GIQ **28** (2024) 1–11

SERIES ON
Geometry, Integrability
and Quantization
ISSN 1314-3247

ENCODING OPTIMUM OF A QUANTUM KEY DISTRIBUTION MODEL

GEORGI BEBROV

Communicated by Ivaïlo M. Mladenov

The work reports a general way to evaluate the encoding optimum of a quantum key distribution model. The evaluation is based on the concept of mutual information and compression. A method for evaluating the encoding optimum is proposed. The original point-to-point quantum key distribution model is subjected to this method. It is shown that this model (and probably any existing model) does not reach its encoding optimum.

MSC: 68P30, 81P68
Keywords: Encoding optimum, quantum key distribution

Contents

1. Introduction

The principles of quantum mechanics [15] (as well as those of special relativity [5]) are the only tools that could be used to construct a key distribution system (or model, or process) being information-theoretically secure (confidential). An example of such a model is the so-called *quantum key distribution* (QKD) [1, 13]. It is based on the impossibility of third parties (eavesdroppers) to extract information out of the communication process without disturbing it. Several prominent QKD

doi: 10.7546/giq-28-2024-1-11