Quantum

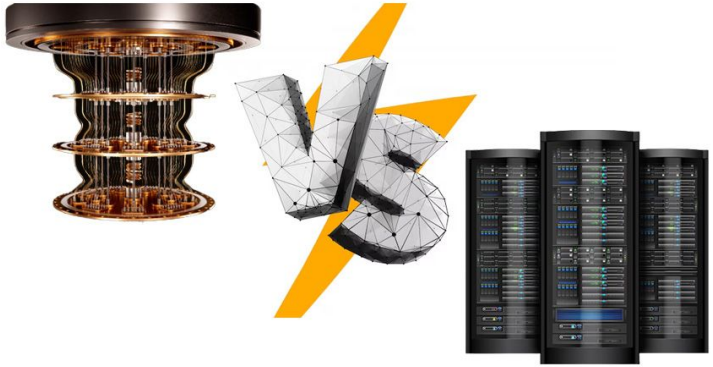
Data Protection

Danae Townsend, Jordi Bru, Ignasi Juez, Mariona Jaramillo

Index

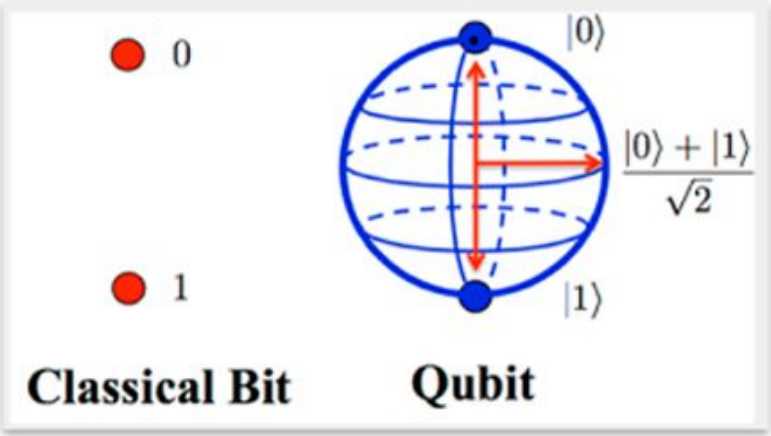
Introduction

- Why do we need quantum computers?
- Supercomputers vs quantum computers



Introduction

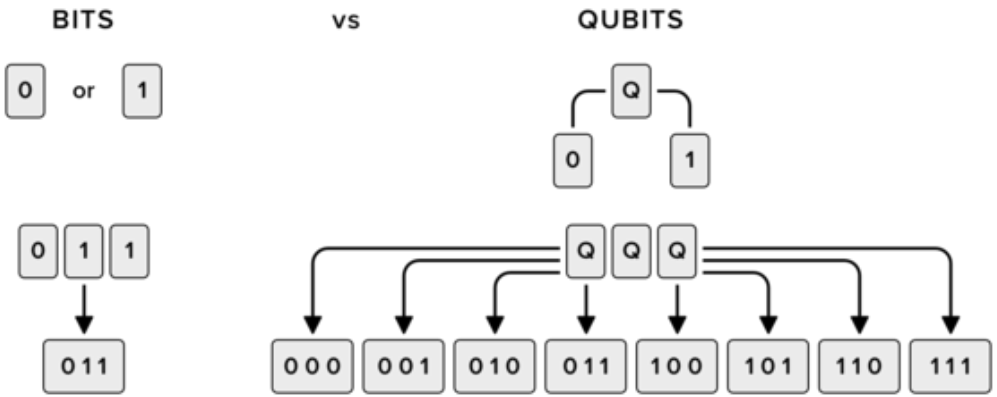
Qubits are the basic unit of information in quantum



Introduction

Qubits are the basic unit of information in quantum and have the following important properties:

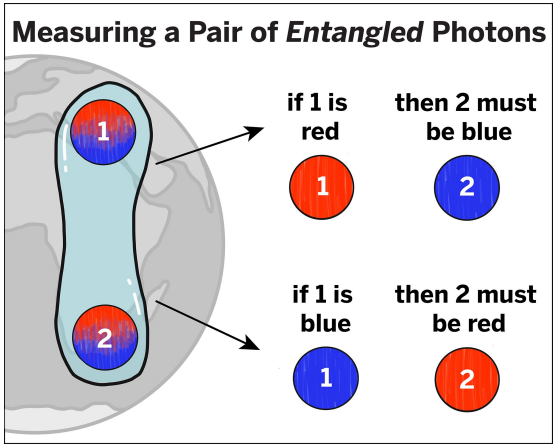
- **Superposition**



Introduction

Qubits are the basic unit of information in quantum and have the following important properties:

- **Superposition**
- **Entanglement**
- **No cloning theorem**

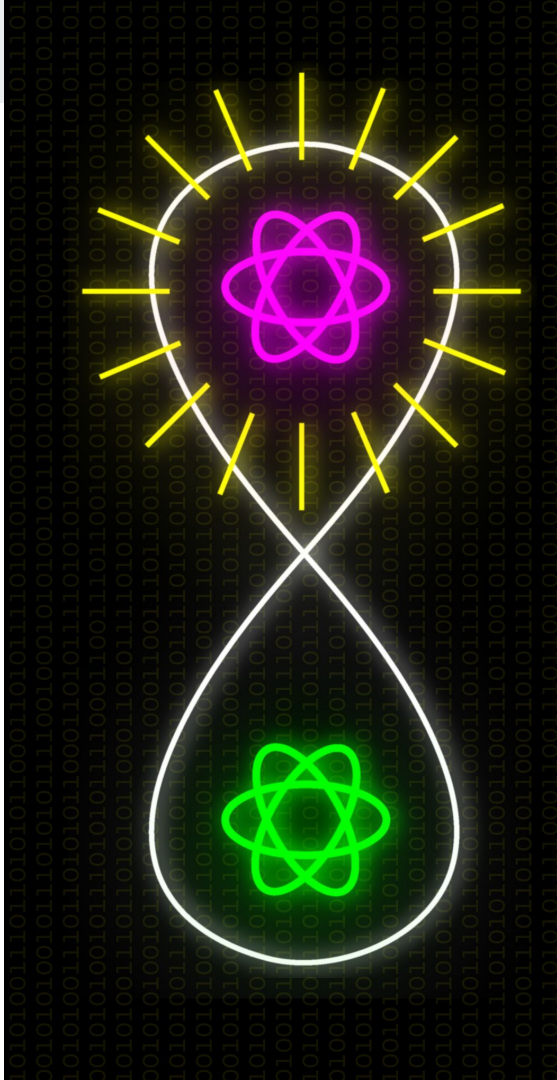


Quantum computing

- **A new approach**
  - Conventional vs quantum
  - faster & efficient
- **n qubits -> 2^n states**
  - complex problems solving

Quantum communication

- A new way of communicating
- Quantum channels immune to eavesdropping
- Secure and private



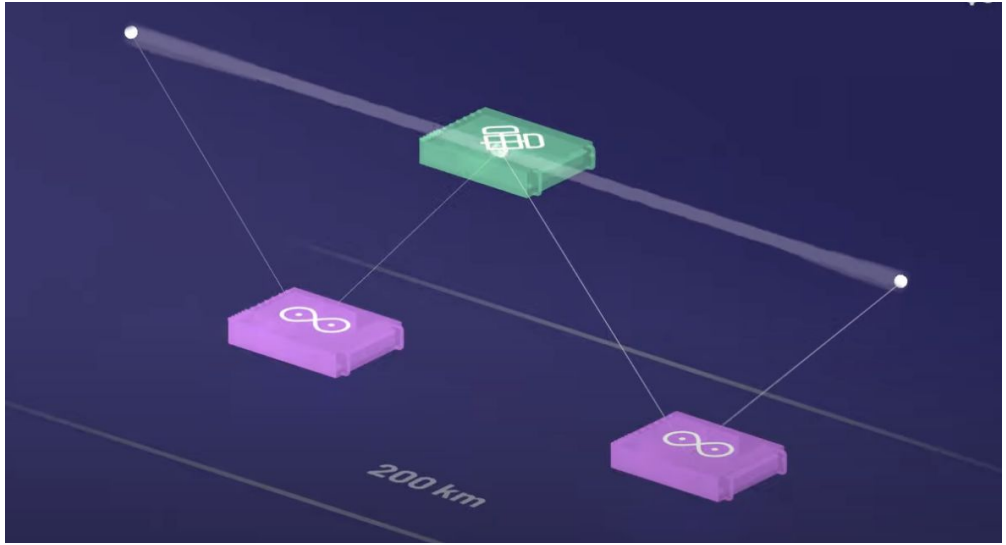
Quantum teleportation

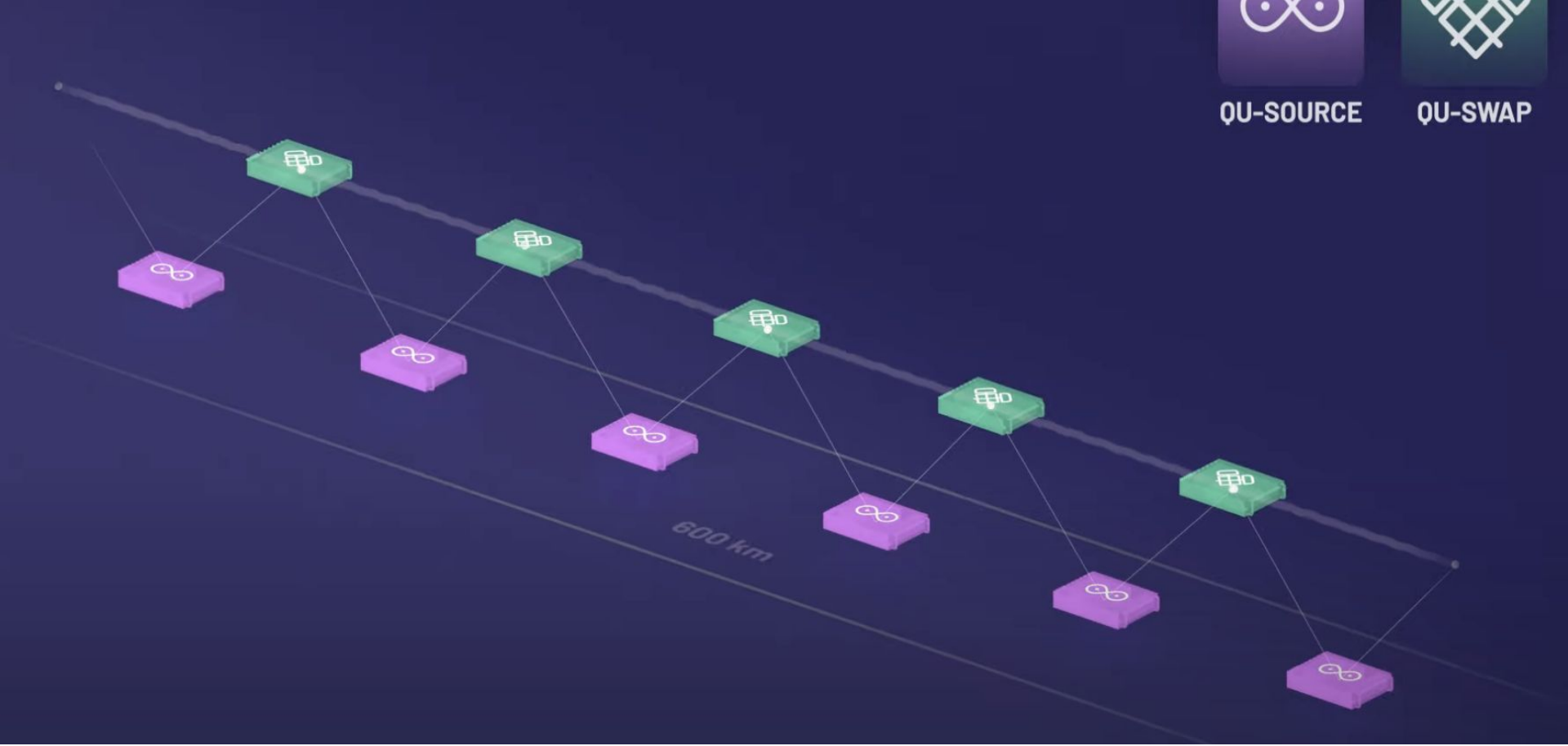
- Transmit quantum states over long distances
- Two parties of entangled particles
  - One measures the quantum state
  - The other operates on the measurement done
  - Quantum state is ‘teleported’

Quantum communication

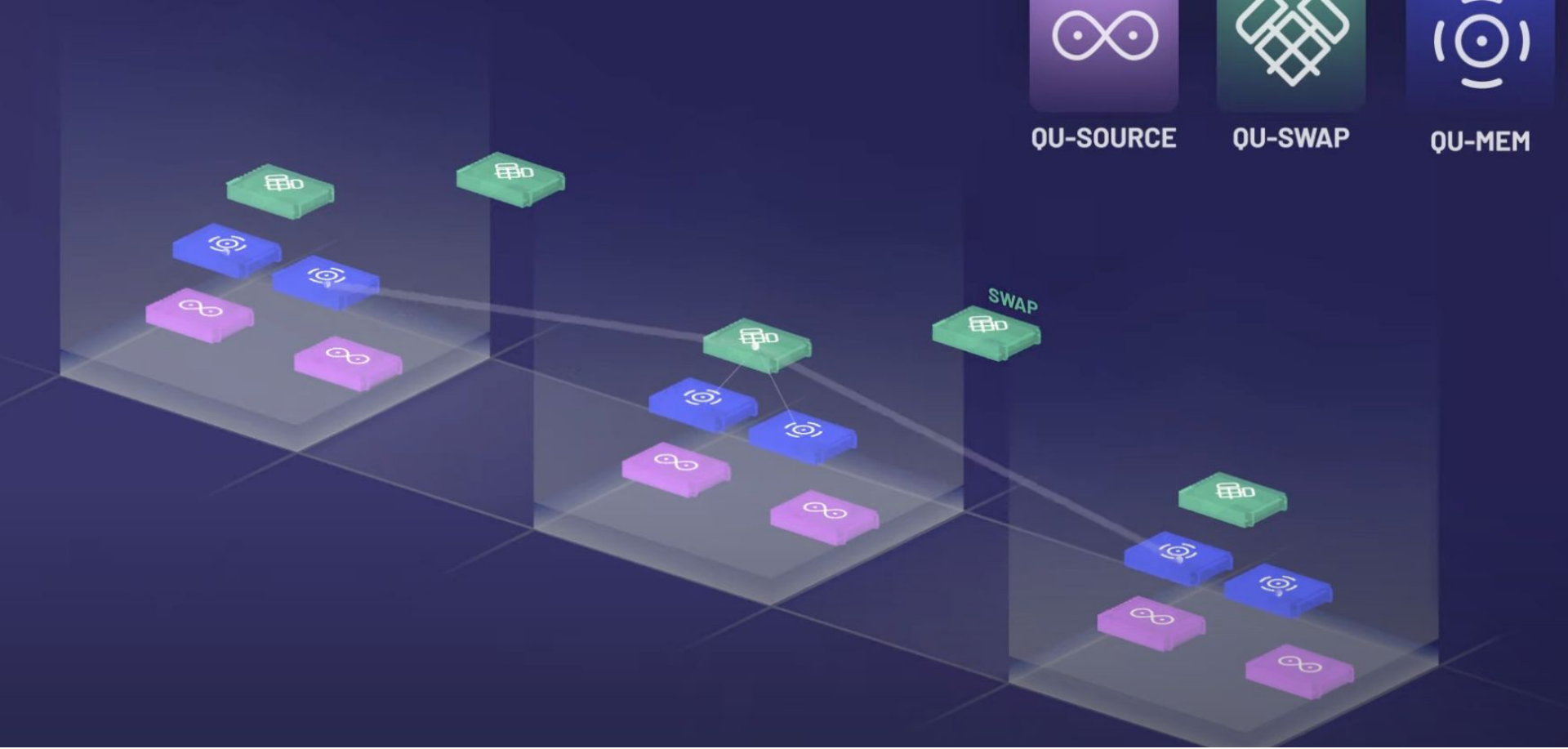
Entanglement swapping

- **A solution to long distance communication**



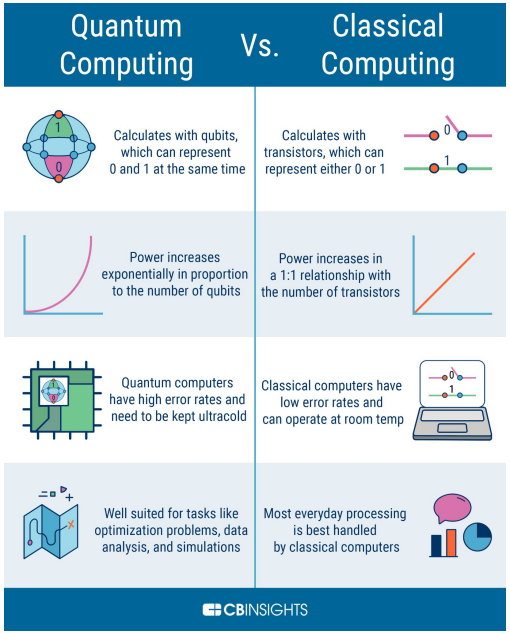


Source: [Quantum repeaters.]

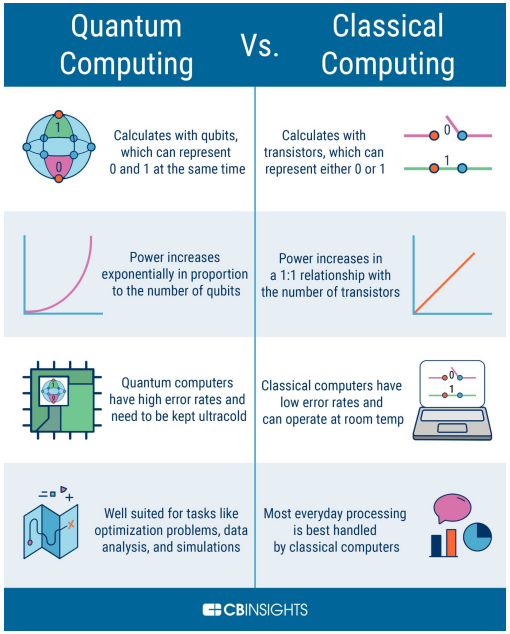


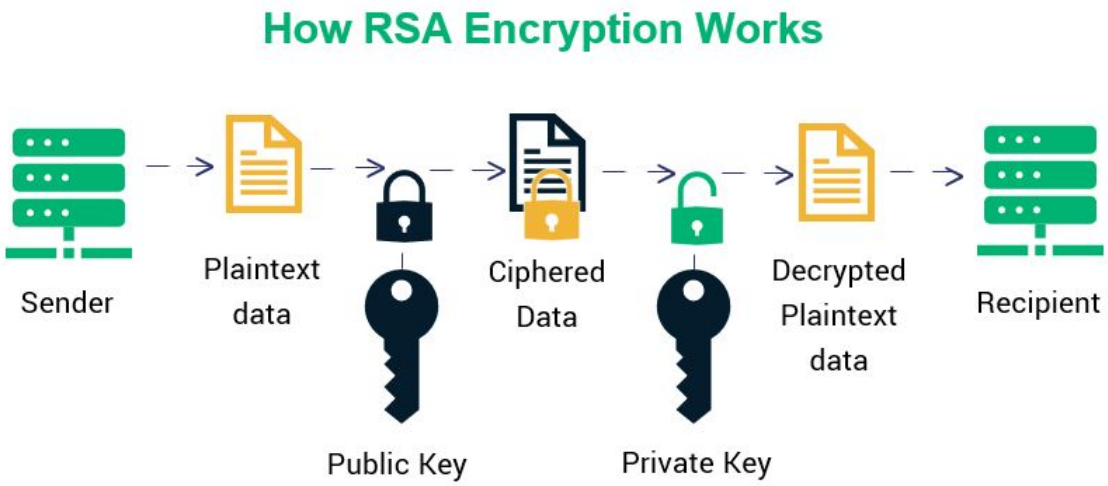
Source: [Quantum repeaters.]

Quantum computing in cryptography

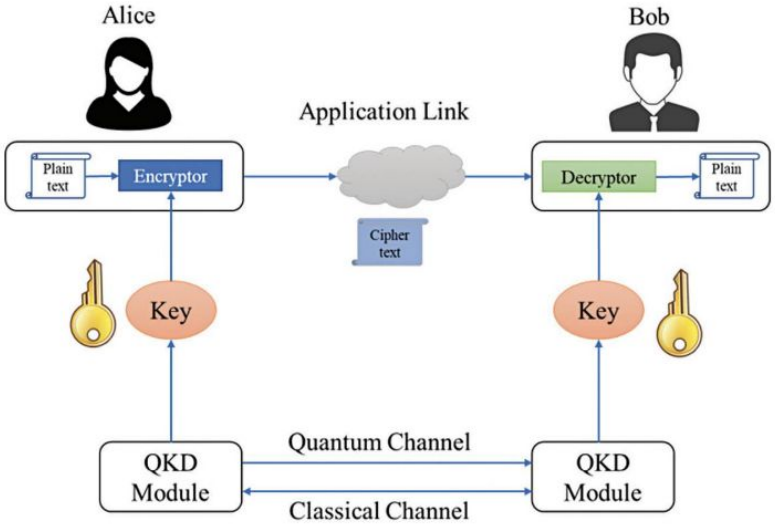


Quantum computing in cryptography



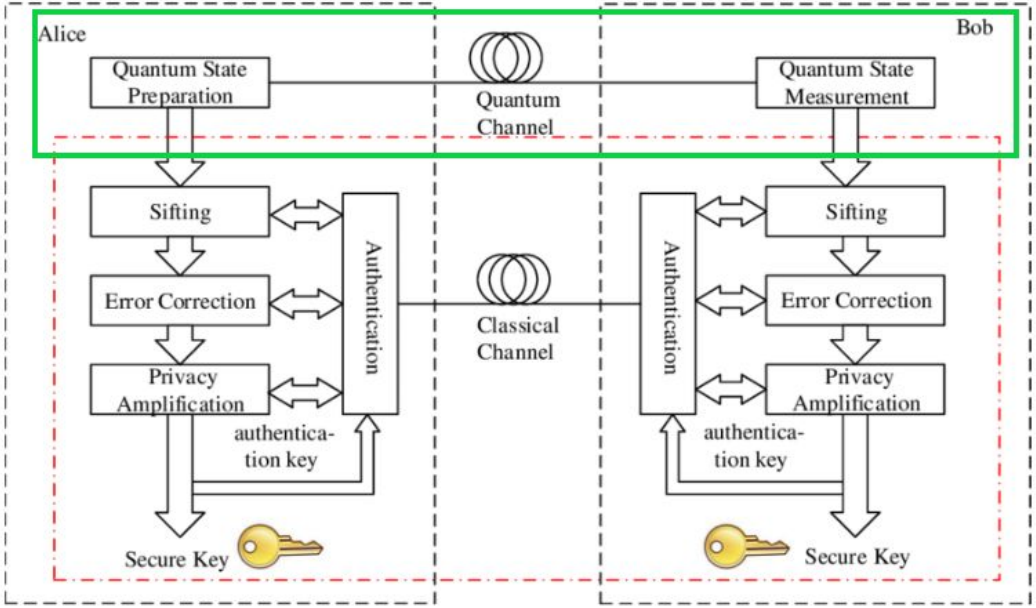


QKD


Alice
Bob
Application Link
Plain text
Encryptor
Decryptor
Plain text
Cipher text
Key
Key
Quantum Channel
QKD Module
QKD Module
Classical Channel

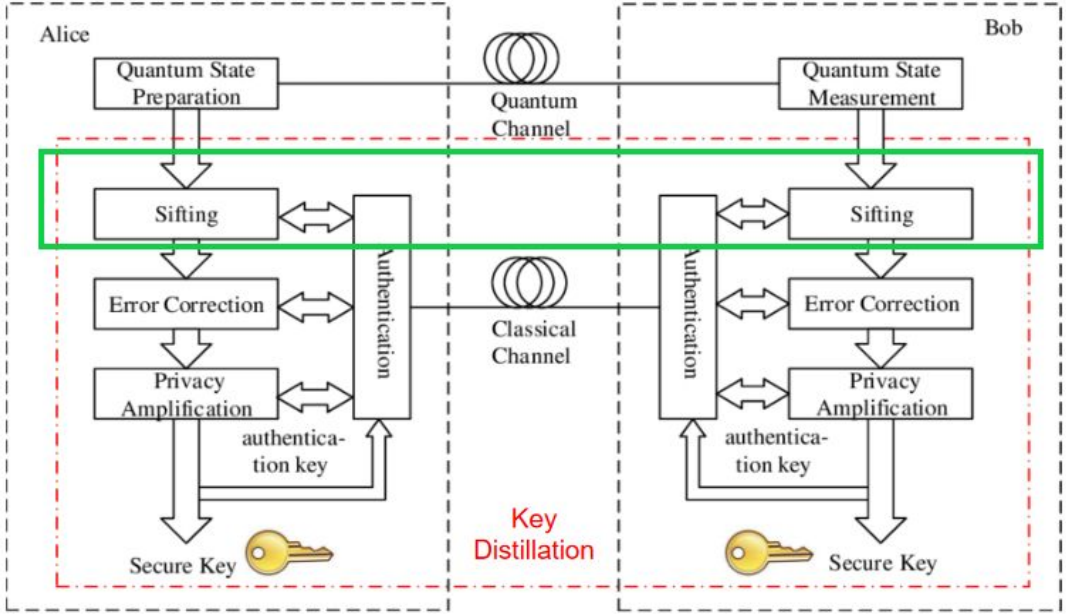
QKD - BB84

- Distribution



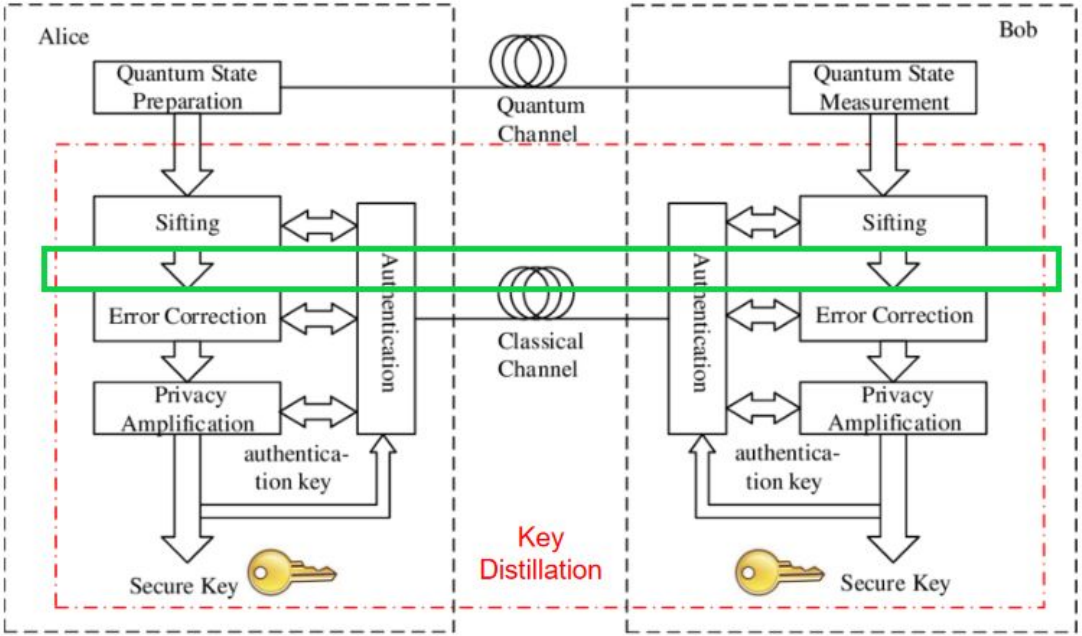
QKD - BB84

- Distribution
- Sifting



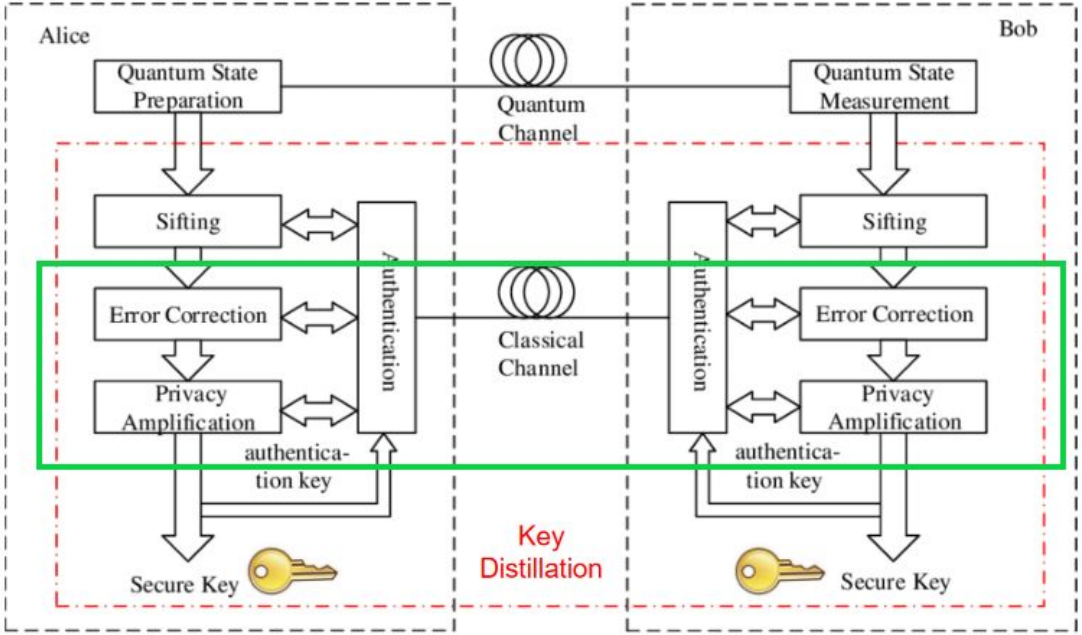
QKD - BB84

- Distribution
- Sifting
- Error estimation and correction



QKD - BB84

- Distribution
- Sifting
- Error estimation and correction
- Privacy amplification



Quantum computing in encrypted data

Cryptography	**Encryption**
Science Encrypting and decrypting Communication practices/techniques Data confidentiality, integrity and authentication	Information Private Cannot be observed Unreadable Unauthorized people

Quantum security systems - quantum **cryptography** protocols - secure and reliable communication and transmission of **information**

Homomorphic and quantum encryption

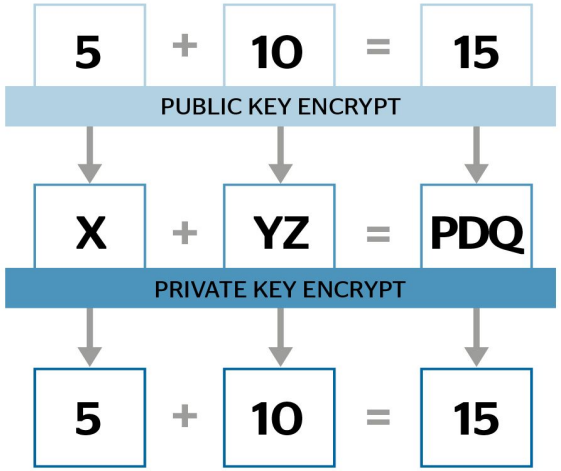
- Credit card information
- Passwords
- Personal information
- Unencrypted files

April 2011:

Homomorphic and quantum encryption

<u>Classic homomorphic</u>

- Technique.
- Mathematical operations.
- result unreadable unless it is decrypted.

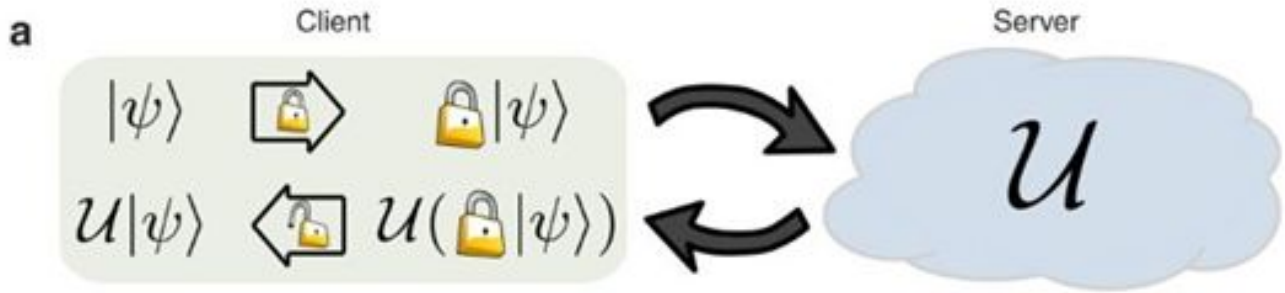


Homomorphic and quantum encryption

<u>Quantum homomorphic</u>

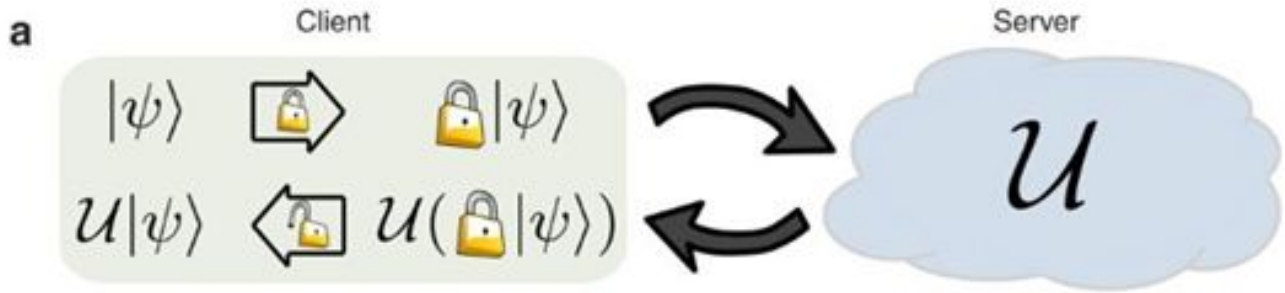
- Theoretically possible. Not practical.
- Suggest a trade-off:
  - Photonic quantum processors
  - Perfect privacy is not required
    - Maximum amount of information is small

Client-server quantum protocol



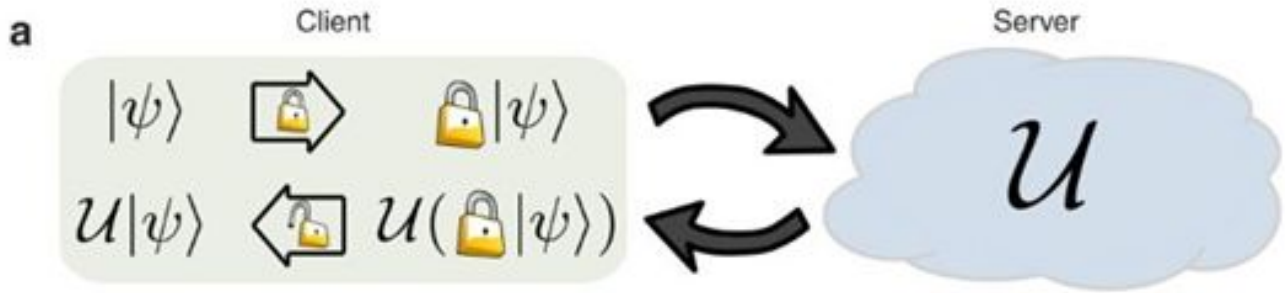
Client **encrypts** and **sends**. Server **executes** quantum **gates** sequentially

Client-server quantum protocol



Requires **one** round off classical communication (**non-Clifford gate - non easily invertible** - loss information - Complex and advance operations)

Client-server quantum protocol



Encrypted qubits are returned to the client for **decryption**. Server does not acquire **knowledge**. Use **fewer** qubits.

Potential risks

- **Environmental factors:** Alteration in the information.
  - Changes in the environment, magnetic coupling.
  - Isolated and controlled.

Current developments

TLS protocol - RSA are vulnerable

IBM:

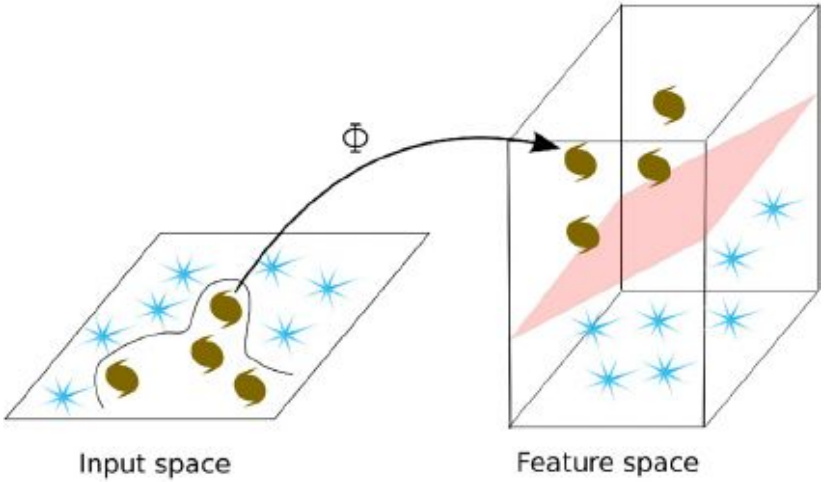
- Key Encapsulation Mechanisms (KEM)
- Digital signature schemes

The National Institute of Standards and Technology (NIST): “protocols are quantum secure”.

- Quantum safe TLS

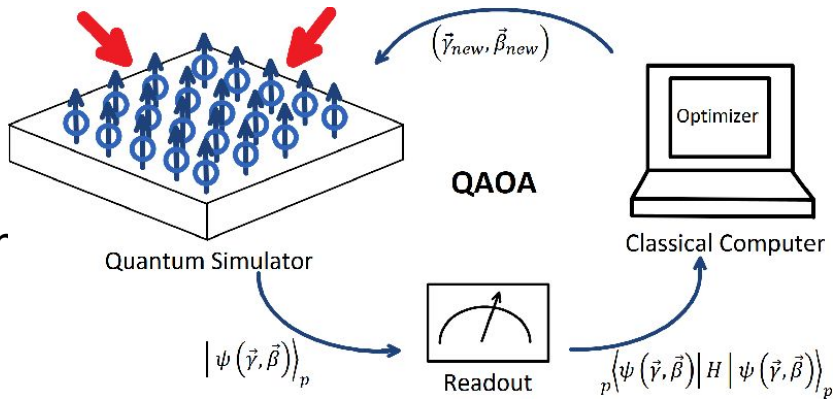
Quantum computing in machine learning

1. Quantum support vector machine (**QSVM**)



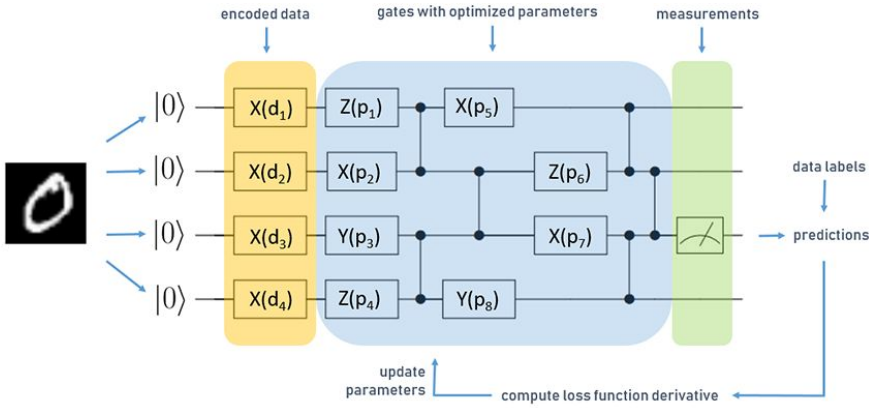
Quantum computing in machine learning

1. Quantum support vector machine (**QSVM**)
2. Optimization problems: Quantum Approximate Optimization Algorithm (**QAOA**)



Quantum computing in machine learning

1. Quantum support vector machine (**QSVM**)
2. Optimization problems: Quantum Approximate Optimization Algorith (**QAOA**)
3. Quantum **neural** networks



References

IBM, Quantum Computing [Online; accessed 17th April 2023 https://www.ibm.com/topics/quantum-computing]

Allende, M., 2022. TECNOLOGÍAS CUÁNTICAS: Una oportunidad transversal e interdisciplinar para la transformación digital y el impacto social.

Israel Physical Society. (n.d.). What are Quantum Computing and Quantum Communication? [Online]. Available: https://www.ippi.org.il/what-are-quantum-computing-and-quantum-communication/

S. V. D. Ruiz, B. F. A. Minga, J. D. C. Soto and E. F. M. Zambrano, "Impact of quantum computing on current technologies," 2022 17th Iberian Conference on Information Systems and Technologies (CISTI), Madrid, Spain, 2022, pp. 1-12, doi: 10.23919/CISTI54924.2022.9820248.

"Cryptography Engineering: Design Principles and Practical Applications" by Bruce Schneier, Niels Ferguson, and Tadayoshi Kohno

https://www.ibm.com/topics/quantum-safe-cryptography

Gisin N, Ribordy G, Tittel W and Zbinden H 2002 Quantum cryptography Rev. Mod. Phys, 4 41.1-41.8

M. Ogburn, C. Turner y P. Dahal, "Homomorphic Encryption", Procedia Comput. Sci., vol. 20, pp. 502–509, 2013. [En línea]. Disponible: https://doi.org/10.1016/j.procs.2013.09.310

Zeuner, J., Pitsios, I., Tan, SH. et al. Experimental quantum homomorphic encryption. npj Quantum Inf 7, 25 (2021).

Thanks for your attention

Jordi Bru

jordi.bru@estudiantat.upc.edu

Danae Townsend

danae.townsend@estudiantat.upc.edu

Mariona Jaramillo

mariona.jaramillo@estudiantat.upc.edu

Ignasi Juez

ignasi.juez@estudiantat.upc.edu