Introduction to Quantum Computing

Frédéric Magniez

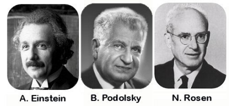
INF554 - Lectures 8 & 9

The genesis

Copenhagen School (Bohr, Heisenberg, …)

- The state of a quantum particule is only fixed after a measurement
- Bennett, Brassard'84: perfectly secure quantum encryption… that can be used in practice!

Paradoxe of Einstein, Podolsky, Rosen'35



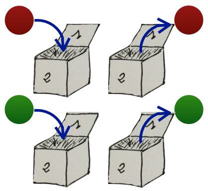
- Very distant particules remain linked!?
- Aspect, Grangier, Roger, Dalibard'82: yes!
- Quantum encryption of Ekert'91 can be *certifiable*

Quantum boxes

© Preskill

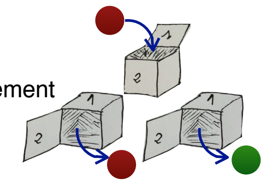
Classical information is encoded using bit (0/1)

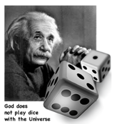
- The measure describes the state of the system
- A random bit is a 'hidden' bit



Quantum information is encoded using quantum-bit

- Several possible measures
- Outcome is determined during the measurement





Quantum key distribution

Problem

- Setting
  - No prior shared secret information between Alice and Bob
  - Authenticated classical channel
- Goal: Get a private key between Alice and Bob
- Application: One-time pad (Miller'1882-Shanon'1945)

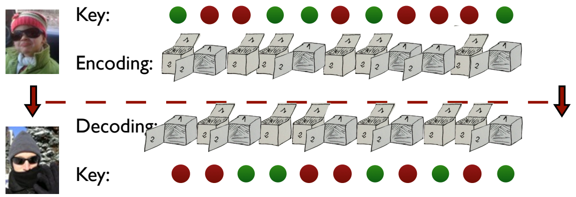
Washington-Moscow hotline (1963)

Classical results

- **Impossible:** all the information is in the canal
- **Possible** (using randomized techniques):
  - **Amplify** the privacy of an imperfect private key

The protocol BB84 [Bennett-Brassard 84]

Protocol: quantum part



Protocol: classical part

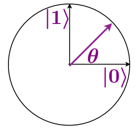
- Reconciliation: Alice and Bob publicly announce their coding choices
  A&B only keep key bits with same choices
- Security: Intercepting and opening a box $\rightarrow$ errors
  A&B check few key bits at random positions
- Privacy amplification: Perfect key using with few other more key bits

Conclusion

- Secrete key generation using an authenticated classical channel
- Small initial private key $\rightarrow$ large private key, with no authenticated channel

Qubit

State



- 2-dimensional unit vector

$$|\psi\rangle = \cos\theta|0\rangle + \sin\theta|1\rangle$$

general case (complex amplitudes):

$$|\psi\rangle = \begin{pmatrix}\alpha\\ \beta\end{pmatrix} = \alpha|0\rangle + \beta|1\rangle, \quad |\alpha|^2 + |\beta|^2 = 1$$

Measure

- Randomized orthogonal projection

$$\alpha|0\rangle + \beta|1\rangle \longrightarrow \boxed{\text{Measure}} \begin{cases} \xrightarrow{|\alpha|^2} |0\rangle \\ \xrightarrow{|\beta|^2} |1\rangle \end{cases}$$

Evolution

- Unitary transformation $G \in \mathcal{U}(2)$ ($\Rightarrow$ reversible)

Definition: $G \in \mathbb{C}^{2\times 2}$ s.t. $G^*G = \mathrm{Id}$

$$|\psi\rangle \longleftarrow \boxed{G} \longrightarrow |\psi'\rangle = G|\psi\rangle$$

$$|\psi'\rangle = G|\psi\rangle \longleftarrow \boxed{G^*} \longrightarrow |\psi\rangle$$

Examples of transformations

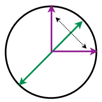
Reversible classical transformation

- Identity

$$|b\rangle \longleftarrow \boxed{\text{Id}} \longrightarrow |b\rangle$$

- Negation

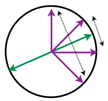
$$|b\rangle \longleftarrow \boxed{NOT} \longrightarrow |1-b\rangle$$



Hadamard transformation

- Definition: half-wave blade at 22,5° $\quad H = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}$

$$|b\rangle \longleftarrow \boxed{H} \longrightarrow \tfrac{1}{\sqrt{2}}(|0\rangle + (-1)^b|1\rangle)$$



- Properties: quantum coin flipping

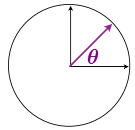
$$|0\rangle \rightarrow \boxed{H} \rightarrow \tfrac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \rightarrow \boxed{\text{Measure}} \begin{cases} \xrightarrow{\frac{1}{2}} |0\rangle \\ \xrightarrow{\frac{1}{2}} |1\rangle \end{cases}$$

$$|b\rangle \rightarrow \boxed{H} \rightarrow \boxed{H} \rightarrow \boxed{\text{Measure}} \longrightarrow |b\rangle$$

STOP Measure does not commute!

Polarization of photons

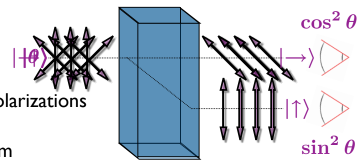
State



- Polarization: 2-dimensional vector

$$|\theta\rangle = \cos\theta|\rightarrow\rangle + \sin\theta|\uparrow\rangle$$

Measure

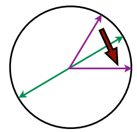


- Calcite crystal
  separates horizontal and vertical polarizations

  STOP A measure modifies the system

Transformation

- Well known transformation: half-wave blade
  orthogonal symmetry around its axis
- Any rotations (possibly with complex angles)



Exercice 1: Quantum key distribution

Implementation

- Explain how to realize the boxes of slide 3
- Implement the protocol of slide 4 using random bits, Hadamard transformations, and measurements

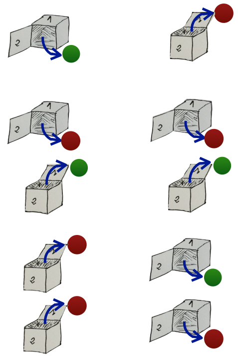
Analysis of a specific attack

- Assume a third party Eves intercepts a photon with probability 1/10, observes it, and forwards the projected photon to Bob
- Assume furthermore that Alice & Bob check each bit of their key with probability 1/10
- Compute
  - The probability Eve learns a bit of the secret key
  - The probability Eve is detected

Entanglement

Principle: 2 distant boxes which remain entangled

- Outcomes are random
  - but correlated if boxes are opened similarly
  - and uncorrelated otherwise



Bell'64 inequality

- Cooperative random game

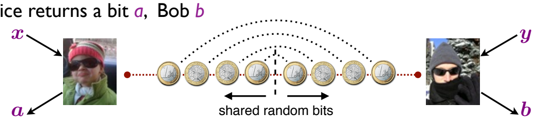
  Classical $\leq$ 75% of victory

  Quantum > 85% of victory
- Experimental verification at Orsay in 1982
- Application: quantum certification

Bell-CHSH inequality as a classical game

Game

- Alice and Bob share random bits but cannot communicate
- Alice receives a random bit x, Bob y
- Alice returns a bit a, Bob b



- Goal: maximize $p = \Pr_{x,y}(a \oplus b = x \wedge y)$

$\wedge$	0	1
0	0	0
1	0	1

$\oplus$	0	1
0	0	1
1	1	0

CHSH inequality [1969]

- The best probabilistic strategy achieves $p=3/4$

Exercice 2: CHSH inequality

Deterministic strategy

- Provide a deterministic strategy achieving $p=3/4$
- Show that no deterministic strategy can achieve p=1
- Conclude that $p\leq 3/4$ for every deterministic strategies

Randomized strategy

- We assume that both players have access to a shared source of randomness, called λ
  - Note: Physicists call λ a *hidden variable*
  - Justify why this is the most powerful model of random ressource
- Let p_λ be the winning probability when λ is fixed
  - Show that there must be some λ such that $p_\lambda \geq p$
- Conclude that the best probabilistic strategy achieves $p=3/4$

n-qubit

State

- $|\psi\rangle \in \mathbb{C}^{\{0,1\}^n}$ such that $|||\psi\rangle|| = 1$

$$|\psi\rangle = \sum_{x\in\{0,1\}^n} \alpha_x |x\rangle \qquad \text{with} \quad \sum_{x\in\{0,1\}^n} |\alpha_x|^2 = 1$$

- Examples
  - Separated 2-qubit: $|00\rangle + |01\rangle = |0\rangle(|0\rangle + |1\rangle)$
  - Entangled 2-qubit: $|00\rangle + |11\rangle \neq |\psi_1\rangle|\psi_2\rangle$ EPR state

Measure

- Randomized orthogonal projection

$$\sum_{x\in\{0,1\}^n} \alpha_x |x\rangle \dashrightarrow \boxed{\text{Measure}} \xrightarrow{|\alpha_x|^2} |x\rangle$$

Evolution

- Unitary transformation $G \in \mathcal{U}(2^n)$ $\quad (G \in \mathbb{C}^{2^n\times 2^n}$ s.t. $G^*G = \mathrm{Id})$

$$|\psi\rangle \dashrightarrow \boxed{G} \dashrightarrow |\psi'\rangle = G|\psi\rangle$$

Mathematical background: Tensor product

Vector spaces

- V, W: vector spaces
- $V\otimes W$ is the free vector space Span ($v\otimes w : v\in V, w\in W$)

  with equivalence relations

  $(v_1+v_2)\otimes w = v_1\otimes w + v_2\otimes w$

  $v\otimes (w_1+w_2) = v\otimes w_1 + v\otimes w_2$

  $(c\cdot v)\otimes w = v\otimes(c\cdot w) = c\cdot(v\otimes w)$

Linear maps

- $S: V\rightarrow X,\quad T: W\rightarrow Y$: linear maps
- $S\otimes T : V\otimes W\rightarrow X\otimes Y$ is the linear map satisfying

  $S\otimes T\ (v\otimes w) = S(v)\otimes T(w)$

  (and extended by linearity)

Applications

- Joint probability distributions on spaces V, W

  $\mathcal{D}(V\times W) = \mathcal{D}(V)\otimes\mathcal{D}(W) \neq \mathcal{D}(V)\times\mathcal{D}(W)$ (: product distributions)

Transformation c–NOT

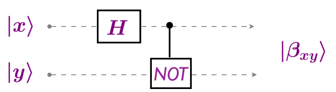
Definition

$$\text{c–NOT}|0b\rangle = |0b\rangle$$
$$\text{c–NOT}|1b\rangle = |1\rangle|(1-b)\rangle$$
$$\text{c–NOT}|ab\rangle = |a\rangle|a\oplus b\rangle$$

$$\text{c–NOT} = \begin{pmatrix} 1000 \\ 0100 \\ 0001 \\ 0010 \end{pmatrix}$$

Representation

Bell basis change



$$|\beta_{00}\rangle = \tfrac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$
$$|\beta_{01}\rangle = \tfrac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$$
$$|\beta_{10}\rangle = \tfrac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$$
$$|\beta_{11}\rangle = \tfrac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$$

Partial measure: 2-qubit case

Measure of first qubit

- Projectors $\quad P_0 = |00\rangle\langle 00| + |01\rangle\langle 01| = |0\rangle\langle 0| \otimes \mathbf{I}_2$

  $P_1 = |10\rangle\langle 10| + |11\rangle\langle 11| = |1\rangle\langle 1| \otimes \mathbf{I}_2$

  $$P_0 \overset{\perp}{\oplus} P_1 = Id$$

- Measure of first qubit

$$|\psi\rangle = a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle \dashrightarrow \boxed{\text{Measure I}} \begin{cases} \xrightarrow{||P_0|\psi\rangle||^2 = a^2+b^2} \frac{1}{||P_0|\psi\rangle||} P_0|\psi\rangle = |0\rangle \frac{a|0\rangle + b|1\rangle}{\sqrt{a^2+b^2}} \\ \xrightarrow{||P_1|\psi\rangle||^2 = c^2+d^2} \frac{1}{||P_1|\psi\rangle||} P_1|\psi\rangle = |1\rangle \frac{c|0\rangle + d|1\rangle}{\sqrt{c^2+d^2}} \end{cases}$$

Generalization

- Partial measure project to a subspace compatible with the observation

  Probability = square norm of the projection

  Outcome = renormalization of the projection

Exercice 3

Partial vs complete measurement

- Consider any two-qubit state, and measure its first qubit and then its second qubit
  - Compute the probability distribution of the outcome
- Conclude that observing the two qubits is equivalent to measuring each qubit individually in any order
  - Note: This can be generalized to any number of qubits

Non-cloning

- Assume there is a unitary map U such that, for every qubit $|\psi\rangle$:

$$U(|\psi\rangle|0\rangle) = |\psi\rangle|\psi\rangle$$

- Compute $U(|\psi\rangle|0\rangle)$ for $|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$
  - using the definition of U
  - using the linearity of U and then again the definition of U
- Get a contradiction and conclude

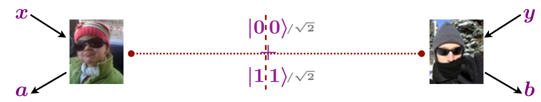
Bell-CHSH inequality as a quantum game

Reminder

- Goal: maximize $p = \Pr_{x,y}(a \oplus b = x \wedge y)$

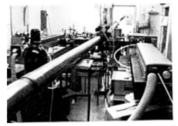
Quantumly

- Alain and Bob share an EPR state



- Bob performs a rotation of angle $\frac{\pi}{8}$
- If $x = 1$, Alice performs a rotation of angle $\frac{\pi}{4}$
- If $y = 1$, Bob performs a rotation of angle $-\frac{\pi}{4}$
- Alice et Bob observe their qubit and send their respective outcomes
- Theorem: $p = \cos^2(\frac{\pi}{8}) \approx 0.85$

Realization: [Aspect-Grangier-Roger-Dalibard: Orsay'82]



Exercice 4: EPR state

Entangles boxes

- Implement the entangled boxes of slide 10 using EPR states

Properties

- Show that applying a unitary U on the first qubit of an EPR state is equivalent to applying the transposed matrix of U on its second qubit

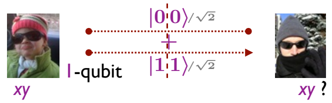
Quantum game

- Prove the theorem of previous slide

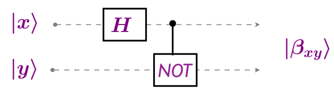
Superdense coding [1992]

Problem

- Alice & Bob share an EPR state: $|\beta_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$
- Alice wants to send two bits *xy* to Bob
- But Alice can only send one qubit to Bob



Bell basis change



$$|\beta_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$
$$|\beta_{01}\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$$
$$|\beta_{10}\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$$
$$|\beta_{11}\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$$

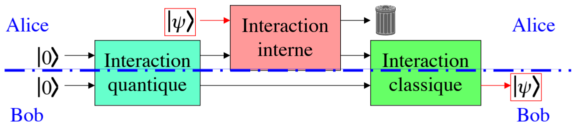
Protocol

- Alice applies to its qubit *NOT*, if *y*=1; and *FLIP*, if *x*=1 $\quad FLIP = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$
  - Alice sends its qubit to Bob
  - Bob performs the inverse of the Bell basis change, and observes *xy*

Problem

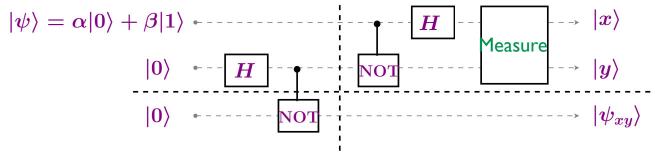
- Alice wants to transmit a qubit $|\psi\rangle$ to Bob
- Bob: far and unknown position to Alice

Realization



The quantum communication does not reveal anything on $|\psi\rangle$!

Circuit



Analysis

- Final state $\frac{1}{2}\sum_{x,y}|xy\rangle|\psi_{xy}\rangle$ with $|\psi_{xy}\rangle = (\mathbf{NOT})^y(\mathbf{FLIP})^x|\psi\rangle$
- By measuring x,y, third qubit is projected to $|\psi_{xy}\rangle$
- After learning x,y, Bob can correct $|\psi_{xy}\rangle$ to $|\psi\rangle$

Realizations

- 1 photon [Zeilinger et al : Innsbruck'97]
- 1 photon, 6 km [Gisin et al : Genève'02]
- 1 atom [Blatt et al : Innsbruck'04]
- Today: over 100km

Problem

- Alice and Bob are fare away
- They want to flip a coin in a fair way
  but they don't trust each other

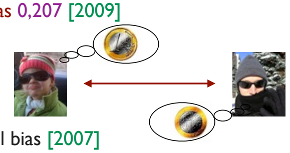
Classically

- Solutions based on harness assumptions of combinatorial problems
- No unconditionally secure solution

Quantumly

- There exists a protocol with maximal bias 0,25 [2001]
- There is no protocol with bias better than 0,207 [2002]
  - There exists a protocol with maximal bias 0,207 [2009]

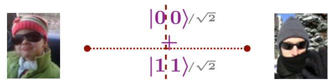
Weak version: election



- Alice wants head
- Bob wants tail
- There exists a protocol with arbitrarily small bias [2007]

Main idea

- Assume Alice & Bob share an EPR state



- Alice & Bob observe their qubit and get bit *a*,*b*

Fact

- *a*=*b* with probability 1
- *a* (resp. *b*) is a uniform random bit

Problems

- Who create the EPR state?
- If Alice does, Bob needs to check that is an EPR state:
  And for instance not $|00\rangle$ → *a*=*b*=0 with probability 1
- In ordert o check the EPR state, Bob needs the 2 qubits
  Then Alice needs to check that Bob gives back the correct qubit

EPR based coin flipping

$|0,0\rangle/\sqrt{2} + |1,1\rangle/\sqrt{2}$

$|0,0\rangle/\sqrt{2} + |1,1\rangle/\sqrt{2}$

Protocol

- Initialization
  - Alice prepares 2 EPR states
  - Alice send the corresponding first qubits to Bob
- Selection
  - Bob select the EPR state that will be use for flipping
  - The other EPR state will be use for checking the honesty of Alice
  - Alice and Bob observe their respective qubit of the *flipping* EPR state
- Checking
  - Alice sends to Bob her qubit of the *checking* EPR state
  - Bob measures the checking EPR state
    - If the measure outcomes is correct, Bob accepts coin
    - Otherwise, Bob declares that Alice has cheated

Theorem

- If both participant are honest, the outcome is a perfect random bit
- If one of the participants is dishonest, the maximal bias is 1/4

Attacks

Goal: increase the probability to get 0

- Bob's attack: measure its 2 qubits, and select the EPR pair giving 0 (if any)
- Alice's attack: $\frac{|00\rangle|\text{EPR state}\rangle}{\sqrt{3}} + \frac{|\text{EPR state}\rangle|00\rangle}{\sqrt{3}}$

NATURE | NEWS

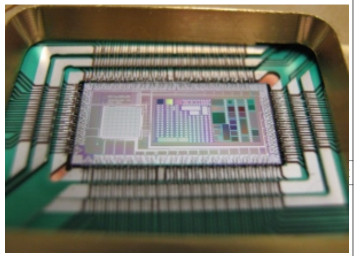
Google and NASA snap up quantum computer

D-Wave machine to work on artificial-intelligence problems.

Nicola Jones

16 May 2013

D-Wave, the small company that sells the world's only commercial quantum computer, has just bagged an impressive new customer: a collaboration between Google, NASA and the non-profit Universities Space Research Association.



The D-Wave Two quantum computer has a 512-qubit processor (pictured) that can do some calculations thousands of times faster than conventional computers.

D-WAVE

The three organizations have joined forces to install a D-Wave Two, the computer company's latest model, in a facility launched by the collaboration — the Quantum Artificial Intelligence Lab at NASA's Ames Research Center in Moffett Field, California. The lab will explore areas such as machine learning — making computers sort and analyse data on the basis of previous experience. This is useful for functions such as language translation, image searches and voice-command recognition. "We actually think quantum machine learning may provide the most creative problem-solving process under the known laws of physics," says a blog post from Google describing the deal.

GETTY IMAGES

NSA seeks to build quantum computer that could crack most types of encryption

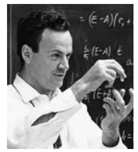
By Steven Rich and Barton Gellman, Published: January 2 E-mail the writers

In room-size metal boxes secure against electromagnetic leaks, the National Security Agency is racing to build a computer that could break nearly every kind of encryption used to protect banking, medical, business and government records around the world.

According to documents provided by former NSA contractor Edward Snowden, the effort to build "a cryptologically useful quantum computer" — a machine exponentially faster than classical computers — is part of a $79.7 million research program titled "Penetrating Hard Targets." Much of the work is hosted under classified contracts at a laboratory in College Park, Md.

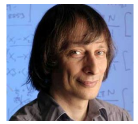
Supercomputer

Feynman'81



- "Can quantum systems be probabilistically simulated by a classical computer? [...] the answer is certainly, No!"

Deutsch'85



- Quantum Turing Machine
- Existence of a universal Turing Machine

Simon, Shor'94

- Quantum algorithms with exponential speedup
- Quantum attack of public-key crypto-systems

n-qubit

- Superposition of all possible values
- 2^n possible values

4 bits can take 2^4=16 values
0000
0001
0010
0011
0100
0101
0110
0111
1000
1001
1010
1011
1100
1101
1110
1111

Parallel computation

Nb of particules in the Universe $\ll 2^{300}$

- In one step, 2^n computations
- But only one outcome can be (randomly) observed!

Strategy

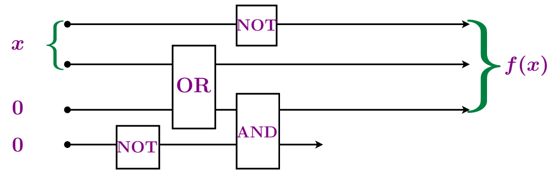
- Combine cleverly those values before measuring them…

Gates

- A gate C is a function on at most **3** qubits
  Example: AND, OR, NOT, ...

Circuit

- A circuit is a sequence of gates $C = C_L \dots C_2 C_1$
  - The size of C is its number L of gates
- C computes a function f if for all input x: $C(x, 0^k) = (f(x), z)$



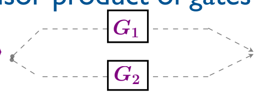
Theorem

- Any function can be computed by a circuit using only NOT, OR, AND gates

Gates $U \in \mathcal{U}(2^k), \quad k = 1, 2, 3$

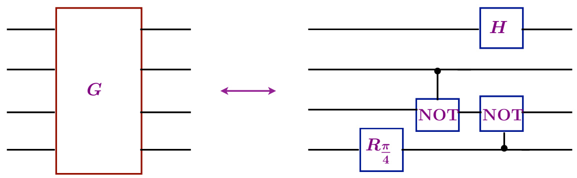
- A quantum gate is a unitary map that acts upon at most **3** qubits

Tensor product of gates

$|\psi_1\rangle|\psi_2\rangle$  $(G_1 \otimes G_2)|\psi_1\rangle|\psi_2\rangle = (G_1|\psi_1\rangle)(G_2|\psi_2\rangle)$

Circuit

- A quantum circuit is a sequence of gates (extended by $\otimes$ Id)



Theorem

- Any unitary can be realized exactly by a circuit
  and approximated using only gates c-NOT and $\sqrt{H}$

Reversible circuit

- A logical circuit is reversible if each gate is reversible
- A reversible circuit is also a quantum circuit
  (since it permutes logical states)

Embedding

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

$f_\oplus : \{0,1\}^{n+m} \to \{0,1\}^{n+m} \qquad f_\oplus(x, y) = (x, y \oplus f(x))$

where: $0 \oplus 1 = 1 \oplus 0 = 1 \qquad 0 \oplus 0 = 1 \oplus 1 = 0$

$u \oplus v = (u_1 \oplus v_1, u_2 \oplus v_2, \dots)$

Theorem

- If a function f can be computed by a logical circuit of size L, then $f_\oplus$ can also be computed by a reversible circuit of size $O(L)$

Universality

- The Toffoli gate (c-c-NOT) is universal for reversible computating
  $T(a, b, c) = (a, b, c \oplus (a \wedge b))$

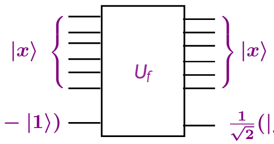
Quantum implementation of classical functions

Normal form

- Function: $f : \{0,1\}^n \to \{0,1\}^m$
- Circuit: $U_f : |x\rangle|0\rangle \mapsto |x\rangle|f(x)\rangle$
  $|x\rangle|y\rangle \mapsto |x\rangle|y \oplus f(x)\rangle$

Alternative form S_f

- Boolean function: $f : \{0,1\}^n \to \{0,1\}$
- Circuit:



$|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ $\quad \frac{1}{\sqrt{2}}(|f(x)\rangle - |1 \oplus f(x)\rangle)$

$= \frac{(-1)^{f(x)}}{\sqrt{2}}(|0\rangle - |1\rangle)$

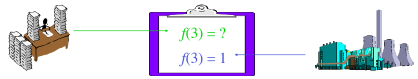
- Conclusion:

$$U_f(|x\rangle \otimes |\psi\rangle) = S_f(|x\rangle) \otimes |\psi\rangle$$

A first quantum algorithm [1992]

Deutsch-Jozsa problem

- Oracle input: $f : \{0,1\}^n \to \{0,1\}$ a black-box function



such that f is either constant or balanced

- Output: 0 iff f is constant

Query complexity

- Deterministic: $2^{n-1}+1$
- Quantum: 1

Special case n=1

- No restriction on f
- Deterministic vs quantum: 2 queries vs 1 query

Quantum solution (n=1)

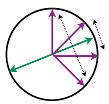
STOP $x \mapsto f(x)$ can be nonreversible!

Reversible implementation of f

$$\alpha|0\rangle + \beta|b\rangle \longrightarrow \boxed{S_f} \longrightarrow (-1)^{f(b)}|b\rangle\, 0\rangle + (-1)^{f(1)}\beta|1\rangle$$

Hadamard gate: half-wave blade at 22,5°

$$|b\rangle \longrightarrow \boxed{H} \longrightarrow \frac{1}{\sqrt{2}}(|0\rangle + (-1)^b|1\rangle)$$



Quantum circuit

$$|0\rangle \longrightarrow \boxed{H} - \boxed{S_f} - \boxed{H} - \boxed{\text{Measure}} \longrightarrow ?$$

Analysis (n=1)

$$|0\rangle \longrightarrow \boxed{H} - \boxed{S_f} - \boxed{H} - \boxed{\text{Measure}} \longrightarrow \begin{cases} f \text{ constant} \to |0\rangle \\ f \text{ balanced} \to |1\rangle \end{cases}$$

Initialization: $|0\rangle$

Parallelization: $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$

Query to f: $\frac{1}{\sqrt{2}}((-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle)$

Interferences: $\frac{1}{2}((-1)^{f(0)}(|0\rangle + |1\rangle) + (-1)^{f(1)}(|0\rangle - |1\rangle))$

Final state: $\frac{1}{2}(((-1)^{f(0)} + (-1)^{f(1)})|0\rangle + ((-1)^{f(0)} - (-1)^{f(1)})|1\rangle)$

General solution for Deutsh-Jozsa

Reversible implementation of f

$$\sum_{x\in\{0,1\}^n} \alpha_x|x\rangle \dashrightarrow \boxed{S_f} \dashrightarrow \sum_{x\in\{0,1\}^n} (-1)^{f(x)}\alpha_x|x\rangle$$

Quantum Fourier transform

$$QFT_n \equiv \begin{array}{c} \dashrightarrow\boxed{H}\dashrightarrow \\ \dashrightarrow\boxed{H}\dashrightarrow \\ \vdots \\ \dashrightarrow\boxed{H}\dashrightarrow \end{array}$$

$$|b\rangle \dashrightarrow \boxed{H} \dashrightarrow \tfrac{1}{\sqrt{2}}(|0\rangle + (-1)^b|1\rangle)$$

$$QFT_n|x\rangle = \frac{1}{2^{n/2}}\sum_y (-1)^{x\cdot y}|y\rangle$$

where $x \cdot y = \sum_i x_i y_i \mod 2$

Quantum circuit

$$|0\rangle \dashrightarrow \boxed{QFT} \dashrightarrow \boxed{S_f} \dashrightarrow \boxed{QFT} \dashrightarrow \boxed{\text{Measure}} \dashrightarrow ?$$

Analysis

$$|0\rangle \dashrightarrow \boxed{QFT} \dashrightarrow \boxed{S_f} \dashrightarrow \boxed{QFT} \dashrightarrow \boxed{\text{Measure}} \begin{cases} \xrightarrow{f \text{ constant}} |00\ldots0\rangle \\ \xrightarrow{f \text{ balanced}} |y\rangle,\ y\neq 00\ldots0 \end{cases}$$

Initialization: $|00\ldots0\rangle$

Parallelization: $\frac{1}{2^{n/2}}\sum_{x\in\{0,1\}^n}|x\rangle$

Query to f: $\frac{1}{2^{n/2}}\sum_{x\in\{0,1\}^n}(-1)^{f(x)}|x\rangle$

Interferences: $\frac{1}{2^n}\sum_{x,y\in\{0,1\}^n}(-1)^{f(x)+x\cdot y}|y\rangle$

Final state: $\left(\frac{1}{2^n}\sum_{x\in\{0,1\}^n}(-1)^{f(x)}\right)|00\ldots0\rangle + \sum_{y\neq 00\ldots0}\alpha_y|y\rangle$

Bernstein-Vazirani

Problem

- Oracle input: $f:\{0,1\}^n \to \{0,1\}$ a black-box function
  such that $f(x) = a\cdot x$
  for some fixed $a \in \{0,1\}^n$
- Output: a

Query complexity

- Randomized: n
  Query $f(0^{i-1}10^{n-i})=a_i$, for $i=1,2,\ldots,n$
- Quantum: 1

Quantum circuit

$$|0\rangle \dashrightarrow \boxed{QFT} \dashrightarrow \boxed{S_f} \dashrightarrow \boxed{QFT} \dashrightarrow \boxed{\text{Measure}} \dashrightarrow |a\rangle$$

Exercice: Analysis

$$|0\rangle \dashrightarrow \boxed{QFT} \dashrightarrow \boxed{S_f} \dashrightarrow \boxed{QFT} \dashrightarrow \boxed{\text{Measure}} \dashrightarrow |a\rangle$$

Initialization:

Parallelization:

Query to f:

Interferences:

Final state:

RSA Challenges

- http://www.rsasecurity.com/rsalabs

Challenge Number	Prize ($US)	Status	Submission Date	Submitter(s)
RSA-576	$10,000	Factored	December 3, 2003	J. Franke et al.
RSA-640	$20,000	Factored	November 2, 2005	F. Bahr et al.
RSA-704	$30,000	Not Factored		
RSA-768	$50,000	Not Factored		
RSA-896	$75,000	Not Factored		
RSA-1024	$100,000	Not Factored		
RSA-1536	$150,000	Not Factored		
RSA-2048	$200,000	Not Factored		

- RSA-640 (193 digits) :

  31074182404900437213507500358885679300373460228427275457201619488232064405180815045563468296717232867824379162728380334154710731085019195485290073377248227835257423864540146917366024776523466093107418240490043721350750035888567930037346022842727545720161948823206440518081504556346829671723286782437916272838
  0334154710731085019195485290073377248227835257423864540146917366024776523466093

  =

  1634733645809253848443133883865090859841783670033092312181110852389333100104508151212118167511579

  x

  1900871281664822113126851573935413975471896789968515493666638539088027103802104498957191261465571

- RSA Algorithm (allows private communication)

  security based on the difficulty of factorizing

One-way functions

- Example: multiplication / factorization
- Bases of modern encryption (Rivest, Shamir, Adleman'77)

RSA challenges (1991-2007)

17 x 19 = ?

667 = ? x ?

- RSA-100, $1,000, 1991
- RSA-640, $20,000, 2005

3107418240490043721350750035888567930037346022842727545720161948823206440518081504556346829671723286782437916272838033415471073108501919548529007337724822783525742386454014691736602477652346609
= ? x ?

Classical reduction

Shor'94

- Factorization can be reduced to period finding (of some arithmetic function)

Quantum tool: Fourier Transform

- FT reveals the period of a signal
- FT is (very) fast on a quantum superposition

3107418240490043721350750035888567930037346022842727545720161948823206440518081504556346829671723
286782437916272838033415471073108501919548529007337724822783525742386454014691736602477652346609
=
1634733645809253848443133883865090859841783670033092312181110852389333100104508151212118167511579
x
1900871281664822113126851573935413975471896789968515493666638539088027103802104498957191261465571

Theorem [Simon-Shor'94]

- Finding the period of *any* function on an abelian group can be done in quantum time poly (log $|G|$)

Order finding

- Input: integers n and a such that $\gcd(a,n)=1$
- Output: the smallest integer $q \neq 0$ such that $a^q = 1 \mod n$
- Reduction to period finding: the period of $x \rightarrow a^x \mod n$ is q

Factorization

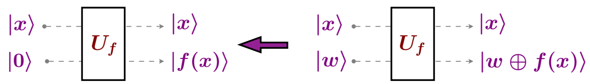
- Input: integer n
- Output: a nontrivial divisor of n

Reduction: Factorization $\leq_R$ Order finding

- Check that $\gcd(a,n)=1$
- Compute the order q of $a \mod n$
- Restart if q is odd or $a^{q/2} \neq -1 \mod n$
- Otherwise $(a^{q/2} - 1)\,(a^{q/2} + 1) = 0 \mod n$
- Return $\gcd(a^{q/2} \pm 1, n)$

Problem

- Oracle input: $f:\{0,1\}^n \to \{0,1\}^n$ a black-box function



such that $\boxed{\exists s \neq 0^n : \forall x \neq y,\ f(x)=f(y) \iff y = x \oplus s}$

- Output: the period s

Complexity

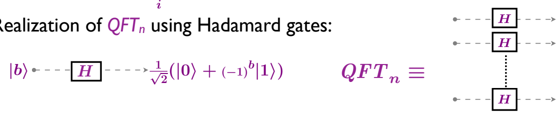
- Randomly: $2^{\Omega(n)}$ queries
- Quantumly: $O(n)$ queries and time $O(n^3)$

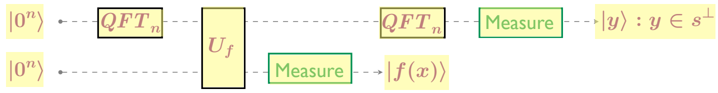
Idea

- Use a Fourier transformation: $\boxed{QFT_n|x\rangle = \frac{1}{2^{n/2}}\sum_y (-1)^{x\cdot y}|y\rangle}$

  where $x \cdot y = \sum_i x_i y_i \mod 2$

- Realization of QFT_n using Hadamard gates:





Initialization: $|0^n\rangle|0^n\rangle$

Parallelization: $\frac{1}{2^{n/2}}\sum_x |x\rangle|0^n\rangle$

Query to f: $\frac{1}{2^{n/2}}\sum_x |x\rangle|f(x)\rangle$

Filter: $\frac{1}{\sqrt{2}}(|x\rangle + |x \oplus s\rangle)|f(x)\rangle$

Partial measure: project to a subspace compatible with the observation

Probability = square norm of the projection

Outcome = renormalization of the projection

Interferences: $\frac{1}{2^{(n+1)/2}}\sum_y ((-1)^{x\cdot y} + (-1)^{(x\oplus s)\cdot y})|y\rangle|f(x)\rangle$

$\frac{1}{2^{(n+1)/2}}\sum_y (-1)^{x\cdot y}(1 + (-1)^{s\cdot y})|y\rangle|f(x)\rangle$

$\frac{1}{2^{(n-1)/2}}\sum_{y:s\cdot y=0} |y\rangle|f(x)\rangle$

Construction of a linear system

- After $n+k$ iterations: $y^1, y^2, \ldots, y^{n+k} \in s^\perp$
- $s \neq 0^n$ is solution of the linear system in t:

$$\begin{cases} y^1 \cdot t = 0 \\ y^2 \cdot t = 0 \\ \vdots \\ y^{n+k} \cdot t = 0 \end{cases} \leftrightarrow \begin{cases} y^1_1 t_1 + y^1_2 t_2 + \ldots + y^1_n t_n = 0 \\ y^2_1 t_1 + y^2_2 t_2 + \ldots + y^2_n t_n = 0 \\ \vdots \\ y^{n+k}_1 t_1 + y^{n+k}_2 t_2 + \ldots + y^{n+k}_n t_n = 0 \end{cases}$$

- The y^i are of rank n-1 with proba $\geq$ 1-1/2^{k+1}
  - System solutions: 0^n and s

Complexity

- Constructing the system: $O(n)$ queries, time $O(n^2)$
- Solving the system: no query, time $O(n^3)$

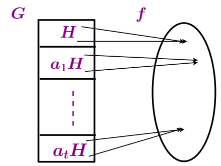
Period Finding(G)

- Oracle input: function f on G such that

  f is *strictly* periodic for some unknown $H \leq G$:

  $f(x) = f(y) \iff y \in xH$

- Output: generator set for H



Examples

- Simon Problem: $G = (\mathbb{Z}_2)^n,\ H = \{0, s\}$
- Factorization : $G = \mathbb{Z},\ H = r\mathbb{Z}$
- Discrete logarithm: $G = \mathbb{Z}^2,\ H = \{(rx, x) : x \in \mathbb{Z}\}$
- Pell's equations: $G = \mathbb{R}$
- Graph Isomorphism: $G = \mathcal{S}_n$

Quantum polynomial time algorithms (in log|G|)

- Abelian groups G: QFT-based algorithm [1995]
- Normal period groups H: QFT-based algorithm [2000]
- Solvable groups G of constant exponent and constant length [2003]
- ...

Hard instances

Shift problem

- Dihedral group $\mathbb{Z}_N \rtimes \mathbb{Z}_2$: sub-exponential time $2^{O(\sqrt{\log N})}$ [2003]

$f(\cdot,0)$

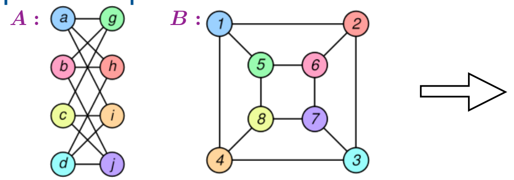
2	5	12	3	9	7	6	10	15	4

shift = -3

$f(\cdot,1)$

3	9	7	6	10	15	4	2	5	12

Graph Isomorphism



A	B
a	1
b	6
c	8
d	3
e	5
f	2
g	4
h	7

- Instance of Period Finding on the symmetric group
  where we just know how to implement *QFT*... [1997]

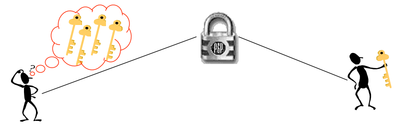
General case

- Polynomial number of queries to *f*, but exponential post-processing time [1999]

Grover search algorithm

Grover problem

- Oracle input : $f : \{0,1\}^n \to \{0,1\}$ such that $\exists! x_0 : f(x_0) = 1$
- Output : x_0
- Constraint : f is a black-box



Query complexity

- Randomized: $\Theta(2^n)$
- Quantum: $\Theta(\sqrt{2^n})$
  $n = 2 \implies 1$ query

Preliminary remarks

Implementation of f

$$\sum_x \alpha_x |x\rangle \dashrightarrow \boxed{S_f} \dashrightarrow \sum_x (-1)^{f(x)} \alpha_x |x\rangle = \sum_x \alpha_x |x\rangle - 2\alpha_{x_0}|x_0\rangle$$

Double Hadamard gate

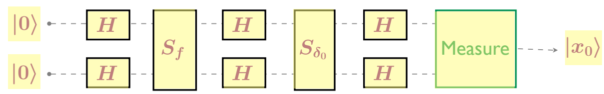
$$|x_1\rangle \dashrightarrow \boxed{H} \dashrightarrow \tfrac{1}{\sqrt{2}}(|0\rangle + (-1)^{x_1}|1\rangle)$$

$$|x_2\rangle \dashrightarrow \boxed{H} \dashrightarrow \tfrac{1}{\sqrt{2}}(|0\rangle + (-1)^{x_2}|1\rangle)$$

$$|x\rangle = |x_1 x_2\rangle \dashrightarrow \boxed{H}\,\boxed{H} \dashrightarrow \tfrac{1}{2}\sum_y (-1)^{x\cdot y}|y\rangle$$

with $x \cdot y = x_1 y_1 + x_2 y_2 \mod 2$

Quantum solution ($n = 2$)



Initialization: $|00\rangle$

Parallelization: $\frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle)$

Query to f: $\frac{1}{2}\sum_x |x\rangle - |x_0\rangle$

Interferences: $|00\rangle - \frac{1}{2}\sum_y (-1)^{x_0\cdot y}|y\rangle$

Query to δ_0: $-|00\rangle - \frac{1}{2}(\sum_y (-1)^{x_0\cdot y}|y\rangle - 2|00\rangle) = -H \otimes H|x_0\rangle$

Final state: $-|x_0\rangle$

Geometrical analysis

Grover operator

$$\cdots \boxed{G} \cdots \overset{\text{def}}{=} \cdots \boxed{S_f} \cdots \boxed{H} \cdots \boxed{-S_{\delta_0}} \cdots \boxed{H} \cdots$$

$\mathrm{Vect}_{\mathbb{R}}(|x_0\rangle, |\mathrm{unif}\rangle)$

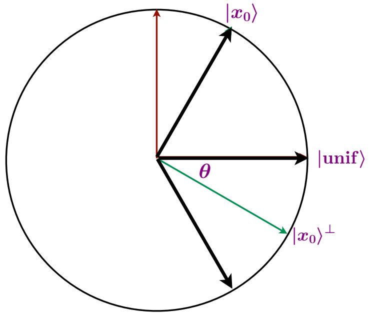
$S_f = -S_{|x_0\rangle} = S_{|x_0\rangle^\perp}$

$-S_{\delta_0} = S_{|00\rangle}$

$H^{\otimes 2} S_{|00\rangle} H^{\otimes 2} = S_{|\mathrm{unif}\rangle}$

$G = S_{|\mathrm{unif}\rangle} S_{|x_0\rangle^\perp} = R_{2\theta}$

with $\sin\theta = \langle \mathrm{unif} | x_0 \rangle = \frac{1}{2}$



After 1 iteration

$|\mathrm{unif}\rangle \mapsto -G|\mathrm{unif}\rangle = -|x_0\rangle$

Geometrical analysis, general case

Grover operator

$$\cdots \boxed{G} \cdots \overset{\text{def}}{=} \cdots \boxed{S_f} \cdots \boxed{H} \cdots \boxed{-S_{\delta_0}} \cdots \boxed{H} \cdots$$

$\mathrm{Vect}_{\mathbb{R}}(|x_0\rangle, |\mathrm{unif}\rangle)$

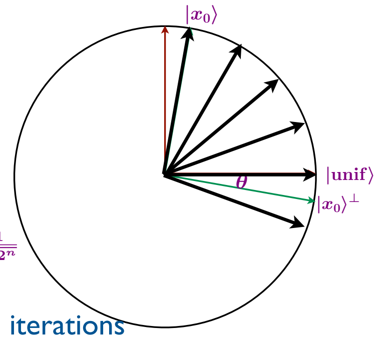
$S_f = -S_{|x_0\rangle} = S_{|x_0\rangle^\perp}$

$-S_{\delta_0} = S_{|00\rangle}$

$H^{\otimes 2} S_{|00\rangle} H^{\otimes 2} = S_{|\mathrm{unif}\rangle}$

$G = S_{|\mathrm{unif}\rangle} S_{|x_0\rangle^\perp} = R_{2\theta}$

with $\sin\theta = \langle \mathrm{unif} | x_0 \rangle = \frac{1}{\sqrt{2^n}}$



After $T = 2/\pi \cdot \sqrt{(2^n)}$ iterations

$|\mathrm{unif}\rangle \mapsto -G^T|\mathrm{unif}\rangle \approx -|x_0\rangle$

How many quantum algorithms exist?

Unstructured problems
- Grover algorithm [1996]

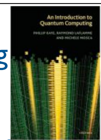
Algebraic problems
- Simon-Shor algorithm [1994]

Well structured problems
- Classical algorithms are optimal!

Problems with few structures
- Quantum walk based algorithms [2003]
  quantum analogy of random walks
- Examples
  - Element Distinctness, Commutativity: $N^{2/3}$ [2004]
  - Triangle Finding: $N^{9/7}$ (lower bound N) [2013]
  - Square Finding: $N^{1.25}$ (lower bound N) [2010]
  - Matrix Multiplication: $N^{5/3}$ (lower bound $N^{3/2}$) [2006]
  - AND-OR Tree evaluation: $\sqrt{N}$ [2007]

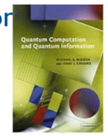
To continue...

An Introduction to Quantum Computing



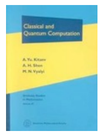
- Authors: Phillip Kaye, Raymond Laflamme, Michele Mosca
- Editor: Oxford University Press

Quantum Computation and Quantum Information



- Authors: Michael A. Nielsen, Isaac L. Chuang
- Editor: Cambridge University Press

Classical and Quantum Computation



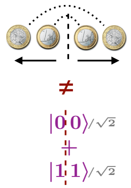
- Authors: A. Yu. Kitaev, A. H. Shen, M. N. Vyalyi
- Editor: American Mathematical Society
- Collection: Graduate Studies in Mathematics

Lecture Notes for Quantum Computation
- Author: John Preskill
- Website: http://www.theory.caltech.edu/~preskill/ph229/

Quantum proofs for classical theorems
- Author: Andrew Drucker, Ronald de Wolf
- Website: http://arxiv.org/abs/0910.3376

Where does the quantum superiority come from?

Entanglement?
- “Classical entanglement” exists: shared randomness
- But quantum entanglement is “stronger”
  - Bell-CHSH inequality and applications



Complex amplitudes?
- No: they can be simulated using only real amplitude

Negative amplitudes?
- Yes: they can induce destructive interferences

Hardness of amplitudes?
- No: amplitudes must be easily computable for being physically realizable

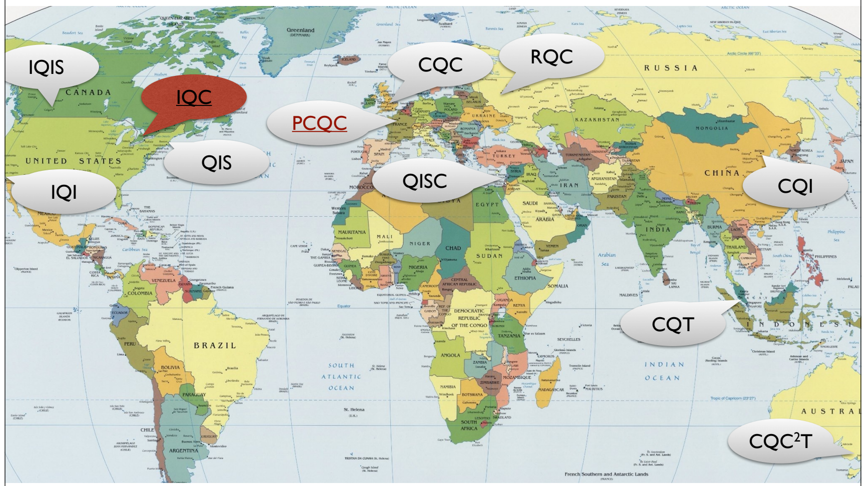
Future

Applications
- Unfalsifiable money, artificial intelligence, …

Quantum computing
- For a better understanding of quantum phenomenon
- New mathematical tool for proving results in classical computing!

Technology
- Computer, intermediate models: boson sampling
- Certification : encryption, random generator, computation

Some quantum centers in the world

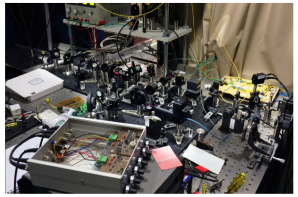


www.pcqc.fr

Welcome

The Paris Centre for Quantum Computing (PCQC) in Paris, France, brings together computer scientists, theoretical & experimental physicists and mathematicians that work in and around Paris. Our goal is to develop novel quantum information and communication technologies and lead the way from a Personal Computer (PC) to a Quantum Computer (QC).

Learn more about PCQC



Highlights

PCQC is official!
PCQC was inaugurated in January 1st, 2014 as a *Federation de Recherche FR3640* between CNRS, Univ Paris Diderot and Telecom ParisTech. The centre has 17 permanent members from the above institutions, as well as from INRIA Paris, Univ Pierre & Marie Curie, CEA, Univ Paris-Sud and Institut d'Optique.

QCRYPT 2014 in Paris
The 4th international Quantum Cryptography QCRYPT conference will be organised in Paris in September 2014.

More news

Openings

PCQC is welcoming applications for a number of PhD and postdoc positions.

In addition, every year, the different French institutions (eg. CNRS, INRIA, Universities) have permanent job openings in Computer Science and in Physics, including quantum information. The application deadline is usually in early January. We recommend interested parties to contact a PCQC member at least two months before the deadline in order to discuss the possibilities and the different application processes.

Learn more about Openings

Events

The PCQC members are organising regularly seminars, workshops, schools or conferences.
You can find more information about upcoming and past events here.
You can also join our mailing list

Join our Mailing List

Name *
First Last

Email *

Submit

cnrs
TELECOM ParisTech
université PARIS DIDEROT PARIS 7