NOKIA Bell Labs

Quantum Cryptography: Quantum Key Distribution (QKD) protocols

Ludovic Noirie (Nokia Bell Labs)

LINCS reading group on "network theory" 2022/10/19

Outline

1. Qubits
2. Bell pairs
3. First protocol for QKD: BB84
4. QKD protocol using Bell's inequalities: E91
5. Today's and future QKD systems

References

Main Articles on quantum cryptography

[**BB84**] Charles H. Bennett and Gilles Brassard, "Quantum cryptography: Public key distribution and coin tossing," in Proceedings of the International Conference on Computers, Systems and Signal Processing, pp. 175-179, Bangalore, 1984, https://arxiv.org/abs/2003.06557, republished in Theoretical Computer Science, vol. 560, 2014, pp. 7–11, https://dx.doi.org/10.1016/j.tcs.2014.05.025.

[**BB89**] Charles H. Bennett and Gilles Brassard, "The dawn of a new era for quantum cryptography: the experimental prototype is working!" ACM SIGACT News, Vol. 20, no. 4, pp 78–80, 1989, https://doi.org/10.1145/74074.74087.

[**E91**] Artur K. Ekert, "Quantum cryptography based on Bell's theorem," Physical Review Letters, Vol. 67, no. 6, pp. 661-663, 1991, https://dx.doi.org/10.1103/PhysRevLett.67.661.

[**BBE92**] Charles H. Bennett, Gilles Brassard and Artur K. Ekert, "Quantum Cryptography," Scientific American, vol. 267, no. 4, 1992, pp. 50–57, http://www.jstor.org/stable/24939253.

Articles on Bell pairs of entangled qubits/photons and Bell's inequality violation

[**EPR1935**] The "EPR" paper (1935): "Can Quantum-Mechanical Description of Physical Reality be Considered Complete?" by Einstein, Podolski and Rosen, https://doi.org/10.1103%2FPhysRev.47.777.

[**Bell1964**] John Bell's original paper on his inequalities, "On the Einstein Podolsky Rosen paradox," Physics, Vol. 1, No. 3, pp. 195-200, 1964, https://journals.aps.org/ppf/pdf/10.1103/PhysicsPhysiqueFizika.1.195.

[**CHSH1969**] John F. Clauser, Michael A. Horne, Abner Shimony, and Richard A. Holt, "Proposed Experiment to Test Local Hidden-Variable Theories," Physical Review Letters, Vol. 23, no. 15, pp. 880-884, 1969, https://dx.doi.org/10.1103/PhysRevLett.23.880.

[**Asp1976**] Alain Aspect, "Proposed experiment to test the nonseparability of quantum mechanics," Physical Review D, Vol. 14, no. 8, pp. 1944-1951, 1976, https://link.aps.org/doi/10.1103/PhysRevD.14.1944.

[**AGR1981**] Alain Aspect, Philippe Grangier and Gérard Roger, "Experimental Tests of Realistic Local Theories via Bell's Theorem," Physical Review Letters, Vol. 47, no. 7, pp. 460-463, 1981, https://dx.doi.org/10.1103/PhysRevLett.47.460.

[**AGR1982**] Alain Aspect, Philippe Grangier and Gérard Roger, "Experimental Realization of Einstein-Podolsky-Rosen-Bohm Gedankenexperiment: A New Violation of Bell's Inequalities," Physical Review Letters, Vol. 49, no. 2, pp. 91-94, 1982, https://dx.doi.org/10.1103/PhysRevLett.49.91.

[**ADR1982**] Alain Aspect, Jean Dalibard and Gérard Roger, "Experimental Test of Bell Inequalities Using Time-Varying Analyzers," Physical Review Letters Vol. 49, no. 25, pp. 1804-1807; 1982, https://dx.doi.org/10.1103/PhysRevLett.49.1804.

[**Nobel2022**] The Nobel Prize in Physics 2022, NobelPrize.org, Nobel Prize Outreach AB 2022, Tue. 11 Oct 2022, https://www.nobelprize.org/prizes/physics/2022/summary/.

Other articles on quantum physics

[**Woo1981**] William K. Wootters, "Statistical Distance and Hilbert Space," Physical Review D, Vol. 23, no. 2, pp. 357-362, 1981, https://link.aps.org/doi/10.1103/PhysRevD.23.357.

[**WZ1982**] William K. Wootters and Zurek Wojciech, "A Single Quantum Cannot be Cloned," Nature, Vol. 299, pp. 802-803, 1982. https://dx.doi.org/10.1038/299802a0.

[**BBC+1993**] Charles Bennet, Gilles Brassard, Claude Crépeau, Richard Jozsa, Asher Peres and William K. Wootters, "Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels," Physical Review Letters, Vol. 70, no. 13, pp. 1895-1899, 1993, https://dx.doi.org/10.1103/PhysRevLett.70.1895.

[**Rov1996**] Carlo Rovelli, "Relational quantum mechanics," International Journal of Theoretical Physics, Vol. 35, pp. 1637–1678, 1996, https://doi.org/10.1007/BF02302261, https://arxiv.org/abs/quant-ph/9609002.

[**Rov2021**] Carlo Rovelli, "The Relational Interpretation of Quantum Physics," to appear in the "Oxford Handbook of the History of Interpretation of Quantum Physics," https://arxiv.org/abs/2109.09170.

Wikipedia pages

https://en.wikipedia.org/wiki/Quantum_mechanics#Mathematical_formulation
https://en.wikipedia.org/wiki/Qubit
https://en.wikipedia.org/wiki/Bloch_sphere
https://en.wikipedia.org/wiki/Bell_state
https://en.wikipedia.org/wiki/Quantum_key_distribution
https://en.wikipedia.org/wiki/BB84
https://en.wikipedia.org/wiki/No-cloning_theorem
https://en.wikipedia.org/wiki/EPR_paradox
https://en.wikipedia.org/wiki/Bell's_theorem
https://en.wikipedia.org/wiki/Aspect%27s_experiment
https://en.wikipedia.org/wiki/Wigner%27s_theorem https://en.wikipedia.org/wiki/Relational_quantum_mechanics

LINCS talks on related topics:

- Filippo Miatto's seminar on "The real fuss with quantum mechanics", about Bell's inequalities (2017/12/06): https://www.lincs.fr/events/the-real-fuss-with-quantum-mechanics/.
- Ludovic Noirie's reading group presentation on "Quantum Internet", QKD being an application case (2020/09/09): https://www.lincs.fr/events/quantum-internet/.
- Don Towsley's seminar on "The Quantum Internet: Recent Advances and Challenges" (2022/02/02): https://www.lincs.fr/events/the-quantum-internet-recent-advances-and-challenges/.
- This reading group presentation on QKD (2022/10/19): https://www.lincs.fr/events/quantum-cryptography-quantum-key-distribution-protocols/.
- Michel Barbeau's seminar on "Work Memory Requirements in Error Susceptible Quantum Networks" (2022/10/26): https://www.lincs.fr/events/work-memory-requirements-in-error-susceptible-quantum-networks/.

Other videos:

Some videos on **"ScienceEtonnante"** YouTube channel & **"Science Étonnante"** website (in French):

1. Quantum communication and BB84 protocol: "La communication quantique et le protocole BB84" (14/12/2019) https://scienceetonnante.com/2019/02/14/bb84/
2. Bell's inequalities and Alain Aspect experiments: "Les inégalités de Bell et les expériences d'Alain Aspect" (23/10/2020) https://scienceetonnante.com/2020/10/23/bell-aspect/
3. A Youtube video of the interview of Alain Aspect by David Louapre: "Alain Aspect : interview complète" (06/11/2020) https://scienceetonnante.com/2020/11/06/alain-aspect-interview-complete/

1. Qubits

1. Qubits as $\frac{1}{2}$-spin particles and the Bloch sphere
2. Qubits as polarized photons and the Poincaré sphere
3. Measurement of a non-entangled qubit
4. Time evolution of a non-entangled qubit
5. Modifying and measuring photonic qubits in practice

1.1. Qubits as $\frac{1}{2}$-spin particles and the Bloch sphere

1.1.1. $\frac{1}{2}$-spin particles are qubits

$\frac{1}{2}$-spin can be viewed as an intrinsic angular momentum (angular momentum = rotation speed of a spinning object) in some oriented axis in our 3D space with the constant value $\frac{\hbar}{2}$.

For a given axis, spin value $-\frac{\hbar}{2}$ in a given orientation is equivalent to $+\frac{\hbar}{2}$ in the opposite orientation.

1.1.2. Qubit states and the Bloch sphere

The qubit (pure) state can be represented by a vector $\vec{s} = \sin(\theta)\cos(\varphi) \cdot \vec{x} + \sin(\theta)\sin(\varphi) \cdot \vec{y} + \cos(\theta) \cdot \vec{z}$ on the unit sphere in 3D, which is called the Bloch sphere.

The orthogonal state (= opposite orientation state for qubit) $|s^\perp\rangle$ in the Hilbert space $\mathbb{C}^2$, for which $\langle s^\perp | s \rangle = 0$, i.e., $|s^\perp\rangle \perp |s\rangle$, is represented by the opposite vector $\vec{s}^\perp = -\vec{s}$ in the Bloch sphere.

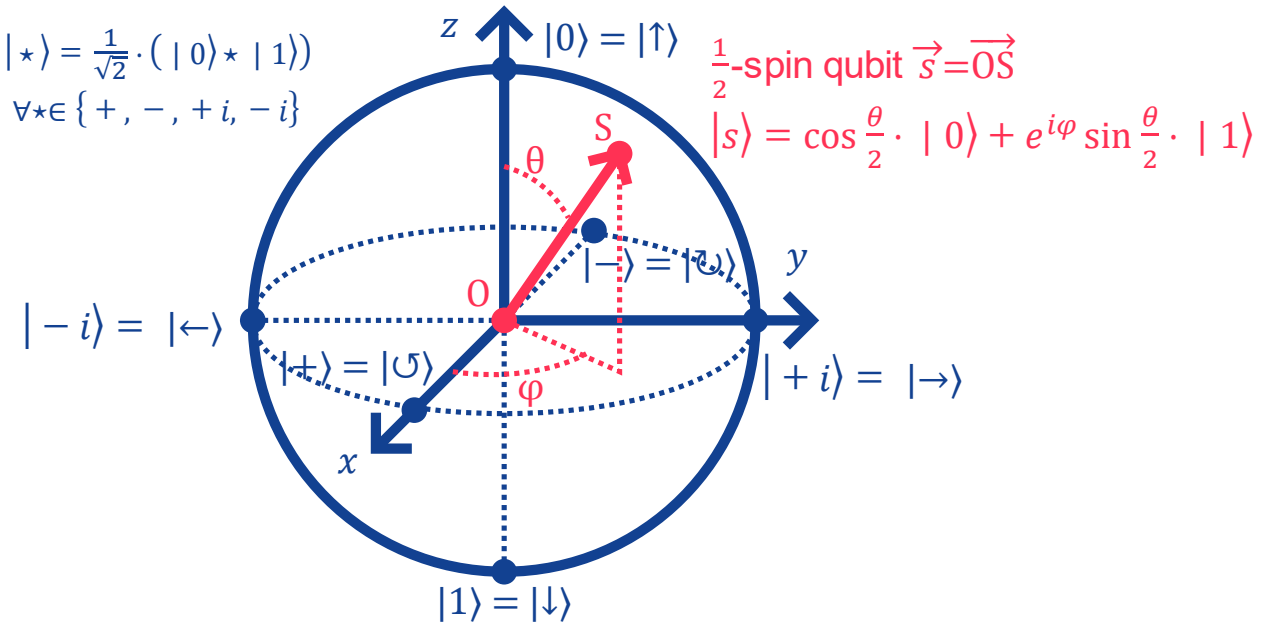
Convention: for any orientation $\vec{s}$, bit value 0 corresponds to $+\frac{\hbar}{2}$, 1 corresponds to $-\frac{\hbar}{2}$.

1-to-1 correspondence with unitary vectors of Hilbert space $\mathbb{C}^2$ in quantum physics:
$|s\rangle = \left(e^{i\eta}\right) \cdot \left(\cos(\theta/2) \cdot |0\rangle + \sin(\theta/2) e^{i\varphi} \cdot |1\rangle\right)$, where $e^{i\eta}$ is the arbitrary phase factor.

Arbitrary phase factor and normalization to 1 $\Rightarrow$ Qubit quantum states of qubits are rays in the Hilbert space $\mathbb{C}^2$, i.e., elements of the projective space $\mathrm{P}\mathbb{C}^2 = \mathbb{C}^2/_{\mathbb{C}\setminus\{0\}}$.

The projective space $\mathrm{P}\mathbb{C}^2$ equipped with its angular distance θ' in the complex vector space $\mathbb{C}^2$ multiplied by 2 is isometric to the Bloch sphere equiped with the angular distance θ in the real vector space $\mathbb{R}^3$: we have $\theta = 2\theta'$.

1.1.3. Bloch sphere graphical representation of qubits



1.2. Qubits as polarized photons and the Poincaré sphere

1.2.1. Photons are also qubits

Photons are 1-spin particles and should have 3 possible spin outcome states when measured on a given axis: $+\hbar$, 0 or $-\hbar$, i.e., -1, 0 or 1.

Because of relativistic effect at light speed c, spin 0 is forbidden.

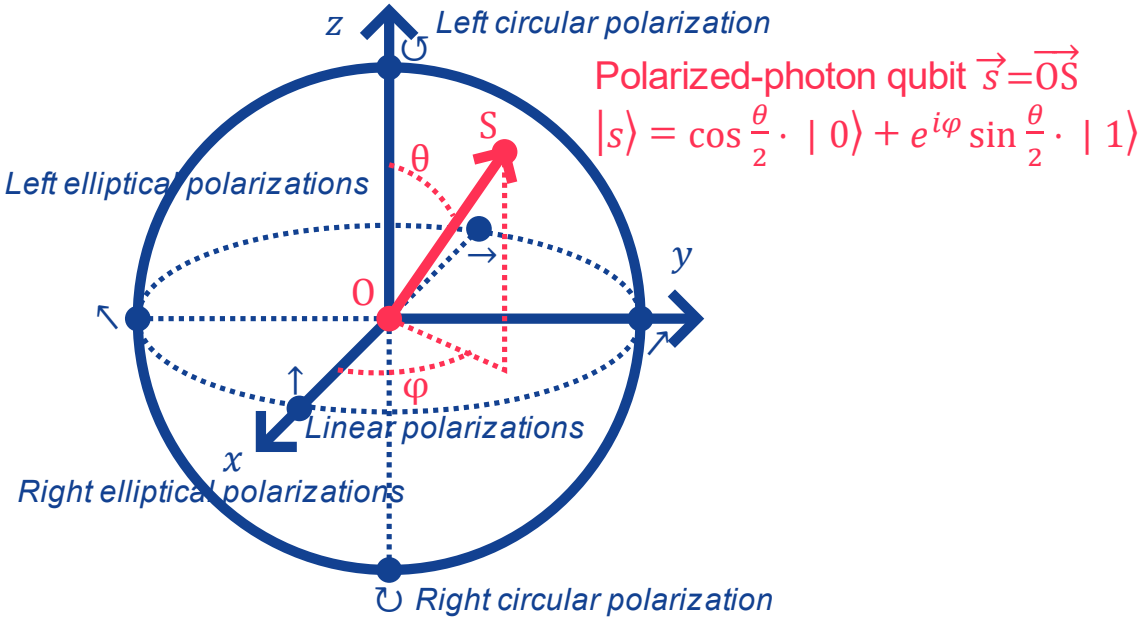
$\Rightarrow$ Photons are qubits that behave like $\frac{1}{2}$-spin particles, but with $\pm\hbar$ spin instead of $\pm\frac{\hbar}{2}$.

More generally, a qubit is any quantum system which, after any measurement, can have only two possible outcome states, these outcome states depending of the measurement.

Physically, the spin of the photon is its polarization: $|0\rangle$ or $+1$ for left-circular polarization, $|1\rangle$ or -1 for righ-circular polarization, and a complex linear combination of both for elliptic or linear polarization.

1.2.2. Polarized photon and the Poincaré sphere

With $\vec{z}$ being the propagation axis of the photon, the Bloch sphere representation of the qubit exactly corresponds to the Poincaré sphere representation of the polarization, where the polarizations $\uparrow$, $\rightarrow$, $\nwarrow$, $\nearrow$, $\circlearrowleft$ and $\circlearrowright$ corresponds respectively to the qubit states $|+\rangle = |\circlearrowright\rangle$, $|-\rangle = |\circlearrowleft\rangle$, $|+i\rangle = |\rightarrow\rangle$, $|-i\rangle = |\leftarrow\rangle$, $|0\rangle = |\uparrow\rangle$ and $|1\rangle = |\downarrow\rangle$, and to the Bloch vectors $\vec{x}$, $-\vec{x}$, $\vec{y}$, $-\vec{y}$, $\vec{z}$ and $-\vec{z}$.



1.3. Measurement of a non-entangled qubit

1.3.1. Single measurement outcome for a non-entangled qubit

We consider a measurement according to the oriented axis $\vec{m}$ (i.e., $|\psi_m\rangle \in \mathbb{C}^2$) on the qubit in the known initial state $\vec{s}$ (i.e., $|\psi_s\rangle \in \mathbb{C}^2$), the measured outcome is $\vec{m}$ with probability proba $[\vec{m}|\vec{s}]$ or $-\vec{m}$ with probability proba $[-\vec{m}|\vec{s}]$ where:

- Probability proba $[\vec{m}|\vec{s}] = \frac{1+\vec{m}\cdot\vec{s}}{2}$ that the output state is $\vec{m}$ and the bit value is 0 (convention);
- Probability proba $[-\vec{m}|\vec{s}] = 1 - proba\,[\vec{m}|\vec{s}] = \frac{1-\vec{m}\cdot\vec{s}}{2}$ that the output state is $-\vec{m}$ and the bit value is 1 (convention);

With the convention: bit value 0 corresponds to $+\frac{\hbar}{2}$ (spin $\vec{m}$), bit value 1 corresponds to $-\frac{\hbar}{2}$ (spin $-\vec{m}$), like z axis.

Because proba $[\vec{m}|\vec{s}] = \frac{\langle\psi_m|\psi_s\rangle\langle\psi_s|\psi_m\rangle}{\langle\psi_m|\psi_m\rangle\langle\psi_s|\psi_s\rangle} = \cos^2\theta_{Hilbert}\,(\psi_m,\psi_s) = \frac{1}{2} + \frac{1}{2}\cos 2\theta_{Hilbert}\,(\psi_m,\psi_s) = \frac{1}{2} + \frac{1}{2}\cos\theta_{BlochSphere}\,(\vec{m},\vec{s})$.

1.3.2. Successive measurement outcomes for a non-entangled qubit

Initial qubit state: $\vec{s}$ (i.e., $|\psi_s\rangle \in \mathbb{C}^2$). The order of measurement matters,the outcomes being different:

(1) First measurement according to the oriented axis $\vec{m}_1$ then second measurement according to the oriented axis $\vec{m}_2$:

Measure outcome after the first measurement: $\vec{m}_1$ with probability $p_1 = \frac{1+\vec{m}_1\cdot\vec{s}}{2}$ or $-\vec{m}_1$ with probability $1-p_1 = \frac{1-\vec{m}_1\cdot\vec{s}}{2}$.

Measure outcome after the second measurement: $\vec{m}_2$ with probability $p_2 = p_1 \times \frac{1+\vec{m}_2\cdot\vec{m}_1}{2} + (1-p_1)\times\frac{1-\vec{m}_2\cdot\vec{m}_1}{2} = \frac{1+\vec{m}_1\cdot\vec{s}\times\vec{m}_2\cdot\vec{m}_1}{2}$ or $-\vec{m}_2$ with probability $1-p_2 = \frac{1-\vec{m}_1\cdot\vec{s}\times\vec{m}_2\cdot\vec{m}_1}{2}$.

(2) First measurement according to the oriented axis $\vec{m}_2$ then second measurement according to the oriented axis $\vec{m}_1$:

Measure outcome after the first measurement: $\vec{m}_2$ with probability $p'_1 = \frac{1+\vec{m}_2\cdot\vec{s}}{2}$ or $-\vec{m}_2$ with probability $1-p_2 = \frac{1-\vec{m}_2\cdot\vec{s}}{2}$.

Measure outcome after the second measurement: $\vec{m}_1$ with probability $p'_2 = p'_1 \times \frac{1+\vec{m}_1\cdot\vec{m}_2}{2} + (1-p'_1)\times\frac{1-\vec{m}_1\cdot\vec{m}_2}{2} = \frac{1+\vec{m}_2\cdot\vec{s}\times\vec{m}_1\cdot\vec{m}_2}{2}$ or $-\vec{m}_1$ with probability $1-p_2 = \frac{1-\vec{m}_2\cdot\vec{s}\times\vec{m}_1\cdot\vec{m}_2}{2}$.

Entropy considerations with (1):

$p_1 = \frac{1+\vec{m}_1\cdot\vec{s}}{2}, p_2 = \frac{1+\vec{m}_1\cdot\vec{s}\times\vec{m}_2\cdot\vec{m}_1}{2}$.

1. If $0 < |\vec{m}_1\cdot\vec{s}| < 1$ and $0 < |\vec{m}_2\cdot\vec{m}_1| < 1$ then $\left|p_2 - \frac{1}{2}\right| < \left|p_1 - \frac{1}{2}\right|$: the entropy strictly increases.

2. If $|\vec{m}_2 \cdot \vec{m}_1| = 1$, i.e., $\vec{m}_2 = \pm\vec{m}_1$, then $p_2 \in \{p_1, 1-p_1\}$, the state (and the entropy) does not change with the second measurment.

3. If $\vec{m}_1 \cdot \vec{s} = 0$ then $p_2 = p_1 = \frac{1}{2}$: the initial knowledge is completely lost after the first measurement, 1 bit of information is renewed.

1.4. Time evolution of a non-entangled qubit

In quantum phisics, the evolution of the quantum state is governed by the Shrödinger equation: $i\hbar\frac{d}{dt}|\varphi(t)\rangle = H|\varphi(t)\rangle$ where H is the Halmitonian operator (energy observable).

If H does not depend on time t, the solution of this equation is $|\varphi(t)\rangle = U(t)|\varphi(0)\rangle$ where $U(t) = e^{-iHt/\hbar}$ is a unitary operator (because H is hermitian).

If H depends on time t, we still have $|\varphi(t)\rangle = U(t)|\varphi(0)\rangle$ where $U(t)$ is a unitary operator depending on time t in a more complex way.

For qubits, unitary operators in $\mathbb{C}^2$ correspond to rotations in $\mathbb{R}^3$ (i.e., isometries that conserve the orientations of 3D bases). Thus the evolution of the qubit states in the Bloch sphere is given by a rotation: $\vec{s}(t) = rot_{\vec{\Delta}(t),\alpha(t)}(\vec{s}(0))$.

The evolution is deterministic, i.e., there is no change in the amount of information an observer has on the observed system.

1.5. Modifying and measuring photonic qubits in practice

1.5.1. Modifying a photonic qubit in practice

Modifying (= quantum processing) a single photonic qubit = rotating its quantum state = modifying the polarization of a photon.

This can be done using waveplates, see https://en.wikipedia.org/wiki/Waveplate:

- Birefringent material that dephases the slow and fast polarization axis of an optical signal by $\Delta\Phi = \Phi_{slow} - \Phi_{fast} = \frac{2\pi(n_{slow}-n_{fast})L}{\lambda}$ with $n_{slow} > n_{fast}$
  - $\uparrow$ or $\rightarrow$: qubit rotation $rot_{\vec{x},\Delta\Phi}$,
  - $\nearrow$ or $\nwarrow$: qubit rotation $rot_{\vec{y},\Delta\Phi}$;

- Half-wave plates with slow polarization axis being:
  - $\uparrow$ or $\rightarrow$: qubit rotation $rot_{\vec{x},\pi} \Rightarrow \Delta\Phi = \pi \Rightarrow (\uparrow,\rightarrow) \rightarrow (\uparrow,\rightarrow)$, $(\nearrow,\nwarrow) \rightarrow (\nwarrow,\nearrow)$ and $(\circlearrowleft,\circlearrowright) \rightarrow (\circlearrowright,\circlearrowleft)$,
  - $\nearrow$ or $\nwarrow$: qubit rotation $rot_{\vec{y},\pi} \Rightarrow \Delta\Phi = \pi \Rightarrow (\uparrow,\rightarrow) \rightarrow (\rightarrow,\uparrow)$, $(\nearrow,\nwarrow) \rightarrow (\nearrow,\nwarrow)$ and $(\circlearrowleft,\circlearrowright) \rightarrow (\circlearrowright,\circlearrowleft)$;

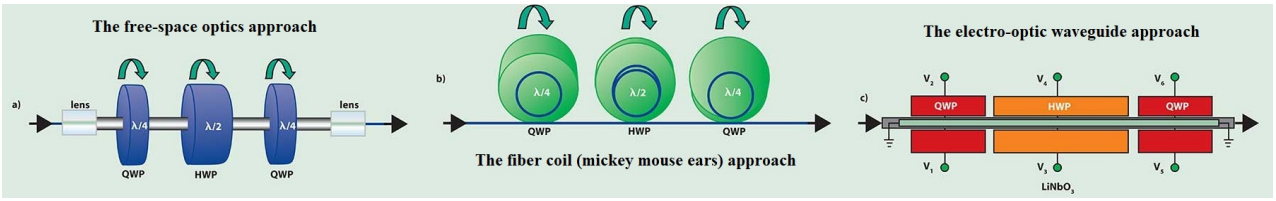
- Quarter-wave plates with slow polarization axis being:
  - $\uparrow$ or $\rightarrow$: qubit rotation $rot_{\vec{x},\pi/2} \Rightarrow \Delta\Phi = \pi/2 \Rightarrow (\uparrow,\rightarrow) \rightarrow (\uparrow,\rightarrow)$, $(\nearrow,\nwarrow) \rightarrow (\circlearrowright,\circlearrowright)$ and $(\circlearrowleft,\circlearrowright) \rightarrow (\nearrow,\nwarrow)$,
  - $\nearrow$ or $\nwarrow$: qubit rotation $rot_{\vec{y},\pi/2} \Rightarrow \Delta\Phi = \pi/2 \Rightarrow (\uparrow,\rightarrow) \rightarrow (\circlearrowright,\circlearrowright)$, $(\nearrow,\nwarrow) \rightarrow (\nearrow,\nwarrow)$ and $(\circlearrowleft,\circlearrowright) \rightarrow (\uparrow,\rightarrow)$.

By combining two wave plates with adequates dephasing and adequate axis positioning, any rotation $rot_{\vec{\Delta},\alpha}$ can be reached.

It can also be reached using 3 waveplates for which one can adequately position the axes: a quater-wave plate (any elliptical polarization $\rightarrow$ some linear polarization) + a half-wave plate (rotates the linear polarization with the desired long axis) + a quater-wave plate (transform it into the desired elliptical polarization). See https://en.wikipedia.org/wiki/Polarization_controller.

This corresponds to the "Mickey mouse ears" in optical fiber testbeds: 1 fiber loop with the right diameter is a quater-wave plate, with two loops we have a half-wave plate.

See for example https://www.photonics.com/Articles/Polarization_in_Fiber_Systems_Squeezing_out_More/a25149:

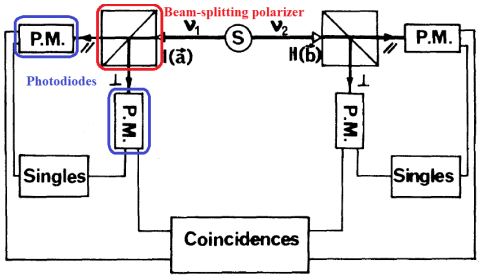


1.5.2. Measuring a photonic qubit in practice

Use of a beam-splitting polarizer + two photo-detectors (photodiodes):

- A beam-splitting polarizer that is oriented according to a given axis splits a light beam into two linear polarizations beams, one polarization corresponding to the given axis and the other one being perpendicular.
- Then, if there is only one photon in the beam, only one of the two photodiodes detects the photon, giving its polarization according to the given axis.

This was used in Aspect's experiments in 1982, in a manual [**AGR1982**] and automatically-varying [**ADR1982**] configurations.



Alain Aspect's experimental setup [AGR1982]

FIG. 2. Experimental setup. Two polarimeters I and II, in orientations $\vec{a}$ and $\vec{b}$, perform true dichotomic measurements of linear polarization on photons ν_1 and ν_2. Each polarimeter is rotatable around the axis of the incident beam. The counting electronics monitors the singles and the coincidences.

2. Bell pairs

1. Bell pair of maximally-entangled qubits
2. Measurement of a Bell pair
3. Usual Bell pairs represented with Bloch spheres
4. Equivalence of Bell pairs
5. Bell pairs in practice

2.1. Bell pair of maximally-entangled qubits

A generic Bell pair BP is a maximally entangled pair of qubits (A, B).

Maximal entanglement = maximal correlation between the qubits = 1 bit of correlation information, because the qubits interacted "totally" between themselves.

Because of this "total" interaction between the qubits, the previous information about the individual qubits is lost. Thus, an observer has no information neither on qubit A nor on qubit B (1 bit entropy for each).

But the observer has 1 bit of correlation information. Thus, if this observer measures the qubit A (respectively the qubit B), then this observer infers the state of the qubit B (respectively the qubit A).

2.2. Measurement of a Bell pair

2.2.1. Relation between the measured state and the infered state when measured on one qubit

If the qubit A is measured according to the oriented axis $\vec{m}_A$, 1 additional bit of information is acquired: the measured outcome of qubit A is $\vec{m}_A$ with probability $\frac{1}{2}$ or $-\vec{m}_A$ with probability $\frac{1}{2}$ (whatever the value of $\vec{m}_A$).

Because of the 1 bit of correlation information, if $\pm\vec{m}_A$ is measured, the inferred qubit state is $f(\pm\vec{m}_A)$.

Some information-based considerations imposes that f is an isometry in 3D space: conservation of the angles, the angular distance being a measure of the distinguisghability between states, see Wootters' statistical distance [**Woo1991**] (two states measured on A or B cannot be more or less easily distinguised on respectively B or A, which imposes the same angles).

There are two kinds of isometries in 3D spaces, related to unitary and antiunitary operators (Wigner's therorem [see https://en.wikipedia.org/wiki/Wigner%27s_theorem on Wikipedia] applied to $\mathbb{C}^2$):

1. Isometries that conserve the orientations of 3D bases: rotations $r^A_{\vec{\Delta},\alpha}$ of oriented axis $\vec{\Delta}$ and angle α, corresponding to unitaty operators in $\mathbb{C}^2$;
2. Isometries that reverse the orientations of 3D bases: improper rotations $ir^A_{\vec{\Delta},\alpha} = ref_{\Delta^\perp} \circ rot_{\vec{\Delta},\alpha} = rot_{\vec{\Delta},\alpha} \circ ref_{\Delta^\perp}$ of oriented axis $\vec{\Delta}$, angle α and plane orthogonal to $\vec{\Delta}$, corresponding to antiunitaty operators in $\mathbb{C}^2$ (planar reflection correspond to conjugation).

Quantum physics $\Rightarrow f = ir^A_{\vec{\Delta},\alpha}$ (it can be any improper rotation, represented by an antiunitary operator).

If the qubit A is measured according to the oriented axis $\vec{m}_A$, the measured outcome of qubit A is $\pm\vec{m}_A$ with probability $\frac{1}{2}$ for each possible outcome, and the inferred qubit B state is $\pm\vec{m}_B = ir^A_{\vec{\Delta},\alpha}(\pm\vec{m}_A) = \pm ir^A_{\vec{\Delta},\alpha}(\vec{m}_A)$.

If, instead, the qubit B is measured according to the oriented axis $\vec{m}_B$, the measured outcome of qubit B is $\pm\vec{m}_B$ with probability $\frac{1}{2}$ for each possible outcome, and the infered qubit A state is $\pm\vec{m}_A = ir^B_{\vec{\Delta},-\alpha}(\pm\vec{m}_B) = \pm ir^B_{\vec{\Delta},-\alpha}(\vec{m}_B)$.

Thus, the Bell Pair $BP_{\vec{\Delta},\alpha}$ is characterized by the improper rotation $ir^A_{\vec{\Delta},\alpha} = ref_{\Delta^\perp} \circ rot_{\vec{\Delta},\alpha} = rot_{\vec{\Delta},\alpha} \circ ref_{\Delta^\perp}$.

The Bell pair state in the Hilbert space $\mathbb{C}^2 \otimes \mathbb{C}^2 = \mathbb{C}^4$ is $\left|BP_{\vec{\Delta},\alpha}\right\rangle = \frac{1}{\sqrt{2}}\left(|s\rangle \otimes AU|s\rangle + |s^\perp\rangle \otimes AU|s^\perp\rangle\right)$ for all qubit states s, where AU is the antiunitary operator corresponding to $ir^A_{\vec{\Delta},\alpha}$.

2.2.2. Measurement of both qubits

We consider the Bell pair $BP_{\vec{\Delta},\alpha}$ of maximally entangled pair of qubits (A,B), characterized by $ir^A_{\vec{\Delta},\alpha}$.

The measurement on qubit A with axis $\vec{m}_A$ then on qubit B with axis $\vec{m}_B$ gives:

1. The first measurement outcome is $\left(\vec{m}_A, ir^A_{\vec{\Delta},\alpha}(\vec{m}_A)\right)$ or $\left(-\vec{m}_A, -ir^A_{\vec{\Delta},\alpha}(\vec{m}_A)\right)$ with probability $\frac{1}{2}$ each;
2. The second measurement outcome is, with $\sigma = \vec{m}_B \cdot ir^A_{\vec{\Delta},\alpha}(\vec{m}_A)$: $(\vec{m}_A, \vec{m}_B)$ with probability $\frac{1+\sigma}{4}$, $(\vec{m}_A, -\vec{m}_B)$ with probability $\frac{1-\sigma}{4}$, $(-\vec{m}_A, \vec{m}_B)$ with probability $\frac{1-\sigma}{4}$, and $(-\vec{m}_A, -\vec{m}_B)$ with probability $\frac{1+\sigma}{4}$.

The measurement on qubit B with axis $\vec{m}_B$ then on qubit A with axis $\vec{m}_A$ gives:

1. The first measurement outcome is $\left(ir^B_{\vec{\Delta},-\alpha}(\vec{m}_B), \vec{m}_B\right)$ or $\left(-ir^B_{\vec{\Delta},-\alpha}(\vec{m}_B), -\vec{m}_B\right)$ with probability $\frac{1}{2}$ each;
2. The second measurement outcome is, with $\sigma' = \vec{m}_A \cdot ir^B_{\vec{\Delta},-\alpha}(\vec{m}_B)$: $(\vec{m}_A, \vec{m}_B)$ with probability $\frac{1+\sigma'}{4}$, $(\vec{m}_A, -\vec{m}_B)$ with probability $\frac{1-\sigma'}{4}$, $(-\vec{m}_A, \vec{m}_B)$ with probability $\frac{1-\sigma'}{4}$, and $(-\vec{m}_A, -\vec{m}_B)$ with probability $\frac{1+\sigma'}{4}$.

Commutation of the two measurements

(1) The outcome after the first measurement depends on the order of measurement of the two qubits except if $\vec{m}_B = \pm ir^A_{\vec{\Delta},\alpha}(\vec{m}_A)$.

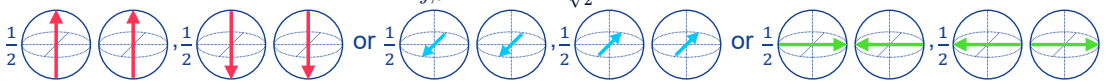
This is in favor of a relational interpretation of quantum physics [**Rov1996, Rov2021**] thats says that the information an observer has on a system (= quantum state) depends on the observer (a kind of generalization of the special or general relativity).

(2) The outcome after the two measurement does not depend on the order of these measurements of the two qubits (they commute):
$\sigma' = \vec{m}_A \cdot ir^B_{\vec{\Delta},-\alpha}(\vec{m}_B) = ir^A_{\vec{\Delta},\alpha}(\vec{m}_A) \cdot ir^A_{\vec{\Delta},\alpha}\left(ir^B_{\vec{\Delta},-\alpha}(\vec{m}_B)\right) = ir^A_{\vec{\Delta},\alpha}(\vec{m}_A) \cdot Id(\vec{m}_B) = \vec{m}_B \cdot ir^A_{\vec{\Delta},\alpha}(\vec{m}_A) = \sigma,$
because $ir^A_{\vec{\Delta},\alpha}$ conserves the scalar product since it is an isometry and $ir^A_{\vec{\Delta},\alpha} \circ ir^B_{\vec{\Delta},-\alpha} = Id.$

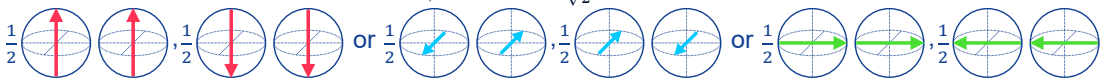
This commutation is due to the fact that the two measurements take place in different locations (locality of interactions).

2.3. Usual Bell pairs represented with Bloch spheres

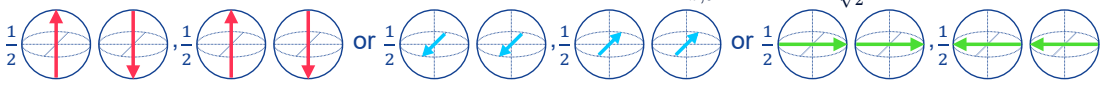
1. Bell pair $BP_{\vec{y},0} = xz$-plane reflection $ir^A_{\vec{y},0} = |\Phi^+\rangle = \frac{1}{\sqrt{2}}(|0\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle)$



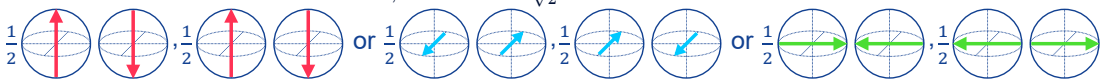
2. Bell pair $BP_{\vec{x},0} = yz$-plane reflection $ir^A_{\vec{x},0} = |\Phi^-\rangle = \frac{1}{\sqrt{2}}(|0\rangle \otimes |0\rangle - |1\rangle \otimes |1\rangle)$



3. Bell pair $BP_{\vec{z},0} = xy$-plane (linear-polarization plane) reflection $ir^A_{\vec{z},0} = |\Psi^+\rangle = \frac{1}{\sqrt{2}}(|0\rangle \otimes |1\rangle + |1\rangle \otimes |0\rangle)$



4. Bell pair $BP_{\vec{s},\pi}$ = point reflection $ir^A_{\vec{s},\pi} = |\Psi^-\rangle = \frac{1}{\sqrt{2}}(|0\rangle \otimes |1\rangle - |1\rangle \otimes |0\rangle)$



2.4. Equivalence of Bell pairs

The Bell Pair $BP_{\vec{\Delta},\alpha}$ is characterized by $ir^A_{\vec{\Delta},\alpha} = ref_{\Delta^\perp} \circ rot_{\vec{\Delta},\alpha} = rot_{\vec{\Delta},\alpha} \circ ref_{\Delta^\perp}$.

The Bell Pair $BP_{\vec{\Delta}',\alpha'}$ is characterized by $ir^A_{\vec{\Delta}',\alpha'} = ref_{\Delta'^\perp} \circ rot_{\vec{\Delta}',\alpha'} = rot_{\vec{\Delta}',\alpha} \circ ref_{\Delta'^\perp}$.

Any improper rotation can be obtain from one given improper rotation combined with the rotation of one of the qubit: $ir^A_{\vec{\Delta}',\alpha'} = rot^A_{\vec{\Delta}'',\alpha''} \circ ir^A_{\vec{\Delta},\alpha}$ with $rot^A_{\vec{\Delta}'',\alpha''} = ir^A_{\vec{\Delta}',\alpha'} \circ ir^A_{\vec{\Delta},-\alpha}$, because the composition of two improper rotations is a rotation.

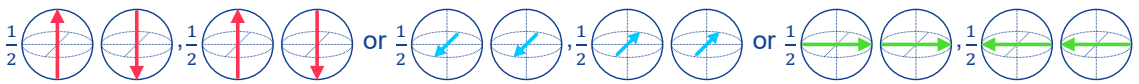
For exemple, using $rot_{\vec{x},\pi} = ir_{\vec{x},0} \circ ir_{\vec{y},0} = ref_{yz,0} \circ ref_{xz,0} = ref_{xz,0} \circ ref_{yz,0}$ on one of the qubits A or B, which is realized with a half-wave plate aligned with the vertical or horizontal polarization axes for polarized photons, $BP_{\vec{y},0}$ is transformed into $BP_{\vec{z},0}$ and $BP_{\vec{z},0}$ is transformed into $BP_{\vec{y},0}$.

2.5. Bell pairs in practice

2.5.1. Bell pair creation

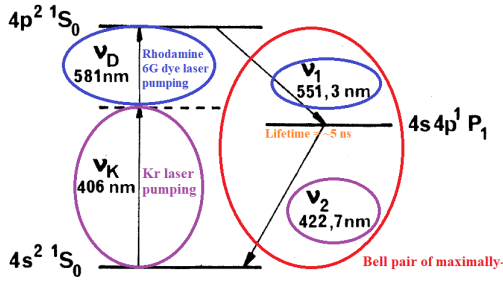
A Bell pair of maximally-entangled photons can be created for example with Calcium atoms:

1. Excitation of an atom of Calcium to a given energy level by laser pumping;
2. Decaying to an intermediate energy level (first photon emission by fluorescence);
3. Then, after a very short delay (~5 ns), successive decaying to the initial energy level (second photon emission by fluorescence);
4. Because of this process, the two photons are emited in opposite directions and have correlated but unknown polarizations: they form the Bell pair $BP_{\vec{z},0} = xy$-plane (= linear-polarization plane) reflection $ir^A_{\vec{z},0} = |\Psi^+\rangle = \frac{1}{\sqrt{2}}(|0\rangle \otimes |1\rangle + |1\rangle \otimes |0\rangle)$.



Note: If one wants another Bell pair, one just needs to rotate one of the two qubits i.e., change the polarization of one of the two photons.

This was used in Aspect's experiments in 1981-1982 [**AGR1981**].

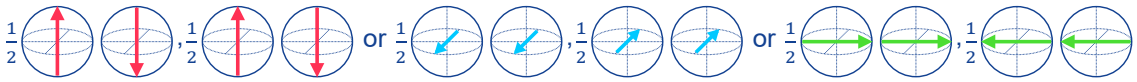


Bell pair source used in Alain Aspect's experimental setup [AGR1981]

FIG. 1. Relevant levels of calcium. The atoms, selectively pumped to the upper level by the nonlinear absorption of ν_K and ν_L, emits the photons ν_1 and ν_2 correlated in polarization.

2.5.2. Bell pair usage for QKD

For example, one can use the Bell pair $BP_{\vec{z},0} = xy$-plane (= linear-polarization plane) reflection $ir^A_{\vec{z},0} = |\Psi^+\rangle = \frac{1}{\sqrt{2}}(|0\rangle \otimes |1\rangle + |1\rangle \otimes |0\rangle)$.



1. If the polarizations of the two photons are measured with the same linear vertical polarization axes $(\uparrow, \uparrow)$, then the measured polarization are $(\uparrow, \uparrow)$, i.e., $(0, 0)$, or $(\rightarrow, \rightarrow)$, i.e., $(1, 1)$, with 50% probability each;

2. If the polarizations of the two photons are measured with the same linear diagonal polarization axes $(\nearrow, \nearrow)$, then the measured polarization are $(\nearrow, \nearrow)$, i.e., $(0, 0)$, or $(\nwarrow, \nwarrow)$, i.e., $(1, 1)$, with 50% probability each;

3. If the polarizations of the two photons are measured with the different polarization axes $(\uparrow, \nearrow)$, then the measured polarization are $(\uparrow, \nearrow)$, i.e., $(0, 0)$, $(\uparrow, \nwarrow)$, i.e., $(0, 1)$, $(\rightarrow, \nearrow)$, i.e., $(1, 0)$, or $(\rightarrow, \nwarrow)$, i.e., $(1, 1)$, with 25% probability each;

4. If the polarizations of the two photons are measured with the different polarization axes $(\nearrow, \uparrow)$, then the measured polarization are $(\nearrow, \uparrow)$, i.e., $(0, 0)$, $(\nearrow, \rightarrow)$, i.e., $(0, 1)$, $(\nwarrow, \uparrow)$, i.e., $(1, 0)$, or $(\nwarrow, \rightarrow)$, i.e., $(1, 1)$, with 25% probability each.

Case 1 and 2: Using the same polarization axis for the measurements of the two maximally-entangled photons leads to the creation of a shared random secret bit between the two measurement sides (same quantum state for both observers of qubits A and B).
This is essentially how QKD works.

Case 3 and 4: Using différent polarization axes for the measurements of the two maximally-entangled photons leads to different quantum states for the observers of qubits A and B before they exchange their information.

For example, in case 3 of measurements with the different polarization axes $(\uparrow, \nearrow)$:

1. The observer of qubit A gets $\uparrow \otimes \uparrow$ with probability 50%,

2. While the observer of qubit B gets $\nearrow \otimes \nearrow$ with probability 50%,

3. Which leads to $\uparrow \otimes \nearrow$ with probability 25% after they exchange the results of their measurements.

This is in favor of a relational interpretation of quantum physics [**Rov1996, Rov2021**] thats says that the information an observer has on a system (= quantum state) depends on the observer (a kind of generalization of the special or general relativity).

3. First protocol for QKD: BB84

Protocol described in [**BB84**].

1. BB84 protocol without eavesdropping

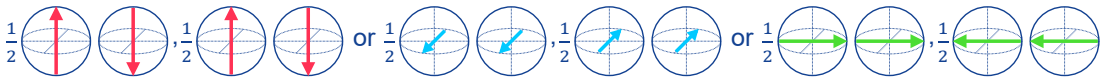
2. BB84 protocol with eavesdropping

3. Experimental setup for BB84

3.1. BB84 protocol without eavesdropping

3.1.1. Example of initial configuration choice for QKD using BB84 protocol

We choose the Bell pair $BP_{\vec{z},0} \sim xy$-plane (linear-polarization plane) reflection $ir^A_{\vec{z},0} = ref_{xy} \sim |\Psi^+\rangle = \frac{1}{\sqrt{2}}(|0\rangle \otimes |1\rangle + |1\rangle \otimes |0\rangle)$.



Alice chooses the two orthogonal measurement axes $\vec{x} \perp \vec{y}$ corresponding to polarization axes ↑ and ↗ (there could be other choices...).

The induced choice of orthogonal measurement axes by Bob is $ir^A_{\vec{z},0}(\vec{x}) = \vec{x} \perp ir^A_{\vec{z},0}(\vec{y}) = \vec{y}$: same choices of polarization axes.

3.1.2. BB84 protocol

(1) Alice receives the qubit A of the Bell pair $BP_{\vec{y},0}$ and Bob the qubit B (quantum channel).

(2) Alice and Bob choose independently and randomly their axes of measurement $\vec{m}_A$ and $\vec{m}_B$ in $\{\vec{x}, \vec{y}\}$, which correspond to ↑ and ↗ polarizations, and they process to the measurement of the qubit they have.

(3) Identifying $\vec{m}_A$ and $\vec{m}_B$ outcome states with binary value 0 and $-\vec{m}_A$ and $-\vec{m}_B$ with binary value 1, the measured bits are:

- If $\vec{m}_A = \vec{m}_B$, $(0,0)$ or $(1,1)$ with probability $\frac{1}{2}$ for both possibilities;
- If $\vec{m}_A \neq \vec{m}_B$, $(0,0)$, $(0,1)$, $(1,0)$ or $(1,1)$ with probability $\frac{1}{4}$ for each possibility.

(4) They communicate their choice of axes (through an **authenticated classical channel** which may be not encrypted) and they consider the random shared secret bit they measured only when $\vec{m}_A = \vec{m}_B$.

Repeating this process $2K$ times in parallel (step 4 should be done after all the qubits have been measured in step 2), Alice and Bob can build a shared secret random key of average size K.

3.1.3. BB84 protocol binary model

The qubits are indexed by $i \in I = \{1, \cdots, n_I\}$.

The choices for measurement axes by Alice ($X = A$) and Bob ($X = B$) are for Bell pair i, with our example, $m_i^X = 0$ for $\vec{x}$ (polarization axis ↑) and $m_i^X = 1$ for $\vec{y}$ (polarization axis ↗) .

The measurement results by Alice ($X = A$) and Bob ($X = B$) on their qubit of the Bell pair i, depending on the measurement axes, are $b_i^X = 0$ for $+\vec{x}$ (↑ polarization) or $+\vec{y}$ (↗ polarization), and $b_i^X = 1$ for $-\vec{x}$ (→ polarization) or $-\vec{y}$ (↖ polarization).

The full set of data for the BB84 protocol is then $\left(\left(m_i^A, b_i^A\right), \left(m_i^B, b_i^B\right)\right)_{i \in I}$.

The index set of Bell pairs for which Alice and Bob chose the same axes is $J = \left\{i \in I \mid m_i^A = m_i^B\right\}$.

The quantum physics laws impose $\forall i \in J, b_i^A = b_i^B$.

Summary of BB4 protocol without evesdropping

Measurement axis m_A	0				0				1				1			
Measurement axis m_B	0				1				0				1			
Probability m_A & m_B	1/4				1/4				1/4				1/4			
Measured bit b_A	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1
Measured bit b_B	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1
Probability b_A & b_B	1/2	0	0	1/2	1/4	1/4	1/4	1/4	1/4	1/4	1/4	1/4	1/2	0	0	1/2
Probability $m_{A/B}$ & $b_{A/B}$	1/8	0	0	1/8	1/16	1/16	1/16	1/16	1/16	1/16	1/16	1/16	1/8	0	0	1/8

3.2. BB84 protocol with eavesdropping

3.2.1. Power of the eavesdropper

The eavesdropper Eve can have almost full power on the communications between Alice and Bob:

- She can intercept and modify the qubits transmitted to Alice and Bob in the quantum channel;
- She can intercept the information exchanged between Alice and Bob on the classical channel (which is authenticated but not encrypted: no *man-in-the-middle* attack on the classical channel);
- She does not know how and what Alice and Bob measure for each qubit, except the fact that the Bell pair is $BP_{\vec{z},0}$ and the initial set $\{\vec{x}, \vec{y}\}$ of orthogonal axes for Alice and Bob measurements.

3.2.2. BB84 method to detect eavesdropping

Alice and Bob process the following additional steps to detect eavesdropping:

(5) Once Alice and Bob have measured all the qubits they received (step 2 of BB84) and have communicated their choice of axes for all of them (step 4 of BB84), they randomly select some of them and they communicates the corresponding measured bits (this is not done in BB84 for the qubits used to build the shared secret random key).

(6) If Eve (eavesdropper) has modify some qubits by some measurements, then, when $\vec{m}_A = \vec{m}_B$, the probability that the corresponding bits measured by Alice and Bob are different is greater or equal to $\frac{1}{4}$, while it would be 0 without Eve intervention. This allows Alice and Bob to statistically evaluate the number of eavesdropped qubits.

(7) Alice and Bob process the step 4 of BB84 for the remaining qubits, and perform a purification process [**BBE92**] to build a shared secret random key taking into account the estimated proportion of qubits that are eavesdropped.

3.2.3. Proof that the minimal threshold for the eavesdropping detection probability is $\frac{1}{4}$

In the following we prove this for the case when Eve measured the qubit B before Bob.

It is also true for the cases when Eve measured the qubit A before Alice of both qubits A and B before Alice and Bob.

The security proof relies on the following facts:

- Alice and Bob choose randomly and independantly the measurement axes between two axes that are orthogonal in $\mathbb{R}^3$, i.e., with angle 45° in $\mathbb{C}^2$;
- Eve does not know the measurement axes choosen by Alice and Bob before they communicate this information;
- Any measurement on one or both qubits breaks the entanglement and the correlation between the qubits of the Bell pair;
- The classical channel is authenticated;
- *No cloning theorem*: a qubit in an unknown state cannot be duplicated [**WZ1982**];
- The quantum physics theory is complete [**EPR1935,Bell1964,ADR1982**].

BB4 protocol with evesdropping with the following Eve's strategy:

1. Eve intercepts the qubit B and measures it according to the oriented axis $\vec{m}_E = \vec{x}$. The measured outcome is $\pm\vec{m}_E$ with probability $\frac{1}{2}$, which imposes $m_A = m_E \Rightarrow b_A = b_E$.
2. Eve sends to Bob the measured qubit, which imposes $m_B = m_E \Rightarrow b_B = b_E$.

Measurement axis m_A	0								0								1								1							
Measurement axis m_B	0								1								0								1							
Measurement axis m_E	0								0								0								0							
Measured bit b_A	0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1
Measured bit b_B	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1
Measured bit b_E	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1
Proba. $m_{A/B/E}$ & $b_{A/B/E}$	1/8	0	0	0	0	0	0	1/8	1/16	0	1/16	0	0	1/16	0	1/16	1/16	0	0	1/16	1/16	0	0	1/16	1/32	1/32	1/32	1/32	1/32	1/32	1/32	1/32

Alice and Bob expect that the condition $m_A = m_B \Rightarrow b_A = b_B$ holds. Thus Eve is detected when $m_A = m_B$ and $b_A \neq b_B$ (orange boxes). The detection probability when $m_A = m_B$ is then $p_{detect} = \frac{1}{4}$.

Similar results with $\vec{m}_E = \vec{y}$. These cases correspond to the worst cases: $p_{detect} \geq \frac{1}{4}$ in all cases (see proof).

Proof (1/3)

Eve intercept the qubit B and measures it according to the oriented axis $\vec{m}_E$ which may or may not be in $\{\vec{x}, \vec{y}\}$. The measured outcome is $\pm\vec{m}_E$ with probability $\frac{1}{2}$.

Because she knows that the Bell pair is $BP_{\vec{z},0}$, her inferred qubit A state is then $ir^B_{\vec{z},0}(\pm\vec{m}_E) = \pm ir^B_{\vec{z},0}(\vec{m}_E)$.

Alice measures qubit A with axis $\vec{m}_A \in \{\vec{x}, \vec{y}\}$. $\vec{m}_A$ is unknown by Eve. The combined Eve + Alice measured outcome is then, with $\sigma_E = \vec{m}_A \cdot ir^B_{\vec{y},0}(\vec{m}_E)$, $(\vec{m}_A, \vec{m}_E)$ with probability $\frac{1+\sigma_E}{4}$, $(\vec{m}_A, -\vec{m}_E)$ with probability $\frac{1-\sigma_E}{4}$, $(-\vec{m}_A, \vec{m}_E)$ with probability $\frac{1-\sigma_E}{4}$ or $(-\vec{m}_A, -\vec{m}_E)$ with probability $\frac{1+\sigma_E}{4}$.

Alice sends to Bob a new qubit E which may depends on what she measured and which can be a mixed state (statistical quantum mechanisms with density operator formalism): $\vec{s}(\pm\vec{m}_E)$ with probability $p(\pm\vec{m}_E)$, and $-\vec{s}(\pm\vec{m}_E)$ with probability $1 - p(\pm\vec{m}_E)$.

She may choose to send the qubit $E = B$ that she measured: $p(\pm\vec{m}_E) = 1$ and $s(\pm\vec{m}_E) = \pm\vec{m}_E$; but she can do other things, including sending a qubit E fully or partially entangled with another quantum system (some aparatus she may use) including the qubit B she measured.

Bob measured with axis $\vec{m}_B \in \{\vec{x}, \vec{y}\}$ the qubit E coming from the interception by Alice of the qubit B. His measured outcome is $\vec{m}_B$ with probability $\frac{1+\sigma_B}{2}$ or $-\vec{m}_B$ with probability $\frac{1-\sigma_B}{2}$ where $\sigma_B(\pm\vec{m}_E) = (2p(\pm\vec{m}_E) - 1)\,\vec{m}_B \cdot \vec{s}(\pm\vec{m}_E)$, but Bob does not know σ_B nor $\pm\vec{m}_E$.

Proof (2/3)

In the remaining parts of the proof, we will prove that, when $\vec{m}_A = \vec{m}_B$, the probability p_{detect} that Alice and Bob detect that someone made a measurement on the qubit B is lower bounded by $p_{detect} \geq \frac{1}{4}$, this lower bound being reached, for example, if $\vec{m}_E \in \{\vec{x}, \vec{y}\}$, $p(\pm\vec{m}_E) = 1$ and $s(\pm\vec{m}_E) = \pm\vec{m}_E$.

The combined Eve + Alice measured outcome is, with $\sigma_E = \vec{m}_A \cdot ir^B_{\vec{y},0}(\vec{m}_E)$: $(\vec{m}_A, \vec{m}_E)$ with probability $\frac{1+\sigma_E}{4}$, $(\vec{m}_A, -\vec{m}_E)$ with probability $\frac{1-\sigma_E}{4}$, $(-\vec{m}_A, \vec{m}_E)$ with probability $\frac{1-\sigma_E}{4}$ or $(-\vec{m}_A, -\vec{m}_E)$ with probability $\frac{1+\sigma_E}{4}$.

When $\vec{m}_A = \vec{m}_B$, we have $\sigma_B(\pm\vec{m}_E) = (2p(\pm\vec{m}_E) - 1)\,\vec{m}_A \cdot \vec{s}(\pm\vec{m}_E)$ and his measured outcome is $\vec{m}_A$ with probability $\frac{1+\sigma_B(\pm\vec{m}_E)}{2}$ or $-\vec{m}_A$ with probability $\frac{1-\sigma_B(\pm\vec{m}_E)}{2}$. This measured outcome is independant of the combined Eve + Alice measured outcome, because Bob's measurement comes after Eve's measurement.

Alice and Bob can detect the eavesdropping when Bob measures $\pm\vec{m}_A$ while Alice measures the opposite $\mp\vec{m}_A$. So we can compute the probability $p_{detect}(\vec{m}_A)$ as a function of $\vec{m}_A$, which is unknown by Eve.

$$p_{detect}(\vec{m}_A) = \frac{1+\sigma_B(+\vec{m}_E)}{2} \times \frac{1-\sigma_E}{4} + \frac{1+\sigma_B(-\vec{m}_E)}{2} \times \frac{1+\sigma_E}{4} + \frac{1-\sigma_B(+\vec{m}_E)}{2} \times \frac{1+\sigma_E}{4} + \frac{1-\sigma_B(-\vec{m}_E)}{2} \times \frac{1-\sigma_E}{4}$$
$$= \frac{1}{2} - \frac{\sigma_B(+\vec{m}_E)\sigma_E}{4} + \frac{\sigma_B(-\vec{m}_E)\sigma_E}{4} = \frac{1}{2} + \frac{(1-2p(\vec{m}_E))\vec{m}_A\cdot\vec{s}(\vec{m}_E)\times\vec{m}_A\cdot ir^B_{\vec{y},0}(\vec{m}_E)}{4} - \frac{(1-2p(-\vec{m}_E))\vec{m}_A\cdot\vec{s}(-\vec{m}_E)\times\vec{m}_A\cdot ir^B_{\vec{y},0}(-\vec{m}_E)}{4}.$$

Proof (3/3)

The choice of $(\vec{m}_A)$ is fully random with $\vec{m}_A \in \{\vec{x}, \vec{y}\}$, thus the probability detection is $p_{detect} = \frac{1}{2}p_{detect}(\vec{x}) + \frac{1}{2}p_{detect}(\vec{y})$.

We thus have $p_{detect} = \frac{1}{2} + \frac{f\left(p(\vec{m}_E),\vec{s}(\vec{m}_E),ir^B_{\vec{y},0}(\vec{m}_E)\right)}{8} - \frac{f\left(p(-\vec{m}_E),\vec{s}(-\vec{m}_E),ir^B_{\vec{y},0}(-\vec{m}_E)\right)}{8}$,
where $f(p,\vec{s},\vec{r}) = (1-2p)(\vec{z}\cdot\vec{s}\times\vec{z}\cdot\vec{r} + \vec{x}\cdot\vec{s}\times\vec{x}\cdot\vec{r}) = (1-2p)(\cos\theta_s\cos\theta_r + \cos\varphi_s\sin\theta_s\cos\varphi_r\sin\theta_r)$.

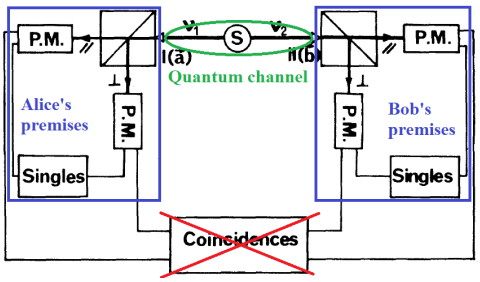
We have $f(p,\vec{s},\vec{r}) \in [-1,+1]$ because $1-2p \in [-1,+1]$ since $p \in [0,+1]$,
and $|\cos\theta_s\cos\theta_r + \cos\varphi_s\sin\theta_s\cos\varphi_r\sin\theta_r| \leq \max\{|\cos(\theta_s-\theta_r)|, |\cos(\theta_s+\theta_r)|\} \leq 1$.

Thus $p_{detect} \geq \frac{1}{4}$.

For $\vec{m}_E = \vec{x}$, $p(\pm\vec{m}_E) = 1$ and $s(\pm\vec{m}_E) = \pm\vec{m}_E = \pm\vec{x}$, we have $ir^B_{\vec{z},0}(\pm\vec{m}_E) = \pm\vec{x}$, which implies that $p_{detect} = \frac{1}{4}$. The probability value is the same with $\vec{m}_E = \vec{y}$.

3.3. Experimental setup for BB84

The quantum channel can be realized using Alain Aspect's experimental set up [**AGR1982,ADR1982**]:



Alain Aspect's experimental setup [AGR1982]

FIG. 2. Experimental setup. Two polarimeters I and II, in orientations $\bar{a}$ and $\bar{b}$, perform true dichotomic measurements of linear polarization on photons ν_1 and ν_2. Each polarimeter is rotatable around the axis of the incident beam. The counting electronics monitors the singles and the coincidences.

The classical channel could be any classical network (e.g., classical Internet communication).

4. QKD protocol using Bell's inequalities: E91

Protocol described in [**E91**].

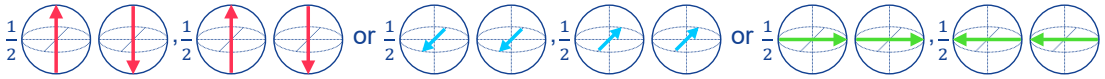
1. Bell's inequalities
2. Usage of Bell's inequalities in E91 protocol

4.1. Bell's inequalities

4.1.1. The inequalities

The Bell's inequalities that are used in the E91 protocol [**E91**] and in Alain Aspect's experiments [**AGR1982,ADR1982**] are a generalization [**CHSH1969**] of the initial Bell's inequalities [**Bell1964**].

We consider the Bell pair $BP_{\vec{z},0} \sim xy$-plane (linear-polarization plane) reflection $ir^A_{\vec{z},0} = ref_{xy} \sim |\Psi^+\rangle = \frac{1}{\sqrt{2}}(|0\rangle \otimes |1\rangle + |1\rangle \otimes |0\rangle)$.



Alice and Bob choose the measurement axes $\vec{m}_A$ and $\vec{m}_B$ in xy plane (linear pôlarization). The measured qubits are b_A and b_B in $\{0,1\}$. For the inequalities, we transforme them into $\{+1,-1\}$ with $b'_A = 1 - 2b_A = (-1)^{b_A}$ and $b'_B = 1 - 2b_B = (-1)^{b_B}$.

Quantum physics rules

The expectation value of the product is $\mathbf{E}\left[b'_A \cdot b'_B | \vec{m}_A, \vec{m}_B\right] = \sum_{(b'_A,b'_B)\in\{+1,-1\}^2} \mathbf{P}\left[b'_A, b'_B | \vec{m}_A, \vec{m}_B\right](-1)^{b_A+b_B}$. With $\mathbf{P}\left[\pm 1, \pm 1 | \vec{m}_A, \vec{m}_B\right] = \frac{1+(\pm\vec{m}_A)\cdot(\pm\vec{m}_A)}{2}$, we get $\mathbf{E}\left[b'_A \cdot b'_B | \vec{m}_A, \vec{m}_B\right] = \vec{m}_A \cdot \vec{m}_B$.

We consider the case where $\vec{m}_A \in \left\{\vec{m}_{A,0}, \vec{m}_{A,1}\right\}$ and $\vec{m}_B \in \{\vec{m}_{B,0}, \vec{m}_{B,1}\}$, and the quantity $S = \mathbf{E}\left[b'_A \cdot b'_B | \vec{m}_{A,0}, \vec{m}_{B,0}\right] - \mathbf{E}\left[b'_A \cdot b'_B | \vec{m}_{A,0}, \vec{m}_{B,1}\right] + \mathbf{E}\left[b'_A \cdot b'_B | \vec{m}_{A,1}, \vec{m}_{B,0}\right] + \mathbf{E}\left[b'_A \cdot b'_B | \vec{m}_{A,1}, \vec{m}_{B,1}\right]$.

The calculation according to quantum physics gives $S = \vec{m}_{A,0} \cdot \vec{m}_{B,0} - \vec{m}_{A,0} \cdot \vec{m}_{B,1} + \vec{m}_{A,1} \cdot \vec{m}_{B,0} + \vec{m}_{A,1} \cdot \vec{m}_{B,1} = \vec{m}_{A,0}\left(\cdot\vec{m}_{B,0} - \cdot\vec{m}_{B,1}\right) + \vec{m}_{A,1} \cdot (\vec{m}_{B,0} + \vec{m}_{B,1})$.

Now we consider the specific case where $\vec{m}_A \in \{\vec{x}, \vec{y}\}$ (0° and 90° angles in plane xy) and $\vec{m}_B \in \left\{\frac{\vec{y}+\vec{x}}{\sqrt{2}}, \frac{\vec{y}-\vec{x}}{\sqrt{2}}\right\}$ (45° and 135° angles in plane xy), This gives $S = \vec{x} \cdot \sqrt{2}\vec{x} + \vec{y} \cdot \sqrt{2}\vec{y} = 2\sqrt{2}$.

Local hidden variables ?

Hypotheses:

1. There are hidden independant variables $\left(a'_0, a'_1, b'_0, b'_1\right) \in \{+1,-1\}^4$ that exist before the measuraments such as, after the measurements, $b'_A = a'_0$ if $m_A = m_{A,0}$, $b'_A = a'_1$ if $m_A = m_{A,1}$, $b'_B = b'_0$ if $m_B = m_{B,0}$, $b'_A = b'_1$ if $m_B = m_{B,1}$ (realism);
2. Alice's choice cannot influence Bob's result or vice versa (locality).

Then $|S| = \left|\mathbf{E}\left[b'_A \cdot b'_B | \vec{m}_{A,0}, \vec{m}_{B,0}\right] - \mathbf{E}\left[b'_A \cdot b'_B | \vec{m}_{A,0}, \vec{m}_{B,1}\right] + \mathbf{E}\left[b'_A \cdot b'_B | \vec{m}_{A,1}, \vec{m}_{B,0}\right] + \mathbf{E}\left[b'_A \cdot b'_B | \vec{m}_{A,1}, \vec{m}_{B,1}\right]\right|$ $\leq \max\left\{\left|a'_0 \cdot b'_0 - a'_0 \cdot b'_1 + a'_1 \cdot b'_0 + a'_1 \cdot b'_1\right|\right\}$.

Looking at all the 16 possibilities for $\left(a'_0, a'_1, b'_0, b'_1\right) \in \{+1,-1\}^4$, one can show that $\left|a'_0 \cdot b'_0 - a'_0 \cdot b'_1 + a'_1 \cdot b'_0 + a'_1 \cdot b'_1\right| = 2$, thus $|S| \leq 2$ (Bell's inequality).

Bell's inequality violation: $S = 2\sqrt{2} > 2$ can be reached with quantum physics, for example when $\vec{m}_A \in \{\vec{x}, \vec{y}\}$ (0° and 90° angles in plane xy) and $\vec{m}_B \in \left\{\frac{\vec{y}+\vec{x}}{\sqrt{2}}, \frac{\vec{y}-\vec{x}}{\sqrt{2}}\right\}$ (45° and 135° angles in plane xy).

4.1.2. From EPR "paradox" to Alain Aspect's experiments

(1935) Einstein, Podolsky an Rosen paradox [**EPR1935**]: If one supposes (1) realism, (2) locality, and (3) quantum mechanics completeness, then there is a contradiction. At least one of the hypotheses is wrong. Einstein and his co-authors thought that (3) was wrong.

(1964 – 1969) Bell's inequalities [**Bell1964, CHSH1969**]: It is possible to check by an experiment if (1 and 2) or (3) is wrong.

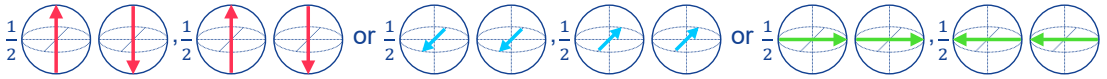
(1982) Alain Aspect's experiments [**ADB1982**]: The Bell's inequalities are violated by the quantum mechanics, (3) is right, (1) or (2) is wrong.

Many people think that (1) is right (realism) and thus (2) is wrong (locality): non-localilty hypothesis. But Einstein's special relativity has always been proven to be right and quantum mechanics do not allow usable information transfer faster than light.

Relational interpretation of quantum mechanism [**Rov1996, Rov2021**]: (1) is wrong (no-absolute-realism but relationalism/relativity) and (2) is right (locality of interactions).

4.2. Usage of Bell's inequalities in E91 protocol

Choice of the Bell pair $BP_{\vec{z},0} \sim xy$-plane (linear-polarization plane) reflection $ir^A_{\vec{z},0} = ref_{xy} \sim |\Psi^+\rangle = \frac{1}{\sqrt{2}}(|0\rangle \otimes |1\rangle + |1\rangle \otimes |0\rangle)$.



Alice has 3 random choices of axis $\vec{m}_A \in \left\{\vec{x}, \frac{\vec{y}+\vec{x}}{\sqrt{2}}, \vec{y}\right\}$ (0°, 45° and 90° angles in plane xy) and Bob has 3 random choices of axis $\vec{m}_B \in \left\{\frac{\vec{y}+\vec{x}}{\sqrt{2}}, \vec{y}, \frac{\vec{y}-\vec{x}}{\sqrt{2}}\right\}$ (45°, 90° and 135° angles in plane xy). There are 9 possibilities for $(\vec{m}_A, \vec{m}_B)$ with probabilit $1/9$ each.

The following cases may happen:

(1) With probability $2/9$, the measurement axes are equal and the measruements will be used by Alice and Bob to build the shared random secret key: $\left(\frac{\vec{y}+\vec{x}}{\sqrt{2}}, \frac{\vec{y}+\vec{x}}{\sqrt{2}}\right)$ and $(\vec{y}, \vec{y})$;

(2) With probability $4/9$, the measurements will be used for the Bell's inequality test, with the measurement axes: $\left(\vec{x}, \frac{\vec{y}+\vec{x}}{\sqrt{2}}\right)$, $\left(\vec{x}, \frac{\vec{y}-\vec{x}}{\sqrt{2}}\right)$, $\left(\vec{y}, \frac{\vec{y}+\vec{x}}{\sqrt{2}}\right)$ and $\left(\vec{y}, \frac{\vec{y}-\vec{x}}{\sqrt{2}}\right)$;

(3) With probability $4/9$, the measurements will not be used with the measurement axes: $\left(\vec{x}, \frac{\vec{y}+\vec{x}}{\sqrt{2}}\right)$, $\left(\frac{\vec{y}+\vec{x}}{\sqrt{2}}, \vec{y}\right)$ and $\left(\frac{\vec{y}+\vec{x}}{\sqrt{2}}, \frac{\vec{y}-\vec{x}}{\sqrt{2}}\right)$.

Without eavesdopping by Eve, Alice and Bob will get $S = 2\sqrt{2}$.

With total eavesdopping by Eve, Alice and Bob will get $|S| \leq \sqrt{2}$ [**E91**].

Thus, the proportion ρ of qubits that are eavesdropped by Eve can be upper-bounded according to what Alice and Bob measure for S: $\rho \leq 2\left(1 - \frac{S}{2\sqrt{2}}\right)$, because $S \leq (1-\rho) \times 2\sqrt{2} + \rho \times \sqrt{2}$.

5. Today's and future QKD systems

1. Some experimental QKD systems
2. Some commercial QKD products
3. QKD Standardization
4. Future of QKD: Quantum Internet

5.1. Some experimental QKD systems

First QKD experiment in 1989, over 0.3 m only [**BB89**]: 64516 light pulses with on average 0.34 photon per pulse → with 9% efficiency reception, about 2000 received pairs of qubits → with 50% worng choice of basies, about 1000 usable pairs of qubits → with distillation and equality confirmation protocols to remove errors, 443 then 403 perfectly shared qubits (i.e., with error $< 10^{-12}$) → with privacy amplification protocol, 175-bit final secret quantum key, with Eve knowing less than $5 \cdot 10^{-9}$ bits of information (!).

Fiber QKD record in 2015: Korzh, B., Lim, C., Houlmann, R. et al., "Provably secure and practical quantum key distribution over 307 km of optical fibre," Nature Photon 9, 163–168 (2015), https://doi.org/10.1038/nphoton.2014.327. About 3 bit/s with 51.8 dB loss (307 km fiber) for 660000-bit key (~3 days). The rate increases to ~900 bit/s for 200 km, and ~10000 bit/s for 100 km.

QKD by satellite in 2017: Liao, SK., Cai, WQ., Liu, WY. et al., "Satellite-to-ground quantum key distribution," Nature Vol. 549, pp. 43–47, 2017, https://doi.org/10.1038/nature23655. They achieved 1000 kbit/s key distribution over 1200 km, with Bell pair creation in the satellite.

Use of more complex realizations of QKD, e.g., Continuous-Variable QKD: For example (CiViQ project), F. Roumestan, A. Ghazisaeidi, J. Renaudier, L. T. Vidarte, E. Diamanti and P. Grangier, "High-Rate Continuous Variable Quantum Key Distribution Based on Probabilistically Shaped 64 and 256-QAM," 2021 European Conference on Optical Communication (ECOC), 2021, pp. 1-4, https://doi.org/10.1109/ECOC52684.2021.9606013. About 67 Mb/s secret key rates on average over a 9.5 km SMF link.

5.2. Some commercial QKD products

A good example is ID Quantique: https://www.idquantique.com/:

- White paper "Understanding Quantum Cryptography" (May 2020): https://marketing.idquantique.com/acton/attachment/11868/f-020d/1/-/-/-/-/Understanding%20Quantum%20Cryptography_White%20Paper.pdf;
- QKD products: Clavis XG QKD System, Cerberis XG QKD System, XGR Series – QKD Platform, Cerberis3 QKD System, Clavis300 Quantum Cryptography Platform, see https://www.idquantique.com/quantum-safe-security/products/#quantum_key_distribution.
  - Cerberis XG QKD System https://www.idquantique.com/quantum-safe-security/products/cerberis-xg-qkd-system/: Quantum Key Distribution for enterprise, government and telco production environments (see datasheet). Performances: 12 dB loss @ 60 km fiber (15 lost qubits each 16 qubits), qubits generated at 1.25 GHz, final key rate 2 kbps, probability of information leakage of 1 bit for 256-bits key is about 10^{-12}.
  - Clavis300 Quantum Cryptography Platform https://www.idquantique.com/quantum-safe-security/products/clavis300-quantum-cryptography-platform/: Integrated Quantum Key Distribution & LEA Encryption System (see datasheet). Performances: Key generation rate 6 kbps @ 12 dB link loss (60 km fiber), max range = 18 dB (90 km fiber), premium version 24 dB.

5.3. QKD Standardization

- QKD group at ETSI: many standard documents.
  See https://www.etsi.org/technologies/quantum-key-distribution

- Quantum Internet Research Group at IRTF: currently 2 draft documents.
  ⇒ QKD is an application case of Quantum Internet.
  See https://irtf.org/qirg.
  See Ludovic Noirie's LINCS reading group presentation on "Quantum Internet", a review of QIRG@IRTF documents (2020/09/09): https://www.lincs.fr/events/quantum-internet/.

5.4. Future of QKD

- Today's QKD systems are limited in distances because of the no-cloning theorem:
  - Few 10s km in fiber communication,
  - Few 100s of km by satellite.
- To increase the distance, one can use of quantum buffers and quantum teleportation (not yet mature technologies).
- Then one can use optical switching to perform quantum routing (mature technology at least for optical circuit switching).

⇒ Quantum Internet to extend QKD between any pair of end points.

Questions?