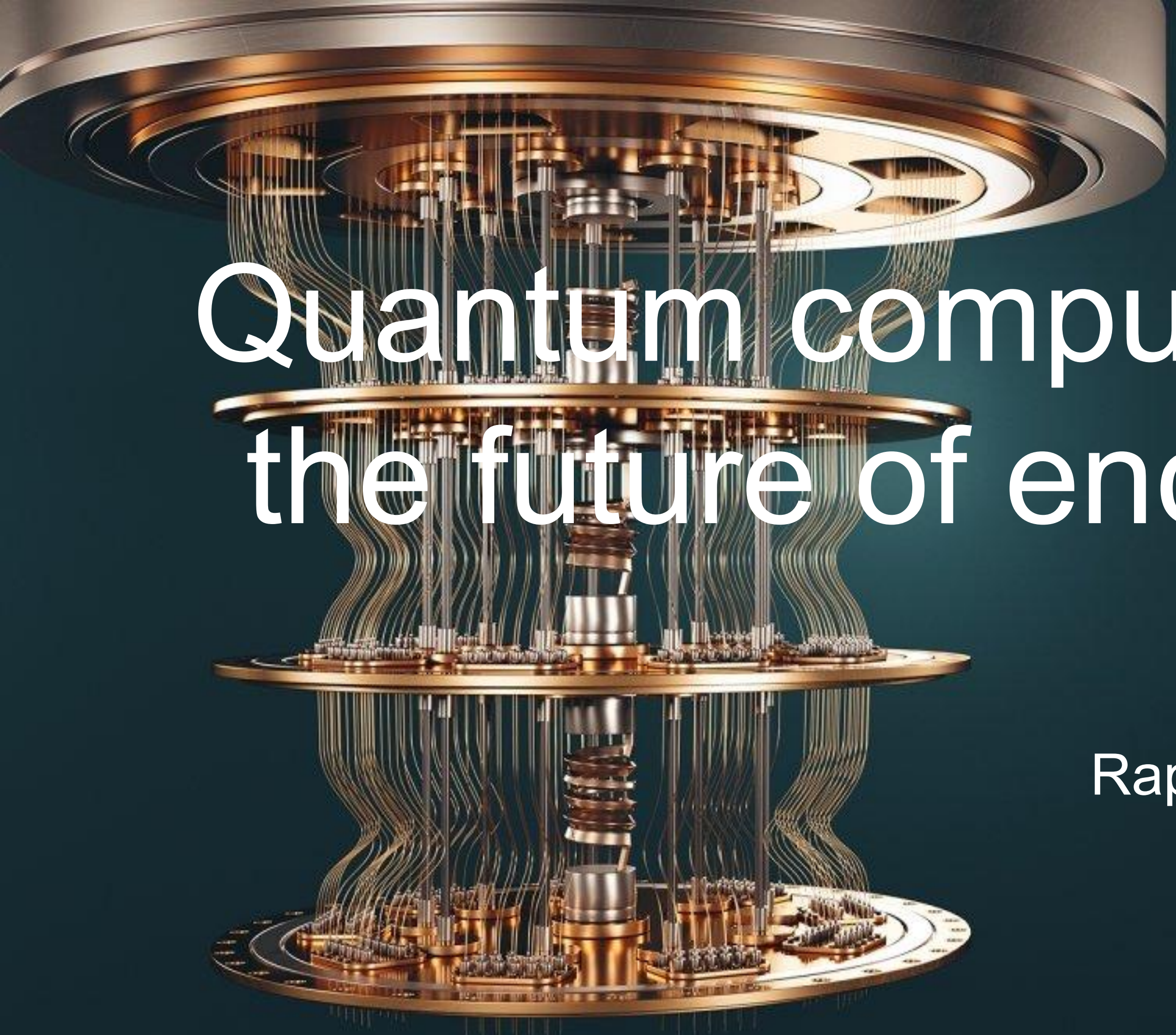
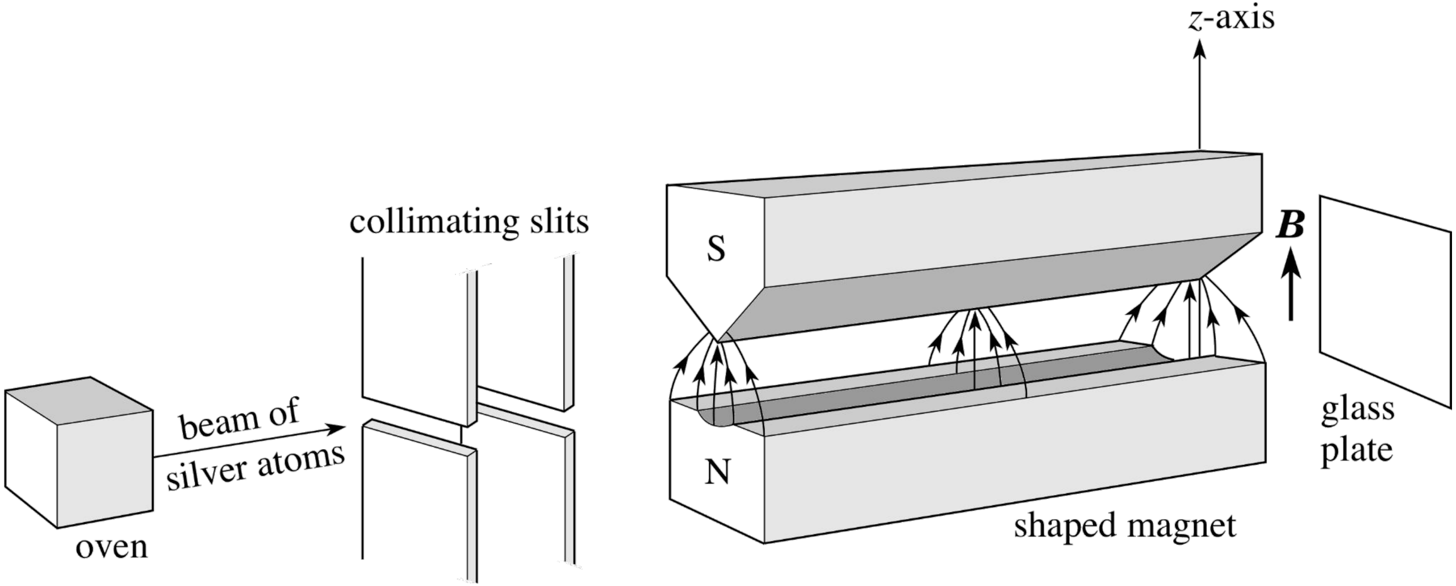


Quantum computers and the future of encryption

Raphaël Maggio-Aprile
Ethan Icet

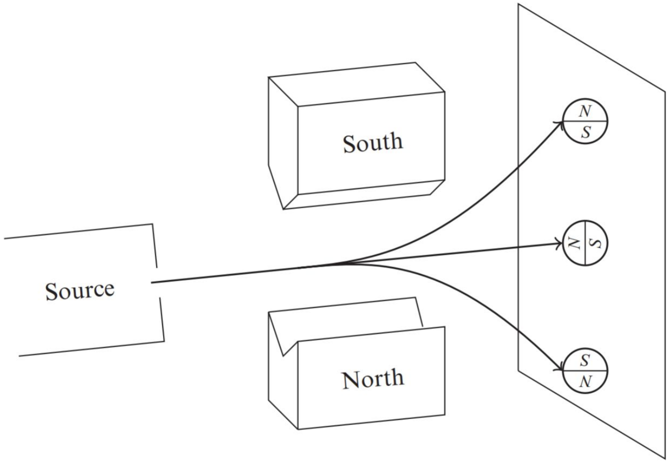
Quantum computer introduction - The Stern-Gerlach experiment

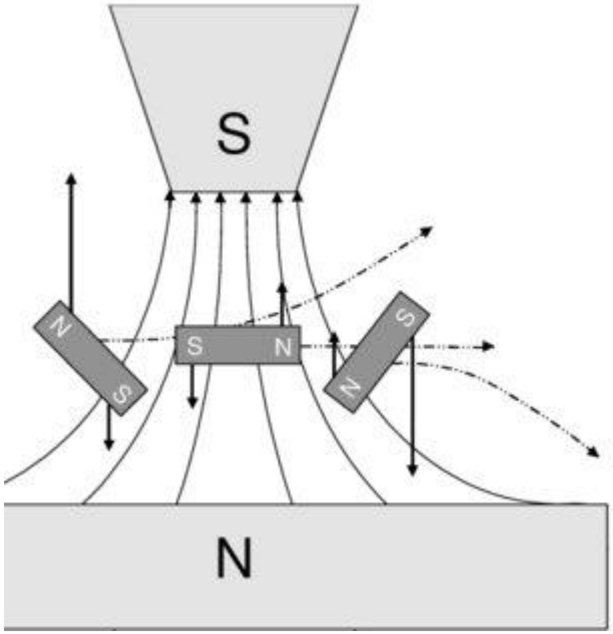
- Beam of silver atoms inside a vertical non-uniform magnetic field
- We observe the final position of the atoms on the glass plate



Quantum computer introduction - The Stern-Gerlach experiment

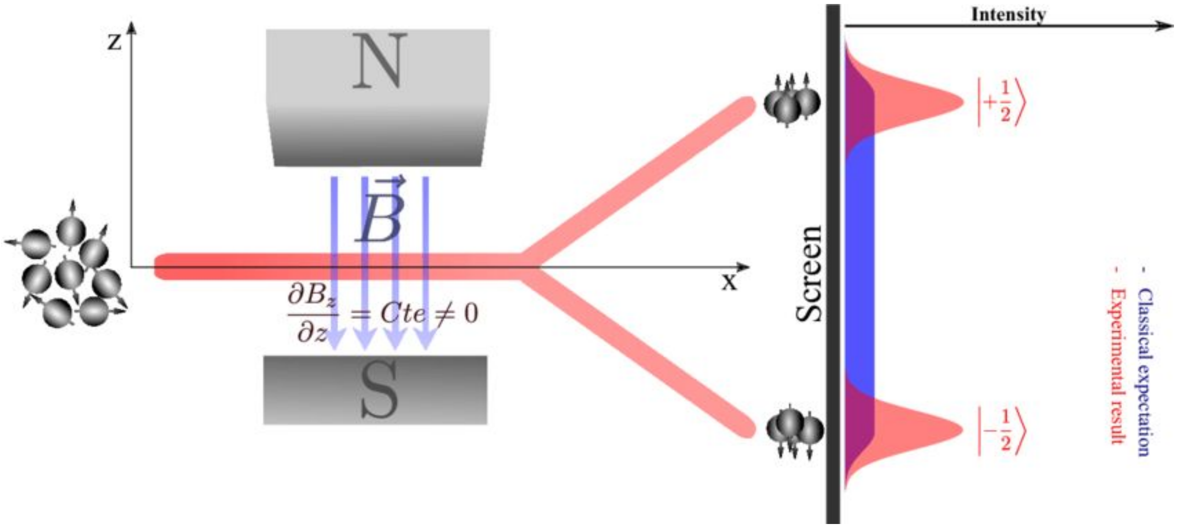
- the trajectory depends on the orientation of the magnet
- with random orientation, the distribution obtained will be continuous and uniform





Quantum computer introduction - The Stern-Gerlach experiment

- Let’s try the experiment with electrons (more exactly with silver atoms)
- we could expect a uniform distribution since the orientation of the atoms are random



Quantum computer introduction - the quantum superposition

- We will note the spin of the electron as being able to take and note these two states $|\uparrow\rangle$, $|\downarrow\rangle$ (bra-ket notation).
- Before its measurement, we say that the state $|\psi\rangle$ of an electron is the superposition of these two states $|\uparrow\rangle$and$|\downarrow\rangle$. Mathematically, this means that $|\psi\rangle$ is a linear combination of the states $|\uparrow\rangle$ and $|\downarrow\rangle$:

$$|\psi\rangle = \alpha \cdot |\uparrow\rangle + \beta \cdot |\downarrow\rangle$$

- where α and β are complex numbers called probability amplitudes such that:

$$|\alpha|^2 + |\beta|^2 = 1$$

Quantum computer introduction - the quantum superposition

- When measure the value of $|\psi\rangle$, we get either $|\uparrow\rangle$ or $|\downarrow\rangle$

- We don't know the value of α and β, but the theory tells us that:

$$\begin{cases} p_{up} = |\alpha|^2 \\ p_{down} = |\beta|^2 \end{cases}$$

  - we can compute those value experimentally !

Quantum computer introduction - from the spin to the qubit

- instead of $|\uparrow\rangle$ and $|\downarrow\rangle$ we will use the kets $|0\rangle$ and $|1\rangle$ as possible measures for our qubits

- The state of a qubit is thus described as this linear combination:

$$\alpha \cdot |0\rangle + \beta \cdot |1\rangle, \alpha, \beta \in \mathbb{C}$$

Quantum computer introduction - more about the bra-ket notation

- a bra can be seen as a row vector and a ket as a column vector:

$$\langle a| = [a_1, \ldots, a_n]$$

$$|b\rangle = \begin{bmatrix} b_1 \\ \vdots \\ b_n \end{bmatrix}$$

- remark: $\langle a| = |a\rangle^\dagger$

Quantum computer introduction - more about the bra-ket notation

- The qubits will often be represented in the following canonical basis:

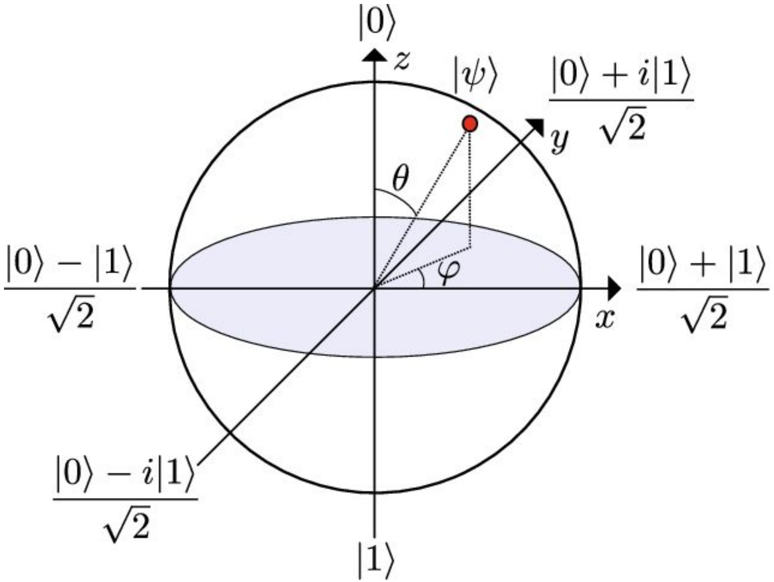
$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$$

$$|1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

- In some cases it is interesting to use several different bases:
  => BB84 protocol / Quantum key distribution

Quantum computer introduction - The Bloch sphere

- We often represent qubits on a the Bloch sphere:



Quantum computer introduction - the tensor product

- We will need to use the tensor product to represent the state of multiple qubits:

$$|a\rangle = \begin{bmatrix} a_1 \\ a_2 \\ a_3 \end{bmatrix}, |b\rangle = \begin{bmatrix} b_1 \\ b_2 \\ b_3 \end{bmatrix}, |a\rangle \otimes |b\rangle = |a\ b\rangle = \begin{bmatrix} a_1 \cdot |b\rangle \\ a_2 \cdot |b\rangle \\ a_3 \cdot |b\rangle \end{bmatrix} = \begin{bmatrix} a_1 b_1 \\ a_1 b_2 \\ a_1 b_3 \\ a_2 b_1 \\ a_2 b_2 \\ a_2 b_3 \\ a_3 b_1 \\ a_3 b_2 \\ a_3 b_3 \end{bmatrix}$$

$$\mathbf{A} \otimes \mathbf{B} = \begin{bmatrix} a_{11}\mathbf{B} & \cdots & a_{1n}\mathbf{B} \\ \vdots & \ddots & \vdots \\ a_{m1}\mathbf{B} & \cdots & a_{mn}\mathbf{B} \end{bmatrix}$$

Quantum computer introduction - the tensor product

- if $\{|0\rangle, |1\rangle\}$ is the canonical basis of $\mathbb{R}^2$ $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$ is the canonical basis of $\mathbb{R}^4$:

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

$$\Rightarrow |00\rangle = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}, |01\rangle = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix}, |10\rangle = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix}, |11\rangle = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix}$$

Quantum computer introduction - Entanglement

- let $|a\rangle$ and $|b\rangle$ be two qubits:

$$|a\rangle = c_0|0\rangle + c_1|1\rangle \text{ et } |b\rangle = d_0|0\rangle + d_1|1\rangle$$

- By using the tensor product, we can represent a system of multiple qubits with one state:

$$|a\rangle \otimes |b\rangle = c_0 d_0|0\rangle \otimes |0\rangle + c_0 d_1|0\rangle \otimes |1\rangle + c_1 d_0|1\rangle \otimes |0\rangle + c_1 d_1|1\rangle \otimes |1\rangle$$
$$\Leftrightarrow$$
$$|ab\rangle = c_0 d_0|00\rangle + c_0 d_1|01\rangle + c_1 d_0|10\rangle + c_1 d_1|11\rangle$$

Quantum computer introduction - Entanglement

$$|a\rangle \otimes |b\rangle = c_0 d_0 |0\rangle \otimes |0\rangle + c_0 d_1 |0\rangle \otimes |1\rangle + c_1 d_0 |1\rangle \otimes |0\rangle + c_1 d_1 |1\rangle \otimes |1\rangle$$

$$\Leftrightarrow$$

$$|ab\rangle = c_0 d_0 |00\rangle + c_0 d_1 |01\rangle + c_1 d_0 |10\rangle + c_1 d_1 |11\rangle$$

- by choosing $r = c_0 d_0, s = c_0 d_1, t = c_1 d_0, u = c_1 d_1$:

$$|ab\rangle = r|00\rangle + s|01\rangle + t|10\rangle + u|11\rangle$$

- where $|r|^2 + |s|^2 + |t|^2 + |u|^2 = 1$ and $ru = st = c_0 d_0 c_1 d_1$

Quantum computer introduction - Entanglement

- Now let's represent the state of our system without imposing $ru = st$:

$$r|00\rangle + s|01\rangle + t|10\rangle + u|11\rangle$$

- We can no longer represent this state is two qubits $|a\rangle$ and $|b\rangle$ if $ru \neq st$.
- This situation is called quantum entanglement.

- You cannot factorize the state of two entangled qubits as $|a\rangle \otimes |b\rangle = |ab\rangle$

Quantum computer introduction - Entanglement : example

- Alice and Bob have two qubits entangled in the following state:

$$\begin{aligned}
&\frac{1}{2}|a_0b_0\rangle + \frac{1}{2}|a_0b_1\rangle + \frac{1}{\sqrt{2}}|a_1b_0\rangle + 0|a_1b_1\rangle \\
&= |a_0\rangle\left(\frac{1}{2}|b_0\rangle + \frac{1}{2}|b_1\rangle\right) + |a_1\rangle\left(\frac{1}{\sqrt{2}}|b_0\rangle + 0|b_1\rangle\right) \\
&= \frac{1}{\sqrt{2}}|a_0\rangle\left(\frac{1}{\sqrt{2}}|b_0\rangle + \frac{1}{\sqrt{2}}|b_1\rangle\right) + \frac{1}{\sqrt{2}}|a_1\rangle\left(1|b_0\rangle + 0|b_1\rangle\right)
\end{aligned}$$

- where $\{|a_0\rangle, |a_1\rangle\}$ is the basis of Alice and $\{|b_0\rangle, |b_1\rangle\}$ the basis of Bob

Quantum computer introduction - Entanglement : example

$$\frac{1}{\sqrt{2}}|a_0\rangle\left(\frac{1}{\sqrt{2}}|b_0\rangle+\frac{1}{\sqrt{2}}|b_1\rangle\right)+\frac{1}{\sqrt{2}}|a_1\rangle\left(1|b_0\rangle+0|b_1\rangle\right)$$

- what happens to the qubit of bob if Alice measures a 0 ($|a_0\rangle$) ?

- The new state of the system will be:

$$|a_0\rangle\left(\frac{1}{\sqrt{2}}|b_0\rangle+\frac{1}{\sqrt{2}}|b_1\rangle\right)$$

- And if Alice measures a 1 ($|a_1\rangle$) ?

- Bob will have a 100% chance of measuring 0 ($|b_0\rangle$) !

=> The measure of Alice affects the measure of Bob !

Quantum computer introduction - Quantum gates: the CNOT gate

- takes 2 qubits as input

$$CNOT(r|00\rangle + s|01\rangle + t|10\rangle + u|11\rangle) = r|00\rangle + s|01\rangle + u|10\rangle + t|11\rangle$$

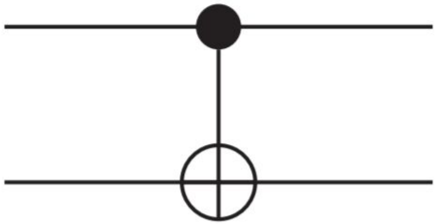
- in matrix notation:

$$CNOT(|\psi\rangle) = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} |\psi\rangle$$

- useful to entangle qubits:
- $\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$ and $|0\rangle$ => $\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$

CNOT

Input	Output
$\|00\rangle$	$\|00\rangle$
$\|01\rangle$	$\|01\rangle$
$\|10\rangle$	$\|11\rangle$
$\|11\rangle$	$\|10\rangle$



Quantum computer introduction - Quantum gates: Hadamard gate

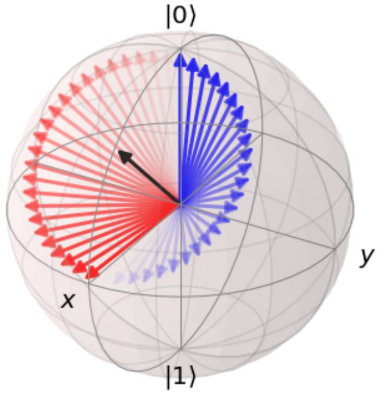
- takes 1 qubits as input
- in matrix notation:

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

$$H^2 = I$$

- useful to create a quantum superposition:

$$H(|0\rangle) = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$$
$$H(|1\rangle) = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$$

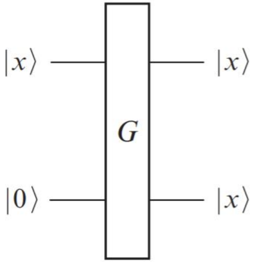


Quantum computer introduction - Quantum gates: more gates

- All the gates are unitary matrices $U^\dagger U = UU^\dagger = I$ of size $2^n \times 2^n$ where n is the number of input qubits

  => All the gates and all the quantum circuits are **reversible**

- Non cloning theorem:
  - we cannot create a copy gate



Operator	Gate(s)	Matrix
Pauli-X (X)	$\boxed{\mathbf{X}}$	$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$
Pauli-Y (Y)	$\boxed{\mathbf{Y}}$	$\begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$
Pauli-Z (Z)	$\boxed{\mathbf{Z}}$	$\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$
Hadamard (H)	$\boxed{\mathbf{H}}$	$\frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$
Phase (S, P)	$\boxed{\mathbf{S}}$	$\begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}$
$\pi/8$ (T)	$\boxed{\mathbf{T}}$	$\begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix}$
Controlled Not (CNOT, CX)		$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$
Controlled Z (CZ)	$\boxed{\mathbf{Z}}$	$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix}$
SWAP		$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$
Toffoli (CCNOT, CCX, TOFF)		$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}$

Quantum computer introduction - Quantum circuits / bruteforce

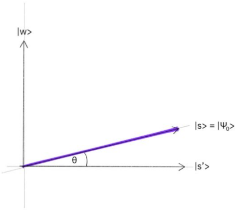
- We have a circuit who encrypts a constant plaintext into a cipher with an input key of n bits
- we have $N = 2^n$ possible keys
- we will put an hadamard gate in front of each input. The initial state will be:

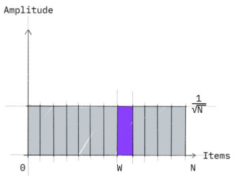
$$\frac{1}{\sqrt{2^n}} \sum_{x=1}^{2^n} |x\rangle = \frac{1}{\sqrt{N}} \sum_{x=1}^{N} |x\rangle$$

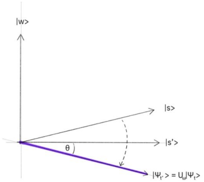
- We will get a random key and a random cipher at each iteration
- Can we increase the amplitude of the solution ?

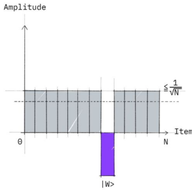
Quantum computer introduction - Groover algorithm

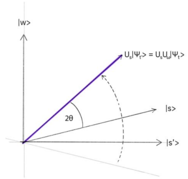
- main idea:
    - we build an oracle that reverse the amplitude of the solution
    - A new transformation will then amplify the negative amplitudes and reduce the positive amplitudes
    - And then the amplitude of the solution is reversed again

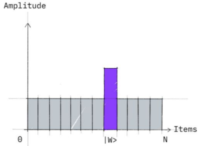


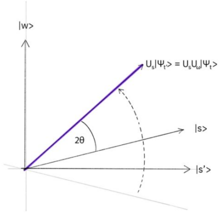


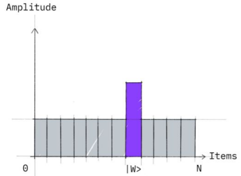


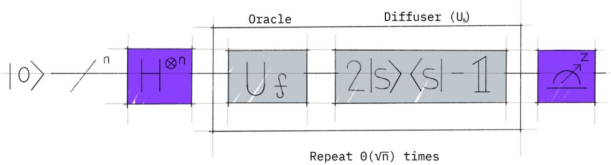












Quantum computer introduction - Groover algorithm

- The optimal value in reached in exactly $\frac{\pi}{4}\sqrt{N}$ steps
- $\frac{\pi}{4}\sqrt{\frac{N}{M}}$ if there is M solutions
- brute force complexity is $\mathcal{O}(\sqrt{N})$ with a quantum computer !

- with our brute force problem:
  - we can find the key in $\mathcal{O}(\sqrt{2^n}) = \mathcal{O}(2^{n/2})$

=> we need to double the size of the key if we want the same complexity

Quantum computer introduction - Why cryptography will break

- Symmetric : Grover’s algorithm
  - Search in a function of domain size N and M solutions
  - $O(N/M) \Rightarrow O(\mathrm{sqrt}(N/M))$
- Asymmetric : Shor’s algorithm
  - Factorization of a number $N \sim 10^d$
  - $O(e^{d\char`^(1/3)}) \Rightarrow O(d^3)$

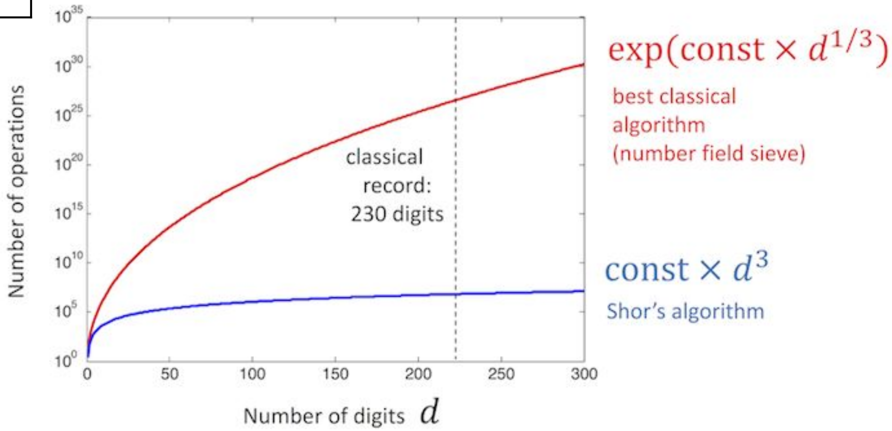
Quantum computer introduction - Shor's algorithm

	Shor's algorithm (Quantum computer)	General number field sieve (Classical computer)
N	$O\left((\log N)^2(\log\log N)(\log\log\log N)\right)$	$O\left(e^{1.9(\log N)^{1/3}(\log\log N)^{2/3}}\right)$
2^{1024}	~ $6 * 10^6$	~ $6 * 10^{25}$
2^{4096}	~ $133 * 10^6$	~ $3 * 10^{46}$

Space Complexity : ~$2 \log_2(N) + 2$ qubits

$2^{1024} \Rightarrow 2050$ qubits

$2^{4096} \Rightarrow 8196$ qubits



Quantum computer introduction - Shor's algorithm

- Pick a random number 1 < g < N
- We want to find the period p being the smallest integer such as

$$g^{x+p}\, mod\, N = g^x\, mod\, N \iff g^p - 1\, mod\, N = 0$$
$$\iff \left(g^{p/2} + 1\right)\left(g^{p/2} - 1\right) = m \cdot N$$

- Then we can find N factors by computing the gcd of N and $g^{p/2} \pm 1$ with euclid's algorithm

- The following conditions must be verified otherwise we pick a new random g
  - p needs to be even otherwise solution are not integer
  - $g^{p/2} \pm 1$ should not be a multiple of N

Quantum computer introduction - Shor's algorithm

314191 = ? * ?

We take a random guess $1 \leq g \leq 314191$, g = 127

g isn't a solution

We want $127^{p/2} \pm 1$, so we have to find p such as 127^p = m * 314191 + 1

$$|x\rangle \Rightarrow |\, x,\, g^x\rangle \Rightarrow |\, x,\, g^x\, mod\, n\rangle$$

$$|1\rangle + |\, 2\rangle + |\, 3\rangle \cdots \Rightarrow \ |\, 1,\, 127\rangle + |\, 2,\, 16129\rangle + |\, 3,\, 163237\rangle \ldots$$

We collapse the output and find r = 686. So the quantum states left are

$$|x + k \cdot p,\, r\rangle$$

$$|x,\, 686\rangle \,+\, |\, x \,+\, p,\, 686\rangle \,+\, |\, x \,+\, 2p,\, 686\rangle \ldots$$

We use the Quantum Fourier Transform

$$|x + k \cdot p\rangle \Rightarrow |\, k/p\rangle$$

We repeat this operation multiple times to find 1/p and so p. Here p = 17388 (it's even !)

we get $127^{8694} \pm 1$

FInally gcd(314191, 127^{8694} + 1) = 829, gcd(314191, 127^{8694} - 1) = 379, indeed 314191 = 829 * 379

Quantum computer introduction - Post-Quantum Cryptography Standardization

- Post-Quantum Cryptography Standardization by Nist
  - 1994: First workshop on quantum computing (by NIST)
  - April 2016: NIST published report about RSA being insecure by 2030
  - December 2016: Announcement at PQCrypto
  - 2017: Deadline for submissions.
  - 2019: Round 2
  - 2020: Round 3
  - ?: Round 4
  - 2024: First standardization documents

1976: Quantum information theory
1980: First description of quantum mechanical model of a computer
1984: BB84 (Quantum key distribution scheme)
1985: Description of Universal quantum computer (~ Universal Turing Machine)
1988: Proposition of a physical realization : photons to transmit qubits and atoms to perform two-qubit operations
1994: Shor's algorithm
1996: Grover's algorithm
2001: Factorization of 15 using Shor's algorithm
2018: 72-qubit quantum chip
2019: 53 qubits computer by IBM
2019: Google's quantum computer achieves quantum supremacy
2019: Factorization of 1,099,551,473,989 using quantum annealing

Quantum computer introduction - Post-Quantum Cryptography Standardization

Type

- Lattice
  - Find the closest points in fields defined with a good and bad base
  - Find added errors in an over-determined system of equation
- Code-based
  - good error-correcting is secret a bad is generated from the good and is the public key (ex: Goppa, reed-salomon)
- Hash-based
  - Uses a merkle tree for One-time signature schemes
- Multivariate
  - Solve systems of multivariate equations
- Braid group
  - See knot theory
- Supersingular elliptic curve isogeny
  - Combine isogeny generated from private elliptic curves
- …

Finalists [edit]

Type	PKE/KEM	Signature
Lattice[a]	• CRYSTALS-KYBER • NTRU • SABER	• CRYSTALS-DILITHIUM • FALCON
Code-based	• Classic McEliece	
Multivariate		• Rainbow

Alternate candidates [edit]

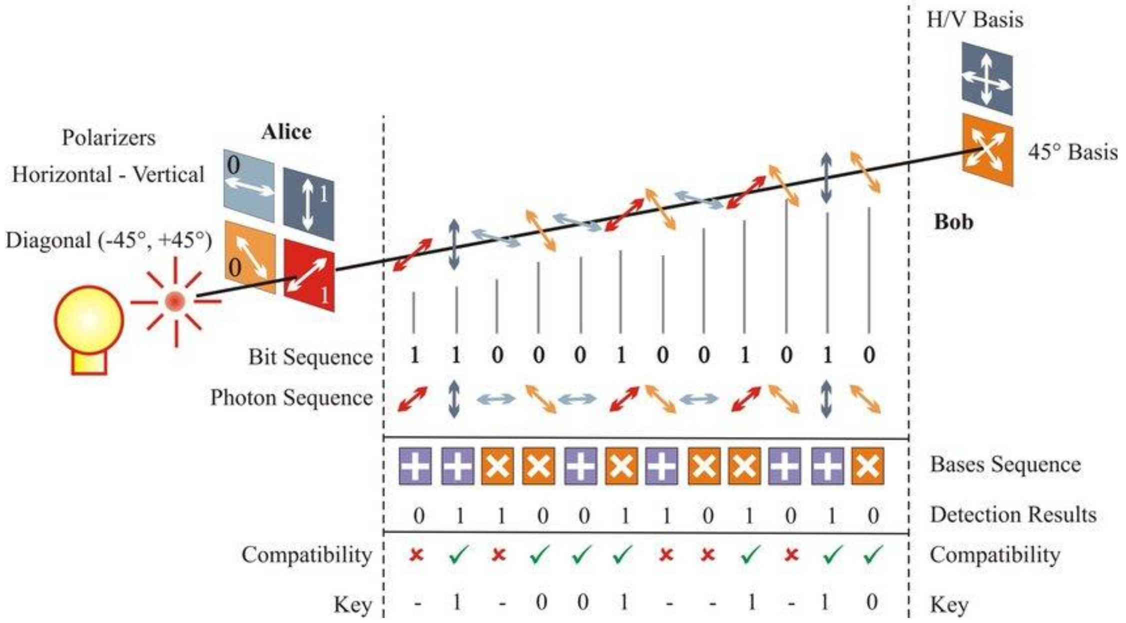
Type	PKE/KEM	Signature
Lattice	• FrodoKEM • NTRU Prime	
Code-based	• BIKE • HQC	
Hash-based		• SPHINCS+
Multivariate		• GeMSS
Supersingular elliptic curve isogeny	• SIKE	
Zero-knowledge proofs		• Picnic

Quantum computer introduction - BB84

- Quantum key distribution
    - BB84

Communication over an authenticated public channel.

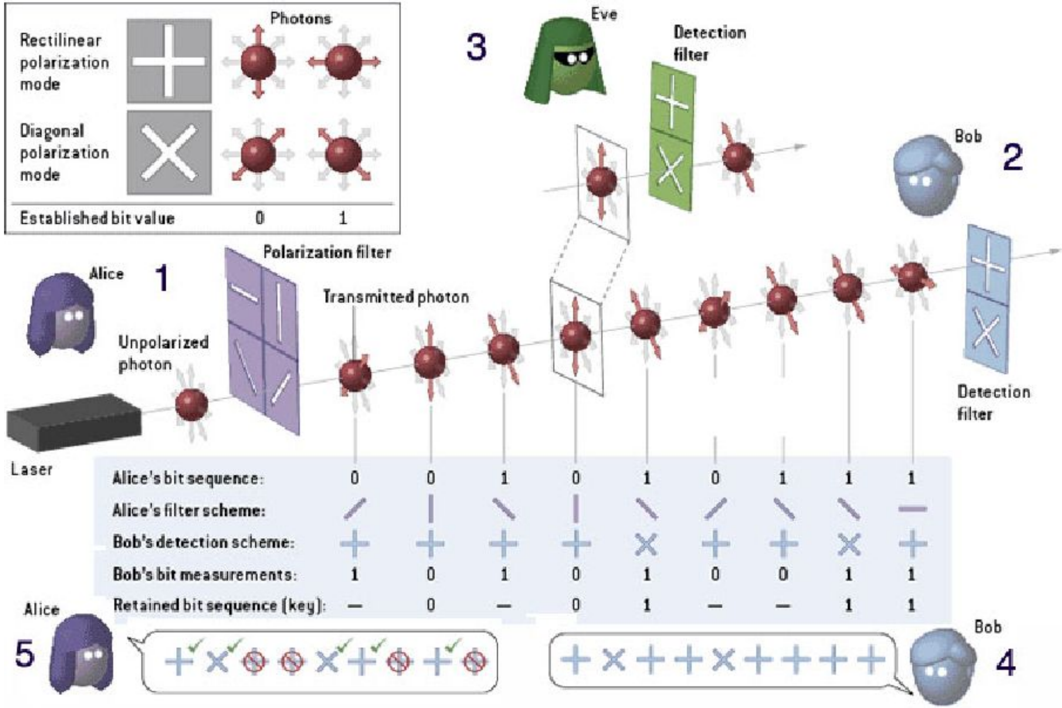
No cloning theorem



Quantum computer introduction - BB84

1. Alice chooses a random sequence of bits encoded in random basis.
2. Bob chooses random basis for the reception.
3. Eve has to guess the original basis to retransmit.
4. Bob shares his configuration
5. Alice answers where they matched
6. Alice and Bob disclose a part of their key for comparison.

Eve has 75% chance to have retrieved each bit. If the disclosed sequences are identical they keep the rest to create a key, otherwise around 25% should differ because of the attacker



Thanks for listening

sources

1. Grover's Algorithm [Internet]. [cited 2021 Nov 10]. Available from: https://qiskit.org/textbook/ch-algorithms/grover.html

2. Josh's Channel. How Quantum Computers Work [Internet]. 2021 [cited 2021 Nov 10]. Available from: https://www.youtube.com/watch?v=3RGEYYJmMtU

3. Microsoft Research. Quantum Computing for Computer Scientists [Internet]. 2018 [cited 2021 Nov 10]. Available from: https://www.youtube.com/watch?v=F_Riqjdh2oM

4. Bernhardt C. Quantum Computing for Everyone. The MIT Press; 2019. 216 p.