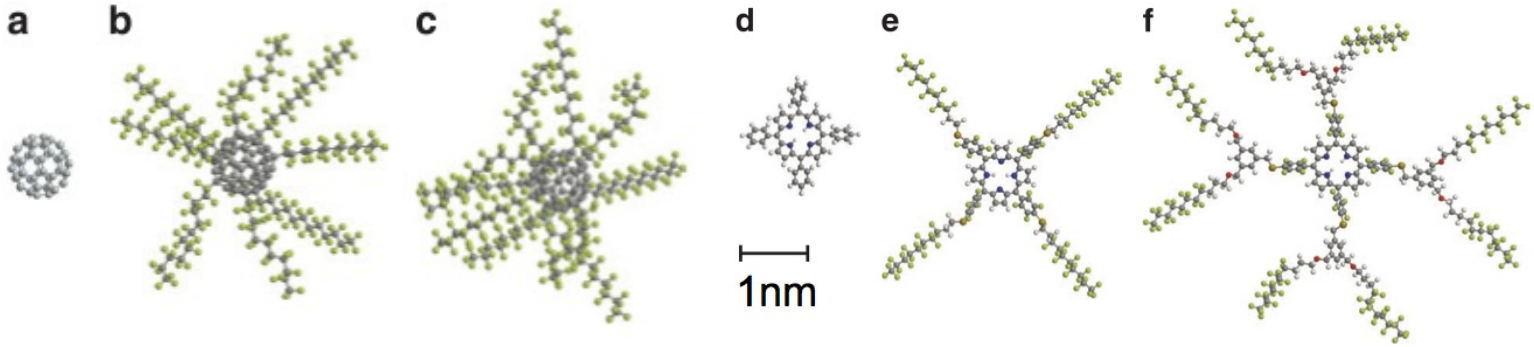
$$|\Psi\rangle = a|\psi_1\rangle + b|\psi_2\rangle \qquad a, b \in \mathbb{C}$$

- From classical bit (two orthogonal states $|0\rangle$ and $|1\rangle$) to quantum-bit , or qubit:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \qquad \alpha, \beta \in \mathbb{C}\,, |\alpha|^2 + |\beta|^2 = 1$$

# State superposition

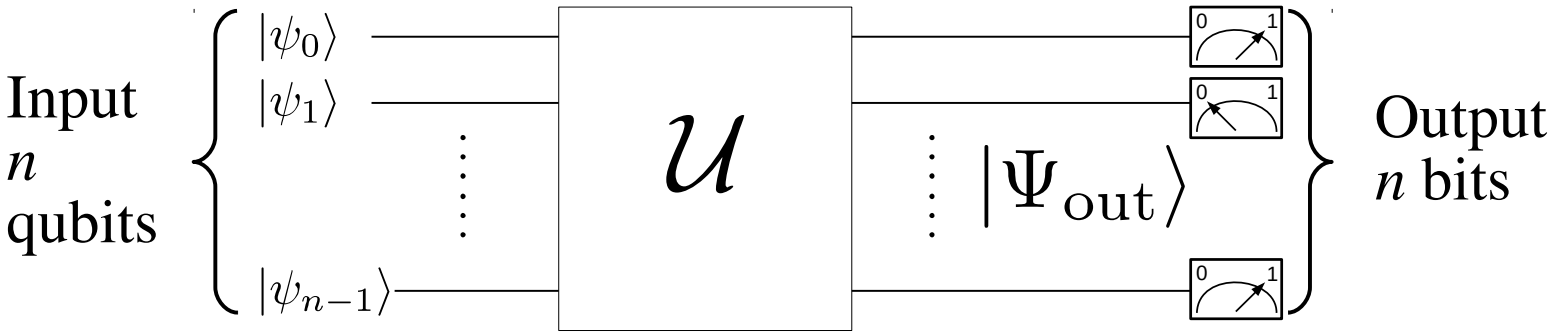



above 10000 AMU, 810 atoms

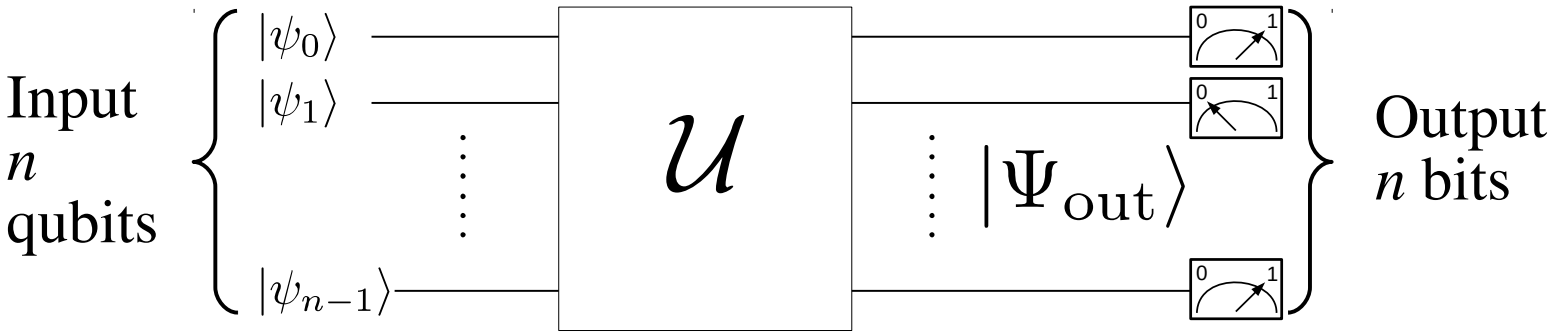
*Matter–wave interference of particles selected from a molecular library with masses exceeding 10000 amu*, **Phys. Chem. Chem. Phys. 15, 14696 (2013)**

# Circuit model of quantum computation



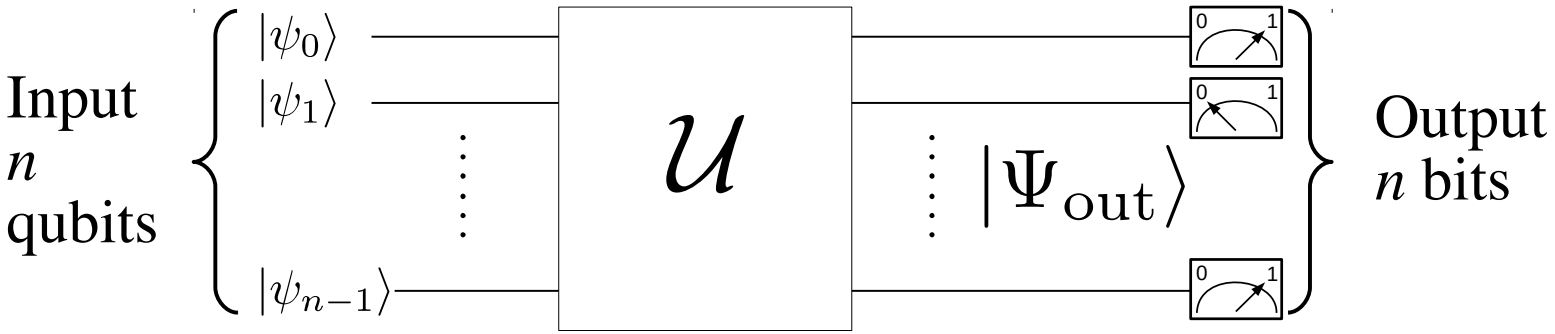

- Prepare the system into $|\Psi_{\text{in}}\rangle = |\psi_0\rangle \otimes |\psi_0\rangle \otimes \cdots \otimes |\psi_{n-1}\rangle$

# Circuit model of quantum computation




- Prepare the system into $|\Psi_{\text{in}}\rangle = |\psi_0\rangle \otimes |\psi_0\rangle \otimes \cdots \otimes |\psi_{n-1}\rangle$
- Manipulate the state into $|\Psi_{\text{out}}\rangle = \mathcal{U}|\Psi_{\text{in}}\rangle$. $\mathcal{U}$ is the algorithm

# Circuit model of quantum computation

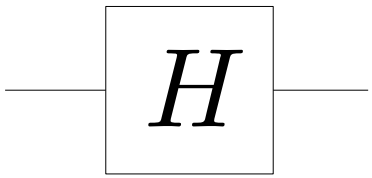



- Prepare the system into $|\Psi_{\text{in}}\rangle = |\psi_0\rangle \otimes |\psi_0\rangle \otimes \cdots \otimes |\psi_{n-1}\rangle$
- Manipulate the state into $|\Psi_{\text{out}}\rangle = \mathcal{U}|\Psi_{\text{in}}\rangle$. $\mathcal{U}$ is the algorithm
- Measure each qubit (usually in the computational basis)

# Universal gates

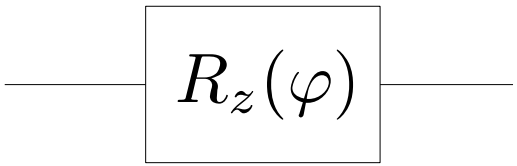
Any quantum algorithm $\mathcal{U}$ can be built by the following universal gates:

## Hadamard



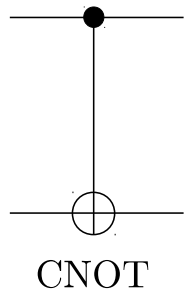

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

## Single qubit rotation




$$R_z(\varphi) = e^{i\frac{\varphi}{2}\sigma_z} = \begin{pmatrix} e^{i\frac{\varphi}{2}} & 0 \\ 0 & e^{-i\frac{\varphi}{2}} \end{pmatrix}$$

## CNOT gate




$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

# Shor algorithm

**Problem 1: factoring**

Given an integer number $N$, find its prime factors.
The best classical algorithm requires $O(e^{n^{1/3}(log_2 n)^{2/3}})$ with $n = log_2 N$

**Problem 2: order finding**

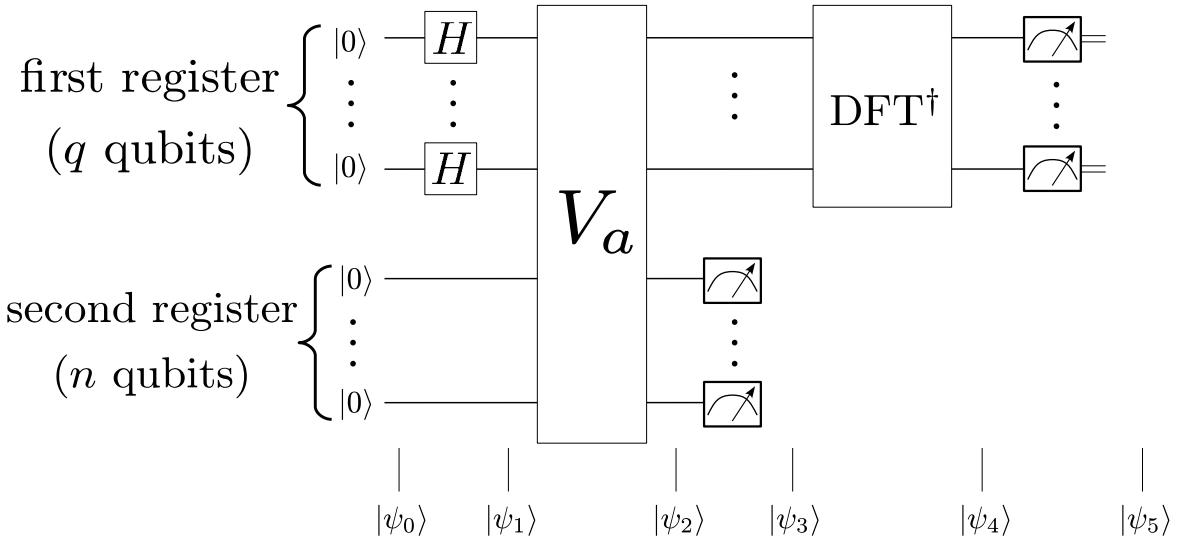
Choose a generic $a$ such that $1 < a < N$. The order $r$ of $a$ modulo $N$ is the minimum positive integer $r$ such that $a^r = 1 \mod N$. Hard (probably superpolinomial) problem.

**Equivalence**

By using $O(n^3)$ classical operations **Problem 1** can be reformulated as **Problem 2**

# Shor algorithm

## Order-finding by quantum computer



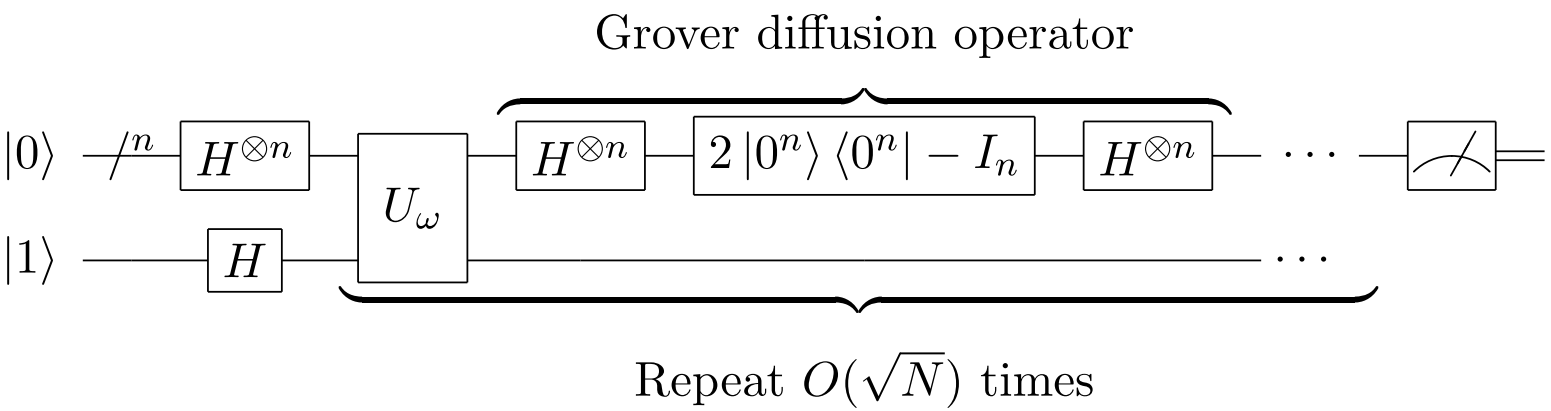

$$V_a : |x\rangle|y\rangle \rightarrow |x\rangle|y \oplus a^x \mod N\rangle$$

- The $V_a$ operation requires $O(n^3)$ gates
- DFT requires $O(n^2)$ gates

# Grover algorithm

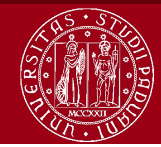
**problem:** find $x_0$ given a quantum black box $U_\omega$ such that

$$U_\omega|x\rangle = \begin{cases} -|x\rangle & \text{for } x = x_0 \\ |x\rangle & \text{for } x \neq x_0 \end{cases}$$




$x_0$ is found with high probability using $O(\sqrt{N})$ evaluations
A classical computer cannot solve the problem with less than $O(N)$ operations

# Summary



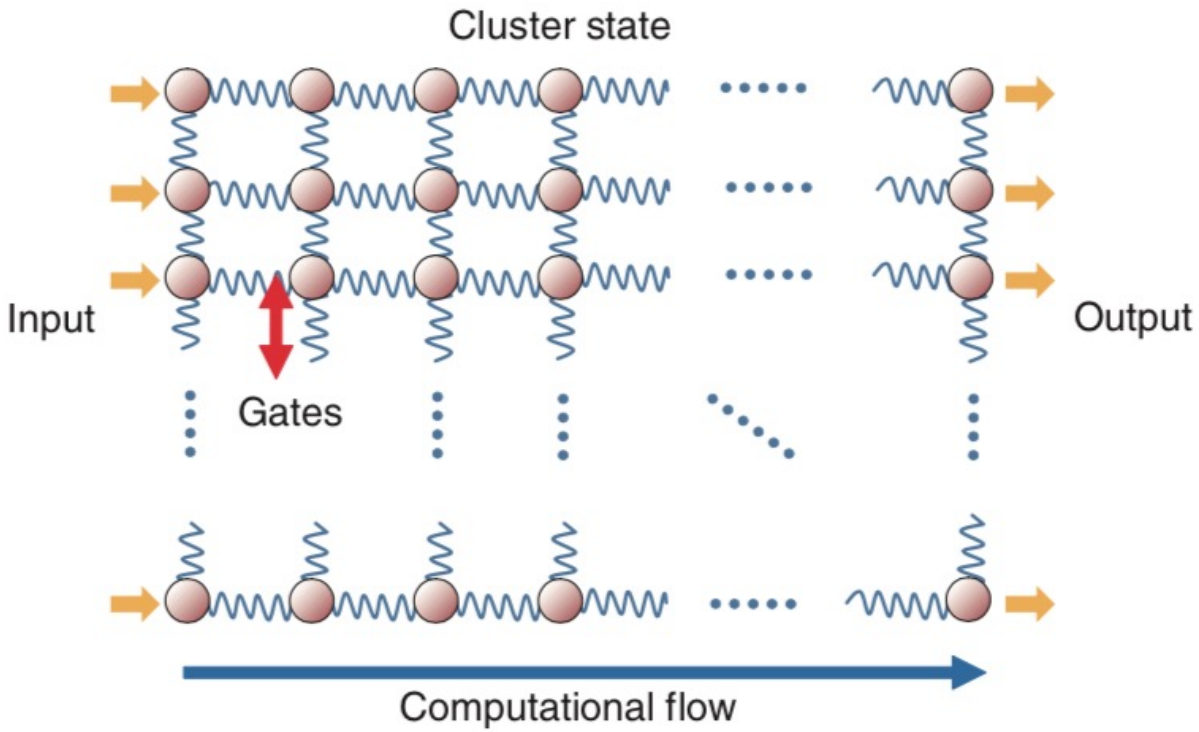
1 Introduction

2 Quantum Computing
- Circuit model
- Alternatives to circuit model
- Implementations

3 Quantum Random Number Generators

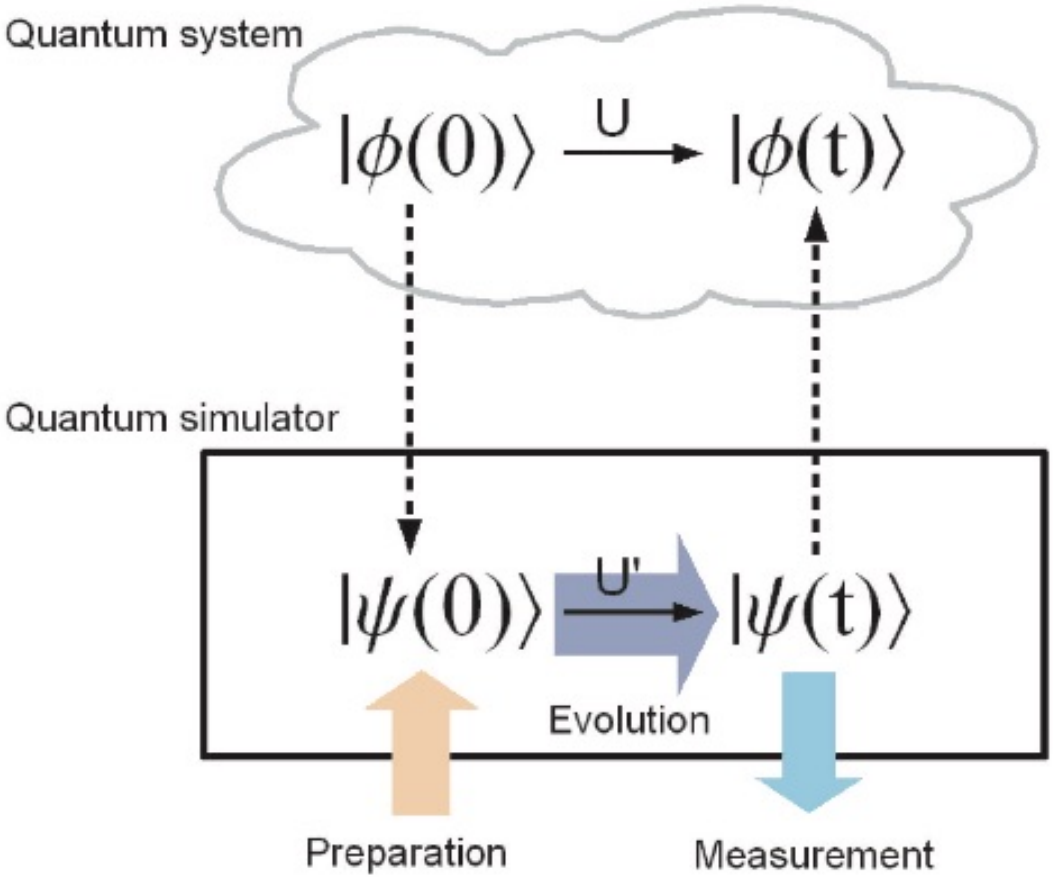
4 Conclusions

# One-way quantum computer



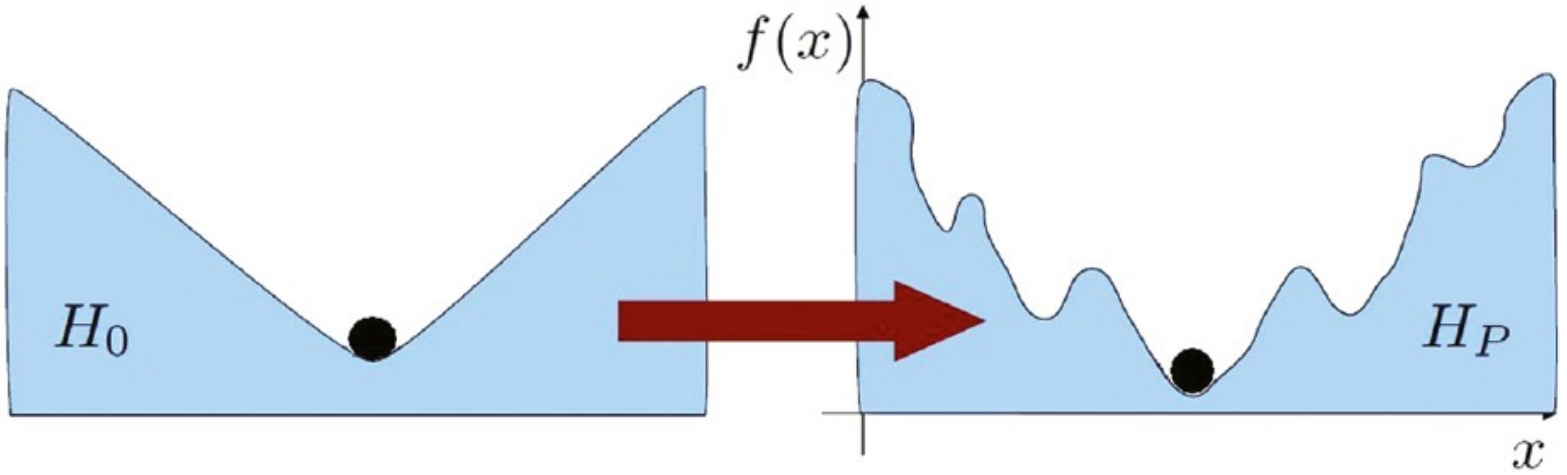

G. Vallone, *et al.*, *One-way quantum computation with two-photon multiqubit cluster states*, **Phys. Rev. A 78, 042335 (2008)**

# Quantum simulation




*Quantum Simulation*, **Rev. Mod. Phys. 86, 154 (2014)**

# Adiabatic Quantum Computing

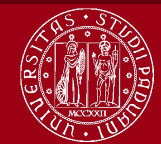



$$H(t) = (1-t)H_0 + tH_P$$

$$T = O(\frac{1}{g_{min}^2})$$

*Adiabatic Quantum Computing*, **Rev. Mod. Phys. 90, 015002 (2018)**

# Summary



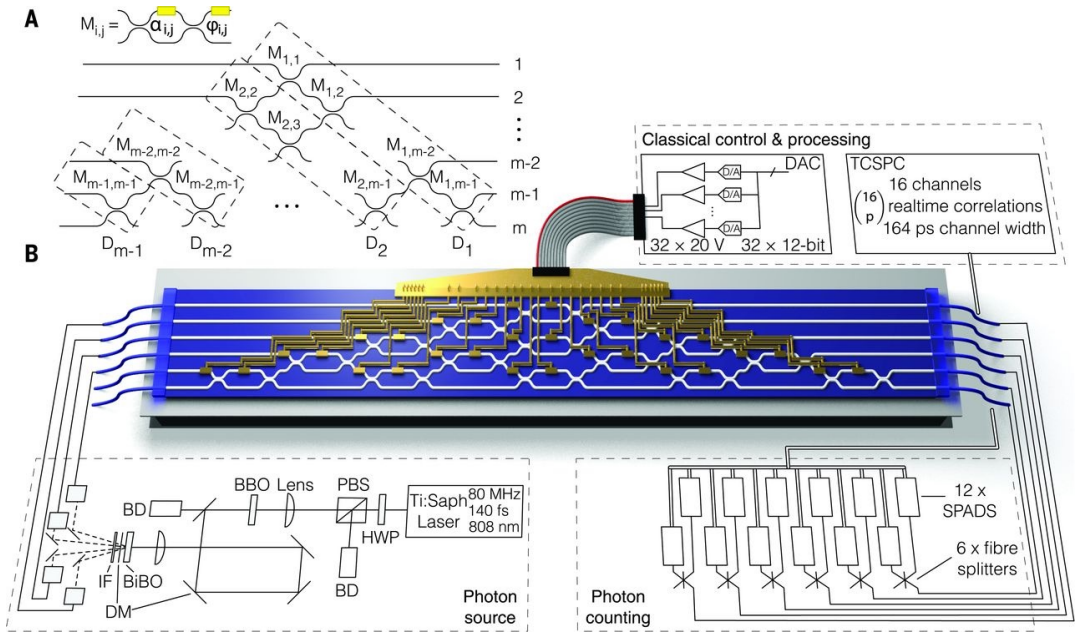
1 Introduction

2 Quantum Computing
- Circuit model
- Alternatives to circuit model
- Implementations

3 Quantum Random Number Generators

4 Conclusions

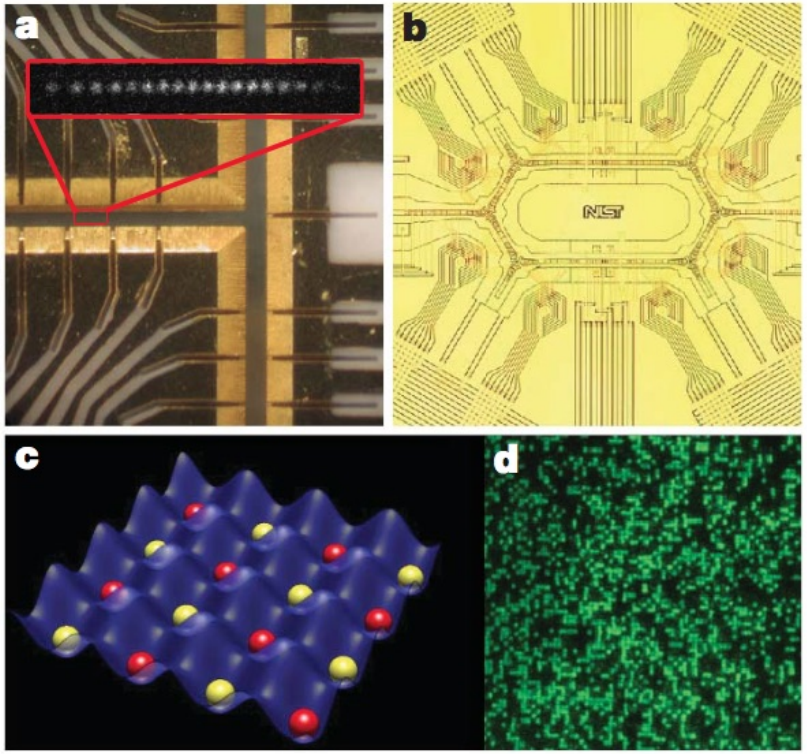
# Photons




Reprogrammable optical circuit that implements all possible linear optical protocols up to the size of the circuit (six photon input)

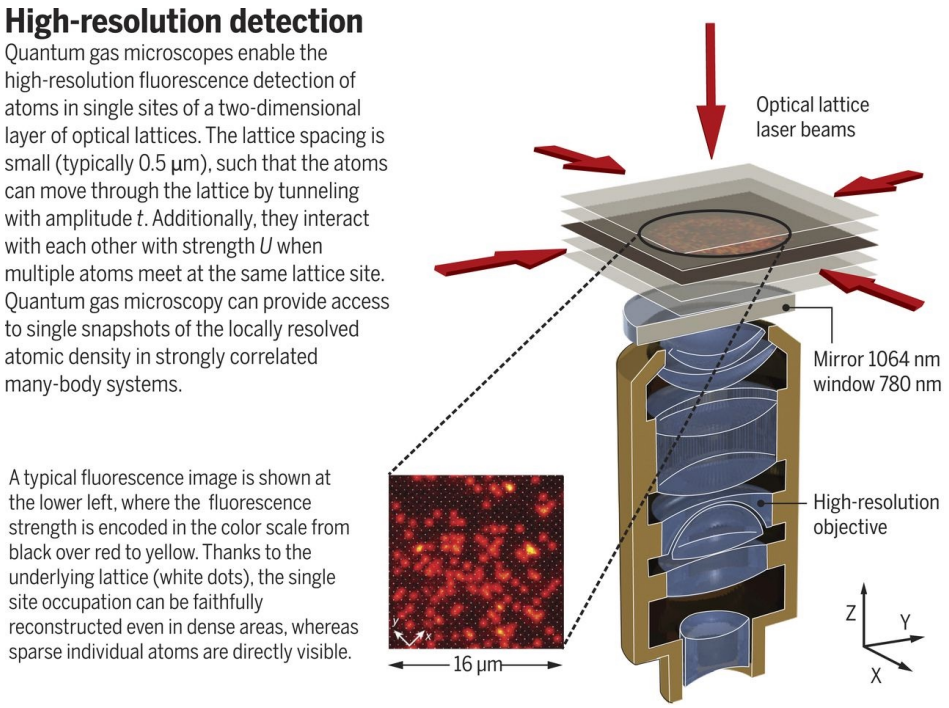
*Universal linear optics*, **Science 349, 711 (2017)**

# Trapped ion




*Quantum computers*,**Nature 464, 45 (2010)**

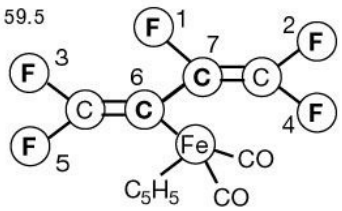
# Ultracol atoms in lattice

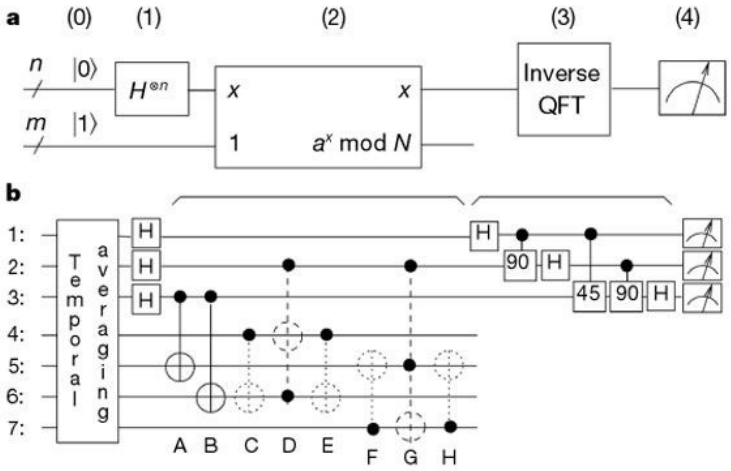



*Quantum simulations with ultracold atoms in optical lattices*, **Science 357, 995 (2017)**

# Nuclear Magnetic Resonance (NMR)

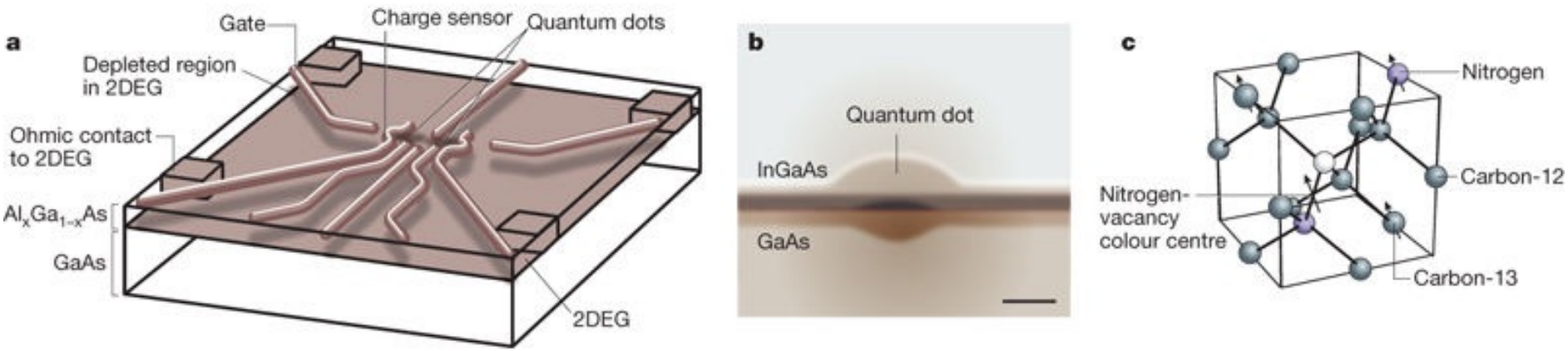
| $i$ | $\omega_i/2\pi$ | $T_{1,i}$ | $T_{2,i}$ | $J_{7i}$ | $J_{6i}$ | $J_{5i}$ | $J_{4i}$ | $J_{3i}$ | $J_{2i}$ |
|---|---|---|---|---|---|---|---|---|---|
| 1 | −22052.0 | 5.0 | 1.3 | −221.0 | 37.7 | 6.6 | −114.3 | 14.5 | 25.16 |
| 2 | 489.5 | 13.7 | 1.8 | 18.6 | −3.9 | 2.5 | 79.9 | 3.9 | |
| 3 | 25088.3 | 3.0 | 2.5 | 1.0 | −13.5 | 41.6 | 12.9 | | |
| 4 | −4918.7 | 10.0 | 1.7 | 54.1 | −5.7 | 2.1 | | | |
| 5 | 15186.6 | 2.8 | 1.8 | 19.4 | 59.5 | | | | |
| 6 | −4519.1 | 45.4 | 2.0 | 68.9 | | | | | |
| 7 | 4244.3 | 31.6 | 2.0 | | | | | | |



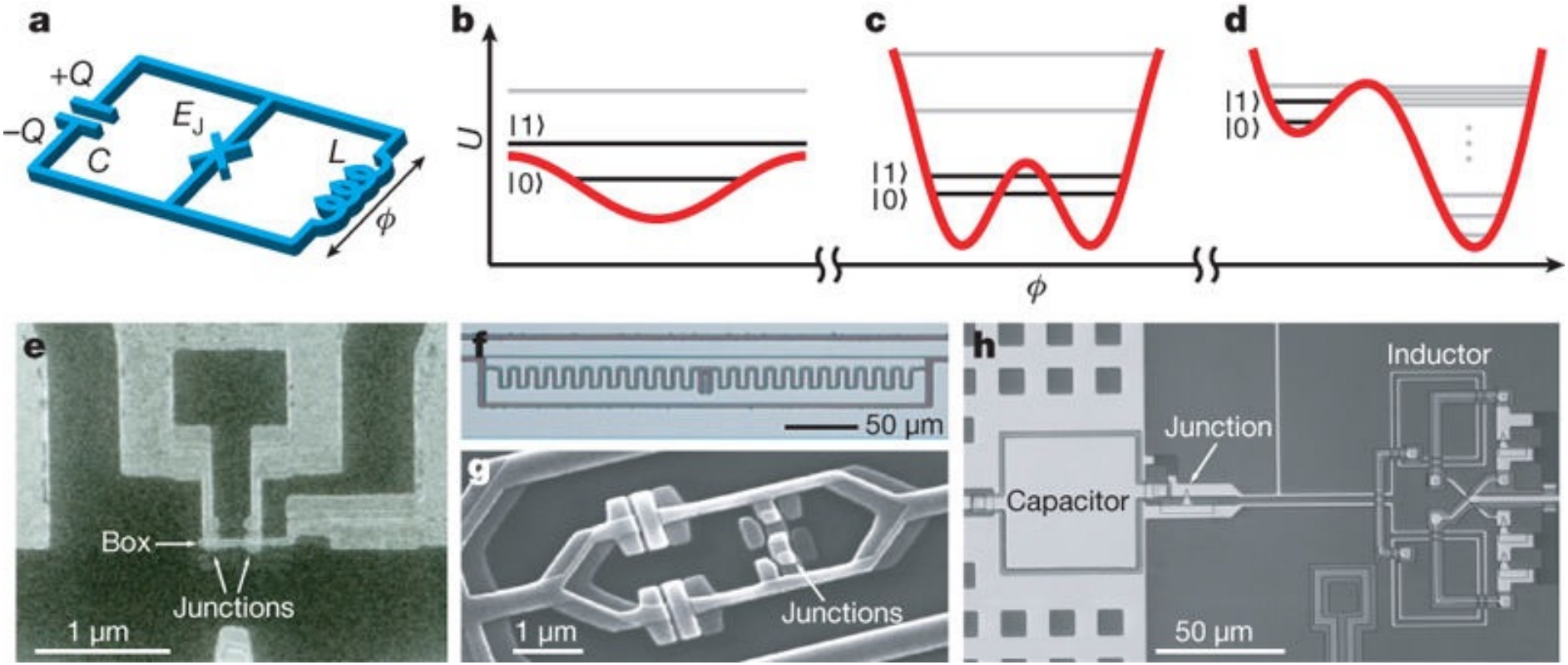

*NMR techniques for quantum control and computation*,
**Rev. Mod. Phys. 76, 1037 (2005)**

# Quantum dots



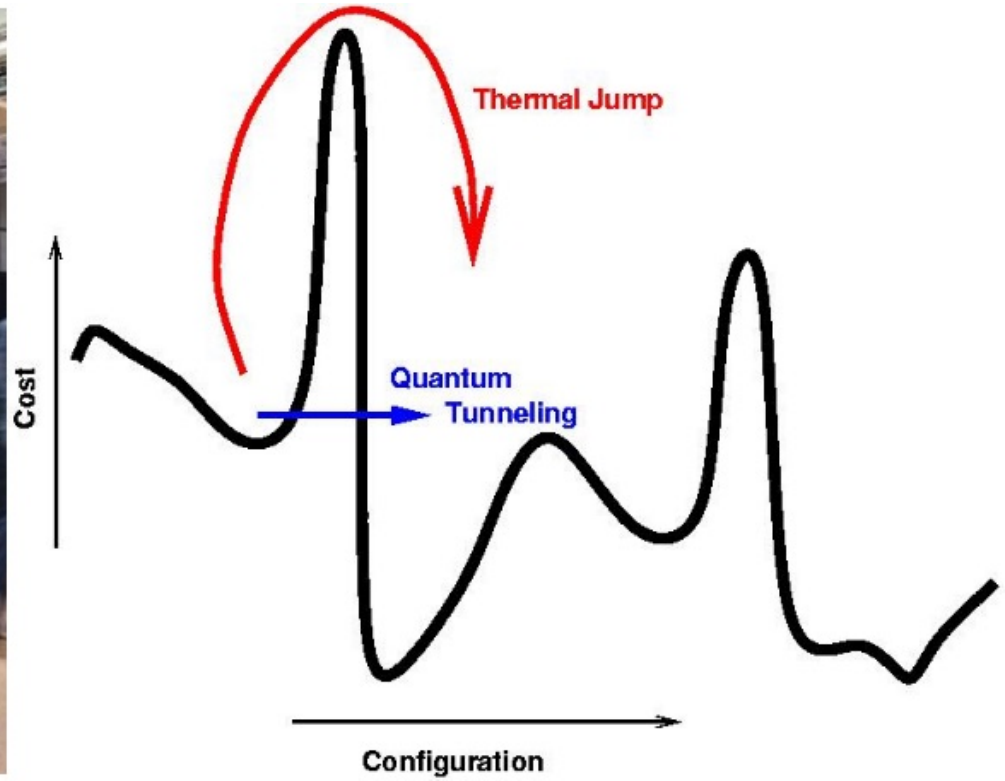

*Quantum computers*, **Nature 464, 45 (2010)**

# Superconducting qubits




*Quantum computers*, **Nature 464, 45 (2010)**

# D-wave

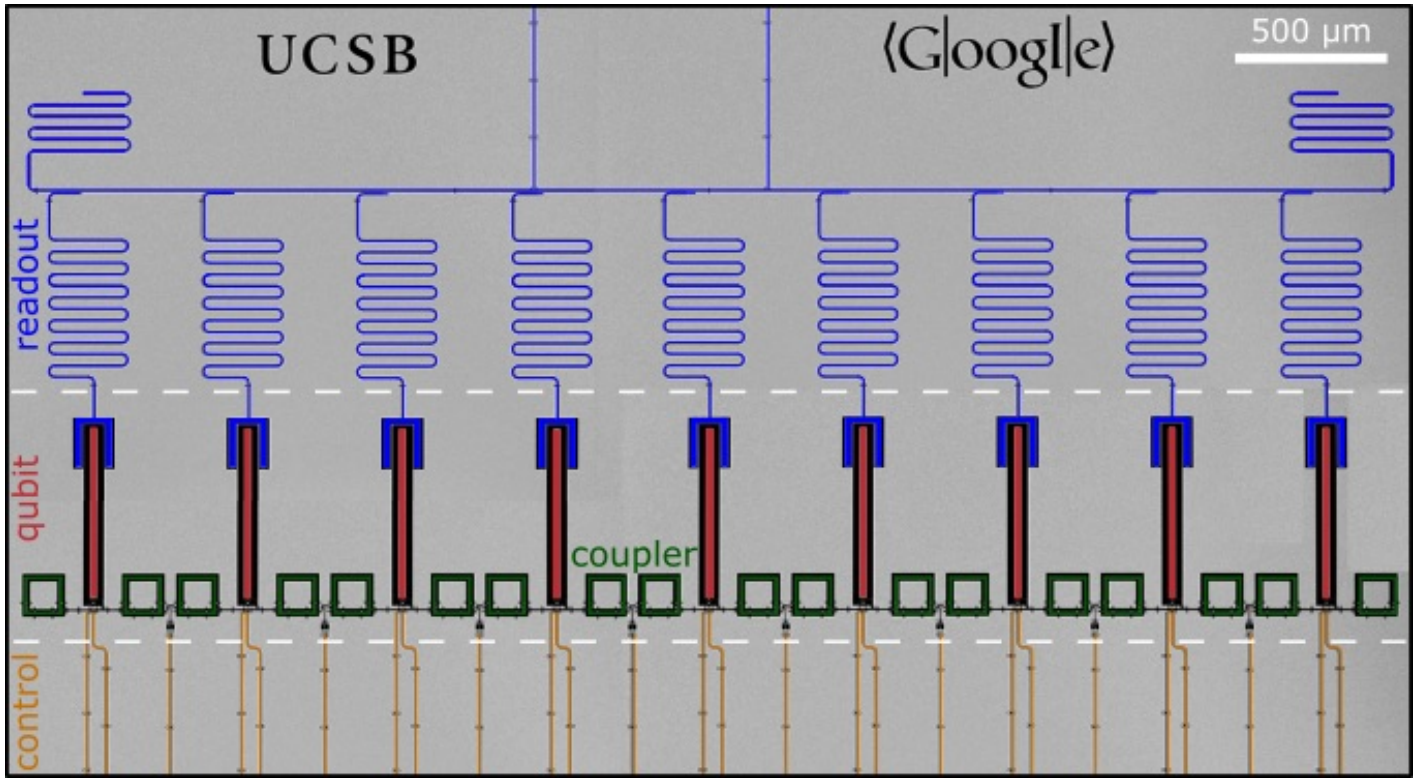




**Quantum annealing**: finding the global minimum of a given function by using quantum fluctuations.

# Google



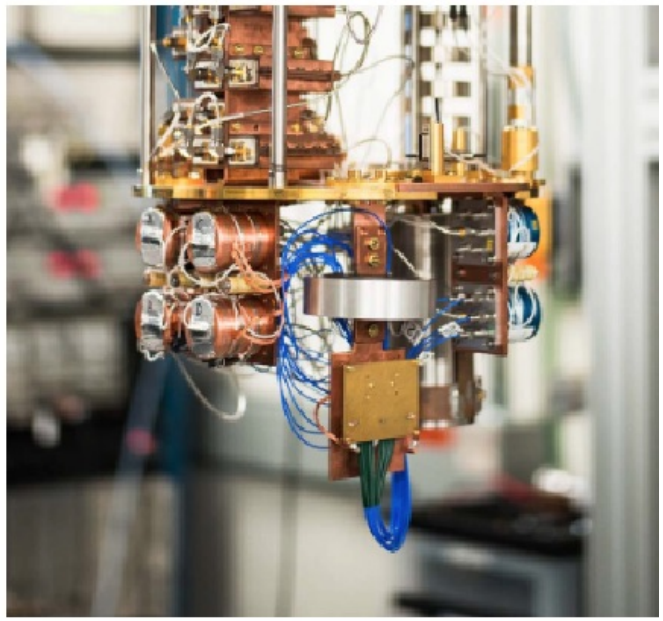
## Superconducting qubit processor




*A blueprint for demonstrating quantum supremacy with superconducting qubits*, [arXiv: 1709.06678]

# IBM

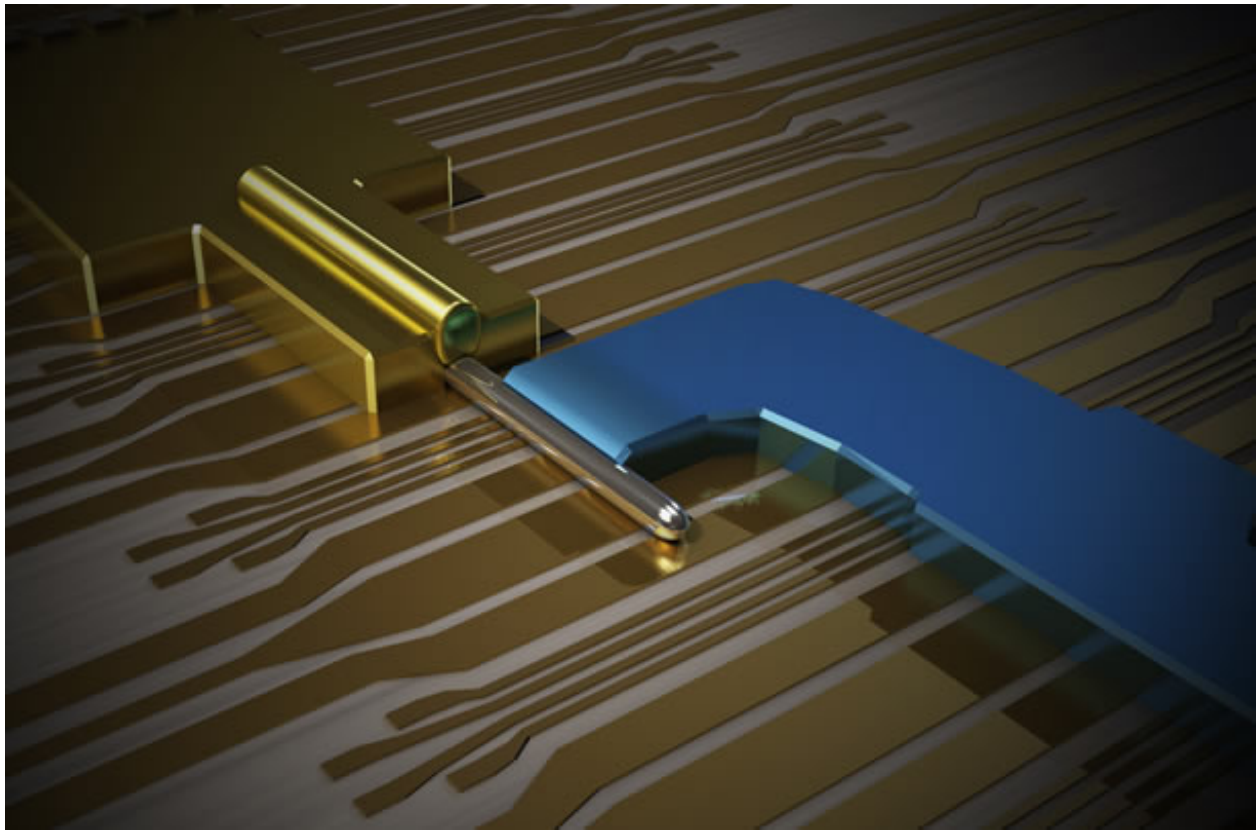
IBM's quantum processors
made up of superconducting transmon qubits

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

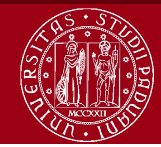
# Microsoft

"Our approach focuses on topological quantum computing through Majorana fermions, which promise to yield fast, stable quantum bits, also known as qubits."



https://www.microsoft.com/en-us/quantum/technology

# Summary



1 Introduction

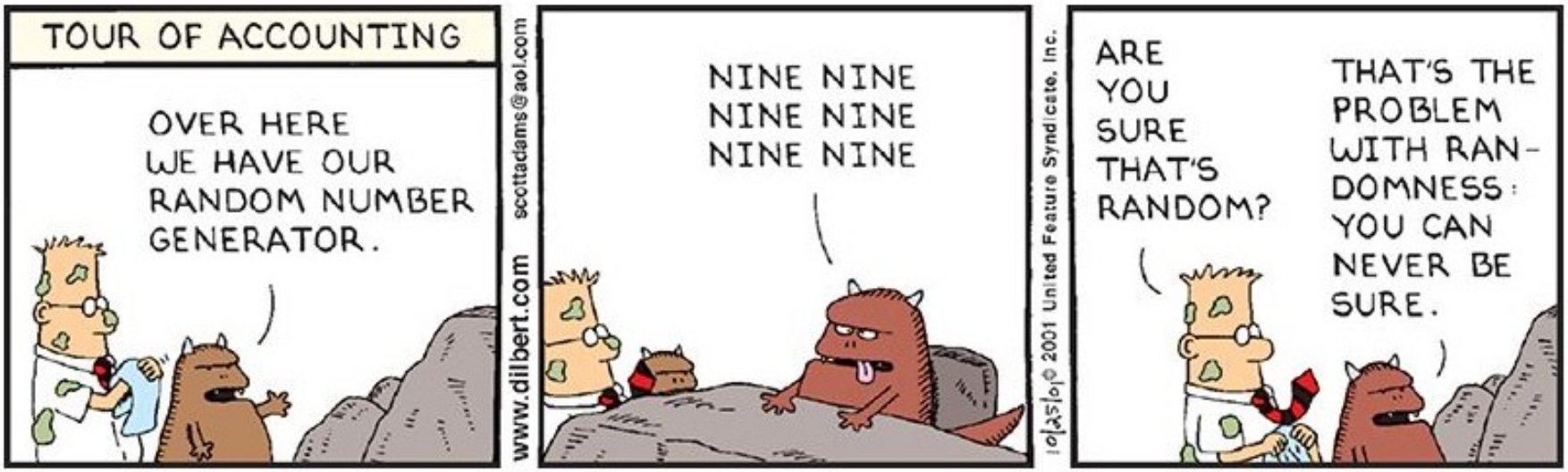
2 Quantum Computing
- Circuit model
- Alternatives to circuit model
- Implementations

3 Quantum Random Number Generators

4 Conclusions

# What is a random number

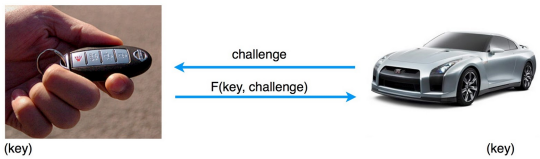
A random number is a number generated by an unpredictable process



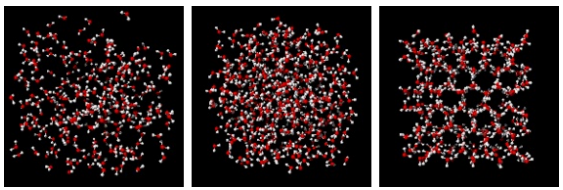
# Why random numbers?


Random numbers are crucial in several applications:

1. Information technology and security (also QKD)




2. Scientific simulation (meteorology, biology, physics...)



3. Lottery/gaming

# Generators based on classical physics

How we generate random numbers?

# Generators based on classical physics

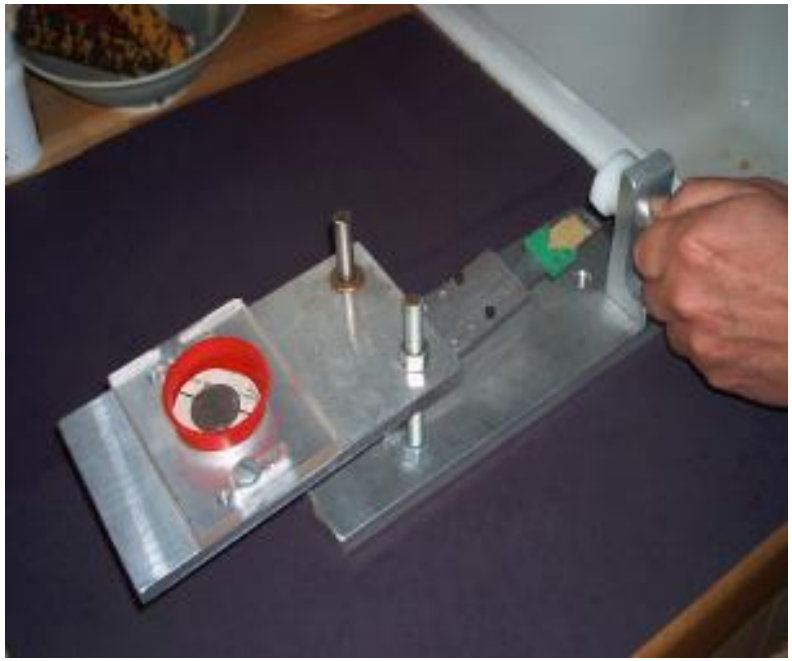
How we generate random numbers?

Head or tail?

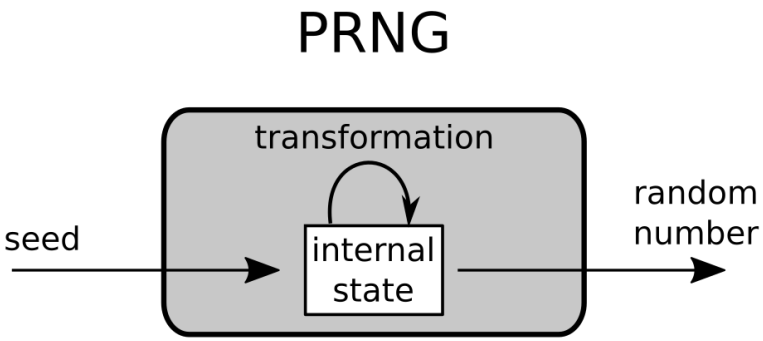
How random is it?

# Generators based on classical physics

Output depends deterministically from initial conditions



# Pseudo Random Number Generators




Pseudo-random numbers are generated by a deterministic algorithm that produces a sequence that “resemble” a random sequence

## PROS

- simple
- fast

## CONS

- period
- not-uniformity
- correlations

# but....

## Von Neumann (1903-1957)

(among the father of information theory

"*Anyone who attempts to generate random numbers by deterministic means is, of course, living in a state of sin*"

# Problems of PRNG

## RANDU

used by IBM from ’60 to ’90

$$V_{k+1} = 65539 \cdot V_k \mod 2^{31}$$

| | |
|---|---|
| $V_1$ | 12589822 |
| $V_2$ | 490623226 |
| $V_3$ | 682947310 |
| $V_4$ | 1829558474 |
| $V_5$ | 535857758 |
| $V_6$ | 1781505818 |
| $V_7$ | 1571347790 |
| $V_8$ | 1984468970 |
| $V_9$ | 2059651006 |
| $V_{10}$ | 940136250 |

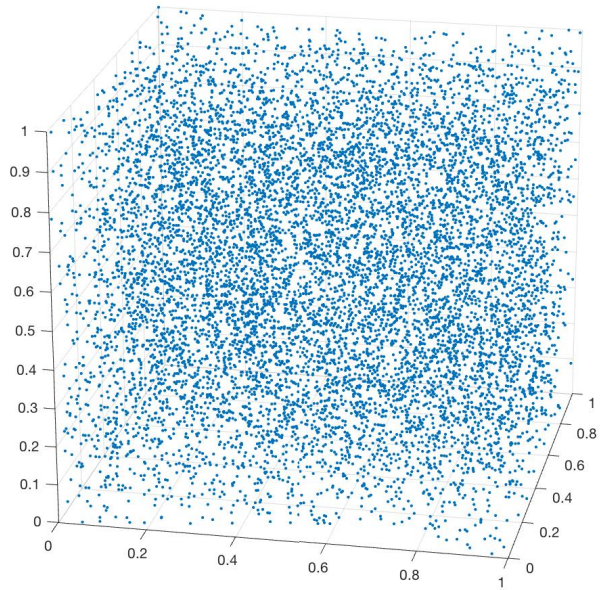
# Problems of PRNG

## RANDU

used by IBM from ’60 to ’90

$$V_{k+1} = 65539 \cdot V_k \mod 2^{31}$$

| | |
|---|---|
| $V_1$ | 12589822 |
| $V_2$ | 490623226 |
| $V_3$ | 682947310 |
| $V_4$ | 1829558474 |
| $V_5$ | 535857758 |
| $V_6$ | 1781505818 |
| $V_7$ | 1571347790 |
| $V_8$ | 1984468970 |
| $V_9$ | 2059651006 |
| $V_{10}$ | 940136250 |



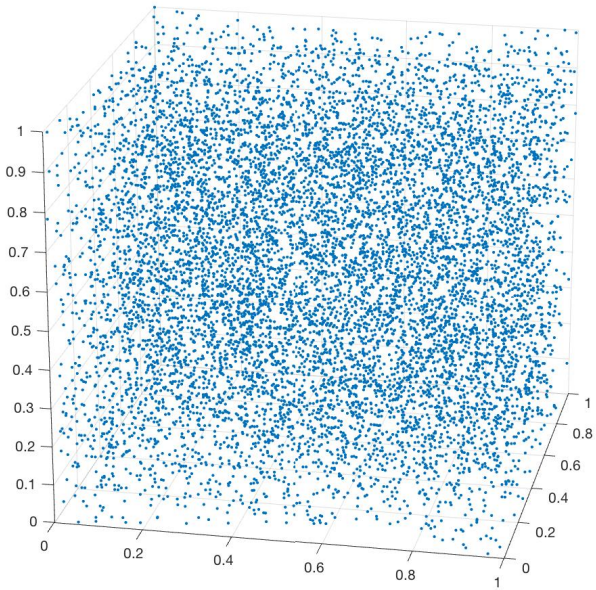
# Problems of PRNG

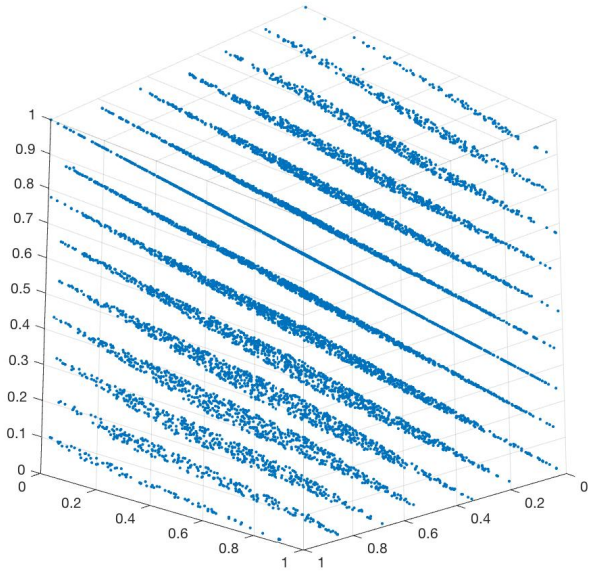
## RANDU

used by IBM from ’60 to ’90

$$V_{k+1} = 65539 \cdot V_k \mod 2^{31}$$

| | |
|---|---|
| $V_1$ | 12589822 |
| $V_2$ | 490623226 |
| $V_3$ | 682947310 |
| $V_4$ | 1829558474 |
| $V_5$ | 535857758 |
| $V_6$ | 1781505818 |
| $V_7$ | 1571347790 |
| $V_8$ | 1984468970 |
| $V_9$ | 2059651006 |
| $V_{10}$ | 940136250 |



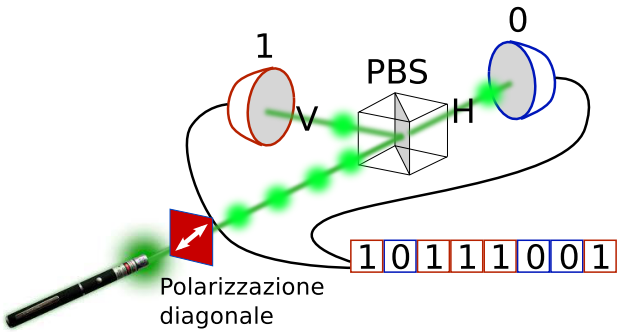
# Flaws in PRNG!

## NSA (National Security Agency) scandal

NSA inserted a “backdoor" in the generator Dual_EC_DRBG certified by NIST

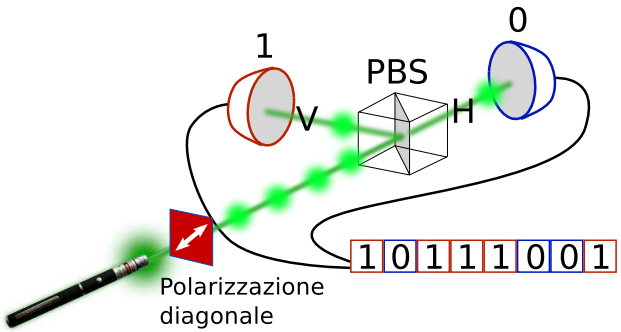

Dual_EC_DRBG was used in several RSA products. In 2013, RSA officially discouraged his clients to use their products with Dual_EC_DRBG.

# Why QRNG?




- RANDOM NUMBERS are needed to encrypt all digital communications (email, social networks) and are essential for QKD

# Why QRNG?

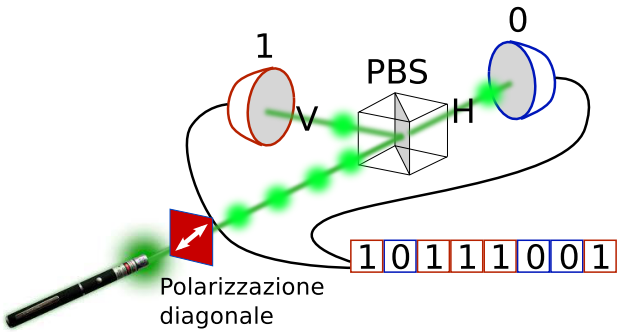



- RANDOM NUMBERS are needed to encrypt all digital communications (email, social networks) and are essential for QKD

What QRNG offer:

- intrinsic randomness of quantum measurements

# Why QRNG?

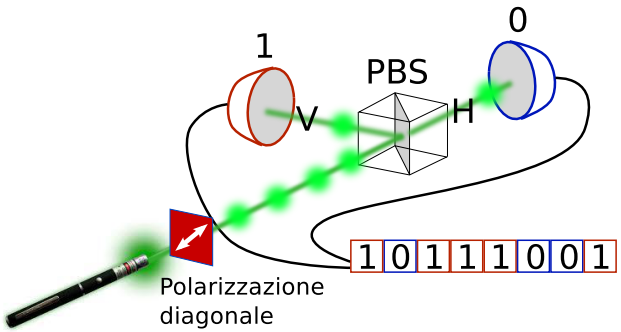



- RANDOM NUMBERS are needed to encrypt all digital communications (email, social networks) and are essential for QKD

What QRNG offer:

- intrinsic randomness of quantum measurements
- outputs not predictable even if the initial state is known

# Why QRNG?

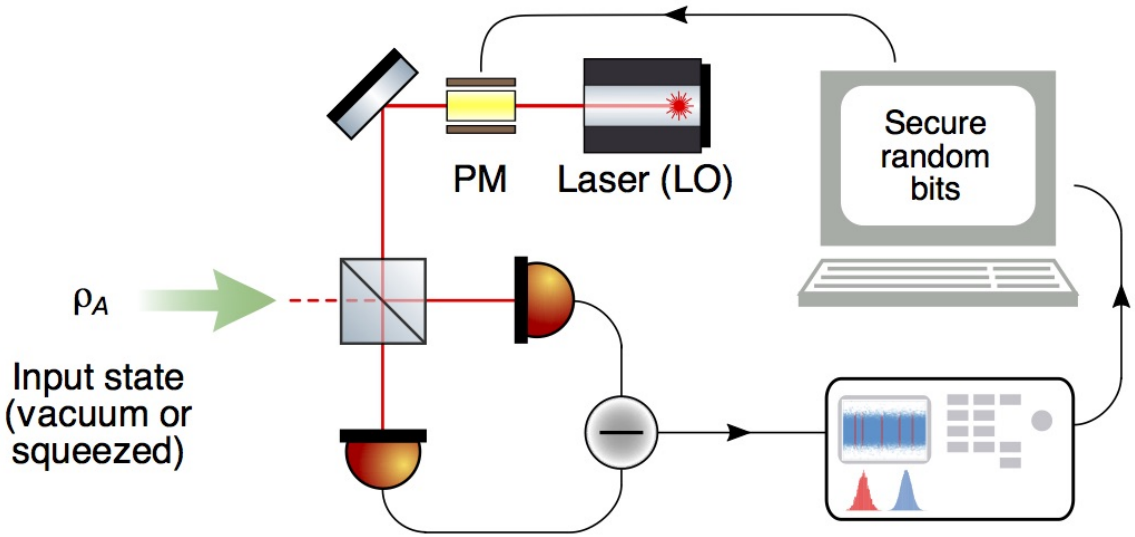



- RANDOM NUMBERS are needed to encrypt all digital communications (email, social networks) and are essential for QKD

What QRNG offer:

- intrinsic randomness of quantum measurements
- outputs not predictable even if the initial state is known
- randomness is not due to ignorance on the initial conditions (like coin tossing)

# QRNG based on vacuum fluctuation




Switch between two conjugate quadratures $\hat{p}$ and $\hat{q}$

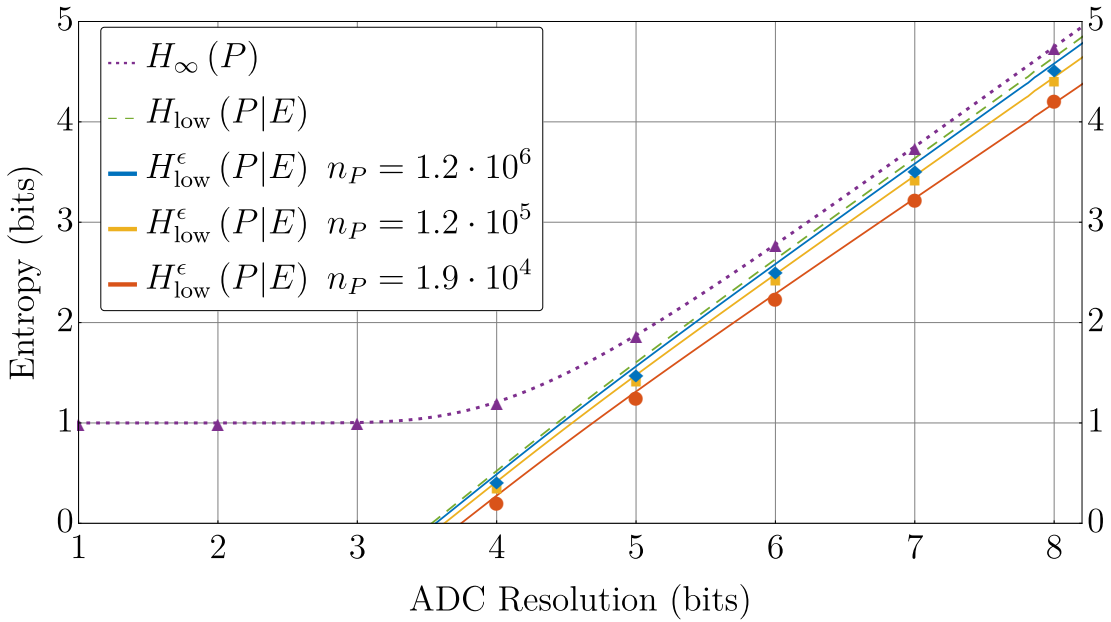
$$P_{guess}(p|E) \leq c(\delta q, \delta p)(\sum_k \sqrt{P(q_k)})^2$$



D. G. Marangon, G. Vallone, P. Villoresi, **Phys. Rev. Lett. 118, 060503 (2017)**

# Randomness estimation

## Finite-size min-entropy evaluation



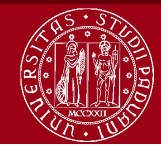

1.25 GSamples/s, 8-bit resolution

Secure bit generation rate of approximately 1.76 Gbit/s (with 5-bit ADC resolution sampling).



D. G. Marangon, G. Vallone, P. Villoresi, **Phys. Rev. Lett. 118, 060503 (2017)**

# Summary



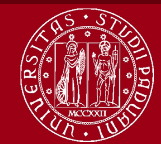
1 Introduction

2 Quantum Computing
- Circuit model
- Alternatives to circuit model
- Implementations

3 Quantum Random Number Generators

4 Conclusions

# Conclusions



- Clear trend in quantum computing: from research groups to large companies
- Are we close to quantum supremacy?
- QRNG as a fundamental tool for simulations and security application

# THANK YOU FOR YOUR ATTENTION!

QuantumFuture

The shift in the communication paradigm

UNIVERSITÀ DEGLI STUDI DI PADOVA

*email:* vallone@dei.unipd.it

http://www.dei.unipd.it/∼vallone

http://quantumfuture.dei.unipd.it/