Information Sciences 285 (2014) 1–23

Contents lists available at ScienceDirect

Information Sciences

journal homepage: www.elsevier.com/locate/ins

Geometrical analysis of physically allowed quantum cloning transformations for quantum cryptography

Laszlo Gyongyosi [a,b,*], Sandor Imre [a]

[a] Quantum Technologies Laboratory, Department of Telecommunications, Budapest University of Technology and Economics, 2 Magyar tudosok krt, Budapest H-1117, Hungary
[b] MTA-BME Information Systems Research Group, Hungarian Academy of Sciences, 7 Nador st., Budapest H-1051, Hungary

ARTICLE INFO

Article history:
Received 28 October 2009
Received in revised form 3 June 2014
Accepted 6 July 2014
Available online 16 July 2014

Keywords:
Quantum cryptography
Quantum key distribution
Quantum communication
Quantum cloning
Continuous variable

ABSTRACT

The security of quantum key distribution (QKD) relies on the no-cloning theorem, which allows no to copy perfectly a quantum system. An eavesdropping activity on the quantum channel perturbs the state of the quantum states, which results in noise at the receiver. The physical layer detection of the eavesdropping activity of the quantum channel requires tomography, which is intractable in experiment. An adequate and equivalent answer for the problem can be proposed through the logical layer. We propose an efficient algorithmical tool to study the eavesdropping activity on the quantum channel and characterize the properties of a quantum cloning-based attack for DV and CVQKD protocols. The physically allowed quantum cloning transformations on a quantum system can be described in terms of information geometry. We propose a computational geometrical method to analyze the cloning activity on the quantum channel and to characterize the noise properties. The security analysis studies the DV (discrete variable) and CV (continuous variable) QKD schemes through the four-state (BB84) and six-state DVQKD protocols and the two-way CVQKD protocol. The proposed geometrical method provides a useful tool to analyze the most powerful attacks against quantum cryptography and the effects of the physically allowed quantum cloning transformations.

1. Introduction

Quantum cryptography [1–4,8–27,43–76] is an emerging technology that provides unconditional secure communication by the fundamental laws of quantum mechanics [81–102]. The QKD (quantum key distribution) protocols represent one of the most important practical applications of quantum information theory. The QKD protocols can be classified into two main classes: DV (discrete variable) and CV (continuous variable) QKD systems.

The first-introduced QKD protocols were based on discrete variables, such as photon polarization. Since the polarization of single photons cannot be encoded and decoded efficiently because of the technological limitations of current physical devices, the CVQKD systems were proposed. In a CVQKD system, the information is encoded on continuous variables by a Gaussian modulation, such as in the position or momentum quadratures of coherent states. In comparison with DVQKD,

* Corresponding author at: Quantum Technologies Laboratory, Department of Telecommunications, Budapest University of Technology and Economics, 2 Magyar tudosok krt, Budapest H-1117, Hungary.
E-mail address: gyongyosi@hit.bme.hu (L. Gyongyosi).

http://dx.doi.org/10.1016/j.ins.2014.07.010
0020-0255/

the modulation and decoding of continuous variables do not require specialized devices and can be implemented efficiently by standard telecommunication networks and technologies that are currently available and in widespread use. As follows, the CVQKD systems can be integrated into the current telecommunication networks by using well-established optical fiber networks and practical technological devices. Both in DVQKD and CVQKD, the appropriate characterization of the eavesdropping activity on the quantum channel has a crucial role in the security proof of the protocol. The no-cloning theorem has an important role in quantum cryptography since it makes it not possible to copy a quantum state perfectly. More precisely, the no-cloning theorem forbids only the achievement of a perfect cloning; however, it allows an eavesdropper to perform imperfect cloning. An eavesdropper can clone in a noisy form the quantum states sent through the quantum channel from a legal sender, Alice, to a legal receiver, Bob [43]. The noise of the quantum channel that is generated by the eavesdropper has different patterns in a DVQKD and CVQKD protocol and can be described by different mathematical backgrounds. On the other hand, the appropriate study of the cloning activity on the quantum channel for each of the DV and CV cases is essential. The physical layer detection of the eavesdropping activity on the quantum channel requires tomography, which is intractable in current practical scenarios. An adequate and equivalent answer for the problem can be given through the logical layer by providing efficient algorithmical tools for this aim. We precisely do this in the work. We propose an efficient algorithmical tool in the logical layer to study the eavesdropping activity on the quantum channel and characterize the properties of a quantum cloning-based attack for DV and CVQKD protocols. The introduced information geometric algorithm provides an efficient solution to give an analogous answer to the methods of physical layer, such as the tomography of the quantum channel by a more flexible tool.

Recently, much work has been devoted to investigate the connections between quantum cloning and quantum state estimation. Quantum state estimation is a useful tool with several important applications of quantum optics, quantum mechanics, and quantum information. This field focuses on the reconstructing of a quantum system from several measurements, where the measurements formulate a tomographically complete set [77–80]. The measurement results form a basis on the Hilbert space of the quantum system, which makes it possible to extract all the relevant information about the given quantum system. These also formulate a data set on which several algorithmical postprocessing steps can be applied to extract as much valuable information from the quantum state as possible. Applying the proposed algorithm on the measurement data also provides a useful framework to process further measurement results obtained in the process of quantum state estimation, and to achieve efficient postprocessing on the obtained data. The proposed algorithm can extract further relevant information from the measurements to characterize the effects of quantum cloning in QKD in the phase space and to construct a sharper picture from the consequences of quantum state perturbation. Combining the fundamentals of quantum state estimation with the proposed information geometric algorithm, acts as an additional resource in the process of quantum state reconstruction allowing further improvements in the precision and effectiveness of the estimation process. In fact, the proposed quantum cloner analysis is directly connected to quantum state estimation because the legal parties of any QKD protocol can establish a precalibration phase before the protocol run, in which the process of quantum state estimation, more precisely the estimation of the eavesdropping activity, can be fully characterized. This relation efficiently allows for proposing our algorithm in a quantum state estimation framework to exploit the additional computational resources provided by our algorithmical tool. This connection further sets a proper framework that permits to appreciate and contextualize the proposed analysis and our geometrical algorithm. We will demonstrate the working mechanism of our algorithm in the phase space for quantum cloning in CVQKD.

In this work, we study the quantum cloning-based attacks and provide an efficient solution for their detection in quantum cryptography. In a QKD protocol, the legal parties can detect the disturbance generated by Eve's (the eavesdropper) cloning activity through the increased noise of the quantum channel. We propose an information geometrical method to study the eavesdropping strategies against DVQKD and CVQKD. The most powerful attacks against QKD are the collective attacks. In a collective attack, Eve is equipped with a quantum memory, and she can perform a collective measurement on the cloned quantum states at the end of the protocol run. In DVQKD protocols, the noise of the quantum channel generated by the eavesdropper can be modeled as an erasing process, while in the CVQKD, the eavesdropping activity adds white Gaussian noise into the transmission. As follows, while in the DV case, the quantum channel can be modeled as an erasure channel; in CVQKD, the appropriate model of the quantum channel is equivalent to a continuous Gaussian channel.

We analyze the most powerful collective attacks, which can be further classified into the DV and CV protocols. For DVQKD, the incoherent quantum cloning-based attack is the eavesdropper's most general strategy; thus, we use the incoherent attack-based attacker model. We show a new method to determine the presence of quantum cloning transformations for DVQKD through the BB84 and the six-state DV protocols, and for CVQKD, through the two-way CVQKD [56] protocol. In a one-way CVQKD system, Alice, the sender, transmits her continuous variables to the receiver, Bob, over a quantum channel. In a two-way system, Bob starts the communication, Alice adds her internal secret to the received message, and this is then sent back to Bob (e.g., one mode of the coupled beam that is outputted from a beam splitter (BS) is transmitted back to Bob). The two-way CVQKD systems were introduced for practical reasons to exceed the limitations of one-way CVQKD, such as low key rates and short communication distances [67].

This paper is organized as follows: In Section 2, the preliminary findings are summarized. In Section 3, we analyze the DVQKD setting and we extend it to the CVQKD. Section 4 proposes the information geometric algorithm. Finally, Section 5 concludes the results.