Quantum Computing Bootcamp Assignment-4

# **Quantum Key Distribution (QKD)**

1. **What is the primary goal of Quantum Key Distribution?**

Ans: **(b)** To establish a secret key between two parties with information-theoretic security based on the laws of quantum mechanics.

1. **Which fundamental quantum mechanical principle guarantees the security of some QKD protocols against eavesdropping?**

Ans: (c) The no-cloning theorem

1. **In the BB84 protocol, what is the purpose of using two different bases for encoding qubits?**

Ans: (b) To detect the presence of an eavesdropper (Eve).

1. **What are the typical carriers of quantum information (qubits) in fiber-optic QKD systems?**

Ans: (c) Photons

1. **What is "quantum bit error rate" (QBER) in the context of QKD?**

Ans: (b) The probability that a transmitted qubit is flipped due to noise or eavesdropping.

1. **Which of the following is a practical limitation of current long-distance QKD systems?**

Ans: (c) Signal loss in the transmission medium.

1. **What process is used after the quantum transmission phase in QKD to obtain a shared secret key?**

Ans: (b) Classical post-processing, including sifting and privacy amplification.

1. **Which QKD protocol utilizes entangled photons?**

Ans: (c) E91

1. **What is the role of "sifting" in the BB84 protocol?**

Ans: (c) To allow Alice and Bob to agree on the qubits encoded and measured in the same basis.

1. **Why is QKD considered "future-proof" against eavesdropping?**

Ans: (b) Because its security is based on the fundamental laws of physics, which cannot be circumvented.

# **Post-Quantum Cryptography (PQC)**

1. **What is the primary motivation for developing Post-Quantum Cryptography?**

Ans: (c) To develop cryptographic systems that are secure against attacks from future quantum computers.

1. **Which mathematical problem forms the basis of many lattice-based PQC schemes?**

Ans: (c) Shortest Vector Problem (SVP) and Learning With Errors (LWE)

1. **What type of code is commonly used in code-based PQC schemes like McEliece?**

Ans: (c) Goppa codes

1. **Which PQC family relies on the difficulty of finding isogenies between elliptic curves?**

Ans: (d) Isogeny-based cryptography

1. **What is a significant advantage of hash-based signatures like SPHINCS+?**

Ans: (b) Their security relies on well-understood properties of cryptographic hash functions.

1. **Which of the following is a major challenge in deploying PQC algorithms?**

Ans: (b) Their significantly larger key and signature sizes compared to current standards.

1. **Which NIST PQC standardization process finalist is based on the Learning With Errors (LWE) problem?**

Ans: (b) CRYSTALS-Kyber

1. **What is the main idea behind multivariate polynomial cryptography?**

Ans: (b) Relying on the difficulty of solving systems of multivariate polynomial equations over finite fields.

1. **Why is it important to standardize PQC algorithms now, even though large-scale quantum computers are not yet widely available?**

Ans: (b) To ensure that secure communication will be possible in the future when quantum computers become a threat, considering the time needed for transition.

1. **Which of the following is NOT a major family of Post-Quantum Cryptography algorithms being considered for standardization?**

Ans: (c) DNA-based cryptography