

Quantum cryptographic ranging

Vittorio Giovannetti¹, Seth Lloyd^{1,2} and Lorenzo Maccone¹

¹ Massachusetts Institute of Technology, Research Laboratory of Electronics,
Cambridge MA 02139, USA

² Massachusetts Institute of Technology, Department of Mechanical Engineering,
Cambridge MA 02139, USA

Received 13 December 2001

Published 29 July 2002

Online at stacks.iop.org/JOptB/4/S413

Abstract

We present a system to measure the distance between two parties that allows only trusted people to access the result. The security of the protocol is guaranteed by the complementarity principle in quantum mechanics. The protocol can be realized with available technology, at least as a proof of principle experiment.

Keywords: Quantum cryptography, positioning, entanglement, biphoton

The following touching problem is addressed in this paper. Alice is lost in the woods. Her friend Bob needs to find her, rescue her, and live happily ever after. On the other hand, the bad wolf Eve also wants to find her, in order to gobble her up. Suppose for simplicity a uni-dimensional forest, Alice and Bob need to find their relative positions (ranging) without giving any hint to Eve. This intent is analogous to the one underlying cryptography, i.e. the exchange of information in a secure fashion. In this respect, we refer to it as a crypto-positioning procedure.

In this paper, we show how the quantum mechanical time-energy uncertainty principle can be employed to measure, in a quantum cryptographically secure fashion, the distance between Alice and Bob. This means that the physical limitations imposed by quantum mechanics do not allow, not even in principle in the ideal case, any kind of eavesdropping on Eve's part. The secure exchange of information, based on analogous 'weird' quantum effects, was shown long ago in [1–3] and technological applications seem to be at hand [4]. Our idea to help Bob in his quest stems from joining Ekert's quantum cryptographic protocol [3] with the recently proposed quantum positioning protocol [5], which allows one to perform ranging using frequency-entangled states.

In [5, 6] we have shown how, by using N frequency-entangled photons, one can obtain an $1/\sqrt{N}$ accuracy enhancement in finding the distance between Alice and Bob over the case in which the N photons are not entangled. This is a *truly* quantum effect that arises from the strong photon correlations between photons originating from the entanglement. This same fact, however, makes the loss of a single photon critical; as shown in [6], when one of the entangled photons that travel from Bob to Alice is lost, the remaining photons yield no information at all on the distance

between the two. Such an apparent drawback turns out to be the key feature in devising the crypto-positioning protocol.

In the following we can limit our analysis to the case $N = 2$. In this situation it is possible to use the state generated by cw-pumped spontaneous parametric down-conversion crystal, in which the two generated photons are anti-correlated in frequency, i.e.

$$|\Psi\rangle \equiv \int d\omega \phi(\omega) |\omega_0 + \omega\rangle_I |\omega_0 - \omega\rangle_S. \quad (1)$$

In equation (1) the notation $|\nu\rangle$ refers to a single photon state of frequency ν , the ket subscripts refer to the two distinct field modes (the signal S and the idler I) generated by the crystal, $2\omega_0$ is the pump frequency, and $\phi(\omega)$ is the two-photon spectral function centred in $\omega = 0$ with bandwidth $\Delta\omega$. The state $|\Psi\rangle$ is one of the best known sources of entanglement currently available and an enormous amount of literature, both theoretical and experimental, is accessible (see, for example, [7] and references therein). Another possibility that can be exploited is the recently proposed 'difference beam state' [8], which displays frequency correlated photons, whereas $|\Psi\rangle$ displays anti-correlation in frequency.

The properties of the entanglement in the state $|\Psi\rangle$ are such that, if one measures the frequency of the signal photon, one would obtain a random value $\omega_0 + \omega$ with probability density $|\phi(\omega)|^2$, but the subsequent measurement on the idler photon will have the predictable outcome $\omega_0 - \omega$ (and vice versa if the measurements are reversed). On the other hand, it is possible to show that, if one measures the time of arrival of the first photon on a detector, then one will be able to predict (with an accuracy of the order of $\Delta\omega^{-1}$) the time of arrival of the second photon on a second detector at a distance L . In fact, the

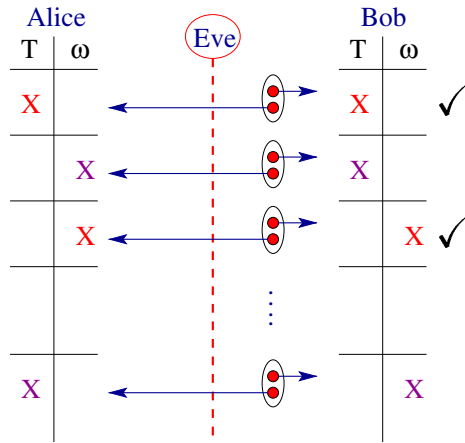


Figure 1. Alice and Bob randomly choose to measure either the time of arrival T or the frequency ω on each copy of the two-photon state $|\Psi\rangle$ they share. They retain only the copies for which their choices agree, i.e. the checked (\checkmark) copies.

(This figure is in colour only in the electronic version)

joint probability of measuring the first photon at time t_1 and the second at time t_2 is given by

$$P_c(t_1, t_2) \propto \left| \int d\omega \phi(\omega) e^{-i\omega(t_1 - t_2 + L/c)} \right|^2, \quad (2)$$

which exhibits a peak centred in $t_2 - t_1 = L/c$ of width proportional to $\Delta\omega^{-1}$. What happens when one measures the frequency of the first photon and the time of arrival of the second? In this case, it is possible to show that the outcome of the time of arrival measurement is completely unpredictable; all the timing information has been ‘erased’ by the frequency measurement. In this respect, the measurement of the frequency of one of the photons has the same effect as the loss of such a photon.

The crypto-positioning procedure, depicted in figure 1, is as follows.

- (1) Bob produces a certain number of labelled copies of the two-photon state $|\Psi\rangle$. For each copy, he sends Alice one of the two photons (e.g. the signal photon).
- (2) For the idler photon he did not send to Alice, Bob randomly measures either the frequency or the time at which it reaches a photodetector placed at a known distance from him.
- (3) In the thick of the woods, Alice receives Bob’s photon and she also randomly chooses to measure either the frequency or the time of arrival.
- (4) Alice and Bob broadcast the kind of measurement (frequency or time of arrival) they have performed on each of the two-photon copies. They discard all the measurement results of the cases in which their choices did not match.
- (5) Alice and Bob exchange the results of the frequency measurements and compare them. If the communication channel is perfect and there is no eavesdropper measuring photon transit times, these results are correlated (namely,

if Alice had obtained the frequency $\omega_0 + \omega$, Bob must have found $\omega_0 - \omega$). In contrast, if Eve is measuring the transit times of the photons, she has unavoidably spoiled the frequency entanglement. Alice and Bob find this out when they compare their data, since it will no longer be correlated.

- (6) Once they have verified that Eve is not tapping on the exchanged photons, Alice broadcasts to Bob all the measurement results of the photon times of arrival. This information is useless to anybody except Bob (who knows the timing information of the other photon of each couple) and this allows him to find the lost Alice through equation (2) which yields the distance L , given the photon times of arrival t_1 and t_2 .

Notice that Eve can measure the frequency of the travelling photons without being detected at step (5) of the protocol. This, however, does not allow her to gain any information on the distance L , and her presence can still be inferred by analysing the time of arrival data in step (6).

The scheme can be straightforwardly adapted to much more complicated scenarios. For example, one may tailor the entanglement to situations in which multiple rescuers are present and they can obtain Alice’s position only if they meet and exchange their data in the spirit of quantum secret sharing protocols. A discussion of the quantum crypto-positioning protocol can also be found in [6].

In conclusion, we have presented a protocol that, using the frequency-entangled state at the output of a parametric down-conversion crystal, allows one to perform quantum crypto-positioning. No matter how many resources the evil Eve devotes to eavesdropping, she will not be able to prevent a happy ending, since only Bob will find Alice!

Acknowledgments

This work was funded by the ARDA, NRO, and by ARO under a MURI program.

References

- [1] Bennett C H, Brassard G and Mermin N D 1992 *Phys. Rev. Lett.* **68** 557
- [2] Bennett C H 1992 *Phys. Rev. Lett.* **68** 3121
- [3] Ekert A K 1991 *Phys. Rev. Lett.* **67** 661
Ekert A K, Rarity J G, Tapster P R and Palma G M 1992 *Phys. Rev. Lett.* **69** 1293
- [4] Naik D S, Peterson C G, White A G, Berglund A J and Kwiat P G 2000 *Phys. Rev. Lett.* **84** 4733
Jennewein T, Simon C, Weihs G, Weinfurter H and Zeilinger A 2000 *Phys. Rev. Lett.* **84** 4729
Ribordy G, Brendel J, Gautier J-D, Gisin N and Zbinden H 2001 *Phys. Rev. A* **63** 012309
- [5] Giovannetti V, Lloyd S and Maccone L 2001 *Nature* **412** 417
- [6] Giovannetti V, Lloyd S and Maccone L 2002 *Phys. Rev. A* **65** 022309
- [7] Mandel L and Wolf E 1995 *Optical Coherence and Quantum Optics* (Cambridge: Cambridge University Press)
- [8] Giovannetti V, Maccone L, Shapiro J H and Wong F N C 2002 *Phys. Rev. Lett.* **88** 183602 (*Preprint* quant-ph/0109135)