Optical and Quantum Electronics (2022) 54:832
https://doi.org/10.1007/s11082-022-04164-y

Enhanced multiparty quantum secret sharing protocol based on quantum secure direct communication and corresponding qubits in noisy environment

Mahsa Khorrampanah[1] · Monireh Houshmand[1] · Mahdi Sadeghizadeh[2] · Hossein Aghababa[3] · Yousef Mafi[3]

Received: 23 March 2022 / Accepted: 1 September 2022 / Published online: 22 October 2022

Abstract
In this study, we propose a new protocol of quantum secret sharing to send four secret bits from the sender to the receivers using quantum secure direct communication and the corresponding qubits. Also, in this protocol, no message-carrying qubit is sent to the receivers via the quantum channel. At first, there are only two receivers and the message is transmitted in such a way that neither of the two receivers can access the secret message alone. If both receivers participate, the secret message will be revealed. In the second step, there are an arbitrary number of receivers. In this case, we use the idea of equivalent qubits similar to J. Wang et al.'s protocol and we add the auxiliary qubit similar to the Y. Liu et al.'s protocol. The efficiency of the protocol is better than the previous works. The efficiency of this protocol is equal to 50% where the efficiency of previous works such as Wang et al. and Liu et al. are 14.29% and 25% respectively. Finally the performance of the protocol is examined in the noisy environment.

Keywords Quantum computing · Quantum cryptography · Qua thentum secret sharing · Quantum secure direct communication · Quantum teleportation

1 Introduction

Due to the growing human need to process the information at a higher speed, we need to build more complex chips. Given that the number of transistors embedded in a chip is directly related to its processing power, more transistors must be used in the chips. On the other hand, to increase the speed of data processing, we need smaller transistors to install and allow the electrons to travel a shorter path. Gordon Moore (Moore 1965) predicted a change in the complexity of microelectronic circuits claiming that the number of

✉ Monireh Houshmand
m.hooshmand@imamreza.ac.ir

[1] Department of Electrical Engineering, Imam Reza International University, Mashhad, Iran

[2] Department of Computer Engineering, Quchan University of Technology, Quchan, Iran

[3] School of Electrical and Computer Engineering, University of Tehran, Tehran, Iran