Design of Quantum Communication Protocols in Quantum Cryptography

Bilal A. Alhayani[1] · Omar A. AlKawak[2] · Hemant B. Mahajan[3] · Haci Ilhan[1] ·
Roa'a Mohammed Qasem[4]

Abstract

Secure communication has developed into one of the most promising disciplines in the contemporary world. This is a highly essential subject for every business and body, and its advancements are increasing significantly. Quantum computing is becoming an increasingly popular kind of contemporary computing. This type of computing makes advantage of the fundamental characteristics of quantum mechanics to process information. Certain of the problems that were present in classical computing, such as the factoring discrete logarithm problem, have already been addressed by some writers in the field of quantum computing QC. Another significant challenge faced by conventional computing is one related to security, which may now be addressed thanks to quantum cryptography protocols. However, researchers have recently shown that even quantum encryption may be vulnerable to hacking. Implementing protocols for quantum cryptography still comes with a number of significant challenges, the most significant of which being quantum bit errors.

Keywords Quantum communication · Quantum cryptography · Physical sciences

1 Introduction

In this modern era, all computing systems, stored data, and communication devices regularly face cyber attacks all over the world. The hackers could steal and store the encrypted data containing important information about policies of government institutions and other organizations to decrypt them later using powerful machines for their benefits. The limitations of conventional computers in addressing various problems necessitate the requirement of better technologies.

✉ Bilal A. Alhayani
  bilalalhayani1@gmail.com

1 Department of Electronics and Communication, Yildiz Technical University, Istanbul, Turkey

2 Department of Energy Engineering, College of Engineering, Al-Mussaib, University of Babylon, Hillah, Babil, Iraq

3 Godwit Technologies, Pune, India

4 Department of Electrical and Computer Engineering, Altinbas University, 34218 Istanbul, Turkey

2 Springer