Quantum Cryptography: A Technical Report Based on Patent Literature

Abstract (Summary)

This report analyzes a collection of patents related to Quantum Cryptography, focusing on inventions that enhance security, improve key distribution methods, and address vulnerabilities in existing cryptographic systems. The patents cover a range of topics, including quantum key distribution (QKD), quantum-resistant cryptography (QRC), quantum entropy management, and secure communication protocols for various applications, from fiber-optic networks to wireless communications. The inventions aim to overcome limitations in traditional cryptography, such as susceptibility to quantum computing attacks and distance limitations in QKD networks.

Background and Context

Traditional cryptographic methods, particularly those relying on public key infrastructure (PKI), face increasing threats from the development of quantum computers. Quantum computers have the potential to break widely used encryption algorithms, such as RSA and ECC, jeopardizing the security of sensitive data and communications. Quantum Cryptography offers solutions to these challenges by leveraging the principles of quantum mechanics to provide provably secure communication channels. Quantum Key Distribution (QKD) is a key technology in this field, enabling the secure exchange of cryptographic keys between two parties. However, QKD systems face challenges such as distance limitations, the need for trusted nodes, and the complexity of integration with existing communication infrastructure. The patents discussed in this report address these challenges and explore new approaches to enhance the security and practicality of quantum cryptography.

Technical Fields of Invention

The patents analyzed span several technological areas within quantum cryptography:

- **Quantum Key Distribution (QKD):** Methods and systems for secure key exchange based on quantum mechanics (WO 2018199426, EP 3886356, WO 2025123881).
- **Quantum-Resistant Cryptography (QRC):** Cryptographic algorithms and systems designed to be secure against attacks from quantum computers (WO 2020178736, WO 2024054691, EP 4221071).
- **Quantum Entropy Management:** Generation and distribution of true random numbers using quantum random number generators (QRNGs) for cryptographic applications (WO 2021075653, WO 2019088689).
- **Secure Communication Protocols:** Hybrid quantum-classical protocols and methods for detecting eavesdropping on optical channels (WO 2024136930, EP 3718248).
- **Quantum Key Management:** Systems and methods for managing and distributing quantum keys in networks (WO 2013048674, WO 2023080344, EP 4224788).
- **Quantum Computing:** Utilizing quantum computing for encryption key stretching (WO 2025052024).
- **Quantum Networks:** Architectures and methods for building secure communication networks using quantum technologies (WO 2016206498, WO 2022142460, WO 2020227141).

Inventions Related to Quantum Cryptography

1. Quantum Key Distribution (QKD) Enhancements

Novelty and Objectives: Several patents focus on improving the performance and security of QKD systems. For example, WO 2018199426 describes a method for continuous-variable QKD (CVQKD) that enhances security and increases the key generation rate by distributing the quantum key in a reverse post-processing manner. EP 3886356 aims to mitigate range limitations in QKD without relying on trusted nodes, preventing key compromise at intermediate nodes. WO 2025123881 addresses the problem of distinguishing user roles and enabling real-time key delivery using a bidirectional key pool. **(Relevant)**

- **Unique Components/Methods:** WO 2018199426 utilizes photon subtraction at the receiver and reverse post-processing. EP 3886356 employs a common intermediate quantum node that measures quantum signals and provides information to both communicating nodes. WO 2025123881 uses service information exchange to determine caller-receiver relationships.

- **Technical Problems Solved:** These inventions address the limitations of QKD systems, such as distance constraints, security vulnerabilities related to trusted nodes, and the need for efficient key management.
- **Improvement:** They provide enhanced security, increased key generation rates, and more practical QKD implementations.

(Relevant)

2. Quantum-Resistant Cryptography (QRC)

- **Novelty and Objectives:** With the looming threat of quantum computers, several patents focus on developing cryptographic algorithms and systems that are resistant to quantum attacks. WO 2020178736 presents a cryptoprocessing circuit and method that implements quantum-resistant cryptoprocessing with low complexity and high speed. WO 2024054691 introduces a quantum public key infrastructure (QPKI) system that includes a quantum-resistant cryptography (QRC)-enabled Certificate Authority. EP 4221071 addresses the problem of updating cryptographic devices to use PQC algorithms in a flexible way. (Relevant)
- **Unique Components/Methods:** WO 2020178736 uses a logic circuit with multiplexers to route random and private sequences. WO 2024054691 implements QRC-enabled IP and Web protocols. EP 4221071 provisions memory for both PQC and non-PQC cryptographic elements and uses non-PQC cryptography to securely update the device to PQC.
- **Technical Problems Solved:** These inventions address the vulnerability of existing cryptographic systems to quantum computing attacks.
- **Improvement:** They provide a pathway to secure communication in a post-quantum world.

(Relevant)

3. Quantum Entropy Management and Distribution

- **Novelty and Objectives:** WO 2021075653 focuses on quantum entropy management and distribution, aiming to solve security vulnerabilities caused by pseudo-random numbers and the difficulty of integrating QRNG hardware into edge devices. WO 2019088689 provides a secure cryptographic key generation method and system that overcomes hacking techniques by using a Physical Unclonable Function (PUF) chip and a Quantum Random Number Generator (QRNG). (Relevant)
- **Unique Components/Methods:** WO 2021075653 delivers quantum entropy via a network to edge devices. WO 2019088689 combines a PUF chip and a QRNG to generate encryption keys.
- **Technical Problems Solved:** These inventions address the limitations of traditional random number generators and the challenges of securing edge devices.
- **Improvement:** They provide a more secure and efficient way to generate and distribute cryptographic keys.

(Relevant)

4. Secure Communication Protocols and Eavesdropping Detection

- **Novelty and Objectives:** WO 2024136930 introduces a hybrid quantum cryptography protocol for optical communications, particularly in long-distance optical communications systems like undersea environments. EP 3718248 aims to solve the problem of vulnerabilities in optical fiber link security by detecting physical layer attacks like eavesdropping. (Relevant)
- **Unique Components/Methods:** WO 2024136930 uses a hybrid quantum cryptography protocol method for secure communications between Secure Node A (SN-A) and Secure Node B (SN-B) over a fiber optic communications network. EP 3718248 sends both a classical message and a quantum signal over the same optical channel and detects eavesdropping on the classical message by monitoring the quantum signal.
- **Technical Problems Solved:** These inventions address the limitations of transmission distance in traditional QKD networks and the vulnerabilities of optical fiber links to eavesdropping attacks.

- **Improvement:** They provide more secure and reliable communication channels.

(Relevant)

5. Quantum Key Management in Networks

- **Novelty and Objectives:** WO 2023080344 focuses on quantum key management in quantum key utilization networks, aiming to solve the problem of limited quantum key resources and decreasing key generation rates with increasing distance between nodes. EP 4224788 aims to improve the security of QKDNs by preventing the Key Management Layer (KML) from storing any secret keys. (Relevant)
- **Unique Components/Methods:** WO 2023080344 uses a confirmation unit that checks quantum key count information between indexed quantum key management system nodes and a navigator that navigates a node path. EP 4224788 has the KML exclusively receive XORed-keys from Core Nodes and send these XORed-keys to the Edge Nodes of the QKD layer.
- **Technical Problems Solved:** These inventions address the challenges of managing and distributing quantum keys in large-scale networks.
- **Improvement:** They provide more efficient and secure key management systems.

(Relevant)

Applicability and Uses

The inventions described in these patents have a wide range of practical applications:

- **Secure Communications:** Protecting sensitive data in various sectors, including finance, government, and military (WO 2013048674, WO 2024136930). (Relevant)
- **Quantum-Resistant Infrastructure:** Upgrading existing PKI systems to be secure against quantum computing attacks (WO 2024054691, EP 4221071). (Relevant)

- **Edge Computing Security:** Securing data and computations in edge devices using post-quantum cryptography (WO 2022206183). (Relevant)
- **Wireless Communication Security:** Enhancing the security of wireless networks using quantum encryption keys (WO 2023158459). (Relevant)
- **Long-Distance Communication:** Extending the range of secure communication using quantum key distribution (WO 2020227141, EP 3886356). (Relevant)
- **Secure Key Exchange:** Providing secure key exchange facilities for existing networks (EP 4418605). (Relevant)
- **Undersea optical networks:** Providing secure transmission in optical communications systems, especially in long-distance optical communications systems like undersea environments (WO 2024136930). (Relevant)

Conclusion

The patents analyzed in this report demonstrate significant advancements in the field of Quantum Cryptography. The inventions address critical challenges in secure communication, key distribution, and protection against quantum computing attacks. By leveraging the principles of quantum mechanics, these technologies offer the potential to create more secure and reliable communication systems for a wide range of applications. The ongoing development and refinement of these technologies will be crucial in ensuring the security of data and communications in the face of evolving cyber threats.

Citations

- WO 2018199426 (Relevant)
- EP 3886356 (Relevant)
- WO 2025123881 (Relevant)
- WO 2020178736 (Relevant)
- WO 2024054691 (Relevant)
- EP 4221071 (Relevant)
- WO 2021075653 (Relevant)
- WO 2019088689 (Relevant)
- WO 2024136930 (Relevant)

- EP 3718248 (Relevant)
- WO 2023080344 (Relevant)
- EP 4224788 (Relevant)
- WO 2013048674 (Relevant)
- WO 2022206183 (Relevant)
- WO 2023158459 (Relevant)
- WO 2020227141 (Relevant)
- EP 4418605 (Relevant)

Contexts: WO 2013048674 :: QUANTUM KEY MANAGEMENT\n
WO 2024136930 :: HYBRID QUANTUM CRYPTOGRAPHY PROTOCOL FOR OPTICAL COMMUNICATIONS\n
WO 2025123881 :: QUANTUM KEY DISTRIBUTION METHOD AND QUANTUM CRYPTOGRAPHY SYSTEM IMPLEMENTED BY BIDIRECTIONAL KEY POOL\n
EP 1768301 :: QUANTUM ENCRYPTION COMMUNICATION SYSTEM\n
EP 4231582 :: METHOD AND DEVICE FOR QUANTUM KEY DISTRIBUTION\n
EP 3718248 :: QUANTUM SECURITY SYSTEMS\n
WO 2025052024 :: QUANTUM ENCRYPTION\n
EP 3896897 :: QUANTUM CRYPTOGRAPHIC DEVICE, QUANTUM CRYPTOGRAPHIC COMMUNICATION FEE CALCULATION SYSTEM, AND QUANTUM CRYPTOGRAPHIC COMMUNICATION FEE CALCULATION METHOD\n
WO 2023107895 :: QUANTUM ENTANGLEMENT DISTRIBUTION SERVICE\n
WO 2018199426 :: METHOD AND APPARATUS FOR QUANTUM KEY DISTRIBUTION ON BASIS OF PHOTON SUBTRACTION FROM RECEIVER\n
WO 2016206498 :: FIRST QUANTUM NODE, SECOND QUANTUM NODE, SECURE COMMUNICATIONS ARCHITECTURE SYSTEM, AND METHOD\n
WO 2021075653 :: INTELLIGENT QUANTUM ENTROPY MANAGEMENT AND DISTRIBUTION SYSTEM\n
EP 3886356 :: METHOD AND SYSTEM OF QUANTUM KEY DISTRIBUTION\n
WO 2022142460 :: CENTRALIZED QUANTUM CRYPTOGRAPHY NETWORK GROUP KEY DISTRIBUTION METHOD AND SYSTEM\n
WO 2006003715 :: QUANTUM ENCRYPTION COMMUNICATION SYSTEM\n
EP 2014009 :: KEY MANAGEMENT AND USER AUTHENTICATION FOR QUANTUM CRYPTOGRAPHY NETWORKS\n
EP 2356772 :: QUANTUM KEY DISTRIBUTION\n
WO 2023080344 :: QUANTUM KEY MANAGEMENT DEVICE AND OPERATION METHOD THEREOF\n
WO 2019088689 :: PUF-QRNG QUANTUM CRYPTOGRAPHIC SECURITY TERMINAL SYSTEM AND CRYPTOGRAPHIC KEY GENERATION METHOD\n
EP 717896 :: SYSTEM AND METHOD FOR KEY DISTRIBUTION USING QUANTUM CRYPTOGRAPHY\n
, WO 2020178736 :: QUANTUM-RESISTANT CRYPTOPROCESSING\n
WO 2024054691 :: A QUANTUM PUBLIC KEY INFRASTRUCTURE (QPKI) SYSTEM\n
WO 2013048674 :: QUANTUM KEY MANAGEMENT\n
WO 2006024939 :: TWO NON-ORTHOGONAL STATES QUANTUM CRYPTOGRAPHY METHOD AND APPARATUS WITH INTRA-AND INTER-QUBIT INTERFERENCE FOR

EAVESDROPPER DETECTION\n
WO 2023107895 :: QUANTUM ENTANGLEMENT DISTRIBUTION SERVICE\n
WO 2023078639 :: QUANTUM-SECURED COMMUNICATION\n
WO 2023158459 :: SYSTEM AND METHOD FOR IMPLEMENTING QUANTUM-SECURE WIRELESS NETWORKS\n
WO 2020227141 :: METHOD OF OPERATION OF A QUANTUM KEY CONTROLLER\n
EP 4221071 :: SYSTEM AND METHOD FOR POST-QUANTUM TRUST PROVISIONING AND UPDATING WITH CONTEMPORARY CRYPTOGRAPHY\n
WO 2020260751 :: ENCRYPTED COMMUNICATION BASED ON QUANTUM KEY\n
WO 2022206183 :: POST-QUANTUM CRYPTOGRAPHY SECURED EXECUTION ENVIRONMENTS FOR EDGE DEVICES\n
EP 3244566 :: PHASE REFERENCE SHARING SCHEMES FOR CONTINUOUS-VARIABLE QUANTUM CRYPTOGRAPHY\n
EP 4224788 :: QUANTUM KEY DISTRIBUTION NETWORK AND QUANTUM-SECURED COMMUNICATION NETWORK INCLUDING THE ABOVE\n
EP 4418605 :: POST-QUANTUM ENCRYPTION KEY DISTRIBUTION METHOD AND A DEVICE\n