Chapter 5
Quantum Cryptography and Post-Quantum Security Strategies

Khalid Hafiz Mir
https://orcid.org/0009-0007-2610-3779
Lovely Professional University, India

Anzah Bashir
Lovely Professional University, India

Isha Batra
Lovely Professional University, India

ABSTRACT

Quantum computing brings about a new problem to traditional cryptographic algorithms; it violates the security of current encryption methods. This chapter is concerned with investigating two areas, quantum cryptography and post-quantum security measures, detailing their concepts, developments, and consequences. Quantum cryptography utilizes the principles of quantum mechanics and particularly makes use of superposition and entanglement. Post-quantum cryptography (PQC), on the other hand, is an approach to constructing cryptographic algorithms that will be immune to quantum attacks while at the same time keeping compatibility with classical methods. The chapter focuses on the aspects of integration between quantum cryptographical advancements and post-quantum algorithmic progressions and mutual distinctions have been explained. Possible shortcomings to scalability, implementation, and standardization issues of both approaches are discussed, as well as an examination of combined QKD and post-quantum algorithms architectures.

DOI: 10.4018/979-8-3693-6925-8.ch005

1. INTRODUCTION

New advancements in the development of quantum computing have charted significant changes in the literature on information security. As problems that may take classical computers thousands of years to solve may be solved in minutes through the use of quantum computing, traditional cryptography like; RSA, ECC, and Diffie-Hellman algorithms are at risk since they hitch their security on the difficulty of factoring large numbers or solving discrete logarithms. This looming challenge necessitates a dual approach: applying some mechanisms of quantum mechanics to improve the security of communications and designing classical cryptographic algorithms immune to the threat of attacks using quantum techniques(Olaoye, n.d.)

Some of the novel approaches for information security are based upon the idea of quantum cryptography, which is the branch of knowledge based on the laws of quantum mechanics. Although spanning a wide variety of fields, the most widely known application is Quantum Key Distribution (QKD) which guarantees the secure exchange of keys through the use of principles such as the quantum superposition and quantum entanglement. These methods offer what has been considered the greatest security possible since any act of spying on a quantum communication disrupts the message transfer (Rupesh, 2023). Despite these relative advantages, there are more important practical problems like high implementation costs, scalability and side-channel attacks that cannot at the current time allow for the widespread use of practical ones.

Conversely, post-quantum cryptography (PQC) is an industry-based solution for a quantum risk. PQC, instead, is centered in the conception of cryptographic algorithms which would hard to be attacked by both quantum and non-quantum structures. These algorithms, which include lattice-based cryptography and hash-based signatures and employ multivariate polynomial equations, are developed to fit perfectly into current communication architectures and, therefore, ready for implementation. In this chapter, it is given a detailed analysis of how quantum cryptography can be combined with post-quantum systems and the background, issues, and potential of both directions (Sood, n.d.). We discuss how the quest for the optimal post-quantum cryptography strategy, which enhances the advantages of QKD and its integration with other modern algorithms, increases. Moreover, the chapter explains several future dominating standardization projects like the NIST post quantum cryptography.