A THREE-PARTY LIGHTWEIGHT QUANTUM KEY DISTRIBUTION PROTOCOL IN A RESTRICTED QUANTUM ENVIRONMENT

Mustapha Anis **YOUNES**

Université de Bejaia, Faculté des Sciences Exactes, Laboratoire de Physique Théorique,
06000 Bejaia, Algérie
Orcid number: 0009-0007-4979-9887
mustaphaanis.younes@univ-bejaia.dz

Sofia **ZEBBOUDJ**

ENSIBS, Université Bretagne Sud,
56000, Vannes, France
Orcid number: 0000-0002-5721-5753
sofia.zebboudj@univ-ubs.fr

Abdelhakim **GHARBI**

Université de Bejaia, Faculté des Sciences Exactes, Laboratoire de Physique Théorique,
06000 Bejaia, Algérie
Orcid number: 0000-0003-2995-3238
abdelhakim.gharbi@univ-bejaia.dz

Abstract

Quantum key distribution (QKD) protocols enable two parties to establish a shared secret key that can later be used to encrypt and decrypt confidential information. By leveraging the fundamental laws of quantum physics, such keys remain secure against an all-powerful quantum adversary. However, most existing protocols require all participants to possess full quantum capabilities, which is unrealistic since not all users can afford or operate advanced quantum devices. Moreover, extending QKD to multipartite scenarios is an active area of research due to its applications, such as broadcasting.

In this work, we propose a novel three-party lightweight quantum key distribution (LQKD) protocol based on the four-particle cluster state within a quantum-restricted environment. The protocol enables a quantum-capable user to simultaneously establish two separate secret keys with two "classical" users who hold limited quantum capabilities. By employing a one-way qubit transmission method, our scheme addresses several limitations found in similar schemes: (1) it eliminates the need for classical participants to use costly quantum devices to defend against quantum Trojan horse attacks; (2) it shortens the qubit transmission distance; and (3) it achieves higher qubit

efficiency. Consequently, the proposed LQKD protocol is both more lightweight and more practical than existing schemes. Furthermore, it is proven unconditionally secure, with a noise tolerance close to that of BB84.