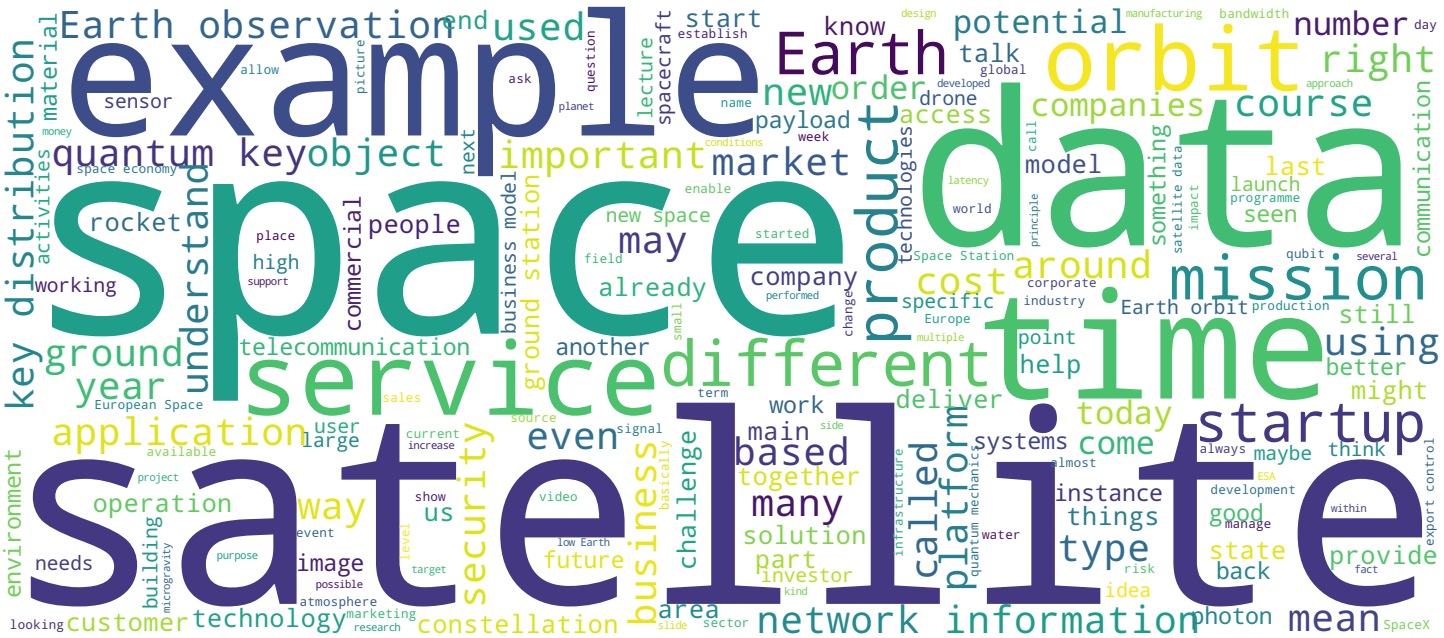
SatCom communications security

New Space Economy

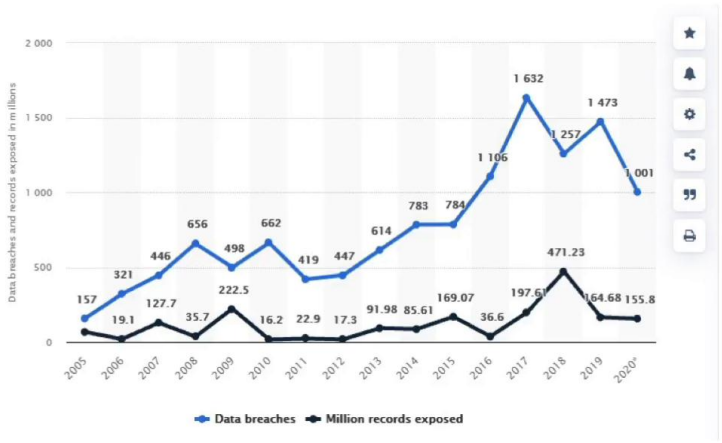
Andrea Alberti
PMOD/WRC

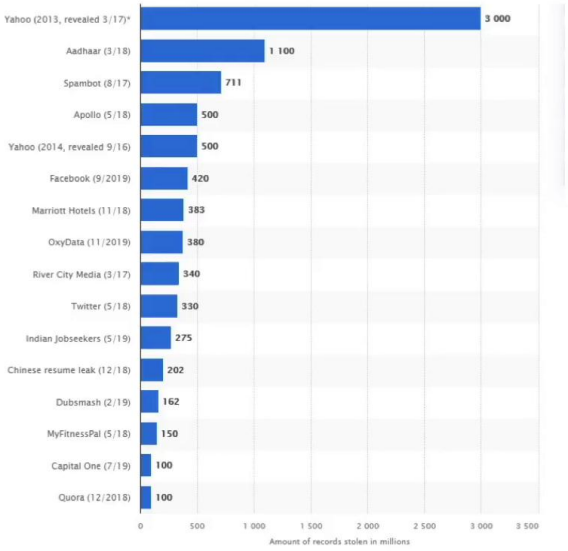


Search MOOC

Video

Quantum Key Distribution





https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/
https://www.statista.com/statistics/290525/cyber-crime-biggest-online-data-breaches-worldwide/

We are missing the perspective of securing our telecommunications. We might have heard about the cyber attacks against administrations, about institutions, and against businesses. In these two plots, there are some data about cyber attacks to organizations. These represent a breach of security, of confidentiality, of privacy. The increasing computing power and the increasing ability of hackers is able, not only to expose private data like mine or yours to potential criminals, but also to block full administrations or governments.

Notes

Summary

0m 05s

Quantum Key Distribution

- QKD can be used to secure communication
  - Governments
  - Administrations
  - Industries
  - Banks
  - Insurances
  - Military

The use of quantum key distribution would implicit increase the security of data protection by the laws of quantum mechanics. Governments, administrations, industries, banks, insurances could leverage on quantum key distributions to protect their data and information. And obviously defense and military, anybody that would want to ensure the highest level of protection to their data and information.

Notes

Summary

0m 47s

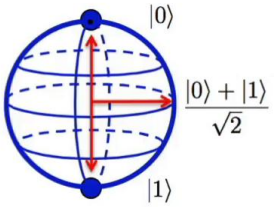
Quantum Key Distribution - Basics

- QKD is used to generate and distribute secret keys only known between shared parties

Classical Bit
0
1

2 Exclusive states

QuBit (photon or electron)



Superposition (0 and 1 at the same time)

https://qoqms.phys.strath.ac.uk/research_qc.html

QKD is based on the principles of quantum mechanics. In a normal digital process, a single, good old classical bit would have two states: either 0 or 1. In quantum communications and quantum computing, electrons or photons are used to transmit quantum information. In this case, they are called quantum bits or qubits. A quantum bit or qubit is a superposition of 0 and 1 at the same time.

Notes

Summary

1m 21s

Quantum Key Distribution - Basics

n qubits

2^n *combinations, at the same time*

https://medium.com/the-research-nest/understanding-the-theory-and-math-behind-qubits-2bf86a56441c

So yes, a single qubit can take two values at once. And in a first approximation, every operation that a qubit is executing is performed on both values at the same time, instead of being performed on an exclusive state of 0s and 1s. So much alike in a normal digital process, n bits lead to the 2_n combination of states. Also, in quantum processing and in quantum mechanics, n bits leads to 2_n states. The difference is that these states, thanks to the superposition, can coexist at the same time.

Notes

Summary

1m 59s

Quantum Key Distribution – Why Space?

- Every interaction with the photon changes their state forever
- Limitation of Ground based fiber infrastructure
  - Network elements alter the state
  - Natural photon degradation along the fiber
- Ground Limits
  - 100-150 km in operational conditions
    1000 km world record

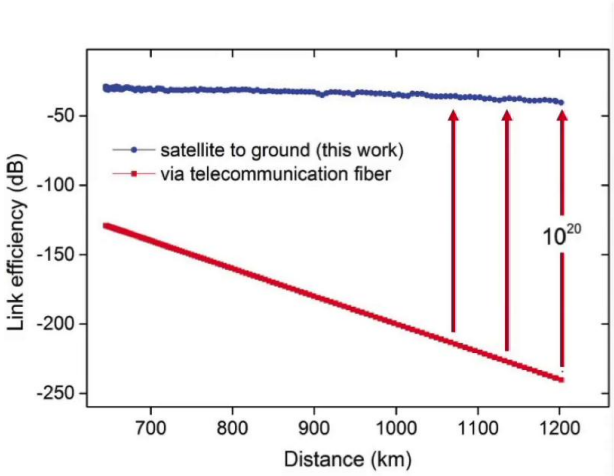
Now we talked about photons and quantum, but why are space assets relevant for quantum key distributions and to protect our information? Briefly, every interaction with a transmitted photon will change its state forever. The ground infrastructure that is fiber-based has two main limitations: firstly, between two communication points, seldomly or never, the fiber is deposited with no interruption. Optical amplifiers, connectors, couplers, routers are placed in order to manage and extend the network. Each of these interactions lead to a potential loss of the desired state. In addition, the state of the photon would change anyhow as it runs along the fiber due to the implicit transmission losses of the material, or photons could simply get lost.

Notes

Summary

2m 55s

Quantum Key Distribution – Why Space?



SK Liao · 2017 "Satellite-to-ground quantum key distribution"

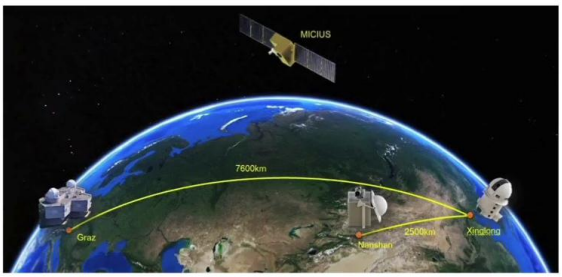
In space instead, or from space to ground, or vice versa, we would only need to worry about the interaction with the atmosphere, or almost.

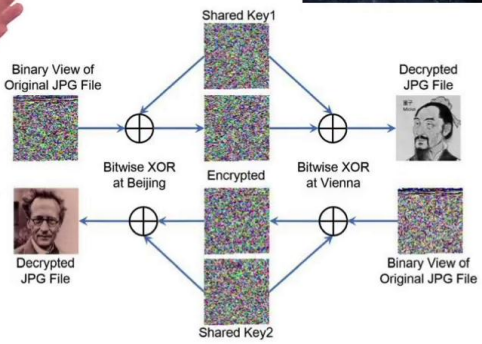
Notes

Summary

4m 01s

Quantum Key Distribution – Where do we stand?





Science
https://phys.org/news/2018-01-real-world-intercontinental-quantum-enabled-micius.html

In quantum key distribution from space, we are still pioneering. Chinese and Austrian scientists have been establishing the first successful use of quantum key distribution through space in 2018 using the Chinese station, Tiangong-2, and a satellite called Micius.

Notes

Summary

4m 13s

Quantum Key Distribution – Where do we stand?

ESA QUARTZ (now EAGLE1) QKD Demonstration Mission (Team Representative, ESA)

ESA SAGA Operational Mission (ESA)

In Europe? In early 2001, European Commissioner, Breton, identified, in an intervention at the European Space Conference, that connectivity and the securing of the digital connections is one of the priorities of European space. Europe is reacting and is preparing the ground for the first demonstrative and operative missions for QKD, respectively: Eagle 1and SAGA. But we are still at a very, very early stage.

Notes

Summary

4m 36s

Quantum Key Distribution
Viable Optical Ground Stations a Key

One of the key elements to enable a commercially viable quantum key distribution from space is the availability and viability of ground stations and how they will interact with the ground infrastructure. In lasercom, we have seen that ground stations shall be located in strategic locations in order to maximize the bandwidth capability. Now for quantum key distribution from space to happen, we have to ask ourselves, what shall we do for security and confidentiality reasons? Shall each business, that needs to exchange quantum keys, needed to establish a ground station on the roof or in the garden? Will this be the commercially viable solution?

Notes

Summary

5m 12s