Quantum Cryptography

Albert Andrea

Eötvös Loránd University, Physics MSc

24/02/2022

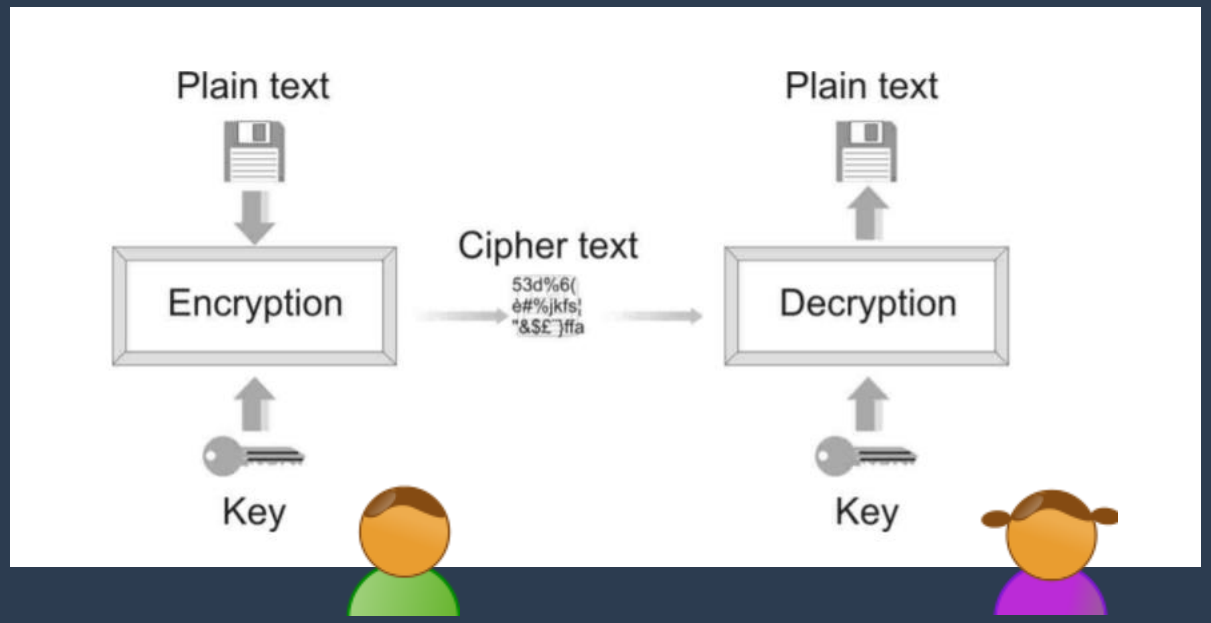
Intorduction

- Quantum cryptography uses the principles of quantum mechanics to encrypt and transmit data in a way that cannot be hacked.

Cryptography

Challenge:
sharing the key

https://marketing.idquantique.com/acton/attachment/11868/f-020d/1/-/-/-/-/Understanding%20Quantum%20Cryptography_White%20Paper.pdf

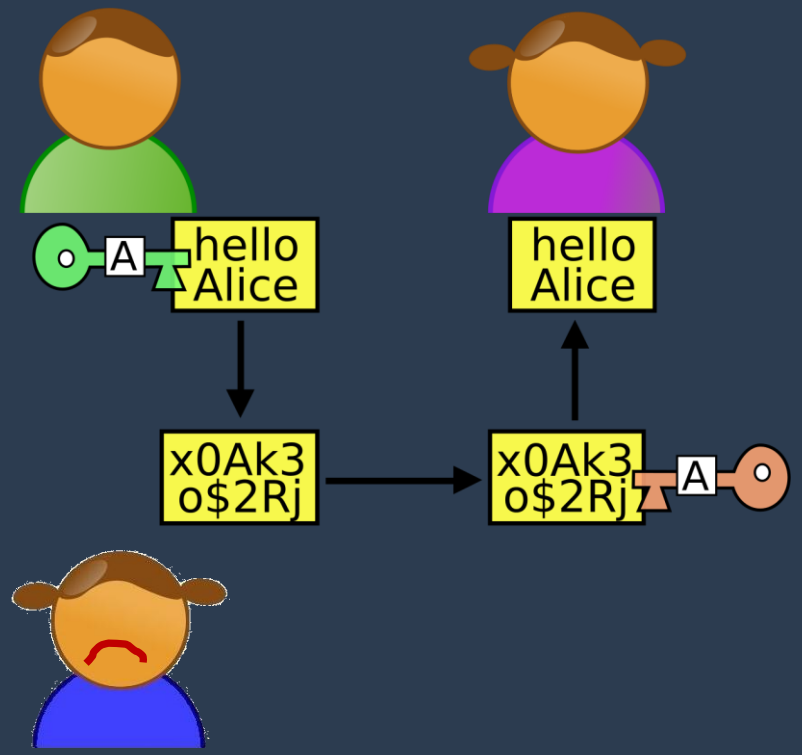


- The sender (Bob) uses a key to encrypt the message.
- He transmits the encrypted message to the receiver.
- The receiver (Alice) decrypts the message with the same key.
- The eavesdropper (Eve) cannot deduce the real message without having the key.

→ "key distribution problem"

Key Distribution

- Solution: public key cryptography
- Briefly:
  - Bob informs Alice he wants to send a secret message.
  - Alice generates a private key and a public key. Retains the private key and sends the public key to Bob (secure one-way channel).
  - Bob uses the public key to encode his message, sends this to Alice who than decodes it with her private key.
  - Eve who has access to their channel cannot recover the private key from the public key.

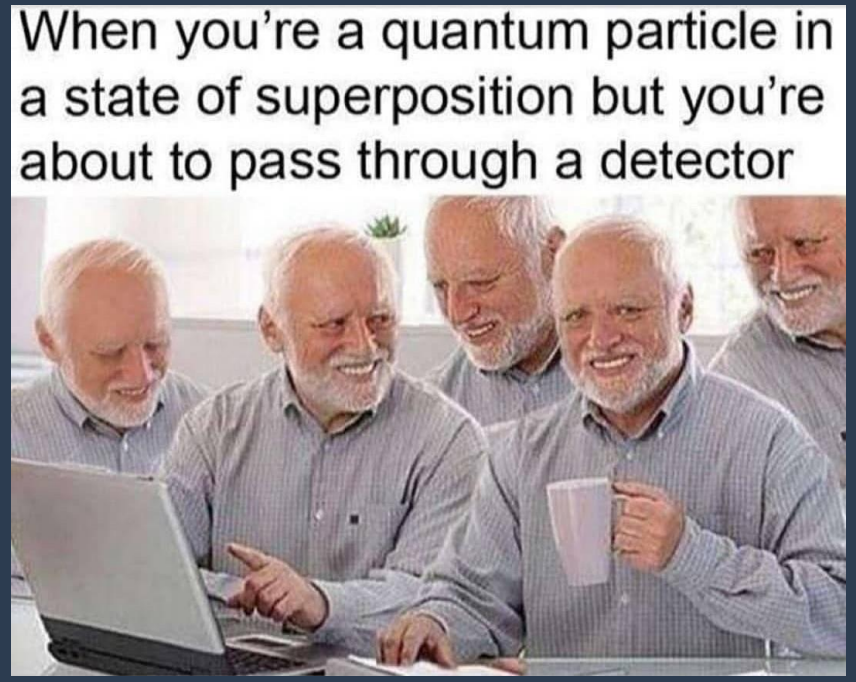


https://en.wikipedia.org/wiki/Alice_and_Bob#/media/File:Asymmetric_cryptography_-_step_2.svg

- The idea of public key cryptography is based on the difficulty in inverting certain mathematical functions, the one-way functions. They are easy to compute but difficult to reverse. (example: factorization – see RSA public-key system)
- The exchange of keys using public key cryptography suffers from two major flaws:
  - It is vulnerable to technological progress: reversing one-way functions can be done, provided one has sufficient computing power or time available.
    - In 1994, Peter Shor, professor of Applied Mathematics at MIT, came up with algorithm which would run on a quantum computer and allow to reverse one-way functions used for all the existing versions of public key cryptography.
  - It is vulnerable to progress in mathematics: mathematicians have not yet been able to prove that public key cryptography is secure. We cannot rule out the existence of classical algorithms able to reverse one-way functions.

Quantum Cryptography

- The exchange of a cryptographic key happens with absolute security guaranteed by the fundamental laws of physics. This key can then be used securely with conventional cryptographic algorithms.
- Since it solves the problem of key distribution, the more correct name for quantum cryptography is Quantum Key Distribution (QKD).
- The basic principle of QKD: observing a quantum object perturbs it in an irreparable way.

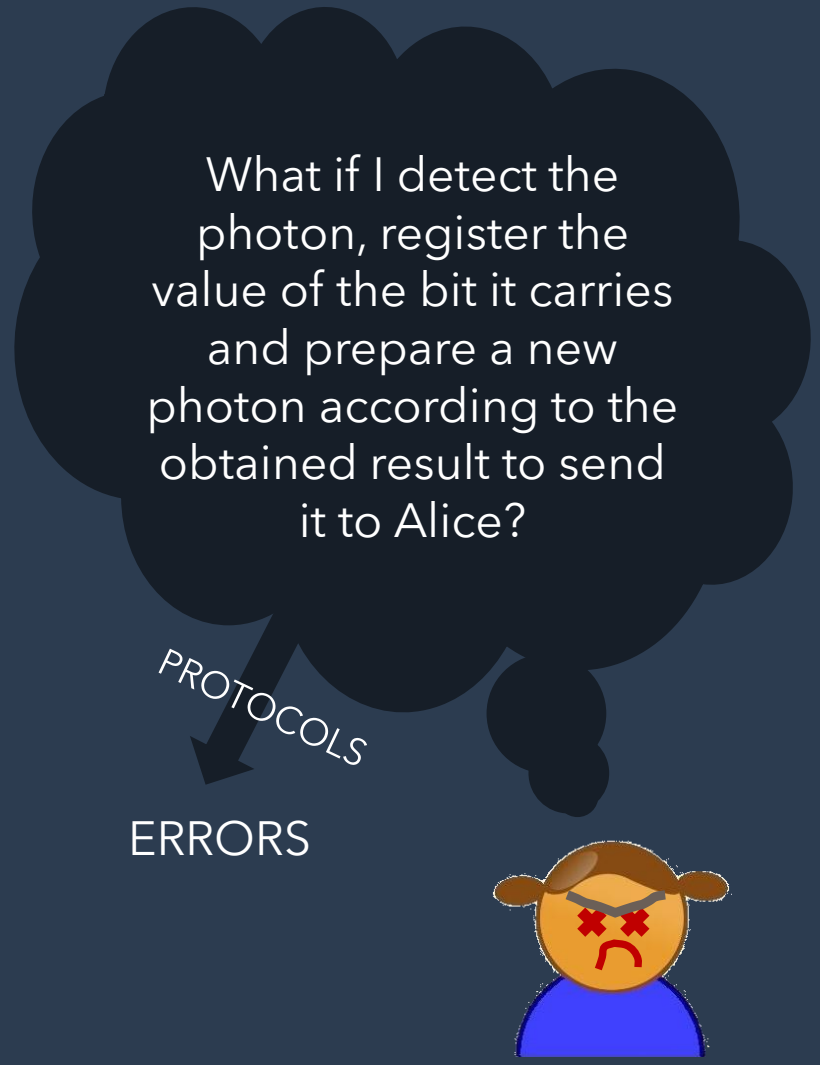


https://ifunny.co/picture/when-you-re-a-quantum-particle-in-a-state-of-9yRdSnNv8

- QKD allows Alice and Bob to detect the presence of Eve: in order to intercept the key she must in some way measure it.
- The process of measuring a quantum system in general disturbs the system → Eve is forced to introduce detectable anomalies ⇒ by transmitting information in quantum states, we can implement a communication system that detects eavesdropping (quantum communication system).
- If the level of eavesdropping is below a certain threshold, a truly secure key can be produced, otherwise no secure key is possible.

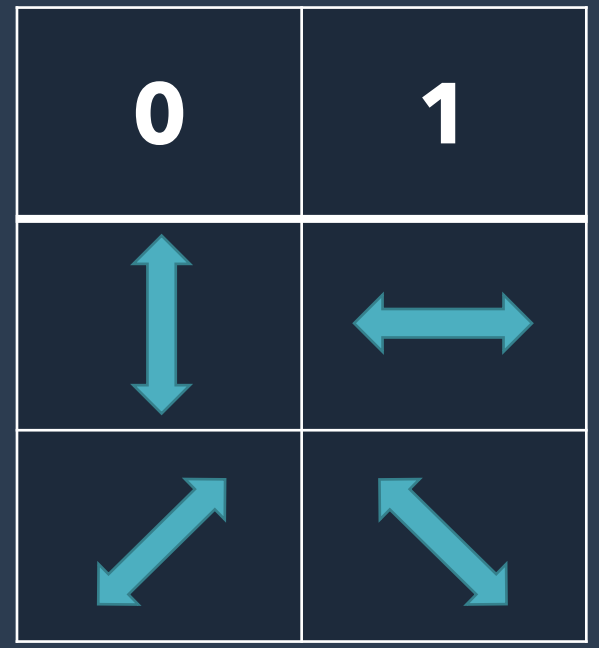
Quantum Communications

- The standard ingredient for quantum communication are photons.
- For each bit of information a single photon is emitted and sent down an optical fiber to the receiver where it is registered and transformed back into an electronic signal.
- Why photons?
  - In order to observe light we must stop it from getting to its destination.
  - We cannot observe half of a photon to measure the value of bit it carries while letting the other half continue its course.

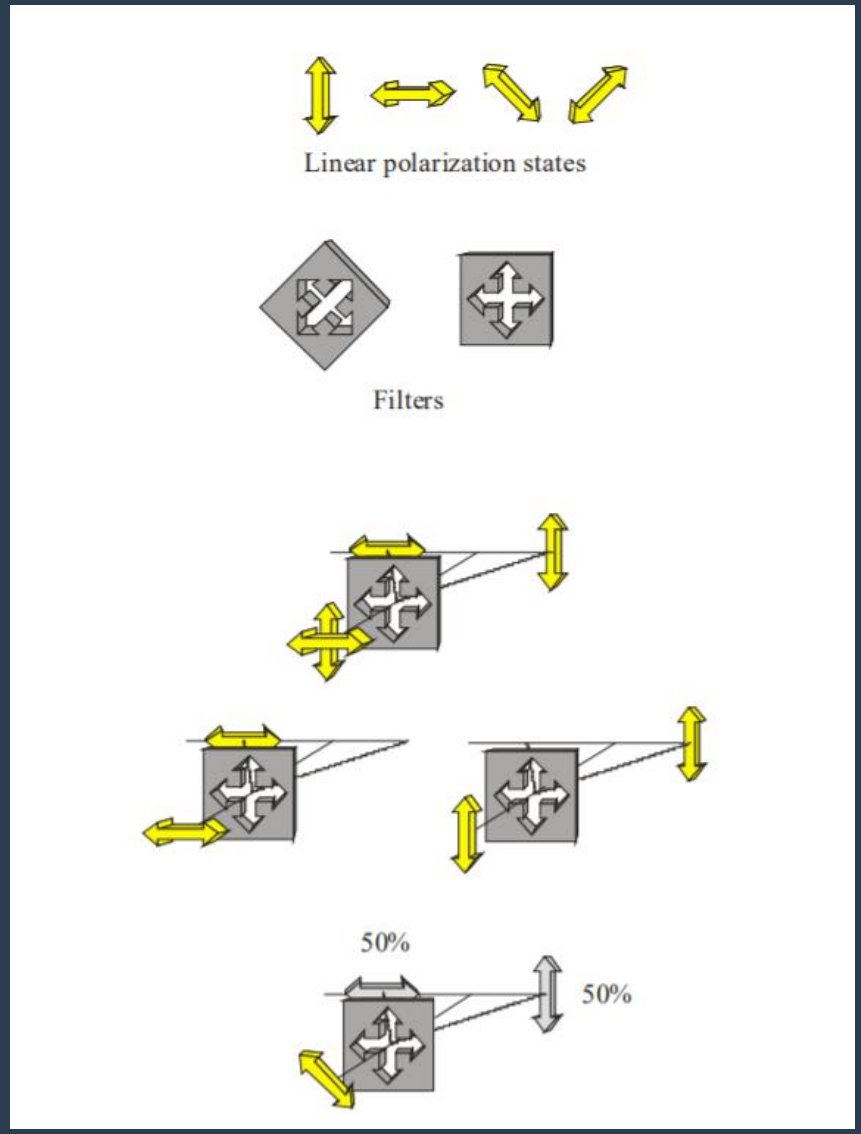


Quantum Key Distribution Protocols

- Here I discuss the BB84 protocol developed by Charles Bennett and Gilles Brassard in 1984. It is the first quantum cryptography protocol.
- In this setting Alice and Bob are exchanging single photons whose polarization states are used to encode bit values over an optical fiber.
- This fiber and the transmission equipment are called the quantum channel.
- We use four different polarization states and agree, for example, that a 1-bit value can be encoded either as a horizontal state or a +45° diagonal one. For a 0-bit value, they will use either a vertical state or a -45° diagonal one.

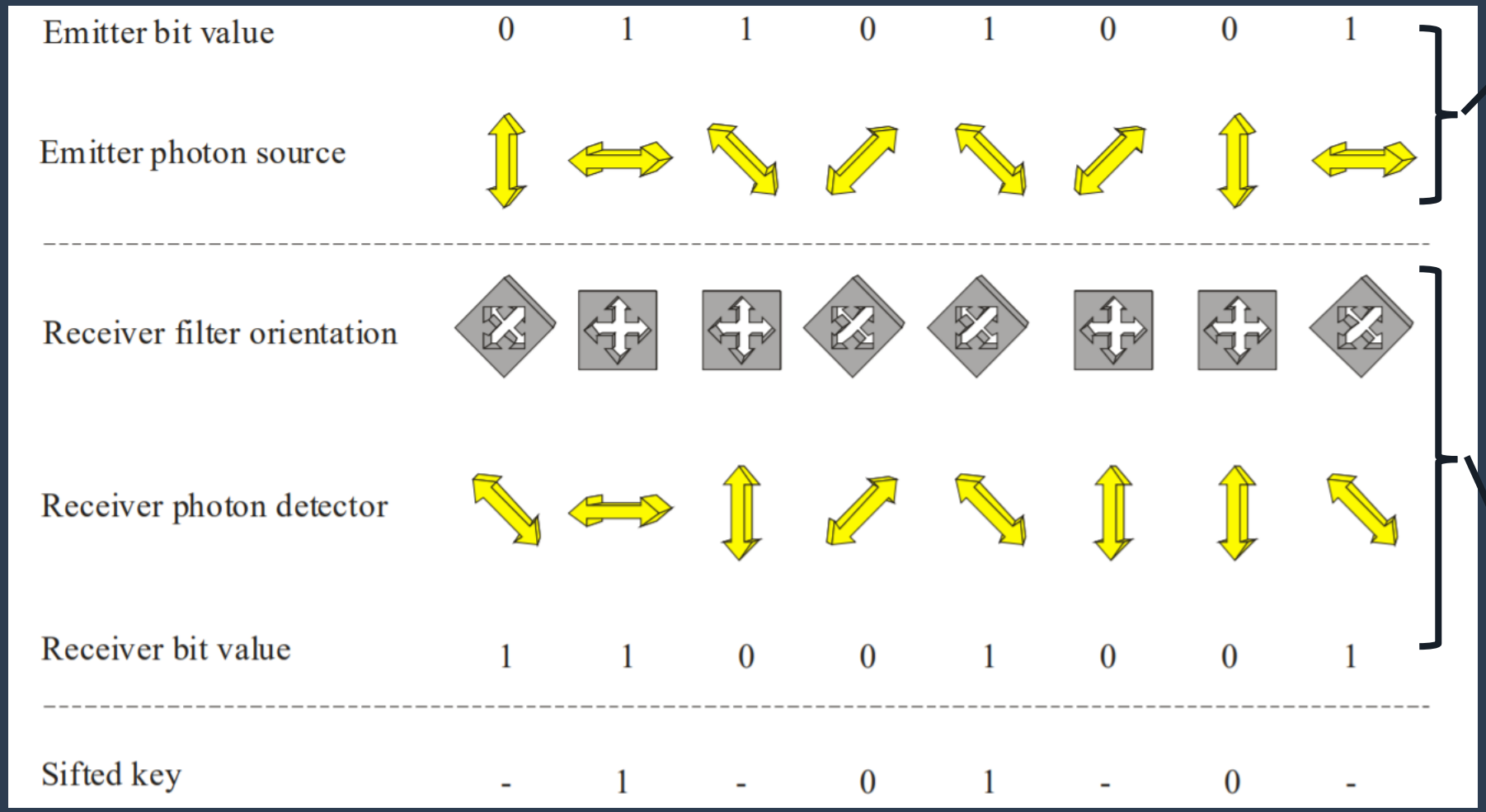


- We can distinguish horizontal states from vertical ones using filters.
- When passing through such a filter the vertically polarized photon is deflected to the right while the horizontally polarized photon is deflected to the left. In order to distinguish between diagonally polarized photons, one must rotate the filter by 45°.
- If a photon is sent through a filter with the incorrect orientation it will be randomly deflected in one of the two directions → impossible to know its orientation before the filter.



https://marketing.idquantique.com/acton/attachment/11868/f-020d/1/-/-/-/-/Understanding%20Quantum%20Cryptography_White%20Paper.pdf

https://marketing.idquantique.com/acton/attachment/11868/f-020d/1/-/-/-/-/Understanding%20Quantum%20Cryptography_White%20Paper.pdf

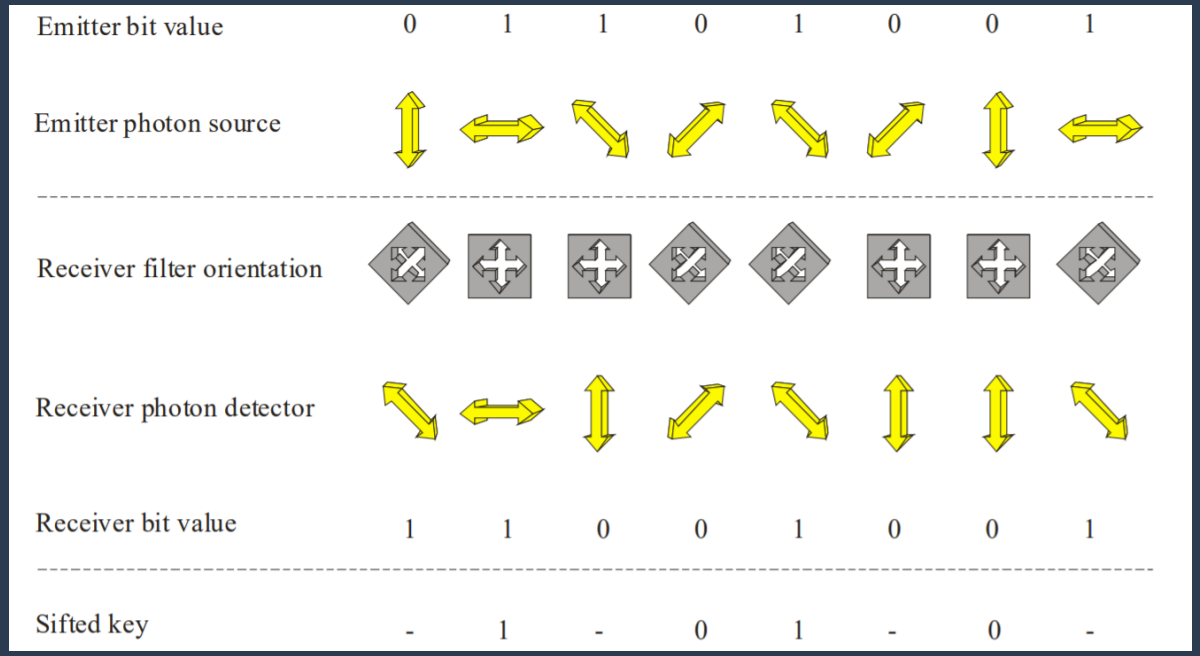


For each bit, the emitter sends a photon whose polarization is randomly selected. He records the orientations in a list.

QUANTUM CHANNEL

For each incoming photon, the receiver randomly chooses the orientation of a filter. She records these orientations, as well as the outcome of the detections.

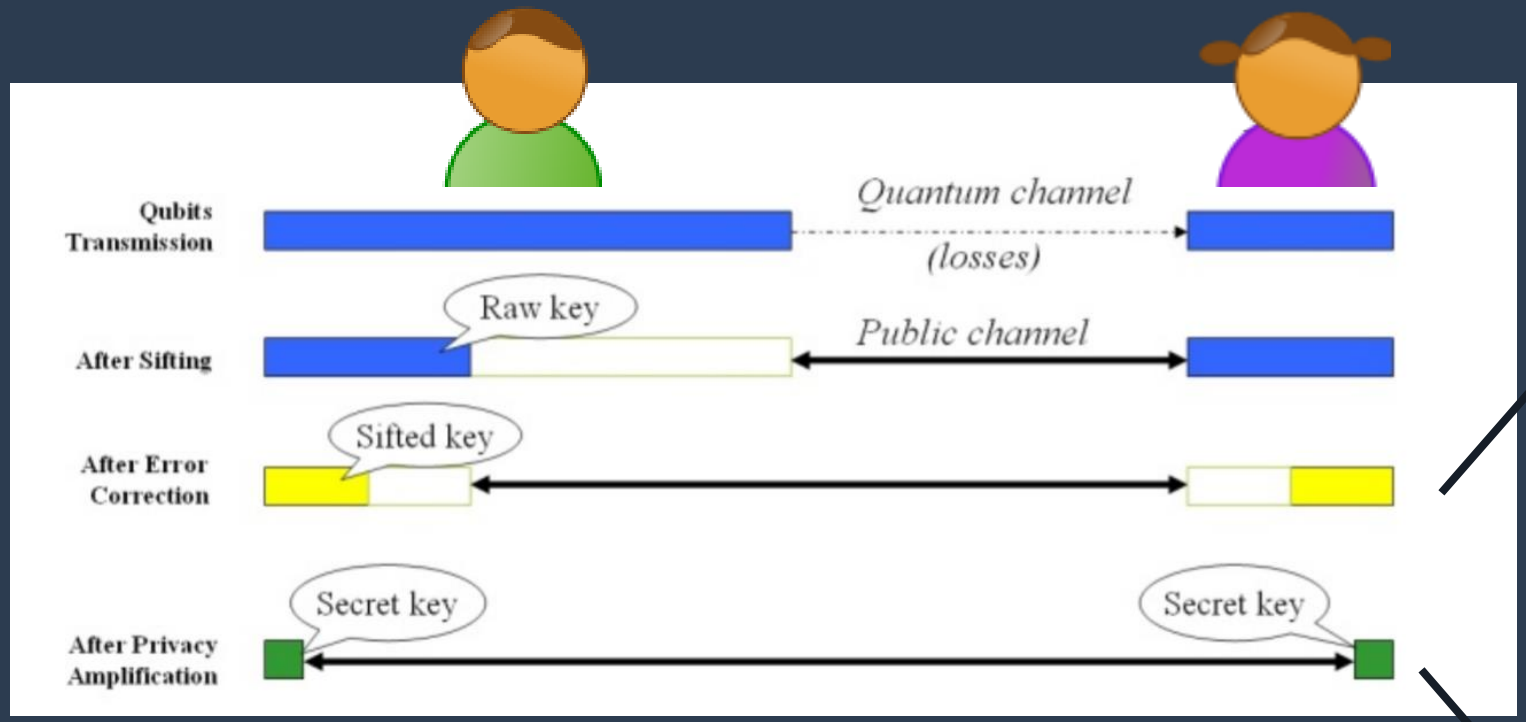
- After the exchange of a large number of photons, the receiver reveals - over a classical channel - the sequence of filter orientations she has used (but not the actual results of her measurements).
- The emitter compares the orientation of the photons he has sent with the corresponding filter orientations. He then announces to the receiver in which cases the orientations were compatible.
- They discard from their lists all the bits corresponding to a photon for which the orientations were not compatible → sifting of the key.



- The sifted key contains a sequence of bits which, in the absence of an eavesdropper, is identical and half the length of the original sequence.
- As verification, they check for the presence of errors by comparing - over a classical channel - a sample of the bits (the bits revealed during this comparison are discarded). If eavesdropping took place, the key would contain errors and the whole procedure is repeated again.

Key Distillation

- The description of the BB84 QKD protocol assumed that the only source of errors in the sequence exchanged by the emitter and the receiver was the action of the eavesdropper.
- Besides the errors introduced by the eavesdropper there is an intrinsic error rate caused by component imperfections or environmental perturbations of the quantum channel (noise). We can attribute all these errors to the eavesdropper.
- Key Distillation is a post processing phase which makes the QKD protocols more robust against noise. It takes place after the sifting of the key and consists of two steps.



https://marketing.idquantique.com/acton/attachment/11868/f-020d/1/-/-/-/-/Understanding%20Quantum%20Cryptography_White%20Paper.pdf

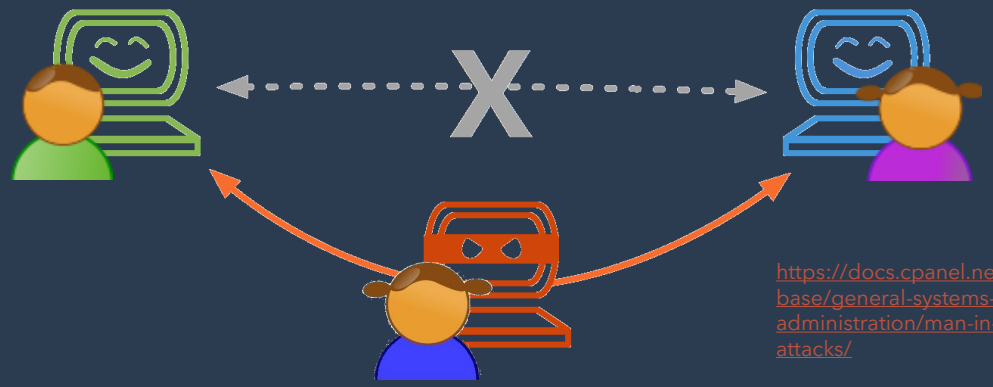
1. Correcting all the errors in the key using a classical error correction protocol. This step also allows to precisely estimate the actual error rate.

2. Compressing the key by an appropriate factor to reduce the information of the eavesdropper (privacy amplification).

Rudimentary Privacy Amplification Protocol

- Let us consider a two bit key which is: 01 and assume that the eavesdropper knows the first bit of the key but not the second one: 0?.
- The simplest privacy amplification protocol consists in calculating the sum of the two bits and to use the resulting bit as the final key: 0+1=1.
- This way, the eavesdropper does not know whether 0 + 0 = 0 or 0 + 1 = 1 is the case. She has no way to decide which one is the correct one. Consequently, she does not have any knowledge on the final key.
- The cost of this privacy amplification protocol is shortening the key by 50%.

- The compression factor depends on the error rate. The higher it is, the more information an eavesdropper may have on the key and the more it must be compressed to be secure.
- Key Distillation works up to a maximum error rate. Above this threshold, the eavesdropper has too much information on the sequence ⇒ it is essential for a quantum cryptography system to have an intrinsic error rate that is well below this threshold – this can be achieved through the system design and the choice of components.
- We also need an authentication step in order to prevent "man in the middle attack". Using a pre-established secret key we can authenticate the first quantum cryptography session (on the classical channel). After each session, part of the key produced is used to replace the previous authentication key.

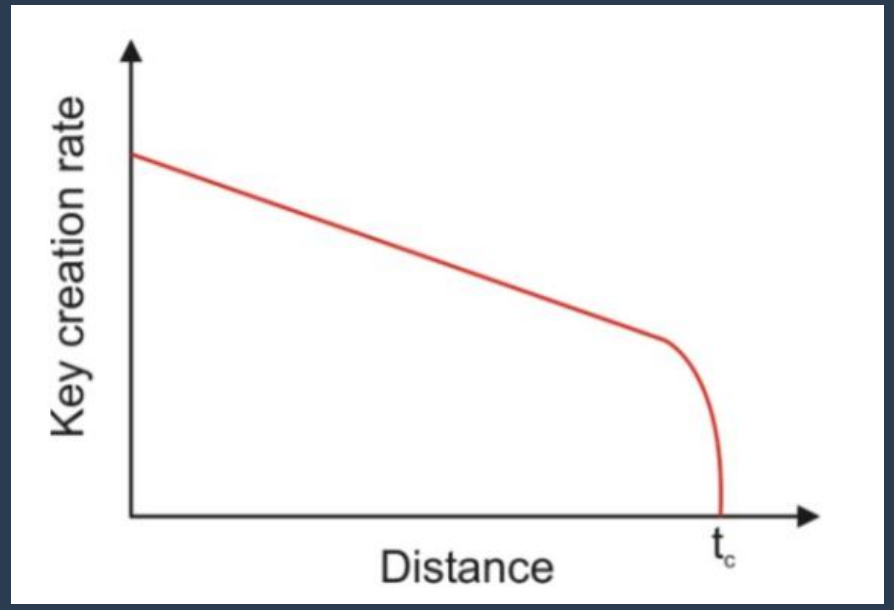


https://docs.cpanel.net/knowledge-base/general-systems-administration/man-in-the-middle-attacks/

Real World Quantum Key Distribution

- The first experimental demonstration of quantum cryptography took place in 1989 and was performed by Bennett and Brassard. A key was exchanged over 30 cm of air ⇒ QKD is possible.
- The first demonstration over optical fiber took place in 1993 at the University of Geneva.

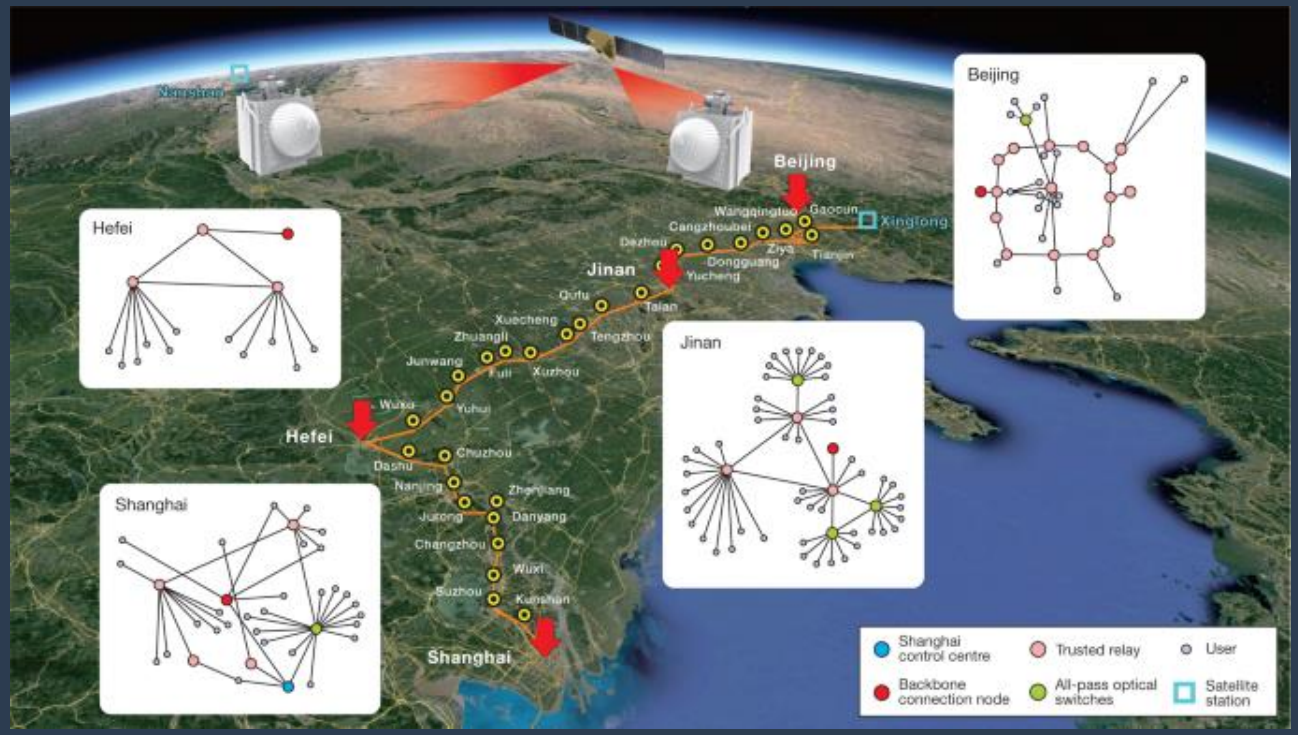
Key exchange rate



https://marketing.idquantique.com/acton/attachment/11868/f-020d/1/-/-/-/-/Understanding%20Quantum%20Cryptography_White%20Paper.pdf

- It is the rate at which a key is exchanged over a certain distance and describes the performance of a QKD system.
- When the distance between the two stations increases, there are two effects reducing the effective key exchange rate:
  - the probability that a given photon reaches the receiver decreases → the raw exchange rate decreases
  - the signal-to-noise ratio decreases → the error rate increases → the effective key creation rate decreases

- Typical key exchange rates for existing QKD systems range from hundreds of kilobits per second for short distances to hundreds of bits per second for greater distances.
- The span of current QKD systems typically reaches hundred kilometers.
- One possible solution to the low key exchange rate at large distances is to set up a network of trusted nodes with QKD repeaters to increase the distance. These nodes have to be trusted and physically secured because the keys are available at each node. This is the approach adopted for the Chinese QKD backbone between Beijing and Shanghai (11000 km long QKD backbone).



https://www.nature.com/articles/s41586-020-03093-8

Perspectives for Future Developments

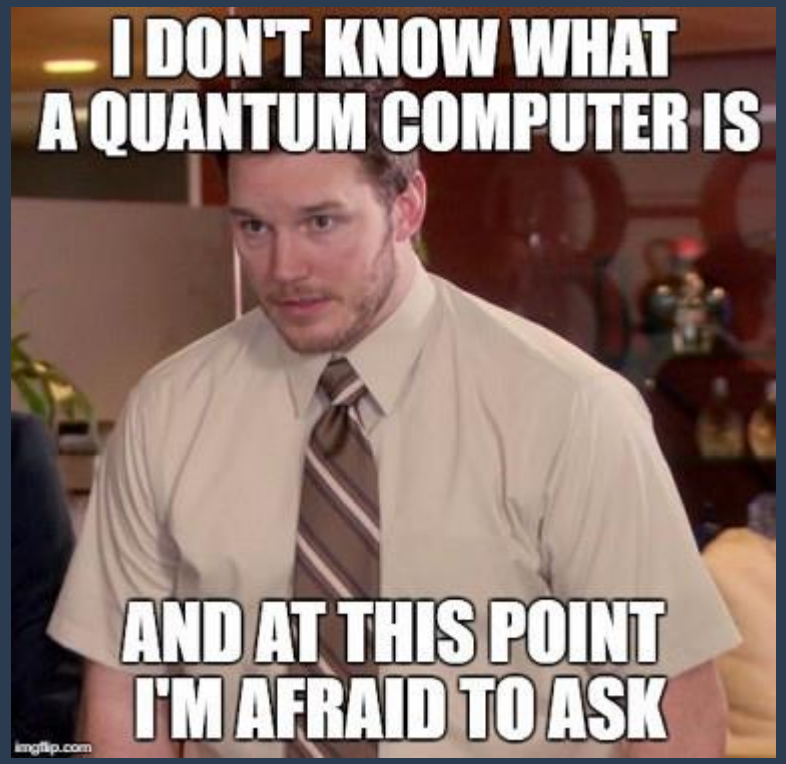
- Increasing the range of the systems and providing a global QKD network.
- Getting rid of the optical fiber: exchanging keys in free space between a terrestrial station and a low earth orbit satellite.
  - An optical link between the ground and the satellite at an altitude of roughly 800 km can be established.
  - The satellite passing over a second station (located thousands of kilometers away from the first one) can retransmit the key.
  - The world's first quantum communication satellite, named Micius was launched by China in 2016.

- Building quantum repeaters: they would rely on quantum teleportation to send a photon from one node to another without measuring its state. They could be used to extend the key exchange range over arbitrarily long distances. Since the state of the photon is not known, the nodes do not have to be trusted anymore.
  - Quantum teleportation has already been realized experimentally, however the quantum memories needed to store the photons at various stages during the transmission are not yet been realized.

Conclusion

- QKD is neither vulnerable to technological nor to mathematical progress.
- QKD provides Quantum-Safe security against the threat of a quantum computer.
- The current distance limitations for QKD will be lifted in the near future through the use of trusted nodes, free space QKD and quantum repeaters.
- QKD networks will soon become a reality.

https://medium.com/@sundeep985/a-peek-into-quantum-computing-vs-cryptography-68a07d380054



References

- https://marketing.idquantique.com/acton/attachment/11868/f-020d/1/-/-/-/-/Understanding%20Quantum%20Cryptography_White%20Paper.pdf
- https://www.qmunity.tech/post/quantum-cryptography-explained
- https://medium.com/@quantum_wa/quantum-cryptography-communication-87d2048eed23
- https://mpl.mpg.de/fileadmin/user_upload/Chekhova_Research_Group/Lecture_4_12.pdf
- http://gva.noekeon.org/QCandSKD/QCandSKD-introduction.html