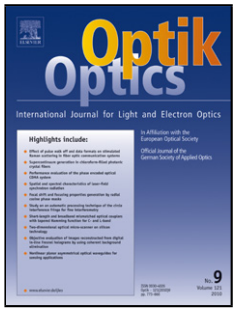

Title: Scheme of the arrangement for attack on the protocol BB84

Author: D.L. Khokhlov

PII: S0030-4026(16)30456-9
DOI: http://dx.doi.org/doi:10.1016/j.ijleo.2016.05.023
Reference: IJLEO 57649

To appear in:

Received date: 14-3-2016
Accepted date: 9-5-2016

Please cite this article as: D.L. Khokhlov, Scheme of the arrangement for attack on the protocol BB84, *<![CDATA[Optik - International Journal for Light and Electron Optics]]>* (2016), http://dx.doi.org/10.1016/j.ijleo.2016.05.023

Scheme of the arrangement for attack on the protocol BB84

D.L. Khokhlov

Sumy State University (Retired), Ukraine

Abstract

In a recent paper, a scheme of the weak measurement of the polarization state of the photon on the basis of the interferometer with two polarizing beam splitters was proposed. In the present paper, a scheme of the arrangement including several such interferometers is considered. The arrangement allows to distinguish four polarization states of the photon used in the quantum key distribution protocol BB84. With the aid of the arrangement, one may perform an intercept-resend attack on the protocol BB84.

Key words: Weak measurement, quantum key distribution, protocol BB84

1 Introduction

In quantum mechanics [1] a single particle may be described by the superposition state. The projective measurement triggers collapse of the superposition state onto one of the pure states constituting the superposition state. Therefore, the projective measurement destroys information about the initial state of the particle. This is used in quantum key distribution, e.g. [2] and reference therein. In the quantum key distribution protocol BB84 [3], Alice sends to Bob photons in the rectilinear (vertical/horizontal polarization) basis and in the diagonal (45 degree/135 degree polarization) basis. Eavesdropper Eve intercepts the photon coming from Alice, performs the projective measurement on it either in the rectilinear or diagonal basis, and then resends the same photon to Bob. By doing so, Eve introduces an error in the signal with the probability 0.25 which may be revealed by Alice and Bob. Thus, the BB84 protocol is secure against the intercept-resend attack using the projective measurement.

Email address: dlkhokhl@rambler.ru (D.L. Khokhlov).