Eur. Phys. J. D **21**, 109–113 (2002)
DOI: 10.1140/epjd/e2002-00172-5

THE EUROPEAN PHYSICAL JOURNAL D

Double entanglement and quantum cryptography*

M. Genovese[a] and C. Novero

Istituto Elettrotecnico Nazionale Galileo Ferraris, Str. delle Cacce 91, 10135 Torino, Italy

Received 23 July 2001 / Received in final form 30 November 2001
Published online 24 September 2002 –

Abstract. We propose a quantum transmission based on bi-photons, which are doubly-entangled both in polarisation and phase. This scheme finds a natural application in quantum cryptography, where we show that an eventual eavesdropper is bound to introduce a larger error on the quantum communication than for a single entangled bi-photon communication, when he steels the same information.

PACS. 03.67.Dd Quantum cryptography – 03.67.Hk Quantum communication – 42.79.-e Optical elements, devices, and systems

The recent fast development of quantum states manipulation techniques has led to new technological applications of quantum mechanics. Among different applications of quantum mechanics to technology the possibility of transmitting absolutely confidential messages is of the greatest interest. This is due to the possibility of creating a key for encoding and decoding secret messages by transmitting single quanta between two parties (usually dubbed Alice and Bob). The underlying principle of quantum key distribution (QKD) is that nature prohibits gaining information on the state of a quantum system without disturbing it (in particular no-cloning theorem guarantees that one cannot generates copies of an arbitrary unknown state). Thus possible eavesdropping by a third party (usually dubbed Eve) can be identified. This is at variance with current methods of public key cryptography, which are based on the supposed, but unproven, classical computational difficulty in solving certain problems, *e.g.* factoring large numbers in prime factors. Furthermore, a quantum computer would efficiently solve these problems [1] breaking these kind of classical cryptographic protocols. From this it arises the great interest in understanding and developing secure quantum cryptographic schemes.

Since the original proposal of quantum cryptography [2], many different protocols for this kind of transmission have been suggested [3–7,9].

For example, in Ekert's protocol [5] entangled pairs are used. Both Alice and Bob receive one particle of the entangled pair. Then they perform a measurement choosing among at least three different selections. Alice and Bob communicate on a classical channel the bases they have used: if measurements were performed in the same basis, they are perfectly correlated and can be used for generating the secret key. The other measurements can be used for a test of Bell inequalities. If a third party, Eve, tries to eavesdrop, she inevitably affects the entanglement between the two particles leading to a reduction of the violation of the Bell inequalities, which allows Alice and Bob to recognise the presence of the spy.

In the BB84 scheme [4] single states are transmitted from Alice to Bob, preparing them at random in four partly orthogonal states (for example, using photons, in polarisation states at 0° and 90°, 45° and 135°). Bob selects the bases for the measurement at random too. Then Alice and Bob communicate on a classical channel the bases they have used (but not the results of course): when they have used the same basis Bob knows Alice's result and *vice versa* and they can build a key. If Eve tries to intercept the message, she inevitably introduces errors, which Alice and Bob can detect by comparing a subsample of the generated key using the classic channel (which in these schemes is supposed to be subject to eavesdropping, but not alterable).

Many different experiments have been realised using the former schemes, demonstrating the feasibility of QKD up to a distance of many kilometers [8,9] both in air and in fibre.

Most of them are based on transmission of single photon states or weak coherent states, where the alphabet is based either on photon polarisation or on photon phase. It must be noticed that in the case of weak coherent states the transmission can, in principle, be unsafe for sometimes the pulses necessarily contain more than one photon leaving the possibility to an eavesdropper of using these events for gaining information about the key without introducing any extra error [10]. The use of single photon sources closes this potential security loophole.

General theorems have been demonstrated (mainly for BB84 protocol) which guarantees the security of quantum cryptography in an ideal case [9,11,12], albeit no complete

* Dedicated to the memory of Carlo Novero.

[a] e-mail: genovese@ien.it

demonstration for every conceivable attack exists[1]. However, real experimental schemes suffer of huge losses and the application of these theorems is limited. Therefore, it is mandatory the search for strategies which restrict the information potentially obtainable by eavesdropping on real channels.

In this paper we propose the realisation of "double entanglement" on a single photon pair to be used for quantum communication. More in details, the bi-photon pair is entangled both in polarisation and in phase, eventually allowing a larger bit transmission for every pair. In the specific scheme that we discuss in the following, the security analysis is based on the sum of the two results obtained for polarisation and phase measurement: we will show that the use of this scheme makes more difficult a successful eavesdropping. This work follows a recent line of research [13] where quantum cryptography using multilevels systems is studied indicating that it leads to an easier detection of an eventual eavesdropper.

The scheme for producing such an entanglement is relatively simple: for example it can be realised placing on the pump beam a Mach-Zender interferometer (whose path length difference is large compared to the pump pulse length) before the non-linear system where a polarisation entangled pair is generated. The pump photon can thus follow the short or the long path originating the superposition [15]:

$$|\Psi_p\rangle = \frac{1}{\sqrt{2}}\left[|s\rangle + \mathrm{e}^{\mathrm{i}\phi}|l\rangle\right] \tag{1}$$

where $|s\rangle$ and $|l\rangle$ denote the photon which has followed the short and the long path respectively and ϕ the phase difference between the two paths.

Then the pump photon creates a photon pair entangled in polarisation by parametric down conversion or in a type II crystal [14] either in two sequential type I crystals [16] (see Fig. 1). The second solution presents some advantages for it does not have the problem of different propagation of idler and signal inside the crystal due to different polarisation in a birefringent medium [17], furthermore every Bell state can be easily obtained. Finally, using two type I crystals and tuning the pump wave length, one can generate an entanglement on two different frequencies: in this case one wave length could, for example, be chosen at the maximum of transmission of an optical fibre or air and the other (the one remaining in Alice's laboratory) at the one maximising detection efficiency. Incidentally, it must also be noticed that by using this scheme one could also easily obtain non-maximally entanglement both in phase (using a not $50\%-50\%$ beam splitter) and polarisation (attenuating the pump between the two crystals or/and using crystals of different lengths) [16]: this possibility has relevance for experiments on foundations of quantum mechanics.

[1] It must be noticed that a completely general security demonstration could even be impossible in presence of Trojan horse attacks, *i.e.* when the eavesdropper can introduce some unwanted material inside Bob lab using unused (for cryptographic transmission) degrees of freedom of the quantum states. The demonstration of security against Trojan horse attacks in reference [11] does note really solve the problem (at least with current technology) because it is based on teleportation, which requires the use of EPR pairs shared with an insecure area where they can be subject to Eve's manipulation.

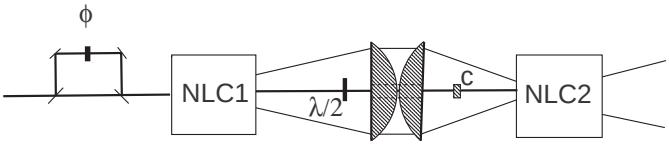

Fig. 1. Scheme for the generation of the double entangled photon pairs. A Mach-Zender interferometer creates a state of the pump photon which is given by the superposition of the states corresponding to the photon following the long and the short path respectively. The pump photon then generates or a horizontally polarised pair in the first type I (NLC1) crystal either (after having been rotated by a $\lambda/2$ wave plate) a vertically polarised one in the second type I (NLC2) crystal. The parametric down conversions of the two crystals are then superimposed using an optical condenser with a hole drilled in the centre for leaving pass the pump undisturbed. The optical path of idler, signal and pump are arranged by means of compensator elements (C) for not introducing any delay among these (see Ref. [16] for details). The superposition of the probability of generating a pair in the first or in the second crystal originates the polarisation entanglement.

Using the two type I crystals scheme, the final bi-photon state is:

$$|\Psi\rangle = \frac{1}{2}\left[|sH\rangle|sH\rangle + |sV\rangle|sV\rangle + \mathrm{e}^{\mathrm{i}\phi}(|lV\rangle|lV\rangle + |lH\rangle|lH\rangle)\right] \tag{2}$$

where H and V denote the horizontal and vertical polarisation respectively, whilst $|s\rangle$ and $|l\rangle$ denote a photon created by a pump photon having travelled *via* the short or the long arm of the interferometer.

This is the state that will be used for quantum transmission.

It must be noticed that this state remains invariant in its form changing the polarisation basis to

$$|\pm\rangle = \frac{1}{\sqrt{2}}\left[|H\rangle \pm |V\rangle\right] \tag{3}$$

in fact the state 2 can be rewritten as:

$$|\Psi\rangle = \frac{1}{2}\left[|s+\rangle|s+\rangle + |s-\rangle|s-\rangle + \mathrm{e}^{\mathrm{i}\phi}(|l+\rangle|l+\rangle + |l-\rangle|l-\rangle)\right]. \tag{4}$$

For implementing quantum communication, one photon is sent to Alice, the other to Bob. Both select the photon by its polarisation (for example using a birefringent prism), choosing different bases and then send it to a Mach-Zender interferometer, which introduces exactly the same difference of travel times, within the coherence time of the down converted photons, through the two arms as the interferometer on the pump (see [15]). Here they can choose different phases for the long arm (see Fig. 2). The probability

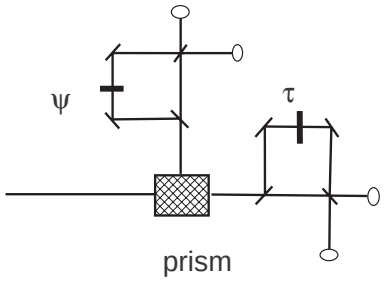

Fig. 2. The scheme for the reception apparatus of Alice and Bob. A prism, properly rotated, allows a polarisation selection. On each arm exiting the prism a Mach-Zender interferometer is inserted with a phase shift on the long arm which is suitably arranged by the observer. Photo-detectors are denoted by an ellipse.

for detection in the central time slot[2] by a given combination of detectors depends on the phases (*e.g.* ϕ, τ_A, ψ_B) of the three interferometers involved in production and detection of the photon pair [15] and on the polarisers' settings. Different choices originate different detection bases.

Therefore, this scheme allows obtaining two independent (as the two entanglement are independent) bits for each received photon, one related to polarisation, the other to phase. When Alice and Bob have chosen the same two bases (both for polarisation and phase) they have two correlated outputs, which they can use for generating the key. The other choices can be used for testing the channel (*e.g.* by means of Bell inequalities in the Ekert's protocol).

In order to identify without error the state, Eve should hit both the bases. This probability is reduced to P^2 respect to P for a single entangled quantum channel.

In order to quantify this statement, let us begin considering the case where Alice and Bob use the BB84 protocol (Eve produces the pair, keeps a photon which she will measure in one of the two bases and send the other to Bob) and the final key is given by the sum (modulo 2) of the two results obtained by Alice and Bob in the two bases when these have been chosen in the same way. In this case the communication channel is a binary symmetric one and the information on the channel is given by [18]

$$I = 1 + p \log_2 p + (1-p) \log_2 (1-p) \qquad (5)$$

where p is the probability for a correct transmission.

Let us begin considering the simplest case where Eve decides to eavesdrop the photons directed to Bob in one of the possible basis used by Alice and Bob, both for the phase and the polarisation ones.

In the case of a single entanglement, if Eve chooses correctly the basis she correctly intercepts the qubit, when she chooses the wrong basis she has a $q_1 = 1/2$ error. After Alice has publicly announced the bases she used, Eve can separate her bits in two sets corresponding to different bases and the Alice-Eve channel information is the average of the ones of the two bases, thus she obtains an information per bit measured $I_{AE} = 0.5$. On the other hand, she has introduced an error on Alice–Bob channel in the 50% of cases when she has chosen the wrong basis leading to $q_{AB} = 1/4$, namely $I_{AB} = 0.189$.

If Alice and Bob use the double entangled scheme, the information on the Alice-Eve channel is now $I_{AE} = 0.25$. Furthermore, she introduces a fraction of errors $q_{AB} = 3/8$ on the Alice–Bob channel, leading to an information on the Alice–Bob channel $I_{AB} = 0.046$.

If Eve intercepts a fraction η of the transmitted photons, she obtains an information $I_{AE} = 0.5\eta$ for the single entangled channel and $I_{AE} = 0.25\eta$ for the double entangled one. In order to obtain the same information she will thus produce an error rate on the Alice–Bob channel 3 times larger for the double entangled channel, making by far easier her identification in this case.

Let us then consider the more interesting case where Eve chooses for eavesdropping an intermediate basis (dubbed the Breidbart basis) for both the phase and the polarisation ones respect to the bases used by Alice and Bob. This choice does not introduce asymmetric errors, making more difficult the identification of the eavesdropper. The probability for Eve to get a wrong result for a single basis is $q_1 = (2-\sqrt{2})/4$. As the final key is given by the sum (modulo 2) of the two results obtained by Alice and Bob in the two bases (for polarization entanglement and for phase entanglement) when these have been chosen in the same way, Eve obtains the right result when she correctly identifies both the number or when she misidentifies both. This leads to a probability, for our scheme, of having a correct interception of $p_2 = q_1^2 + (1-q_1)^2 = 3/4$, which gives, for equation (5), $I_{AE} = 0.189$. Furthermore, Eve introduces a fraction of errors $q_{AB} = 3/8$ on the Alice–Bob channel, leading to $I_{AB} = 0.046$.

On the other hand for the single entanglement, Eve has a q_1 error rate leading to $I_{AE} = 0.399$ and produces $1/4$ of error rate on the Alice–Bob channel, with $I_{AB} = 0.189$.

Eavesdropping a fraction η of the photons going to Bob, she obtains an information $I_{AE} = 0.399\eta$ for the single entangled channel and $I_{AE} = 0.189\eta$ for the double entangled one. In order to obtain the same information she shall thus produce an error rate on the Alice–Bob channel $19/6$ larger for the double entangled channel, which, as before, results in a much larger chance of identifying the eavesdropping in the double entangled case.

This result can also be obtained looking to the case where Alice and Bob adopt an error correction procedure. If they eliminate all the errors and Eve has intercepted a fraction η of photons, the upper limit on the information she could eavesdrop is [19] $I^c_{AE} = (1-r)\eta\alpha I_{AE}$ (where r is the error fraction that she introduces), *i.e.* $I^c_{AE} = 0.299\eta\alpha$ for the single entangled channel, whilst this is reduced to $I^c_{AE} = 0.118\eta\alpha$ for the double entangled channel, where α is the reduction factor of the key length during the error correction procedure (*i.e.* the ratio between the bits available to Alice and Bob before and after the correction procedure). Therefore, this result shows once again that

[2] Corresponding to the two indistinguishable situations when the pump photon has followed the short (long) arm of the interferometer and the two down converted photons both the long (short) one (see [15]).

(even if an exhaustive discussion of the value of α is missing [19]) the use of the double entangled channel allows a large improvement of the transmission security.

As a further example, let us consider the effect on a simple implementation of Ekert's protocol, like the one realised in reference [20]. In this case Alice and Bob measure their photons each on two bases. One of the bases of Bob and Alice coincides and therefore, when both use this basis, they obtain perfectly correlated results, which are used to build the key. The other results are used for measuring the Wigner inequality:

$$W = p(\chi, \psi) + p(\psi, \omega) - p(\chi, \omega) \geq 0 \qquad (6)$$

where $p(\chi, \psi)$ is the coincidence probability function for the measurement settings χ and ψ of Alice and Bob respectively. This inequality is always satisfied for any local realistic theory, but it is violated in quantum mechanics for an appropriate choice of settings. The maximal violation is $W = -1/8$. If Eve intercepts a fraction η of photons, she reduces the violation of equation (6). The reduction is evaluated considering that in a $(1 - \eta)$ fraction of the cases the value of W is left unmodified, whilst in a fraction η the value of W must be calculated considering the effect of Eve on the transmission (which is easily obtained by calculating the effect on the density matrix). In the implementation of reference [20] the detection efficiency of each photon path is 5% and the inequality (6) is measured with a 10% relative uncertainty. If Eve eavesdrops the photons on the commune basis, she obtains perfect information of the key for the intercepted photons. However, a 10% relative uncertainty on the measurement of the Wigner function requires that Eve must intercept a fraction of 6.7% or smaller of the photons addressed to Bob for remaining undetected.

If a double entangled channel is used, Eve would affect the value of two Wigner inequalities at the same time, this requires that she reduces (for not being discovered) the intercepted fraction to 4.7%, leading to a reduction of a factor 0.7 for the eavesdropped information in comparison with the single entangled channel.

Finally, as a last example, let us consider the case where Eve decides to eavesdrop on a generic basis given by a superposition of the basis states $|sH\rangle$, $|lH\rangle$, $|sV\rangle$ and $|lV\rangle$. She chooses at random the basis for the measurement, using a generic SO(4) (SO(2) for the single entanglement) transformation of the previous basis: in this way, on average, no asymmetric error is introduced. After having performed the measurement, Eve passes the photon to Bob exactly in the same state she found it in. In order to understand the effect of such a procedure we have performed a Monte Carlo simulation of the eavesdropping, evaluating the errors on the Alice–Bob channel. Our numerical results shows that the errors on the Alice–Bob channel are increased of a factor 1.25 about for the double entangled channel respect to the single entangled one, leading to an easier detection of the eavesdropper in the double entangled channel for this example as well.

A general discussion of security in presence of joint or coherent attacks is beyond the purpose of this work, however, it is evident how the presence of a double entanglement makes much more complicate the use of a translucent interception scheme as, for example, the one described in reference [21]. Thus one can expect that double entanglement should also be efficient in increasing security against these kinds of eavesdropping.

In summary, we have shown that the use of states entangled on two (or eventually more) quantum degrees of freedom at the same time allows a safer communication for realistic quantum channels. We have also proposed a scheme for obtaining such a double entanglement, which can be easily realised with a simple modification of present experiments. Finally, let us mention that the states, whose generation is described in this paper, may have relevant applications to the studies of foundations on quantum mechanics [22].

We would like to acknowledge support of ASI under contract LONO 500172 and of MURST *via* special programs "giovani ricercatori" Dip. Fisica Teorica Univ. Torino.

References

1. P.W. Shor, SIAM Rew. **41**, 303 (1999)
2. S. Wiesner, Sigact News **15**, 78 (1983)
3. See for example S.J. Lomonaco, `quant-ph 9811056` and references therein; see also "Special issue of Quantum Communication", J. Mod. Opt. **41**, 12 (1994)
4. C.H. Bennet, G. Brassard, Proc. Int. Conf. Comput. Syst. Sign. Process. 175 (1984)
5. A.K. Ekert, Phys. Rev. Lett. **67**, 661 (1991)
6. C.H. Bennet, Phys. Rev. Lett. **68**, 3121 (1992)
7. See for example: M. Czachor, Phys. Lett. A **257**, 107 (1999); A.K. Ekert *et al.*, Phys. Rev. A **257**, 157 (1999); W. Tittel, H. Zbinden, N. Gisin, Phys. Rev. A **63**, 042301 (2001)
8. W.T. Buttler *et al.*, Phys. Rev. Lett. **84**, 5652 (2000); W. Tittel *et al.*, Phys. Rev. Lett. **84**, 4737 (2000); H. Zbinden, Appl. Phys. B **67**, 743 (1998); W.T. Buttler *et al.*, Phys. Rev. Lett. **81**, 3283 (1998); A.V. Sergienko *et al.*, Phys. Rev. A **60**, R2622 (1999); P. Tapster *et al.*, communications at *ICQI 2001*, Rochester, NY; T. Jennewein *et al.*, Phys. Rev. Lett. **84**, 4729 (2000)
9. See for example M.A. Nielsen, I.L. Chuang, *Quantum computation and Information* (Cambridge, 2000); D. Bouwmeester *et al.*, *The physics of quantum information* (Springer, 2000); N. Gisin *et al.*, `quant-ph 0101098` and references therein
10. T. Durt, Phys. Rev. Lett. **83**, 2476 (1999); N. Lutkenhaus, Acta Phys. Slov. **49**, 549 (1999); G. Brassard, T. Mor, B. Sanders, `quant-ph 9906074`
11. H.K. Lo, H.F. Chau, Science **283**, 2050 (1999)
12. D. Meyers, in *Proc. of Crypto 96*, Springer-Verlag, p. 343; E. Biham, T. Mor, Phys. Rev. Lett. **78**, 2256 (1997); Phys. Rev. Lett. **79**, 4034 (1997); A.K. Ekert *et al.*, Phys. Rev. A **50**, 1047 (1994); H.E. Brandt *et al.*, Phys. Rev. A **56**, 4456 (1997); C.A. Fuchs *et al.*, Phys. Rev. A **56**, 1163 (1997); K.J. Blow, J.D. Phoenix, J. Mod. Opt. **40**, 33 (1993); S.E. Barnett *et al.*, J. Mod. Opt. **40**, 2501 (1993)

13. H. Bechmann-Pasquinucci, W. Tittel, Phys. Rev. A **61**, 062308 (2000); H. Bechmann-Pasquinucci, A. Peres, quant-ph 0001083; M. Bourennane *et al.*, quant-ph 0106049; N.J. Cerf *et al.*, quant-ph 0107130; D. Bruss, C. Macchiavello, quant-ph 0106126
14. T.E. Kiess *et al.*, Phys. Rev. Lett. **71**, 3893 (1993); P.G. Kwiat *et al.*, Phys. Rev. Lett. **75**, 4337 (1995)
15. J. Brendel *et al.*, Phys. Rev. Lett. **82**, 2594 (1999); W. Tittel *et al.*, Phys. Rev. Lett. **84**, 4737 (2000)
16. L. Hardy, Phys. Lett. A **161**, 326 (1992); G. Brida, M. Genovese, C. Novero, E. Predazzi, Phys. Lett. A **268**, 12 (2000), *Proc. of QCM&C 3*, edited by P. Tombesi, O. Hirota (Kluwer Capri, 2000), p. 399; for a similar scheme see also: A.G. White *et al.*, Phys. Rev. Lett. **83**, 3103 (1999)
17. T.E. Keller, M.H. Rubin, Phys. Rev. A **56**, 1534 (1997); Y.H. Kim *et al.*, Phys. Rev. A **63**, 062301 (2001) and references therein
18. R.B. Ash, *Information Theory* (Dover, New York, USA, 1990)
19. B. Huttner, A.K. Ekert, J. Mod. Opt. **41**, 2455 (1994)
20. T. Jennewein *et al.*, Phys. Rev. Lett. **84**, 4729 (2000)
21. M. Genovese, Phys. Rev. A **63**, 044303 (2001) and references therein
22. See for example: A.V. Belinskii, Phys. Uspekhi **40**, 305 (1997)