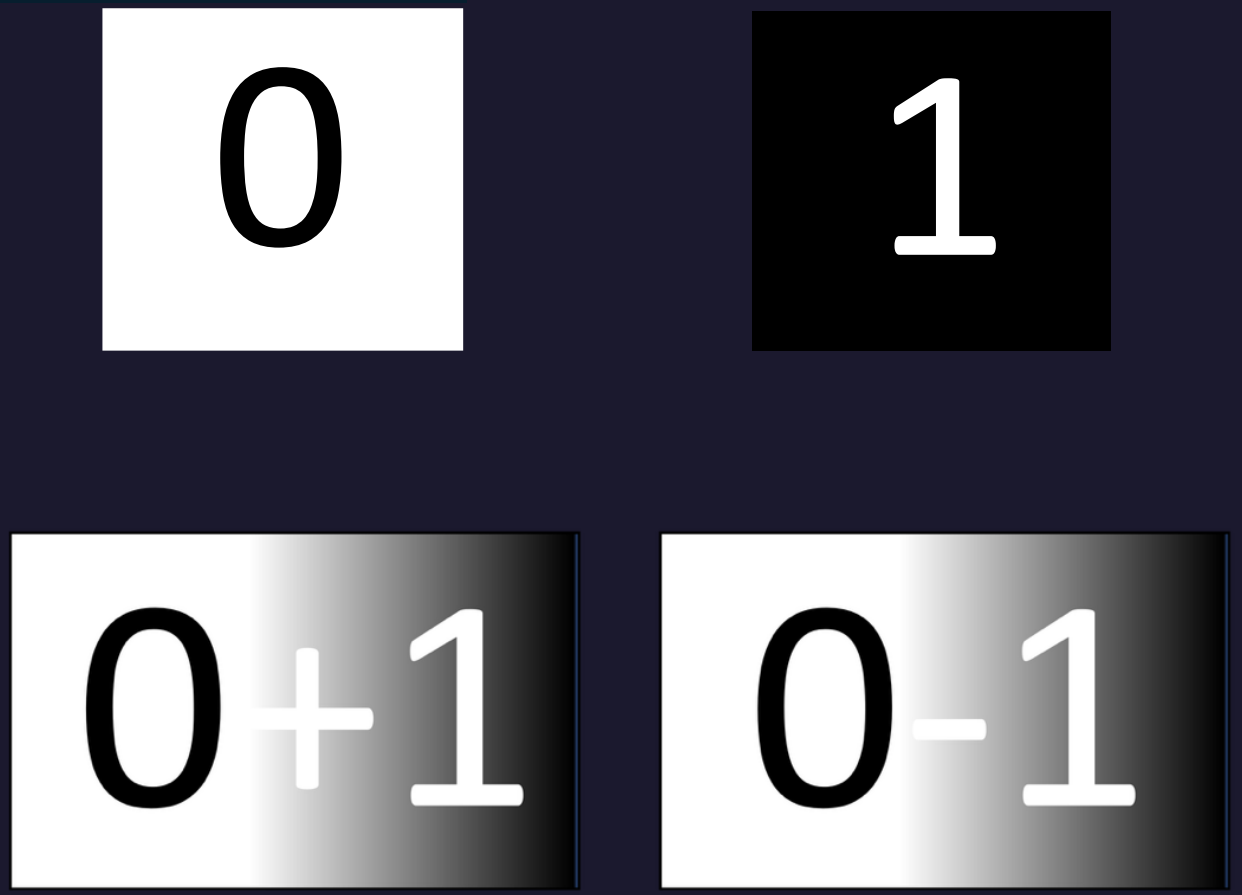
Metrology for Quantum Communication

Wolfgang Tittel

University of Geneva



Metrology for Quantum Communication



Wolfgang Tittel

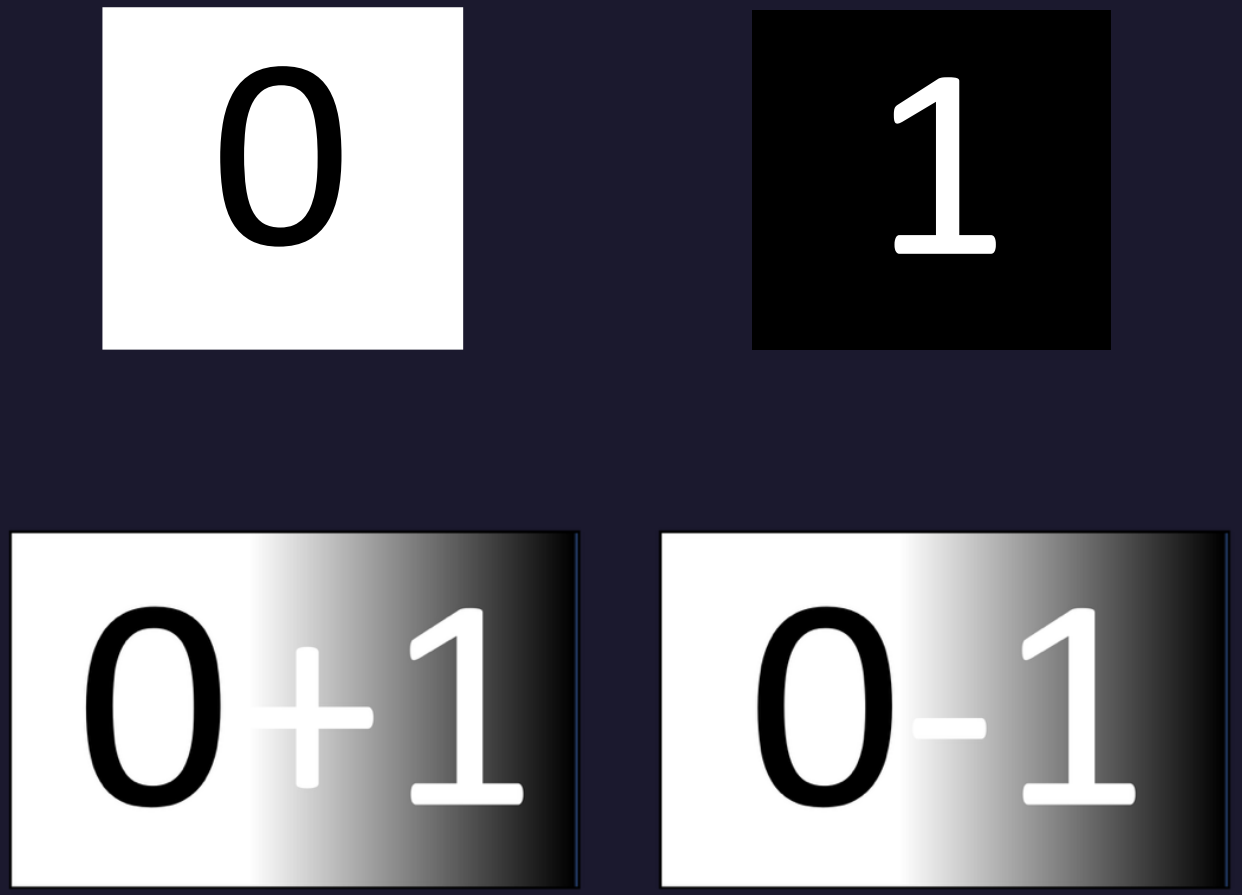
University of Geneva

UNIVERSITÉ DE GENÈVE

⟨S|Q|I⟩ Swiss Quantum Initiative

Metrology for Quantum Communication

- Communication security in a world with quantum and classical computers
- Quantum key distribution and physics-based security
- Metrology for Quantum Communications

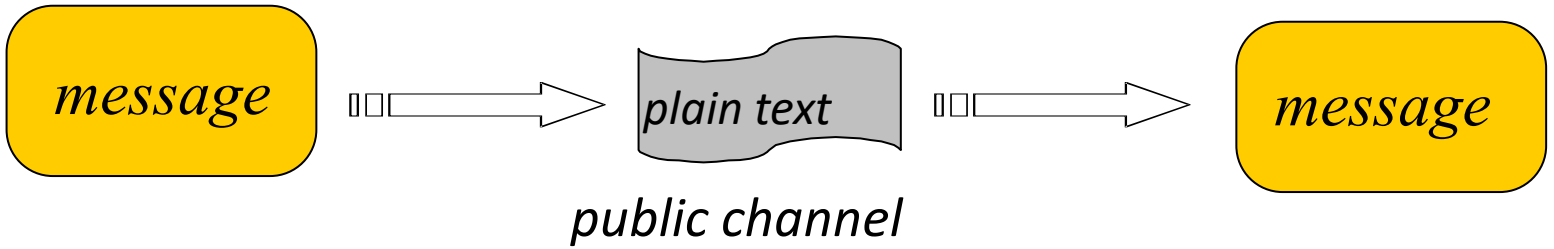


UNIVERSITÉ DE GENÈVE

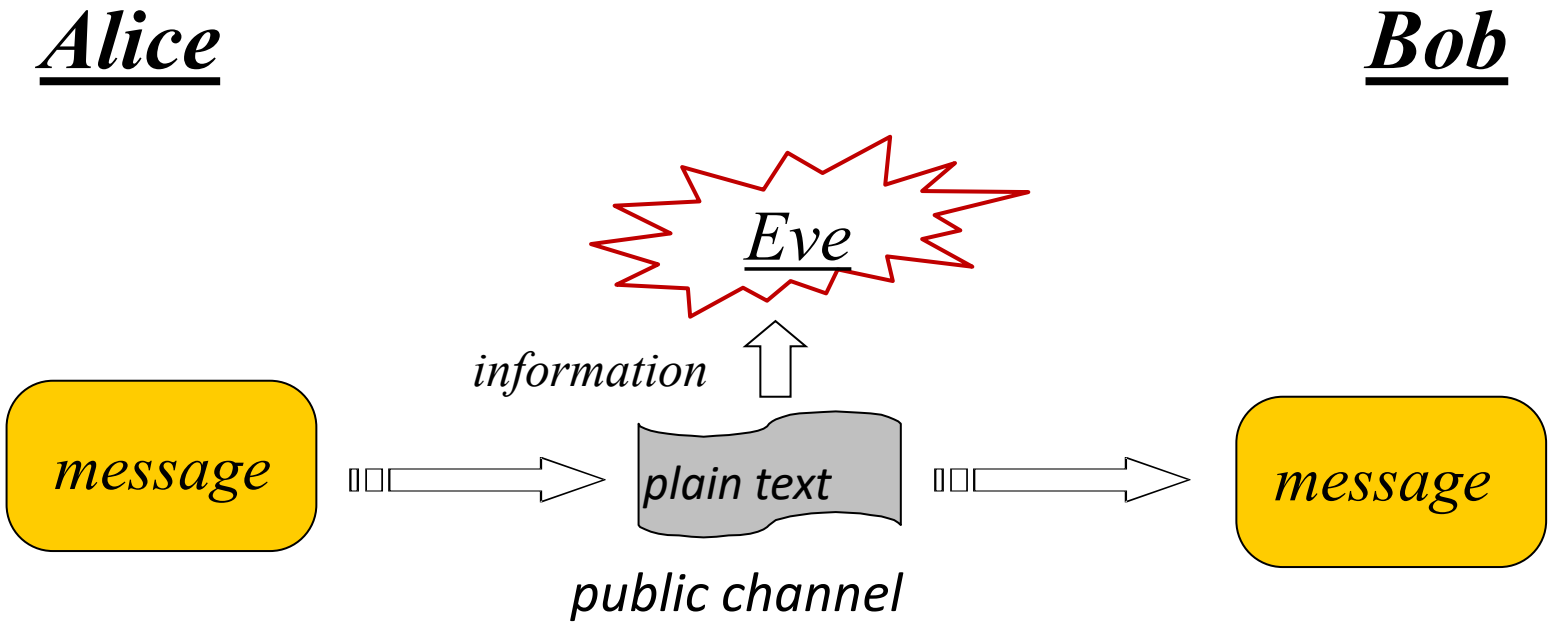
⟨S|Q|I⟩ Swiss Quantum Initiative

Communication over public channels

Alice ***Bob***

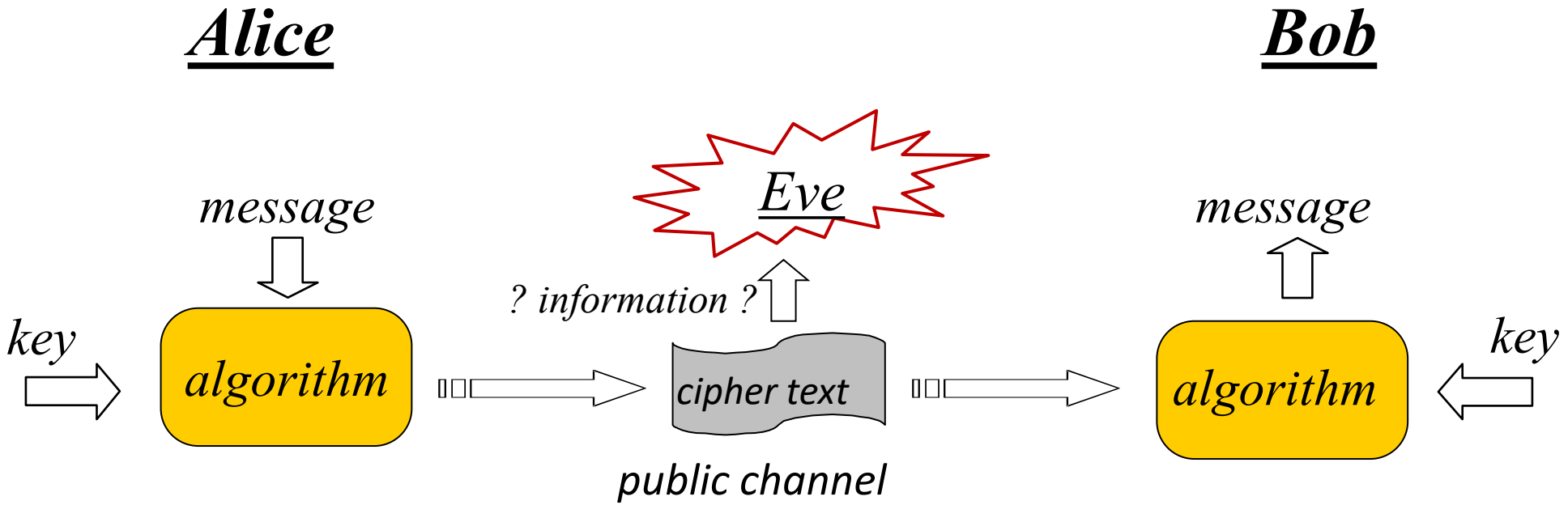


Secure communication over public channels



We have to encrypt confidential messages

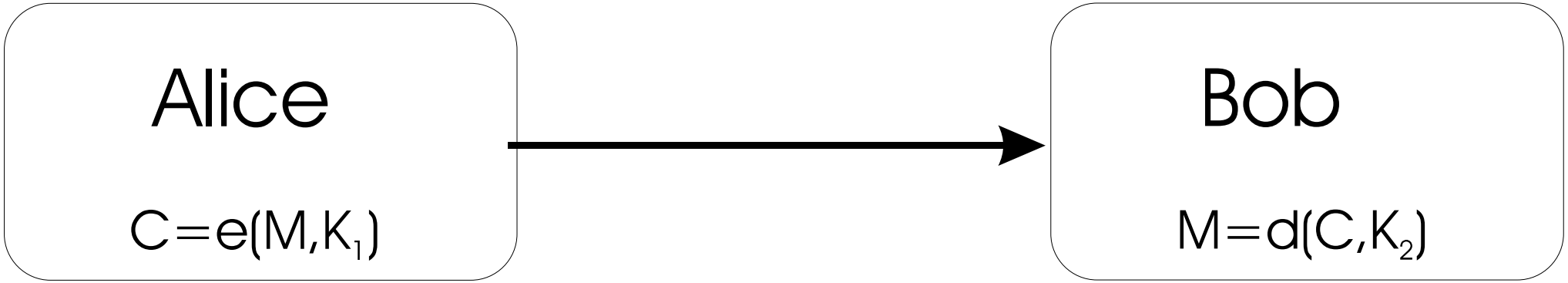
Secure communication over public channels



Asymmetric crypto (modern crypto)

Public key cryptography, e.g. RSA (1978)

e: encryption
d: decryption
M: message
C: ciphertext
K_i: keys



Computationally secure, e.g. based on difficulty of prime factorization

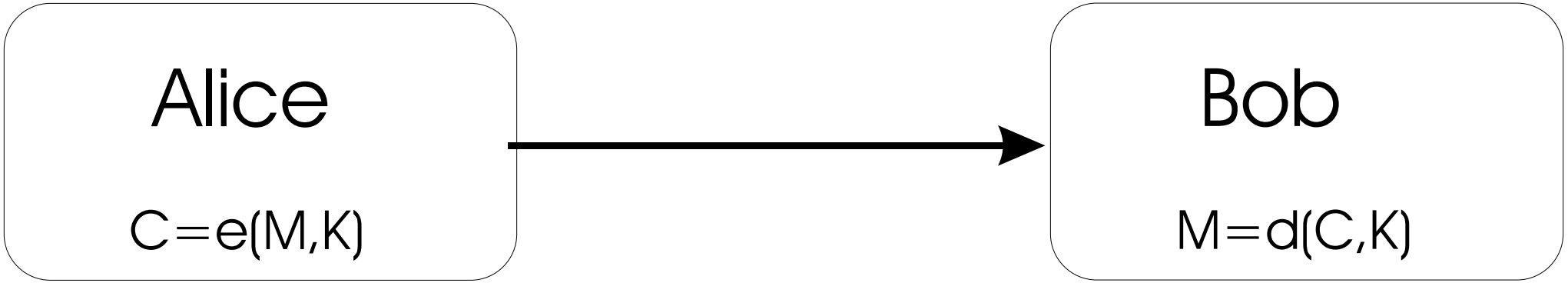
Threats to current public key crypto

- Better classical algorithms
- More powerful classical computers
- Quantum computer (breaks RSA and ECC)

RSA and ECC depreciate in 2030, and are disallowed starting 2035 (NIST, 2024). They are being replaced by post-quantum cryptography.



Symmetric crypto



e: encryption
d: decryption
M: message
C: ciphertext
K: key

Symmetric crypto

No encryption

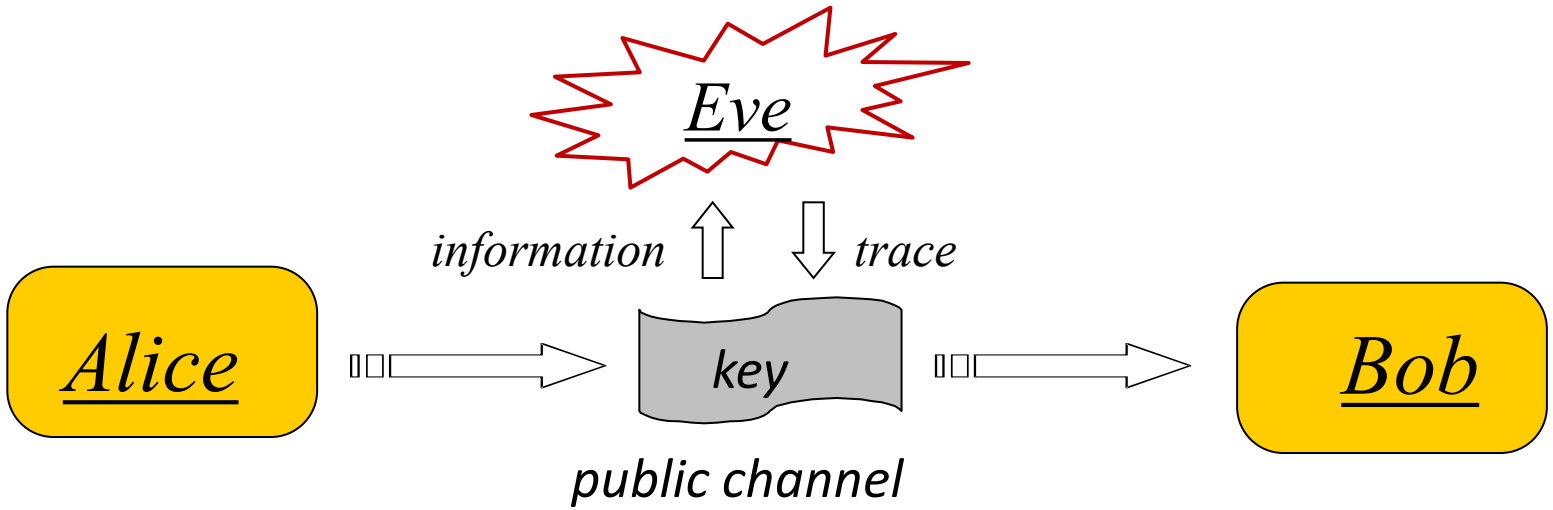
AES (256 bits)

One-time pad



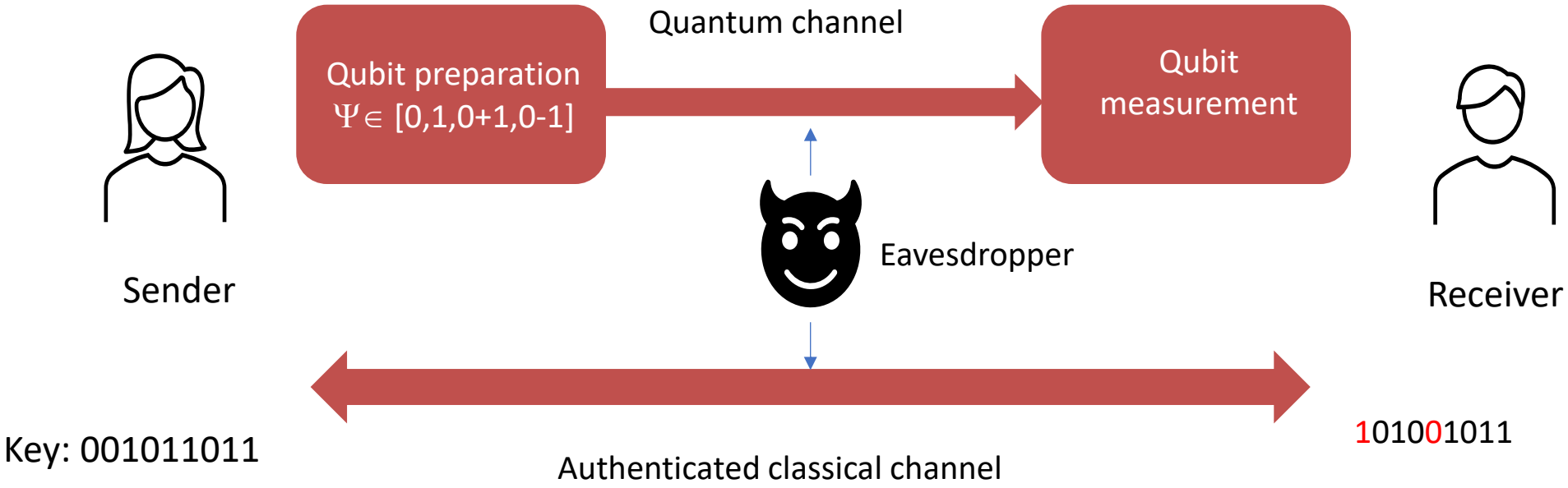
“security”

Desirable key distribution



Use secret key, otherwise discard key

Quantum Key Distribution



Provable (information theoretic) security based on physics, not mathematics

UNIVERSITÉ DE GENÈVE

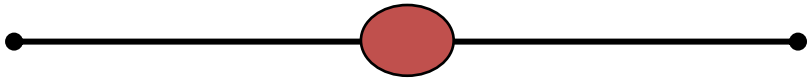
- P2P
- Range up to 150 km over telecom fibers (ID Quantique Clavis)
- Typical key rate: 14’000 AES-256 Keys per hour @ 24 dB-loss link

QKD over long distances and networks



Trusted node

- To increase the total distance, QKD links of limited length are joined using trusted nodes
- Classical crypto can be added to avoid the message to become cleartext in these nodes
- Quantum repeaters are expected to replace the trusted nodes in future



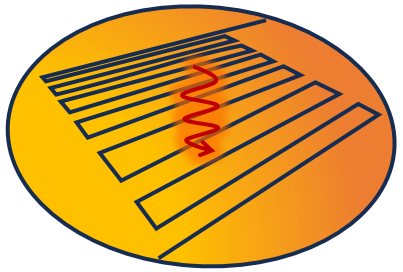
Quantum repeater



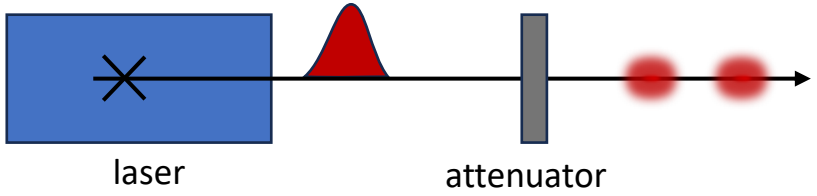
UNIVERSITÉ DE GENÈVE

Swiss Quantum Initiative

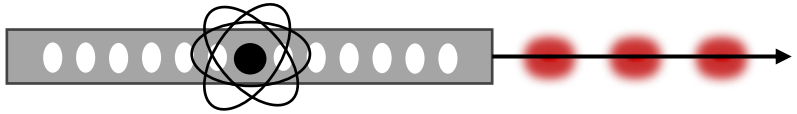
Some typical components

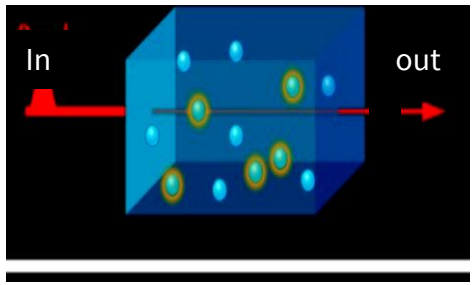


- Attenuated laser pulses, single and pairs of photons
- Single-photon detectors
- Quantum random number generators
- Quantum memories

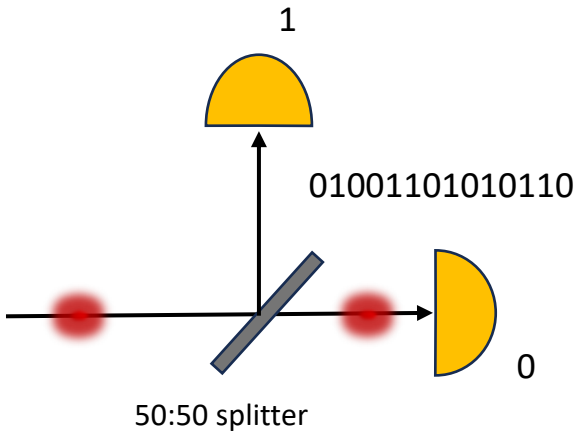


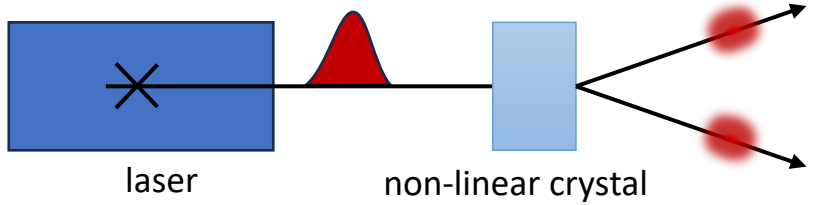
Need for traceable specifications





$$|\psi'\rangle = \mathbb{1}|\psi\rangle$$





UNIVERSITÉ DE GENÈVE

Can we trust?



Qubit preparation
$\Psi \in [0,1,0+1,0-1]$

Quantum channel

Qubit measurement

Sender

Eavesdropper

Receiver

Key: 001011011

101001011

Authenticated classical channel

Need for certification

UNIVERSITÉ DE GENÈVE

⟨S|Q|I⟩ Swiss Quantum Initiative

Conclusion: Metrology for quantum communication

Traceable specifications of quantum communication technology

Certification of quantum communication technology

THANK YOU !

UNIVERSITÉ DE GENÈVE

⟨S|Q|I⟩ Swiss Quantum Initiative