
# Quantum key distribution using a two-way quantum channel

Marco Lucamarini, Stefano Mancini

PII: S0304-3975(14)00695-1
DOI: 10.1016/j.tcs.2014.09.017
Reference: TCS 9867

To appear in: *Theoretical Computer Science*

Received date: 2 March 2009
Accepted date: 5 January 2011

Please cite this article in press as: M. Lucamarini, S. Mancini, Quantum key distribution using a two-way quantum channel, *Theor. Comput. Sci.* (2014), http://dx.doi.org/10.1016/j.tcs.2014.09.017

# Quantum Key Distribution using a Two-way Quantum Channel

Marco Lucamarini[1]

*School of Science and Technology, University of Camerino*
*via Madonna delle Carceri, 9 - 62032 Camerino, Italy*

Stefano Mancini

*School of Science and Technology, University of Camerino*
*via Madonna delle Carceri, 9 - 62032 Camerino, Italy*

**Abstract**

We review a quantum key distribution protocol, recently proposed by us, that makes use of a two-way quantum channel. We provide a characterization of such a protocol from a practical perspective, and consider the most relevant individual-particle eavesdropping strategies against it. This allows us to compare its potentialities with those of the standard BB84 protocol which uses a one-way quantum channel.

*Keywords:* Quantum cryptography and communication security

## 1. Introduction

Since the seminal works by Bennett and Brassard [1] and by Ekert [2] Quantum Key Distribution (QKD) has made impressive progresses [3], which can be roughly grouped into two main categories: on the one side there are theoretical progresses, among which the unconditional security of QKD is the most relevant one [4, 5, 6, 7, 8]; on the other side there are experimental progresses, almost exclusively in the field of quantum optics, which recently led to long-haul and high-rate QKD experiments [9, 10, 11, 12]. The relevance of these advances

[1]Presently at Cambridge Research Laboratory, Toshiba Research Europe Ltd., 208 Cambridge Science Park, Milton Road, Cambridge, CB4 0GZ, United Kingdom