

- Motivation for QKD
  - Limitations of Classical Cryptography
- Quantum Key Distribution
  - Definition
  - Historical Context
  - Real-World Applications
  - Notable Implementations
  - Challenges
  - Future Perspectives
- Conclusion: Why QKD?
- References



# Motivation

---

- How secure do you think our current communication methods will be in the face of a quantum computer (QC)?
- Can we **afford to wait** until quantum computers are mainstream before we start thinking about secure communication?
- If someone could **intercept** your secure communication **today** and **decrypt later** (e.g., ten years from now), would you still consider it safe?
  - This strategy is a.k.a. retrospective decryption
- What if there was a way to **detect any eavesdropper** trying to listen to our communication immediately?

# Limitations of Classical Cryptography

- Classical public key cryptography relies heavily on:
  - **Mathematical algorithms** (e.g., RSA: factorization of large numbers)
  - **Computational complexity** (v. unconditional security)
    - Problems infeasible to solve with current technology
- There are risks related to long-term effectiveness
  - **Computational advances** (e.g., increasing processing power)
  - The potential future advent of **quantum computers**
    - Algorithms difficult for classical computers could become easily solvable with QC
    - Shor's algorithm (1994), is a quantum algorithm capable of efficiently factoring large integers and solving the discrete logarithm problem
    - Large-scale, practical QCs could render **current public-key cryptosystems obsolete**
    - They would **allow the decryption of previously secure communications**



# Limitations of Classical Cryptography

---

- Vulnerabilities in **key generation**
- Vulnerabilities in **key exchange (KE)**
  - Classical KE protocols involve the exchange of keys over a potentially insecure channel
  - An eavesdropper with sufficient computational power could intercept and decipher these keys, compromising the security of the encrypted communication
- No **security proofs** for classical public key cryptography algorithms
  - Cryptanalytic attacks (i.e., ways to solve specific math problems) may improve significantly
  - Unknown adversaries may produce undisclosed breakthroughs
- Potential for **symmetric key brute force attacks**
  - The **key space** is usually large enough to make this impractical with current technology
  - QCs could use [Grover's algorithm](#) to speedup the attack, effectively halving the **security level** of [symmetric key cryptography](#)

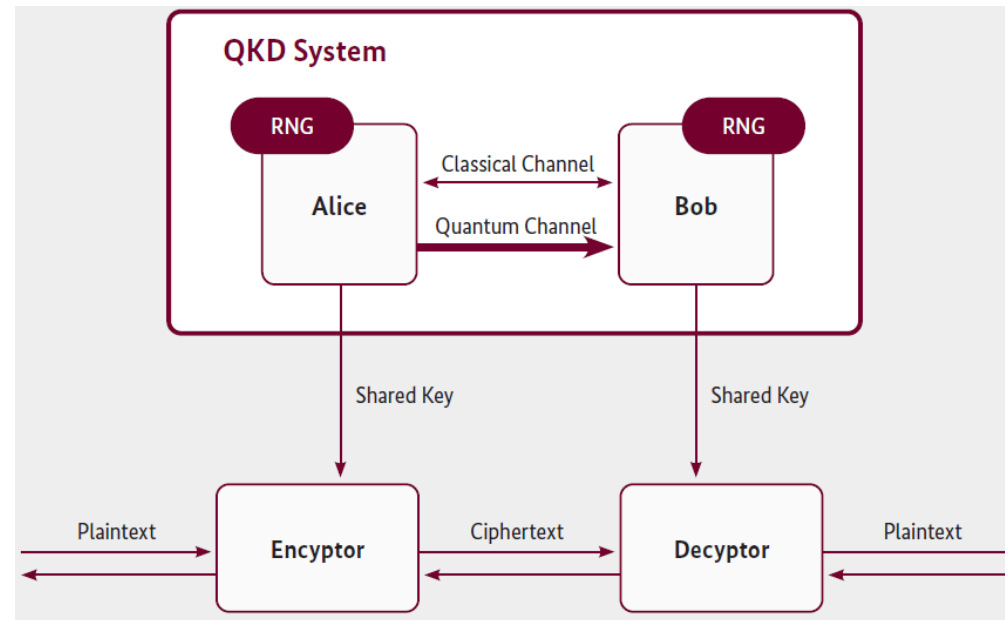
# Quantum Key Distribution (QKD)

- **QKD** is a method that uses the principles of quantum mechanics to **securely distribute encryption keys** between two parties
  - The two parties are commonly referred to as Alice and Bob
  - QKD ensures the secrecy and integrity of these keys
  - The security of QKD is not based on computational hardness assumptions
  - The fundamental principles of quantum physics provides a level of security that, in theory, cannot be compromised even by a QC
  
- **The key feature of QKD**
  - Ability to **detect eavesdropping** during the key exchange process
  - If a third party (commonly named Eve) attempts to intercept a key, QKD protocols guarantee that this interference will be noticed
  - When Alice and Bob detect such disturbances, they can **discard the compromised key** and start the key exchange process again



# Quantum Key Distribution

- QKD constitutes **one part of a cryptographic system**
- QKD **does not transmit data directly**
  - Mirrors the functionality of **asymmetric key agreement schemes**
    - Authentication of the peers
    - Generation and secure distribution of cryptographic keys between them
    - Use of the shared keys by a symmetric encryption algorithm (e.g., [AES](#), [one-time pad](#))



**A Prepare & Measure  
QKD system (BSI22)**

## Quantum encryption

- **OTP is an information-theoretically secure algorithm**
  - OTP encryption provides “**perfect security**”
  - **Not suitable** to use in most **traditional settings**
- **OTP come with several requirements, e.g.:**
  - Must be as long as the message to be encrypted
  - Must be random
  - Must not be reused
- A **high-performance QKD** is required if an **OTP** needs to be exchanged
  - In practice, the QKD system must produce a longer keystream
  - A limited rate, currently is a problem
- **Hybrid solution**
  - Encrypt with a symmetric cipher and then with an OTP



- QKD is **distinct from**
  - **Quantum computing**
    - A type of computing that uses the principles of quantum mechanics to solve problems
    - Unlike classical computers, which use bits as the smallest unit of data (representing 0 or 1), QCs use **qubits**
    - Qubits represent and store multiple states simultaneously due to quantum phenomena such as superposition and entanglement
    - This allows quantum computers to **perform certain calculations much faster than classical computers**
  - **Post-Quantum Cryptography (PQC)**
    - A type of cryptography designed to be secure against the potential threats posed by QCs
    - Traditional cryptography can be broken by the power of quantum computing
    - **PQC uses mathematical problems that are difficult for both classical and QCs to solve**
    - Consequently, it ensures data remains safe even in the age of quantum technology

- The concept of QKD was first proposed in the **early 1980s**
  - A period marked by growing awareness of the potential and limitations of classical cryptographic methods
  - Researchers begun to **explore alternatives to classical encryption**
  
- The foundational idea of QKD was introduced by Bennett & Brassard (1984)
  - They developed the **BB84 protocol**
    - Demonstrated how information (as **classical bits**) could be represented as **qubits**
    - Utilized the principles of quantum mechanics to create a method of secure communication / key exchange
  - The protocol could, in principle, detect any eavesdropping attempt
    - The process of measuring these qubits inherently disturbed their state, thereby revealing the presence of an eavesdropper



- 1991:
  - [Artur Ekert](#) proposed an alternative QKD protocol
  
- Late 1990s and early 2000s:
  - **Experimental implementations** of QKD began to emerge
  - Advances in technology enabled the **practical realization** of QKD systems
    - Initially over short distances in lab settings
    - Later over increasingly longer distances using optical fibers and free-space optics
  
- More recently:
  - Emergence of **commercial QKD products** and **pilot networks**
  - Companies and research institutions invest in the development of QKD to secure sensitive communications
    - Particularly in sectors like finance, government, and military

## ➤ QKD use cases

- Currently, niche (high-security) applications
- Secure point-to-point links
- Defense in depth (e.g., as a complement to PQC)
  
- **Financial Sector**
  - Transactions and communications
    - Highly sensitive data and significant monetary transactions make them prime targets for cyberattacks
- **Government and Defense**
  - Military and diplomatic communications
    - Critical need to protect sensitive / classified information and communication channels
- **Critical Infrastructure**
  - Power Grids, water treatment, transportation systems (air traffic control, rail networks, etc.), other utilities
    - Increasingly becoming targets for cyberattacks
- **Healthcare**
  - Protecting communication of patient data between hospitals, and research institutions, ensuring patient privacy and compliance with regulations
  - Secure data transmission for remote consultations (telemedicine, telehealth)



# Notable Implementations of QKD

- SECOQC Project (Europe), 2004 - 2008:
  - Successfully demonstrated QKD over a **metropolitan area** network in Vienna, Austria, establishing a prototype for secure communication
- SwissQuantum Network (Switzerland), 2009 – 2011:
  - One of the earliest **commercial QKD networks**
  - Highlighted the potential for integrating QKD into existing communication networks
- Tokyo QKD Network (Japan), 2010 - Today:
  - The network demonstrated secure communication links over distances
  - Showcases the practical deployment of QKD in **urban environments**
- Micius Quantum Satellite (China), 2016 - Today:
  - Launched the world's first **quantum communication satellite**
  - The Micius satellite project demonstrated the feasibility of **satellite-based QKD**
  - The aim is to overcome the distance limitations of fiber-optic QKD and pave the way for **global quantum communication networks**

- QKD comes with **unique qualities** and **unique limitations**
- **Distance limitations**
  - Photon loss in optical fibers
    - QKD over fiber-optic cables is limited by photon loss, which increases with distance
      - Currently, QKD systems can operate effectively over distances of a few hundred kilometers
    - **Photons'** minimal interaction with their environment, ability to travel long distances, compatibility with existing optical infrastructure, and support for quantum properties like superposition and entanglement make them highly suitable as qubits
  - Quantum repeaters
    - **Active devices** in the quantum channel are interpreted as **eavesdropping devices**
    - Need to amplify the quantum signal without measuring it
      - Preserve the quantum state
    - Practical and scalable quantum repeaters remains a significant **technical challenge**



## ➤ Cost and infrastructure

### ➤ High initial costs

- QKD systems require **specialized equipment**
  - Single-photon detectors
  - Quantum Random Number Generators ([QRNGs](#))
  - ...
- Secure apparatus and processes
  - Untrusted components may leak information
- **Dedicated communication links** (physical **point-to-point** nature)

### ➤ Integration/interoperability with existing networks

- Requires significant upgrades and engineering modifications
- Compatibility with current infrastructure needs to be addressed to enable **seamless deployment**

# Challenges of QKD

- **Rate of key generation**
  - QKD currently generates/transmits keys at a slower rate (a few Mbps) compared to classical methods
  - **Problematic for applications requiring high data throughput**
  - OK if a small key (e.g., an AES 256-bit key) needs to be exchanged
  - Research is ongoing to improve the efficiency and key generation rate of QKD
- **Scalability**
  - Network scalability to support large networks with multiple nodes and users is challenging
  - Developing a **robust and scalable quantum network infrastructure** is a long-term goal
- **Standardization and interoperability**
  - **Lack of standards** is a challenge for widespread adoption
    - Need to ensure **compatibility** and **seamless integration** across different systems and vendors
  - **Regulatory and compliance** issues wrt emerging technologies
    - Must be addressed to ensure the **secure and lawful deployment** of QKD systems



- **QKD is not immune to attacks**
  - There are **security proofs** for theoretical **QKD protocols**
  - There are **no security proofs** for **QKD hardware/software implementations**
  - Upcoming **QKD standards** on:
    - Methodology to implement and test QKD hardware, Interoperability, Certification
  - Difficult to quantify the actual security of particular implementations
    - **Commercial QKD systems have been shown to be vulnerable** in the past
      - Mostly due to implementation flaws or side-channel attacks
      - Photon Detector Blinding Attack, Time-Shift Attack, Side-Channel Attacks
  - Do not yet fully know how to correctly implement
  - QKD systems have so far **received less scrutiny** compared to traditional cryptosystems
    - Need to apply the lessons learned in the past to QKD
    - A thorough and standardized analysis of QKD is required before using it in sensitive domains

- **QKD attacks** (and countermeasures)
  - Photon number splitting attack
  - Trojan-horse attack
  - Denial-of-Service attack
  - Tampering with the QKD equipment
  - Software vulnerabilities
  - Large-scale QKD deployment creates other security issues (security composition)
  - Social engineering
  - Insider attacks
  - ...
- **Media:** security is based on the “**laws of physics**”
- **Practice:** QKD security is highly **implementation-dependent**



# Future Perspectives of QKD

- QKD is positioned to play a **crucial role in the evolution of secure communications**
- **Technological advancements** in QKD
  - Development of **quantum repeaters** to overcome distance limitations
    - Ongoing research aims to develop practical and scalable quantum repeaters
  - **Satellite-based QKD**
    - The future may see a **constellation of quantum satellites** that provide global coverage for secure communication
  - **High-speed and efficient QKD systems**
    - Researchers are exploring various techniques to increase the efficiency (e.g., key generation rates) of QKD protocols
    - Advances in integrated photonics enable the **miniaturization** and integration of QKD components onto a single chip
    - Developing high-speed **QRNGs** will further enhance the security and performance of QKD
  - **Integration with classical communication infrastructure**
    - **Hybrid quantum-classical networks**
    - Efforts are underway to develop industry standards and protocols for QKD
    - The aim is to ensure seamless integration with classical networks and facilitate the deployment of QKD on a large scale

- Vision of the **quantum internet**
  - A global network that uses quantum signals to transmit information securely and perform tasks that are impossible or inefficient with classical networks
  - The primary function of the quantum internet will be secure communication using QKD
  
- **(Quantum-enhanced) applications** of the quantum internet
  - Secure communications
  - Distributed quantum computing
  - Quantum cloud computing
  - Quantum teleportation
  
- **Ongoing research** and development efforts in quantum communication technologies are steadily bringing the quantum internet closer to reality



# Conclusion: Why QKD?

- **Advantages of QKD over classical cryptography**
  - **Unconditional security**
    - Robust against any future advances in computing, including quantum computing
    - Even if a malicious actor possesses unlimited computational resources (including a QC), QKD can still ensure secure key distribution (v. computational security)
  - **Eavesdropping detection** in real-time
    - If an eavesdropping attempt is detected, the compromised key is discarded
    - A new key exchange can be initiated
  - **Forward Secrecy**
    - Each key exchange generates a new, unique key that is immediately discarded after use
    - Ensures that even if a key is compromised in the future, past communications remain secure
- **QKD** is partly an alternative to **PQC**
  - PQC is vulnerable to algorithmic advances

# Conclusion: Why QKD?

---

- **Notable implementations**
  - Showcase QKD's potential to secure communication on local/global scales
- **Future perspectives: Towards the quantum internet**
  - QI will enable new applications
  - QI requires **continued innovation** and collaboration across multiple fields
    - Including quantum physics, engineering, computer science, and cybersecurity
- QKD offers a **proactive solution** to future-proof data security **in anticipation of emerging technological threats**



## Conclusion: Why QKD?

---

- The shift towards quantum-safety is a **strategic necessity** for governments, businesses, and organizations
- The development & deployment of QKD are influenced by **geopolitical factors**
  - Nations may view QKD as a strategic technology that offers a **competitive advantage** in cybersecurity
- The deployment of QKD is influenced not only by technological and scientific factors but also by **policy** and **political considerations**
  - Different countries and governmental agencies have **varying approaches** and priorities regarding QKD
  - **Strong proponents:** see QKD as a strategic asset that enhances national security and positions them as leaders in quantum technology
  - **Skeptical or cautious stances:** cite concerns about the technology's scalability, cost, and practical deployment challenges

# Conclusion: Why QKD?

## ➤ Strong proponents

### ➤ European Union

- **EU digital sovereignty:** “... the EU must ensure its technological and digital sovereignty in the cyber field. The EU’s capacity to act will depend on its ability to master and develop cutting edge technologies for cybersecurity and cyber defense in the EU...” [EC22]
- No QKD manufacturer is established in the EU (2023)
- **Several initiatives:** [EuroQCI](#) ([HellasQCI](#), etc.)
- The European Quantum Communication Infrastructure was launched in 2019
- First implementation phase started in 2023
- [National projects](#), [Industrial projects](#), [European Quantum Industry Consortium](#)
- Space segment: [Eagle 1](#) to be launched in 2025/2026





# Conclusion: Why QKD?

---

- **Strong proponents**
  - China
    - A frontrunner in the development and deployment of QKD
  - Japan
- **Skeptical or cautious**
  - US, UK
    - Some agencies and policymakers argue that QKD might not be the most practical solution for securing communications
    - They suggest that PQC could provide similar levels of security without the complex infrastructure requirements of QKD
- Current trend: a **balanced approach** that includes both **QKD** and **PQC**
- All continue to invest in QKD research to overcome known limitations

- ANSSI, Should Quantum Key Distribution be Used for Secure Communications? 2022 ([link](#))
- BSI, Quantum-safe cryptography – fundamentals, current developments and recommendations, May 2022 ([link](#))
- Diamanti, Security and implementation of differential phase shift quantum key distribution systems, 2006 ([link](#))
- European Council, EU Policy on Cyber Defence, Nov. 2022 ([link](#))
- Genkin, Pachmanov, Pipman, Tromer, Stealing Keys from PCs using a Radio: Cheap Electromagnetic Attacks on Windowed Exponentiation, 2015 ([link](#))
- ISO/IEC 15408-1:2022, Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 1: Introduction and general model, 2022 ([link](#))
- Jain, Stiller, Khan, Makarov, Marquardt, Leuchs, Risk analysis of Trojan-horse attacks on practical quantum key distribution systems, 2014 ([link](#))
- NIST Glossary ([link](#))
- NSA, Quantum Key Distribution (QKD) and Quantum Cryptography (QC) ([link](#))
- Ramona Wolf, Quantum Key Distribution, Lecture Notes in Physics, 2021 ([link](#))
- UK NCSC, Preparing for Quantum-Safe Cryptography, Nov. 2020 ([link](#))
- Cryptool 2, The BB84 Quantum Key Exchange Protocol Explained ([link](#))





HellasQCI - Quantum Communication Infrastructure for Greece



Co-funded by  
the European Union

This project is co-funded by the European Union  
under the Digital Europe Programme grant agreement No. 101091504.

