International Journal of Theoretical Physics (2021) 60:3744–3759
https://doi.org/10.1007/s10773-021-04865-2

n-Bit Quantum Secret Sharing Protocol Using Quantum Secure Direct Communication

Mohammad Sadegh Sadeghi-Zadeh[1] · Mahsa Khorrampanah[2] · Monireh Houshmand[1] · Hossein Aghababa[3] · Yousef Mafi[3]

Received: 25 October 2020 / Accepted: 9 June 2021 / Published online: 2 September 2021

Abstract
The proposed quantum secret sharing protocol in this article conveys n bit secret messages from the sender to the n receivers making use of a secure direct communication. In this protocol, all users work together to access their secrets. As a result, the security of the proposed protocol is high. The channel used in this design is an entangled 2n-qubit state. The efficiency of this design has been compared with other designs and it turns out that the efficiency of the proposed protocol is equal to that of the best designs. We demonstrate that this protocol is more efficient than the only n-user confidential subscription plan. Also, all stages of the design in a noisy space have been examined.

Keywords Quantum computing · Quantum cryptography · Quantum secret sharing · Quantum secure direct communication

1 Introduction

Quantum information science [1–4] is a combination of information science and quantum mechanics. One of the most important branches of this science is quantum cryptography [5–8]. Quantum cryptography began with the discovery of key distribution which provided unconditional security for communication among users.

The first quantum key distribution protocol was proposed by Bennett and Brassard [9]. In this protocol, the key is distributed with unconditional security. Later, the key distribution method was used to encrypt and decrypt confidential information [10, 11].

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

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

[2] Department of Electrical and Computer Engineering, University of Tabriz, Tabriz, Iran

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