Lectures on Quantum Computing

Mourad Telmini
mourad.telmini@fst.utm.tn

University of Tunis El Manar
Faculty of Science de Tunis, Department of Physics

Kingdom of Morocco
Ministry of Higher Education, Scientific Research and Innovation

THE EIGHTH BIENNIAL AFRICAN SCHOOL OF FUNDAMENTAL PHYSICS AND APPLICATIONS (ASP2024)

Co-organized by Cadi Ayyad University and Mohammed V University at Faculty of Science Semlalia, Marrakesh, Morocco

April 15th–19th and July 7th–21st, 2024

Outline of the lectures

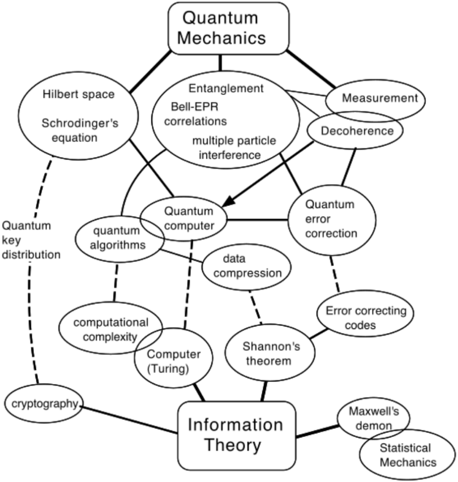
UNESCO International Year of Quantum Science and Technology IYQ2025

INTERNATIONAL YEAR OF
Quantum Science and Technology

100 years of quantum is just the beginning...

An international partnership of major scientific bodies and academies is preparing a resolution for the 2024 General Conference of the United Nations Educational, Scientific and Cultural Organization (UNESCO) and the 2024 General Assembly of the United Nations to proclaim 2025 the **International Year of Quantum Science and Technology**. This year-long initiative would celebrate the profound impacts of quantum science on technology, culture, and our understanding of the natural world.

Classical information vs Quantum information



[1]

[1] Andrew Steane 1998 Rep. Prog. Phys. 61 117

Classical Information : Shannon Theory

Claude Shannon
1916-2001

- Defined the quantity of information produced by a source by a formula similar to the equation that defines thermodynamic entropy in physics :

$$H = -\sum_i p_i \log_2 p_i$$

Classical Information : Shannon Theory

Claude Shannon
1916-2001

- Defined the quantity of information produced by a source by a formula similar to the equation that defines thermodynamic entropy in physics :

$$H = -\sum_i p_i \log_2 p_i$$

- Analyzed the ability to send information through a communications channel, proving the existence of a maximum transmission rate that could not be exceeded (bandwidth).

Classical Information : Shannon Theory

Claude Shannon
1916-2001

- Defined the quantity of information produced by a source by a formula similar to the equation that defines thermodynamic entropy in physics :

$$H = -\sum_i p_i \log_2 p_i$$

- Analyzed the ability to send information through a communications channel, proving the existence of a maximum transmission rate that could not be exceeded (bandwidth).
- Demonstrated mathematically that even in a noisy channel with a low bandwidth, essentially perfect, error-free communication could be achieved by keeping the transmission rate within the channel's bandwidth and by using error-correcting schemes (redundancy)

Noiseless and noisy Shannon theorems

[2]

- Noiseless channel case:

Claude Shannon
1916-2001

[2] S. Barnett, Les Houches Summer School lectures 2009

Noiseless and noisy Shannon theorems

[2]

Claude Shannon
1916-2001

- Noiseless channel case:
    - FRCN SCHL F PHSCS HS NTRSTNG LCTRS

[2] S. Barnett, Les Houches Summer School lectures 2009

Noiseless and noisy Shannon theorems

[2]

Claude Shannon
1916-2001

- Noiseless channel case:
  - FRCN SCHL F PHSCS HS NTRSTNG LCTRS
  - AFRICAN SCHOOL OF PHYSICS HAS INTERESTING LECTURES

[2] S. Barnett, Les Houches Summer School lectures 2009

Noiseless and noisy Shannon theorems

[2]

Claude Shannon
1916-2001

- Noiseless channel case:
    - FRCN SCHL F PHSCS HS NTRSTNG LCTRS
    - AFRICAN SCHOOL OF PHYSICS HAS INTERESTING LECTURES
- Noisy channel case :
    - WNTM NARMQN THRS S FN

[2] S. Barnett, Les Houches Summer School lectures 2009

Noiseless and noisy Shannon theorems

[2]

Claude Shannon
1916-2001

- Noiseless channel case:
  - FRCN SCHL F PHSCS HS NTRSTNG LCTRS
  - AFRICAN SCHOOL OF PHYSICS HAS INTERESTING LECTURES
- Noisy channel case :
  - WNTM NARMQN THRS S FN
  - WUANTFM INAORMAQION THEORS US FUN

[2] S. Barnett, Les Houches Summer School lectures 2009

Noiseless and noisy Shannon theorems

[2]

Claude Shannon
1916-2001

- Noiseless channel case:
  - FRCN SCHL F PHSCS HS NTRSTNG LCTRS
  - AFRICAN SCHOOL OF PHYSICS HAS INTERESTING LECTURES
- Noisy channel case :
  - WNTM NARMQN THRS S FN
  - WUANTFM INAORMAQION THEORS US FUN
  - QUANTUM INFORMATION THEORY IS FUN

[2] S. Barnett, Les Houches Summer School lectures 2009

Shannon Theory

For more details about Shannon Information Theory :

From Classical to Quantum Shannon Theory

Mark M. Wilde
Hearne Institute for Theoretical Physics
Department of Physics and Astronomy
Center for Computation and Technology
Louisiana State University
Baton Rouge, Louisiana 70803, USA

July 16, 2019

Introduction to Quantum Information

- The computers that we use every day, process information according to the rules of classical binary logic.

Introduction to Quantum Information

- The computers that we use every day, process information according to the rules of classical binary logic.
- The hardware part operates according to the rules of quantum mechanics (semiconductors, transistors, etc.), but the quantum properties at the fundamental scale (superposition, entanglement, non-locality, etc.) are not fully exploited.

Introduction to Quantum Information

- The computers that we use every day, process information according to the rules of classical binary logic.
- The hardware part operates according to the rules of quantum mechanics (semiconductors, transistors, etc.), but the quantum properties at the fundamental scale (superposition, entanglement, non-locality, etc.) are not fully exploited.
- The purpose of Quantum Information Theory is precisely to take advantage of these properties in order to perform tasks which are impossible to realize with classical computers.

Introduction to Quantum Information

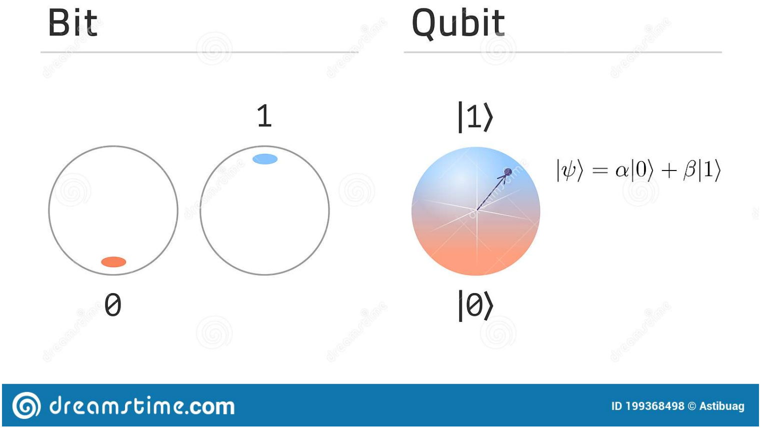
- The computers that we use every day, process information according to the rules of classical binary logic.
- The hardware part operates according to the rules of quantum mechanics (semiconductors, transistors, etc.), but the quantum properties at the fundamental scale (superposition, entanglement, non-locality, etc.) are not fully exploited.
- The purpose of Quantum Information Theory is precisely to take advantage of these properties in order to perform tasks which are impossible to realize with classical computers.
- The most known applications of quantum information are Quantum Computing, with the focus on the physical implementation of a universal quantum computer, and Quantum Cryptography for the secure transmission of information.

Quantum computing vs classical computing

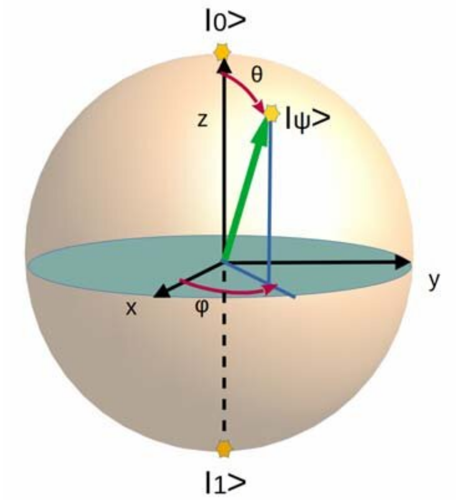
SpinQ Gemini Quantum computer

Laptop classical computer

Classical bit vs Quantum bit

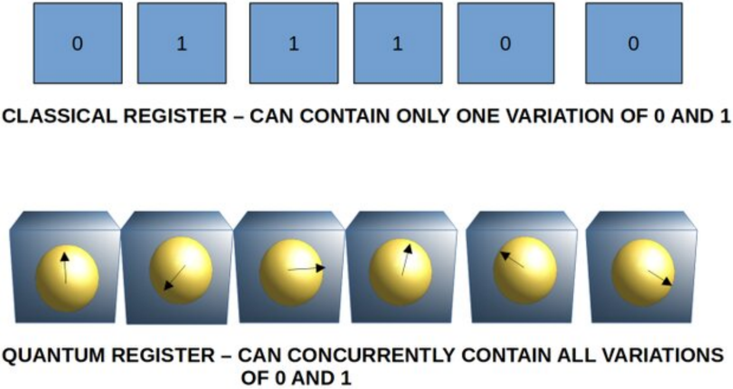


Qubit representation: Bloch Sphere



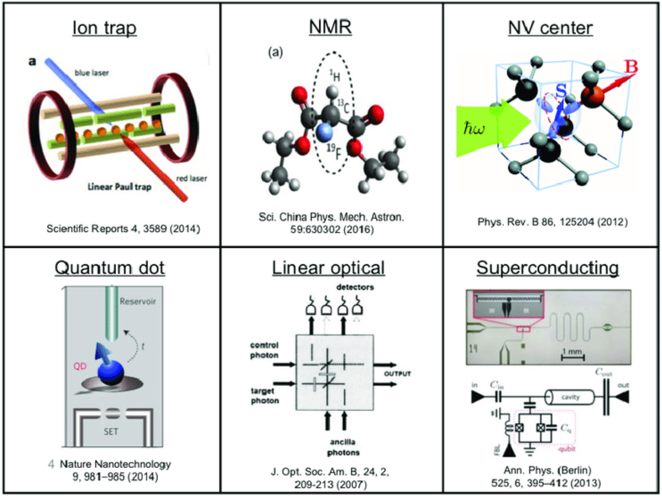
Credits : S. Simonović, Adv. Tech. and Mat. **46-2** , 24-31 (2021)

Classical and quantum register



Credits : S. Simonović, Adv. Tech. and Mat. **46-2** , 24-31 (2021)

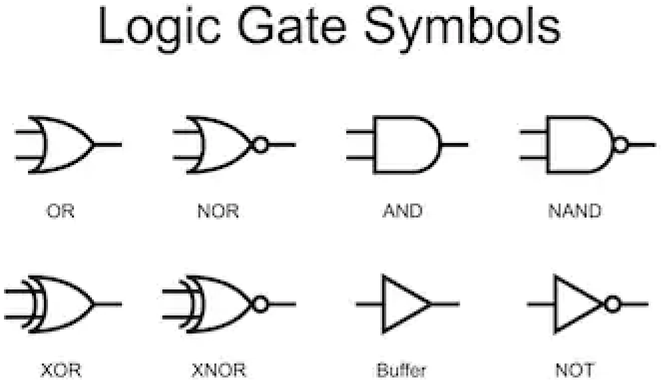
Qubit technologies



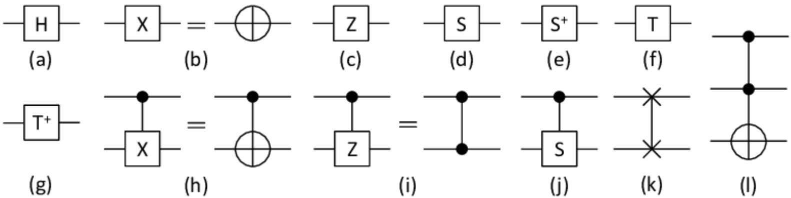
... many more

Credit : Amundson and Sexton-Kennedy, EPJ Web of Conferences **214** 09010 (2019)

Classical gates



Quantum gates



Classical computing

- Given a register of n bits (for example one byte), what operations can we do with it?

0	1	1	0	0	0	0	1

Classical computing

- Given a register of n bits (for example one byte), what operations can we do with it?

0	1	1	0	0	0	0	1

- The value of one or more bits can be changed, which makes it possible to scan the entire field of possible codes.

Classical computing

- Given a register of n bits (for example one byte), what operations can we do with it?

0	1	1	0	0	0	0	1

- The value of one or more bits can be changed, which makes it possible to scan the entire field of possible codes.
- Any other operation, like swapping two bits, ultimately comes down to the first operation.

Classical computing

- Given a register of n bits (for example one byte), what operations can we do with it?

0	1	1	0	0	0	0	1

- The value of one or more bits can be changed, which makes it possible to scan the entire field of possible codes.
- Any other operation, like swapping two bits, ultimately comes down to the first operation.
- Example: Addition

Classical computing

- Given a register of n bits (for example one byte), what operations can we do with it?

0	1	1	0	0	0	0	1

- The value of one or more bits can be changed, which makes it possible to scan the entire field of possible codes.
- Any other operation, like swapping two bits, ultimately comes down to the first operation.
- Example: Addition
0	1	1	0	0	0	0	1

$+$

Classical computing

- Given a register of n bits (for example one byte), what operations can we do with it?

0	1	1	0	0	0	0	1

- The value of one or more bits can be changed, which makes it possible to scan the entire field of possible codes.
- Any other operation, like swapping two bits, ultimately comes down to the first operation.
- Example: Addition

  -

0	1	1	0	0	0	0	1

$+$

  -

0	1	0	0	1	0	1	1

$=$

Classical computing

- Given a register of n bits (for example one byte), what operations can we do with it?

0	1	1	0	0	0	0	1

- The value of one or more bits can be changed, which makes it possible to scan the entire field of possible codes.
- Any other operation, like swapping two bits, ultimately comes down to the first operation.
- Example: Addition

	0	1	1	0	0	0	0	1
+	0	1	0	0	1	0	1	1
=	1	0	1	0	1	1	0	0

Classical computing

- Given a register of n bits (for example one byte), what operations can we do with it?

0	1	1	0	0	0	0	1

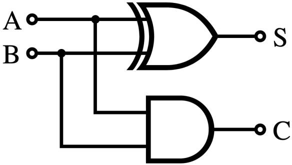
- The value of one or more bits can be changed, which makes it possible to scan the entire field of possible codes.
- Any other operation, like swapping two bits, ultimately comes down to the first operation.
- Example: Addition

	0	1	1	0	0	0	0	1
+								
	0	1	0	0	1	0	1	1
=								
	1	0	1	0	1	1	0	0

- Decimal: 193+139=332

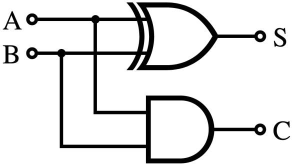
Half-adder Circuit

- The half-adder circuit is built from an XOR gate and a AND gate (we will come back to this)



Half-adder Circuit

- The half-adder circuit is built from an XOR gate and a AND gate (we will come back to this)

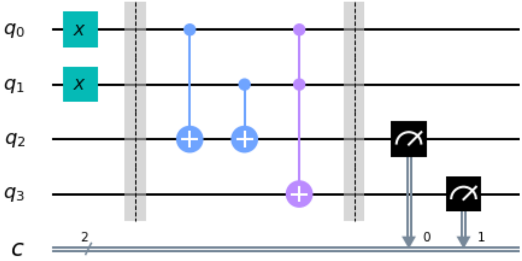


- It takes two bits A and B as input and delivers 2 outputs, the sum S and the carry C,

bit 1	bit 2	sum	carry
0	0	0	0
0	1	1	0
1	0	1	0
1	1	0	1

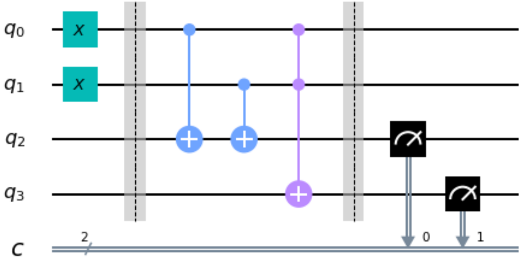
Half-adder Quantum Circuit

- Here's a taste of what a half-adding quantum circuit looks like:



Half-adder Quantum Circuit

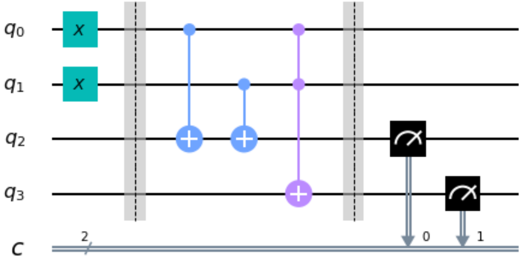
- Here's a taste of what a half-adding quantum circuit looks like:



- For now, it seems complicated, but at the end of this talk, this kind of circuit will become clear.

Half-adder Quantum Circuit

- Here's a taste of what a half-adding quantum circuit looks like:



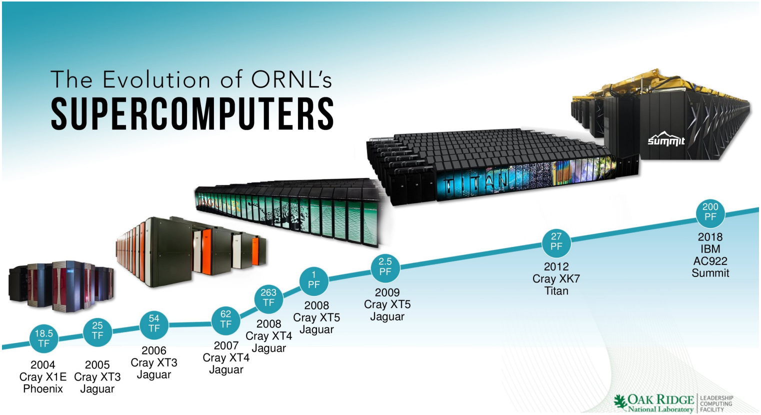
- For now, it seems complicated, but at the end of this talk, this kind of circuit will become clear.
- But already know at this level that this circuit is formed by quantum gates X, $CNOT$ and $Toffoli$!
- Question : What would be the result of $(193 + 139)$ if we use a quantum full-adder ?

Supercomputers

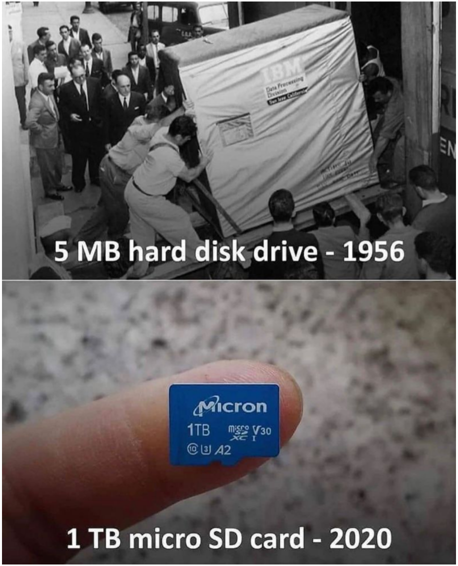
ENIAC 1945
50 KFLOPS
167 m^2, 150 kW

IBM Summit 2018
200 PFLOPS
873 m^2, 13 MW
219 kms of cabling

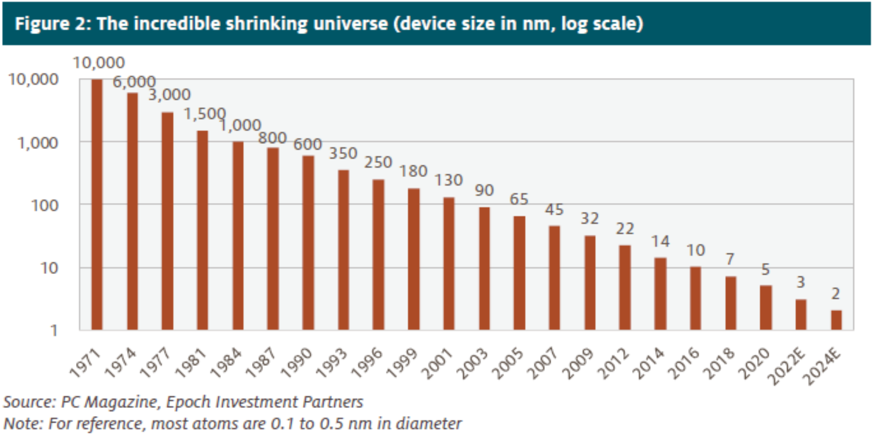
Classical Supercomputers



Evolution of storage capacities



Limits of miniaturization: Moore's Law



Epoch perspectives, 11 February 2021

Limits of computing power

- Are today's computers sufficient to perform the calculations we need ?

Limits of computing power

- Are today's computers sufficient to perform the calculations we need ?
- Yes, to a certain extent.

Limits of computing power

- Are today's computers sufficient to perform the calculations we need ?
- Yes, to a certain extent.
- However, for some problems we reach a limit. For example, factoring large numbers, used to encrypt messages (RSA protocol) and ensure the security of communications and transactions related to e-commerce, electronic signatures, etc.

Complexity classes

- To better understand the difficulty of the factoring problem, here are some examples of mathematical problems as well as the scale laws of the number of operations n with the number of bits (or digits) as well as the complexity classes:

Problem	Operations	Class
Addition of 2 numbers of n bits	n	P
Multiplication of 2 numbers of n bits	n^2	P
FFT de n bits	$n\log(n)$	P
Factoring a number of n bits	$2^{n/2}$	NP
Travelling salesman problem (n towns)	$e^{n\log(n)}$	NPC

Complexity classes

- To better understand the difficulty of the factoring problem, here are some examples of mathematical problems as well as the scale laws of the number of operations n with the number of bits (or digits) as well as the complexity classes:

Problem	Operations	Class
Addition of 2 numbers of n bits	n	P
Multiplication of 2 numbers of n bits	n^2	P
FFT de n bits	$n\log(n)$	P
Factoring a number of n bits	$2^{n/2}$	NP
Travelling salesman problem (n towns)	$e^{n\log(n)}$	NPC

- Current computer architectures are unable to deal with complex problems due to a lack of efficient algorithms.

Cryptography

- Until the 1970s, known encryption systems were based on the principle of symmetric cryptography, where the same (secret) key is used to encrypt and decrypt a message.

Cryptography

- Until the 1970s, known encryption systems were based on the principle of symmetric cryptography, where the same (secret) key is used to encrypt and decrypt a message.
- In 1978, R. Rivest, A. Shamir and L. Adleman described the first public system of asymmetric cryptography (named after their initials RSA), based on the properties of prime numbers and factorization. In such a system, two keys are used: one is used to encrypt, the other to decipher.

Cryptography

- Until the 1970s, known encryption systems were based on the principle of symmetric cryptography, where the same (secret) key is used to encrypt and decrypt a message.
- In 1978, R. Rivest, A. Shamir and L. Adleman described the first public system of asymmetric cryptography (named after their initials RSA), based on the properties of prime numbers and factorization. In such a system, two keys are used: one is used to encrypt, the other to decipher.
- The key used to encrypt is accompanied by a large integer, the product of two large primes kept secret (of the order of 200 digits, see RSA numbers). To calculate the decryption key, the only known method requires knowing the two prime factors.

RSA Protocol

- The security of the RSA system is based on the fact that it is easy to find two large prime numbers p and q (using primality tests) and multiply them to have $N = p \times q$, but that it would be difficult for an attacker to find these two numbers (p, q) knowing N. This system also allows the creation of digital signatures, and has revolutionized the world of cryptography.

RSA Protocol

- The security of the RSA system is based on the fact that it is easy to find two large prime numbers p and q (using primality tests) and multiply them to have $N = p \times q$, but that it would be difficult for an attacker to find these two numbers (p, q) knowing N. This system also allows the creation of digital signatures, and has revolutionized the world of cryptography.
- It is a protocol widely used today for the secure communication of information (telecommunications, electronic commerce, defense, etc.)

RSA Protocol

- The security of the RSA system is based on the fact that it is easy to find two large prime numbers p and q (using primality tests) and multiply them to have $N = p \times q$, but that it would be difficult for an attacker to find these two numbers (p, q) knowing N. This system also allows the creation of digital signatures, and has revolutionized the world of cryptography.
- It is a protocol widely used today for the secure communication of information (telecommunications, electronic commerce, defense, etc.)
- Example : calculate 11×17 and 137×211

RSA Protocol

- The security of the RSA system is based on the fact that it is easy to find two large prime numbers p and q (using primality tests) and multiply them to have $N = p \times q$, but that it would be difficult for an attacker to find these two numbers (p, q) knowing N. This system also allows the creation of digital signatures, and has revolutionized the world of cryptography.
- It is a protocol widely used today for the secure communication of information (telecommunications, electronic commerce, defense, etc.)
- Example : calculate 11×17 and 137×211
- find (p, q), for $N = 667$ and $N = 82919$

RSA Protocol

- The security of the RSA system is based on the fact that it is easy to find two large prime numbers p and q (using primality tests) and multiply them to have $N = p \times q$, but that it would be difficult for an attacker to find these two numbers (p, q) knowing N. This system also allows the creation of digital signatures, and has revolutionized the world of cryptography.
- It is a protocol widely used today for the secure communication of information (telecommunications, electronic commerce, defense, etc.)
- Example : calculate 11×17 and 137×211
- find (p, q), for $N = 667$ and $N = 82919$
- Answers : $(p, q) = (23, 29)$ and $(p, q) = (283, 293)$

RSA numbers

- RSA-200 : made up of 200 digits in decimal

  27997833911221327870829467638722601621070446786955

  42853756000992932612840010760934567105295536085606

  18223519109513657886371059544820065767750985805576

  13579098734950144178863178946295187237869221823983

RSA numbers

- RSA-200 : made up of 200 digits in decimal

  27997833911221327870829467638722601621070446786955
  42853756000992932612840010760934567105295536085606
  18223519109513657886371059544820065767750985805576
  13579098734950144178863178946295187237869221823983

- Calculation carried out on a network of computers required a CPU time equivalent to 75 years on an Opetron processor @ 2.2GHz (F. Bahr et al 2005)

RSA numbers

- RSA-200 : made up of 200 digits in decimal

  27997833911221327870829467638722601621070446786955
  42853756000992932612840010760934567105295536085606
  18223519109513657886371059544820065767750985805576
  13579098734950144178863178946295187237869221823983

- Calculation carried out on a network of computers required a CPU time equivalent to 75 years on an Opetron processor @ 2.2GHz (F. Bahr et al 2005)
- The prime factors of RSA200 are :

$$\begin{aligned} p =& 35324619344027701212726049781984643686711974001976 \\ & 25023649303468776121253679423200058547956528088349 \\ q =& 79258699544783330333470858414800596877379758573642 \\ & 19960734330341455767872818152135381409304740185467 \end{aligned}$$

RSA numbers

- The current record, dating from 2009, for the largest factored number (RSA-768): formed by 232 digits in decimal

$$
\begin{array}{r}
1230186684530117755130494958384962720772853569595 3\\
3479219732245215172640050726365751874520219978646 9\\
3899564749427740638459251925573263034537315482685 0\\
7917026122142913461670429214311602221240479274737 7\\
94080665351419597459856902143413
\end{array}
$$

- The calculation carried out on a network of computers required approximately two years of calculation, that is to say a CPU calculation time equivalent to 2000 years on an Opetron processor running at 2.2GHz.

RSA-2048: the beast

25195908475657893494027183240048398571429282126204
03202777713783604366202070759555626401852588078440
69182906412495150821892985591491761845028084891200
72844992687392807287776735971418347270261896375014
97182469116507761337985909570009733045974880842840
17974291006424586918171951187461215151726546322822
16869987549182422433637259085141865462043576798423
38718477444792073993423658482382428119816381501067
48104516603773060562016196762561338441436038339044
14952634432190114657544454178424020924616515723350
77870774981712577246796292638635637328991215483143
81678998850404453640235273819513786365643912120103
97122822120720357

RSA challenge

- The RSA-2048 number formed of 617 digits, or 2048 binary digits.

RSA challenge

- The RSA-2048 number formed of 617 digits, or 2048 binary digits.
- There was a challenge launched with a prize of USD 200,000 (canceled in 2007).

RSA challenge

- The RSA-2048 number formed of 617 digits, or 2048 binary digits.
- There was a challenge launched with a prize of USD 200,000 (canceled in 2007).

RSA challenge

- The RSA-2048 number formed of 617 digits, or 2048 binary digits.
- There was a challenge launched with a prize of USD 200,000 (canceled in 2007).
- With current technology, it is estimated that the time required, on a single processor, to factor this number would be larger than the age of the universe !!!

RSA challenge

- The RSA-2048 number formed of 617 digits, or 2048 binary digits.
- There was a challenge launched with a prize of USD 200,000 (canceled in 2007).
- With current technology, it is estimated that the time required, on a single processor, to factor this number would be larger than the age of the universe !!!
- This time can be reduced by resorting to parallelization. If we accept a calculation period of 10 years, we would have to use a cluster of computers that would cover the surface of Tunisia several times, which would cost 10^{18} USD and would require an electric power of 10^{12} megawatt, which would exhaust all the world's fossil fuel resources in one day !!! (J. Preskill 2012)

The second quantum revolution

- Fortunately, we are living in great times!

The second quantum revolution

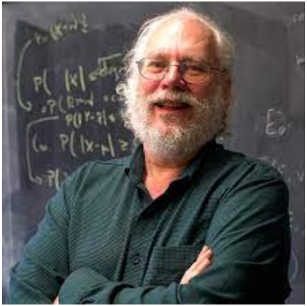
- Fortunately, we are living in great times!
- A century after the birth of quantum mechanics, we are in the midst of what is called the second quantum revolution, with as corollary a rapid development of quantum technologies, including quantum computing.

The second quantum revolution

- Fortunately, we are living in great times!
- A century after the birth of quantum mechanics, we are in the midst of what is called the second quantum revolution, with as corollary a rapid development of quantum technologies, including quantum computing.
- Quantum information gives hope, and it is reasonable to think that we will be able to solve the problem of factorization of large numbers and many others within a reasonable period of time.

The second quantum revolution

- Fortunately, we are living in great times!
- A century after the birth of quantum mechanics, we are in the midst of what is called the second quantum revolution, with as corollary a rapid development of quantum technologies, including quantum computing.
- Quantum information gives hope, and it is reasonable to think that we will be able to solve the problem of factorization of large numbers and many others within a reasonable period of time.
- A major breakthrough was made in 1994 by Peter Shor, who developed a quantum factorization algorithm.

- 

Peter Shor
(ICTP Dirac medal 2017)

Shor's algorithm

- Without going into details, and assuming the existence of a perfect quantum computer, the algorithm developed by Peter Shor promises to factor a number of 500 digits, which should take more than the age of the universe on a current processor, in just 2 seconds !!!

Shor's algorithm

- Without going into details, and assuming the existence of a perfect quantum computer, the algorithm developed by Peter Shor promises to factor a number of 500 digits, which should take more than the age of the universe on a current processor, in just 2 seconds !!!

- Physicists made a first rough estimate for RSA-2048 and found that with a quantum computer formed of 10,000 logical qubits and 10 million physical (superconducting) qubits, spaced 1 cm apart for the wiring, which would cost "only" 100 billion USD, and using a modest electric power of 10 MW, would get the job done in 16 hours !!! (J. Preskill 2012)

- Shor's algorithm works thanks to quantum properties : Superposition and Entanglement

Outline of the lectures

1. Lecture 1 : Introduction to Quantum Computing

2. Lecture 2 : Basics of Quantum Computing