Chapter 7
QKD Protocol for Securing the Communication With Real-Life Application Scenarios

Hasan Abbas Al-Mohammed
Qatar University, Qatar

Elias Yaacoub
Qatar University, Qatar

Khalid Abualsaud
Qatar University, Qatar

ABSTRACT

QKD is a technique for sharing a secret key between two parties by utilizing quantum mechanics. Two well-known protocols that contributed to securing the communication are BB84 and E91. This chapter discussed the principle of quantum security and cryptography and emphasizes the recent developments and potential applications of new and emerging applications of these techniques in security in current applications or the future; moreover, different scenarios for using QKD lengths such as seeds for generating keys to encryptions messages, using QKD as key for DES or AES algorithms, also, using QKD in real-life scenarios such as healthcare in personal area networks for protecting the privacy of the patients' data, or railway monitoring scenarios to encrypt the collected data generated by the sensors are discussed.

DOI: 10.4018/978-1-7998-9522-0.ch007

Copyright © 2024, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.

INTRODUCTION

Due to increased attack number and complexity, uniformly linked computers, attack speed, and attack tool availability and simplicity, all these facts make hacking the number one crime to worry about, as security incidents grew from 3.4 million in 2009 to reach 42.4 in 2014. Cryptanalysis is the science of stopping unofficial access to private information, as well as protecting the secrecy and security of files and other data. The difficulties of certain numerical procedures, including integer factorization or indeed the discrete logarithms problem, are the foundation of today's encryption technology. Nevertheless, because these challenges are not typically recognized to be difficult for a malevolent person with quantum computation abilities, the resulting cryptographic protocols are supposedly weak (Babber & Singh, 2021).

Code-based cryptosystems, such as the Diffie-Hellman key exchange and the Rivest-Shamir-Adleman (RSA) and ElGamal cryptosystems, are among the most promising encryptions that still rely on the hardness of the integer factorization or discrete logarithm problems (Fernandez-Carames, 2019).

Quantum computers are now the digital world's reality. It is a fact that as a new invention arrives, it acts as a solution to the current challenges, but also carries fresh security concerns as are the case for Quantum Computing. By quickly solving complex mathematical problems, these machines are able to crack the existing public key infrastructure, such that can be broken by Shor's algorithm. In addition, post-quantum cybersecurity is now one of the most widely studied areas of cryptology to model the age of the post quantum computer such as multivariate public key cryptosystem(Broadbent & Schaffner, 2016).

Hence, new attack surfaces are now being presented in the IoT environment. Such attack areas are triggered by interconnected and interdependent IoT systems. As a result, the protection against the threats is at greater danger in IoT applications than in other applications, and conventional cryptographic solutions may be inefficient for these kinds of technologies.

The formation of symmetric keys between remote parties over an insecure network is one of the most fundamental cryptographic primitives, and it underlies many modern cryptographic techniques. To do this, public-key encryption is frequently utilized.

Quantum key distribution (QKD), like classical public-key cryptography, permits key establishment over an untrusted network. This technique is identified as the distribution of the keys (quantum), therefore the abbreviation QKD. The safety of the QKD is based on quantum mechanics phenomena (natural) rather than the sophistication of numerical issues, and it can be demonstrated also in contradiction of an eavesdropper, Eve, who possesses infinite computing capacity.

19 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage: www.igi-global.com/chapter/qkd-protocol-for-securing-the-communication-with-real-life-application-scenarios/352411

Related Content

DNA Fragment Assembly Using Quantum-Inspired Genetic Algorithm
Manisha Rathee, Kumar Dilipand Ritu Rathee (2021). *Research Anthology on Advancements in Quantum Technology (pp. 228-245).*
www.irma-international.org/chapter/dna-fragment-assembly-using-quantum-inspired-genetic-algorithm/277775

Efficient Power Grid Management Using Quantum Computing and Machine Learning
S. Aslam, G. Tabita, J. S. V. Gopala Krishnaand Manesh R. Palav (2024). *Real-World Challenges in Quantum Electronics and Machine Computing (pp. 43-57).*
www.irma-international.org/chapter/efficient-power-grid-management-using-quantum-computing-and-machine-learning/353097

Navigating the Complexities of Agile Transformations in Large Organizations
Pushan Kumar Dutta, Arvind Kumar Bhardwajand Ankur Mahida (2024). *Quantum Computing and Supply Chain Management: A New Era of Optimization (pp. 315-330).*
www.irma-international.org/chapter/navigating-the-complexities-of-agile-transformations-in-large-organizations/351829

New Trends of Edge Computing Techniques for Trusting Analysis of Networks
Samaher Al-Janabi (2023). *Handbook of Research on Quantum Computing for Smart Environments (pp. 364-387).*
www.irma-international.org/chapter/new-trends-of-edge-computing-techniques-for-trusting-analysis-of-networks/319878

Tunable Attenuator Based on Hybrid Metal-Graphene Structure on Spoof Surface Plasmon Polaritons Waveguide
Aymen Hlaliand Hassen Zairi (2022). *Technology Road Mapping for Quantum Computing and Engineering (pp. 154-164).*
www.irma-international.org/chapter/tunable-attenuator-based-on-hybrid-metal-graphene-structure-on-spoof-surface-plasmon-polaritons-waveguide/300522