Available online at www.sciencedirect.com
ScienceDirect
Optics and Lasers in Engineering 45 (2007) 463–467
OPTICS and LASERS in ENGINEERING

Quantum communication exploiting above threshold OPO intensity correlations and polarization encoding

A. Porzio[a,*], V. D'Auria[a,b], P. Aniello[b,c], M.G.A. Paris[d], S. Solimeno[a,b]

[a]*Coherentia—INFM unità di Napoli, Italy*
[b]*Dipartimento di Scienze Fisiche, Università "Federico II", Italy*
[c]*INFN sez. Napoli Complesso Universitario di Monte Sant'Angelo, via Cintia, 80126 Napoli, Italy*
[d]*INFM and Dipartimento di Fisica, Universita' degli studi di Milano, Italia, via Celoria 16 I-20133, Milano, Italy*

Available online 26 July 2006

Abstract

We present a continuous variable quantum communication protocol based on bright continuous-wave twin-beams generated by a type-II OPO. Intensity correlation between the beams is used in conjunction with a binary randomization of polarization to guarantee security and reveal eavesdropping actions. The scheme presented is asymmetric. Bob (the receiver) retains one of the beams and sends the other one to Alice after a random rotation of its polarization. The cryptographic key elements are encoded through amplitude modulation by Alice, who sends back her beam to Bob after a second rotation of the polarization. Eventually, the beams are detected by Bob after a further random polarization rotation. The security of the system and the possibility of revealing the eavesdropping action in the case of an individual attack are demonstrated by evaluating the bit error rates.

Keywords: Quantum communication; Twin-beams; Optical parametric oscillatior

1. Introduction

In recent years there has been an increasing interest in exploiting typical features of quantum mechanical systems in order to implement communication schemes showing a high level of security. Such secure schemes can be employed for implementing a quantum key distribution (QKD) protocol: a way for safely sharing a secret key between two distant parties (say, Alice and Bob) [1,2].

Since the first proposal of Bennett and Brassard [3], there has been an increasing number of experimental realizations of QKD with discrete variables, essentially based upon single photon systems [2]. In these systems the information is randomly encoded on a couple of non-commuting variables. By this strategy, one obtains that any *eavesdropper* (say, Eve) is forced to *guess* which observable has to be measured. Eve is likely to make the wrong guess half of the times, thus revealing her presence to Alice and Bob through back-action.

QKD concepts have been extended to continuous variable (CV) systems [4,5]. It has been argued that a general CV secure quantum communication protocol should be discussed in terms of the bit error rate (BER). In particular, the quantum mechanical limits to the minimum extra-disturbance that Alice and Bob are able to detect on their data have been established. It has also been shown that entanglement is a precondition for realizing secure communication schemes [6].

EPR CV beams—i.e. twin-beam—have already been employed in two quantum communication experiments [7,8]. The Caltech group [7] has shown that EPR CV correlations improve the signal-to-noise ratio (SNR) in transmitting a coherent message. A simplified version of this scheme [8] uses a single EPR beam traveling between Alice and Bob.

More recently, it has been shown that it is possible to realize QKD by using coherent beams [9–11]. In these schemes, two random Gaussian variables are encoded in two non-commuting observables by means of both phase and amplitude modulation.

In all the above-mentioned CV schemes the measurements at the receiver are implemented by homodyne

*Corresponding author. Tel.: +39 081 676188; fax: +39 081 676346.
E-mail address: alberto.porzio@na.infn.it (A. Porzio).

0143-8166/$ - see front matter © 2006 Elsevier Ltd. All rights reserved.
doi:10.1016/j.optlaseng.2005.07.012

detectors, requiring the remote control of the local oscillator (LO) phase, or the transmission of both the LO and the carrier beams.

In addition to these experiments, there have been some further proposals for CV QKD [12–14]. The scheme of Ref. [12] is based on simultaneous homodyne detection at the two stations, whereas the very recent proposal [13] avoids homodyne detection and exploits quantum dense coding on EPR beams [15], together with the possibility of changing EPR correlation in an OPA working randomly either as an amplifier or a de-amplifier. In Ref. [14], a scheme employing the photon number correlation in a seeded OPA is discussed. This scheme exploits both polarization entanglement and photon number correlation of the down-converted pulses, with the difference in the signal and idler photons used for coding. A photodiode with a high dynamical range is needed at the receiver, in order to discriminate a relative difference in the photon number of the order of 10^{-3} to -10^{-4}. The latter scheme has been recently object of a preliminary feasibility experiment [16].

In the present paper, we propose a CV communication protocol whose security relies on quantum correlations between continuous-wave (CW) twin-beam generated in an above threshold type-II OPO [17–20]. The main features of this scheme are:

(1) intrinsically asymmetric with the receiver ruling the transmission;
(2) direct detection, which avoids drawbacks of homodyne detectors;
(3) a single beam travels back and forth Alice–Bob;
(4) data encoded by sub-shot-noise amplitude modulation, and protected by random polarization rotations.

The proposed scheme can be regarded as a base for a QKD protocol. Its nature will be discussed in terms of transmission BER and the possibility of revealing interceptions will be evaluated for the single attack scheme.

2. Quantum communication using bright twin beams

The present CV protocol is schematically depicted in Fig. 1. Before the transmission starts the two communicating parties agree on a public channel on modulation/demodulation frequency Ω and fix the bit duration time (referred to in the follows as "time slot").

Bob (receiver) generates a twin-beams by a type-II OPO and spatially separates the two orthogonally polarized components ("signal" and "idler") by a polarizing beam-splitter (PBS_1). One of the beams (f.i. the idler) is retained by Bob while the other one travels back and forth the two parties. Once the beams are separated Bob rotates the signal polarization by an angle ϕ randomly chosen and sends it to Alice.

On her side Alice (sender) encodes each bit as follows. For every time slot she decides to apply or not an amplitude modulation, at frequency Ω, to the signal (say: bit $1 \Leftrightarrow$ modulation "on", bit $0 \Leftrightarrow$ modulation "off"). She tunes the modulation depth so as to hide its effects below the shot-noise-level (SNL). At the end, Alice changes once again the beam polarization by choosing at random between 0 and $\pi/2$. Eventually, the beam carrying the bit value, is sent back toward the receiver station.

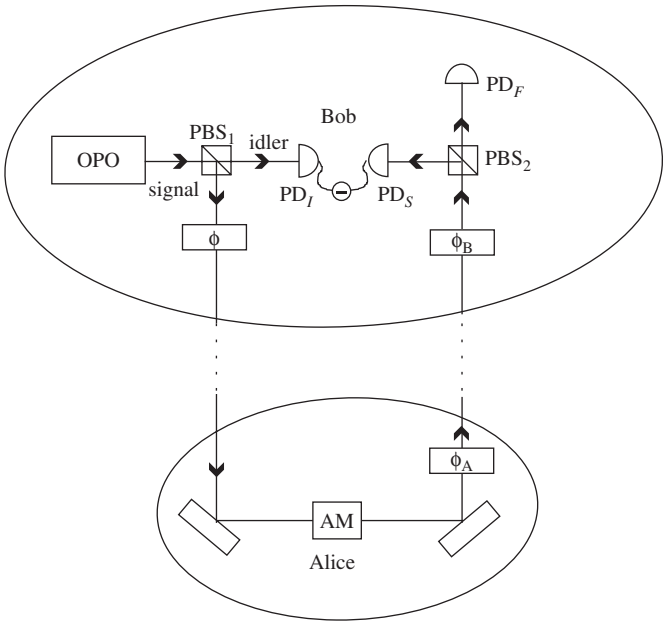

Fig. 1. Schematic of the quantum cryptographic protocol. Bob generates CW twin-beam and sends one of them to Alice's station where the key bits are encoded by means of amplitude modulation. The beam travels back to Bob where intensity difference measurements are implemented. The random polarization changes, indicated by the angles ϕ, ϕ_A, and ϕ_B, are used to protect data.

Bob recovers the bit value by detecting simultaneously the signal + idler beams and exploiting their quantum correlation. As a first step he rotates randomly the polarization ($\phi_B = -\phi$ or $\phi_B = \pi/2 - \phi$). Next, if the total polarization change $\phi + \phi_A + \phi_B$ is equal to 0 or π, the signal impinging on PBS_2 is totally reflected toward the photodiode (PD_S) and the paired beams are detected and the bit recovered from the difference photocurrent. On the contrary, if $\phi + \phi_A + \phi_B = \pi/2$ the signal is transmitted toward PD_F which measures a non-zero mean photocurrent. In the latter case, occurring on average half of the times, Bob marks the corresponding time slot as no-data.

Notice that in virtue of the EPR correlation the SNR of the signal-idler difference is better than that of the signal alone. On the other side, the polarization procedure randomizes the QKD protocol. In this way both the sender and the receiver do not know "a priori" if the bit sent (received) in a particular time slot would be or not part of the final bit array.

Once Alice has sent N bits to Bob, they need to distill the final array. To do this, using a public channel, Bob reveals to Alice, for each time slot, the value of the angle $\phi_B + \phi$. Alice, knowing ϕ_A, compute $\phi + \phi_B + \phi_A$ and discard the