BRNO UNIVERSITY OF TECHNOLOGY FACULTY OF INFORMATION TECHNOLOGY

Excel@FIT 2023

Quantum key distribution

Author: Bc. Martin Litwora   Supervisor: prof. Dr. Ing. Pavel Zemčík, dr. h. c.

Danger of quantum computers

Table 1: Security Comparison

Type of Attack	Symmetric Encryption			Public Key Encryption		
		Key Length	Bits of Security		Key Length	Bits of Security
Classical Computers	AES-128	128	128	RSA-2048	2048	112
	AES-256	256	256	RSA-15360	15,360	256
Quantum Computers	AES-128	128	64	RSA-2048	2048	25
	AES-256	256	128	RSA-15360	15,360	31

Figure 1: Encryption comparison [1]

Bits of security is a number of steps needed to crack the algorithm by the most efficient attack. For example 64 bits of security means 2^{64} steps to break the algorithm.

Solutions:

1) Post-quantum algorithms. Some algorithms are in process of standardization by NIST. They are based on the shortest vector problems (lattice-based cryptography)
2) Doubling the key size for symmetric cryptography (not a proper solution)
3) Using a one-time pad with a QKD system. Vernam Cipher (OTP) is proven to be unbreakable. However, requires a new key for every message. The key must be at least the same size as the message and truly random

For devices that are limited by battery and computational power, it is necessary to find a proper cryptographic solution that is secure and saves the device's resources

What is QKD?

- Distribution of random secret keys over the quantum channel
- Implements many different cryptographic protocols
- Security is based on quantum mechanics. In general, measuring a quantum state disturbs the system. If an attacker tries to measure the key he introduces the detectable anomaly

Problems:

- Low key rate (around 3kbits/s)
- Single photon generator is complex and expensive technology -> photons are generated in pulses that contains a low number of photons (COW protocol)
- Limited channel distance of the optical fibres (today usually between 60 to 100 km) -> using satellites and laser transfers for long distances. The record is a quantum channel from China to Austria (over 7600 km) [2]

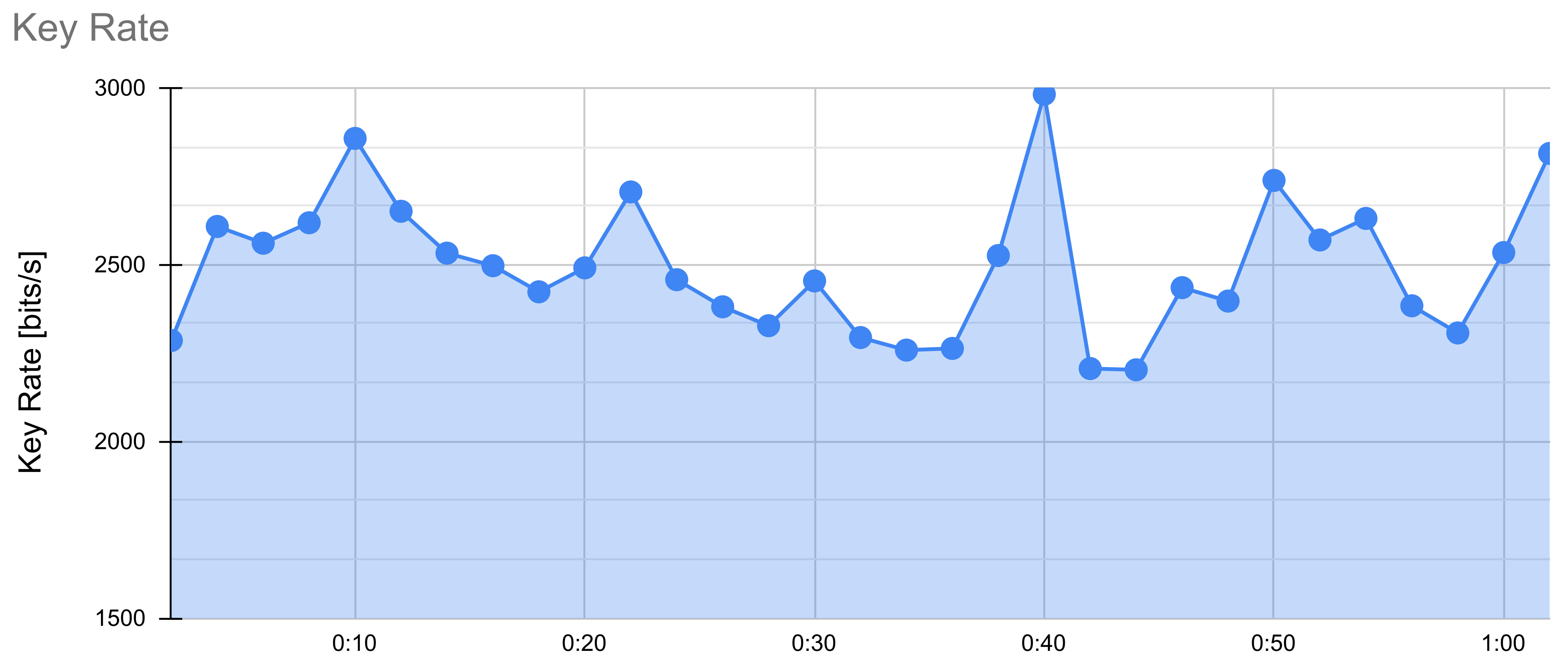

Figure 2: Key rate during one hour

Measured average key rate of the fibre optics channel 2.506 kbit/s

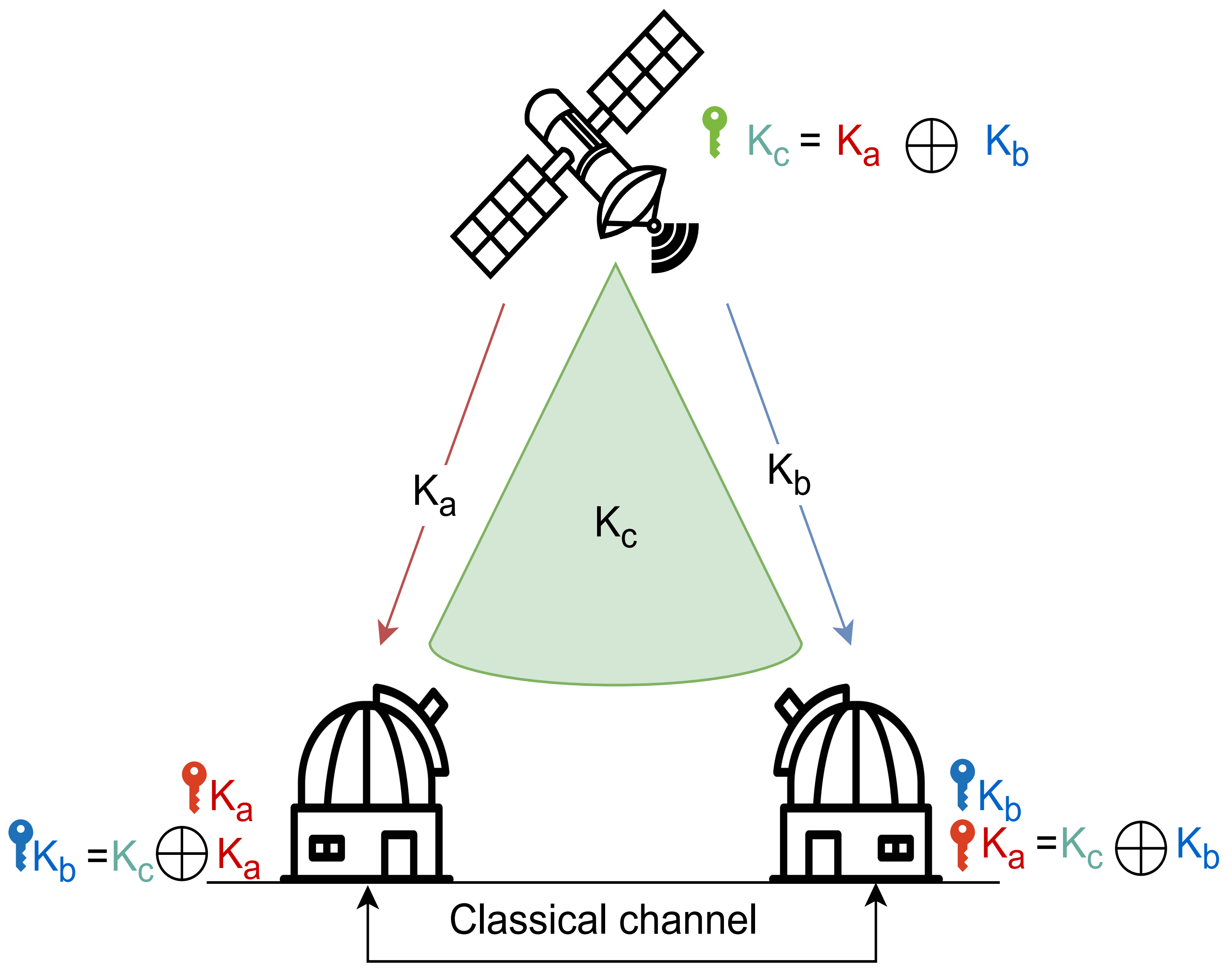

Figure 3: Key distribution over the satellite link

Satellite fly in the Low Earth Orbit (LEO) and serve as a transmitter of the signal (downlink). The ground station needs to have a line of sight with the satellite. It is possible to use multiple satellites that would communicate with each other.

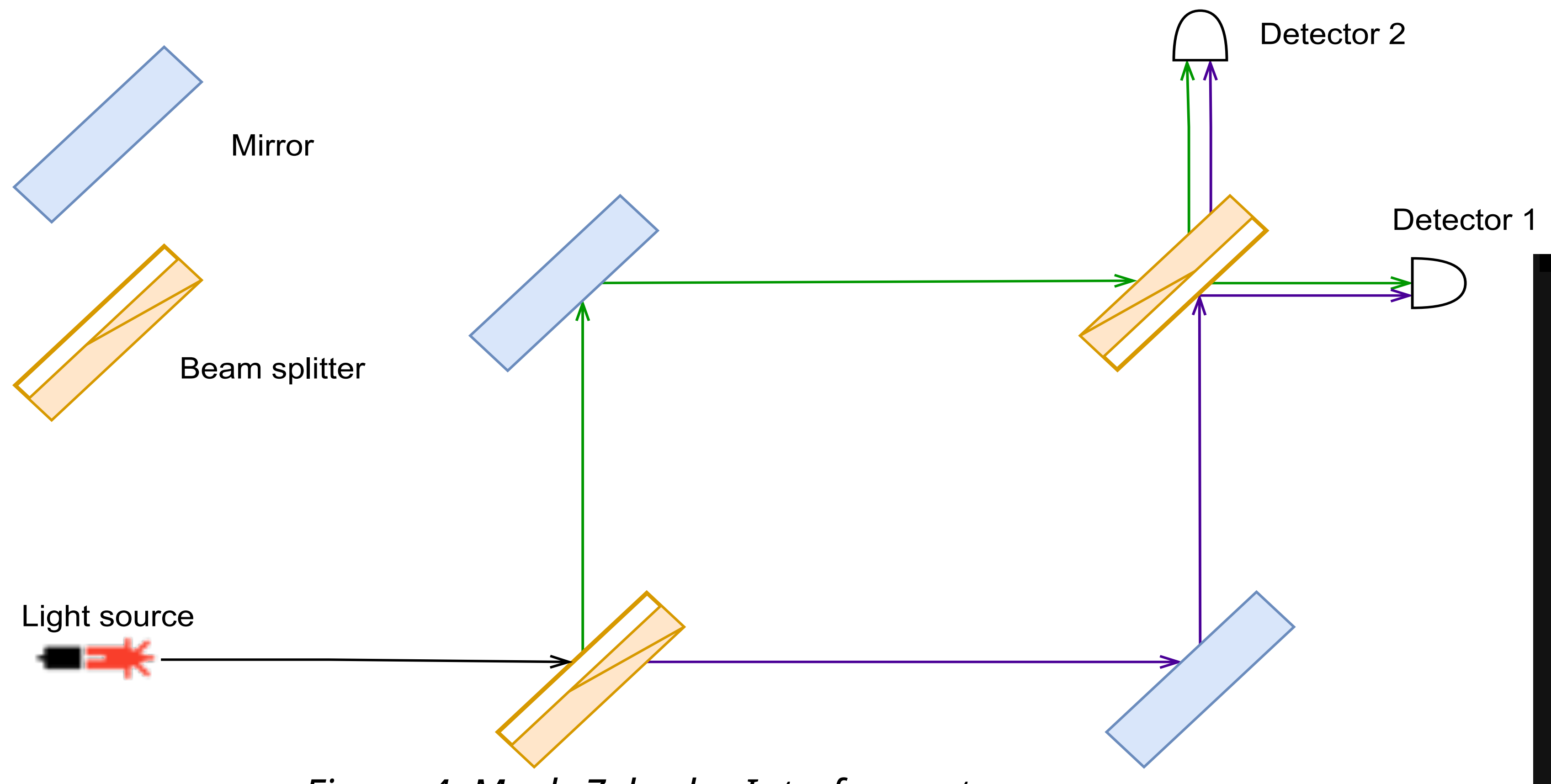

Figure 4: Mach-Zehnder Interferometer

Used to check the coherence of incoming pulses. If the coherence is disturbed it may indicate the presence of an intruder. The imperfections of the channel and the detectors need to be taken into account.

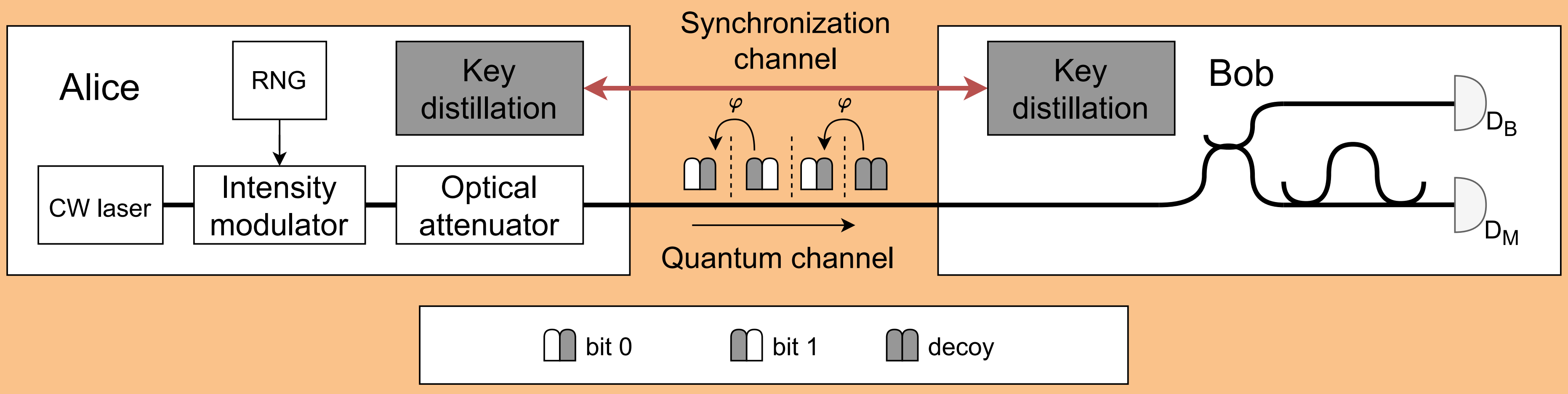

Figure 5: COW Protocol

The Coherent One Way protocol uses time-bin encoding. Bits are represented by a pair of consecutive pulses. The grey colour indicates that the pulse contains photons with mean photon number $\mu = 0.5$. The decoy pulses are used to detect the presence of an attacker. The key distillation serves for QBER calculation and filtration of decoy bits.

Problems with laser transfers in the free space:

- Complicated synchronization between satellite and ground stations
- The atmosphere that is up to 10 km high can negatively impact the signal. For example: clouds, fog, rain, atmospheric turbulences, and high background solar noise

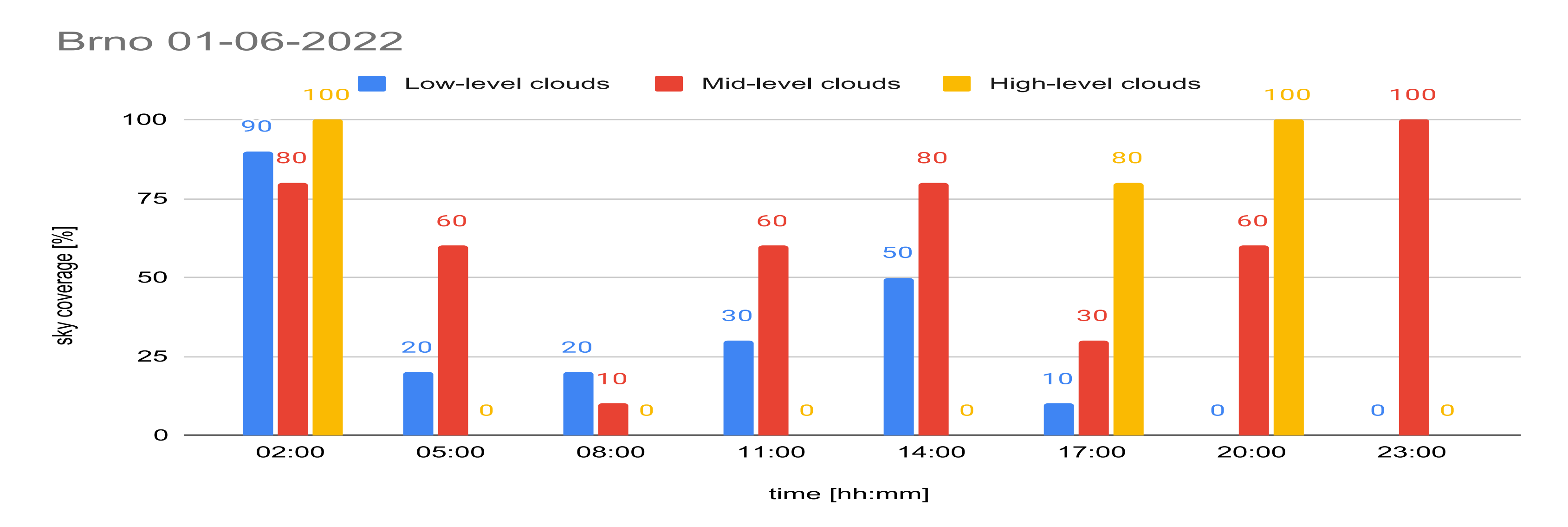

Figure 6: Cloud coverage on 1st June 2022

Clouds are the most dominant issue

Goal:

- Measure the attenuation of the fibre optic quantum channel
- Simulate the attenuation of the free space laser communication that is affected by clouds. Different cloud types can have different attenuation indexes. Cloud forecast can differ during the year (winter is usually more cloudy than summer)

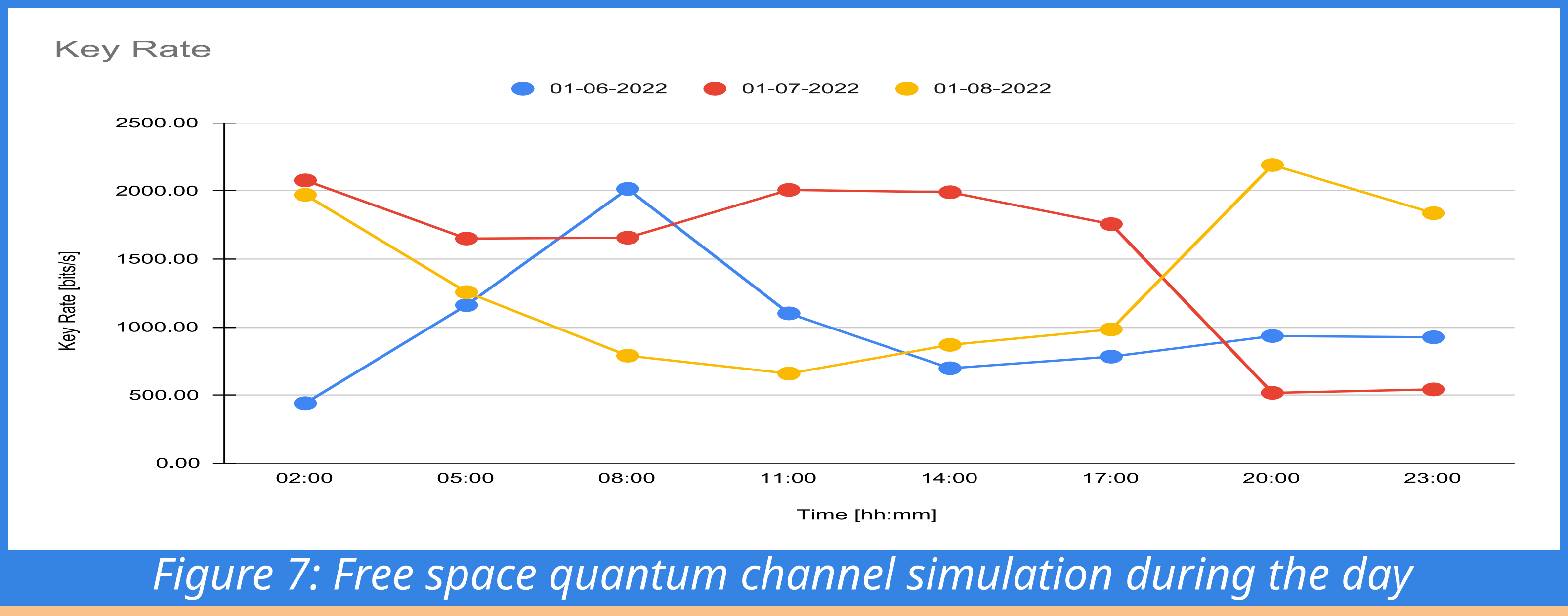

Figure 7: Free space quantum channel simulation during the day

[1] Karen Martin: Waiting for quantum computing, TechBeacon, 15. August 2018. [cit. 2023-04-20], https://techbeacon.com/security/waiting-quantum-computing-why-encryption-has-nothing-worry-about

[2] Satellite-Relayed Intercontinental Quantum Network. *Phys. Rev. Lett.* American Physical Society. January 2018, volume. 120, n. 3, DOI: 10.1103/PhysRevLett.120.030501. https://link.aps.org/doi/10.1103/PhysRevLett.120.030501.

Brno University of Technology, 2023