# Positioning and clock synchronization through entanglement

Vittorio Giovannetti,[1] Seth Lloyd,[1,2] and Lorenzo Maccone[1]
[1]*Massachusetts Institute of Technology, Research Laboratory of Electronics, 50 Vassar Street, Cambridge, Massachusetts 02139*
[2]*Department of Mechanical Engineering, Massachusetts Institute of Technology, 3-160, Cambridge, Massachusetts 02139*
(Received 27 July 2001; revised manuscript received 10 September 2001; published 4 January 2002)

A method is proposed to employ entangled and squeezed light for determining the position of a party and for synchronizing distant clocks. An accuracy gain over analogous protocols that employ classical resources is demonstrated and a quantum-cryptographic positioning application is given, which allows only trusted parties to learn the position of whatever must be localized. The presence of a lossy channel and imperfect photodetection is considered. The advantages in using partially entangled states is discussed.

DOI: 10.1103/PhysRevA.65.022309 PACS number(s): 03.67.−a, 42.50.Dv, 03.65.−w

## INTRODUCTION

From the realm of thought experiments, quantum entanglement has recently become exploitable for various applications and almost ready for technological implementations in fields such as quantum cryptography [1]. Other applications for entanglement and squeezing have been proposed in fields such as interferometric measurements [2], frequency measurements [3,4], lithography [5], algorithms [6], etc. In this paper a recent proposal [7] to exploit entanglement and squeezing to enhance the accuracy of position measurements and clock synchronization is thoroughly analyzed.

In Sec. I the proposal of [7] is briefly reviewed and the notation that will be employed is presented. The positioning protocol is derived and its main features are described. In Sec. I A it is shown that our protocol gives an enhancement in accuracy by comparing it with classical procedures that employ analogous resources. In Sec. I B its use in a cryptographic context is addressed. In particular, two different cryptopositioning schemes are derived that prevent nontrusted parties to recover the position of what must be localized. The first is essentially a classical protocol, but allows an accuracy enhancement of the localization procedure over the unentangled case. The second is a quantum cryptopositioning scheme derived from the quantum cryptographic BB84 protocol [1]. In Sec. II the analysis of the protocol is given in the presence of loss, by considering the possibility that some photons are lost through dissipative processes during their travel or at the detection stage. The loss of a single photon in the maximally entangled state makes the resulting state completely useless. On the other hand, the loss of a photon in the unentangled case is not so dramatic since information on the time of arrival of the pulse may still be obtained by measuring the times of arrival of the remaining photons. However, by comparing the time of arrival information that can be obtained in the two cases, one sees that one still does better by using entangled states in a wide range of cases. The robustness to loss stems from the fact that the accuracy gain obtained through entanglement is high enough to beat the classical (unentangled case) accuracy even when some of the time of arrival data must be discarded. In Sec. III, the assumption of using maximally entangled states is relaxed. There is a trade-off between the degree of entanglement (or the accuracy gain) and the robustness to noise, as was also shown in Ref. [4]. A higher robustness against loss ensues by decreasing the degree of entanglement, at the cost of reducing the accuracy gain achievable. Given the loss of the available channel, one will have to optimize the states to be employed. A scheme that is analogous to fault-tolerant quantum computation is presented. It is possible to protect, at least partially, the entanglement from the loss by devising entangled states where the loss of one or more photons allows some information to be retained from the photons that do arrive. An example of such states is derived in detail.

## I. POSITIONING THROUGH ENTANGLEMENT

In this section a brief review of the method proposed in Ref. [7] is given. The positioning problem is defined and the formalism that will be used in the rest of the paper is laid out. In Sec. I A the enhancement in the positioning obtained by using entangled-squeezed states is given and analyzed, by comparing it to what one would obtain with classical states of equal spectral characteristics. Section I B is devoted to discussing the use of the proposed protocol in a cryptopositioning context.

For the sake of simplicity, consider the one-dimensional case in which one party (say Alice) wants to measure her distance from the detectors' position $x$ by sending a light pulse to each of the $M$ detectors that are placed in a known position. Alice's position can be obtained by measuring the pulses' travel time average $\langle t\rangle$ divided by the pulses' velocity. Given the spectral characteristics of each pulse, its time of arrival $t_i$ will have an intrinsic indetermination. The unsurpassable limit for classical measurements is given by the shot-noise limit: one must at least measure a single photon. The accuracy of the distance $x$ measurement depends on the variance $\Delta t^2$ of the statistical variable average time of arrival $\langle t\rangle$. This variance can be related to the intrinsic accuracy $\Delta\tau^2$ achievable on the measurement of the single photon time of arrival, which, in turn, will ultimately depend on the photon's bandwidth.

The formalism is now introduced. The probability to detect a photon at time $t$ and at position $x$ in an ideal photodetector with infinite time resolution is given by the formula [8,9]

$$P(t)\propto\langle E^{(-)}(t-x/c)E^{(+)}(t-x/c)\rangle, \qquad (1)$$

 

where the ensemble average is the expectation on the quantum state of the radiation. All actual photodetectors are of course nonideal, but the fundamental limit to the error introduced by the nonideal features of photodetectors is given by the bandwidth of the photodetector rather than the bandwidth of the detected photon [10]. In addition, this error can, in principle, be made as small as desired by devoting more resources (of energy, power, etc.) to the photodetection process. In Eq. (1), the signal field at time $t$ is given by

$$E_i^{(-)}(t) \equiv \int d\omega\, a_i^\dagger(\omega) e^{i\omega t}, \quad E_i^{(+)} \equiv (E_i^{(-)})^\dagger, \tag{2}$$

where $a_i(\omega)$ is the field annihilator of a quantum of frequency $\omega$ at the $i$th detector position. In the continuous Fock space formalism [11] of Eq. (2), the field annihilation operator is not dimensionless and satisfies the commutation relation

$$[a_i(\omega), a_j^\dagger(\omega')] = \delta_{ij}\delta(\omega - \omega'), \tag{3}$$

where the Kronecker delta accounts for the independence of the channels. The electromagnetic field has been quantized so that $E^{(-)}E^{(+)}$ is given in units of photons per second. For $M$ different communication channels, each of which may receive more than one photon, Eq. (1) generalizes to

$$P_M(t_{i,k}; N_i) \propto \left\langle : \prod_{i=1}^{M} \prod_{k=1}^{N_i} E_i^{(-)}(t_{i,k}) E_i^{(+)}(t_{i,k}) : \right\rangle, \tag{4}$$

where $t_{i,k}$ is the time of arrival of the $k$th photon in the $i$th channel, $N_i$ is the number of photons detected in the $i$th channel, and the detection time is shifted by the detector's position $x_i$: $t_{i,k} \to t_{i,k} + x_i/c$. The probability $P_M(t_{i,k}; N_i)$ must be normalized so that, when integrated over all the arrival times $t_{i,k}$, it gives the probability of detecting $N_i$ photons in the $i$th channel. In the case of unit quantum efficiency $\eta = 1$ (when no photons are lost through dissipative processes), this is also the probability of having $N_i$ photons in the channel. In the case $\eta < 1$ this is not true anymore, because there is a probability $1 - \eta$ that a photon will be lost in the channel or at the photodetection stage. A detailed analysis of this case is given in Sec. II. In the cases of coherent states and of states with definite number of photons that will be considered here, this choice of normalization allows us to use the formula (4) instead of the more complicated conditional joint probability (see [9], Chap. 14.8) of measuring *only* $N_i$ photons at times $t_{i,k}$ and no more in each of the $M$ channels.

Consider the situation where all the detectors are placed at the same position $x$. The probability $P_M(t_{i,k}; N_i)$ of Eq. (4) contains all the timing information relative to the transmitted pulses sent by Alice. In particular, the average time of arrival $\langle t \rangle$ needed for the position measurement can be obtained by taking the average of the quantity

$$T \equiv \frac{1}{M} \sum_{i=1}^{M} \frac{1}{N_i} \sum_{k=1}^{N_i} t_{i,k} \tag{5}$$

over the probability $P_M(t_{i,k}; N_i)$, namely,

$$\langle t \rangle = \sum_{N_i} \int dt_{i,k} P_M(t_{i,k}; N_i) T, \tag{6}$$

where the sum is performed on the values of $N_i$ for all $i$ and the integration is performed on all the $t_{i,k}$. The statistical error in determining $\langle t \rangle$ from the measurement results is given by the variance of $T$. This variance is dependent on the shape of the probability $P_M$, which in turn depends on the quantum state of the impinging light pulses, through Eq. (4).

### A. Quantum enhancement

Consider first the case of unit quantum efficiency $\eta = 1$, where no photons are lost. The $M$ coherent pulses a "classical" Alice would send to the reference detectors are described by a state of the radiation field of the form

$$|\Psi\rangle_{\rm cl} = \bigotimes_{i=1}^{M} \bigotimes_{\omega} |\alpha[\phi(\omega)\sqrt{N}]\rangle_i, \tag{7}$$

where $\omega$ is the pulses' carrier frequency, $\phi(\omega)$ is their spectral function, $|\alpha[\lambda(\omega)]\rangle$, is a coherent state of frequency $\omega$ and amplitude $\lambda(\omega)$ directed towards the $i$th detector, and $N$ is the mean number of photons in each pulse. The pulse spectrum $|\phi(\omega)|^2$ has been normalized so that $\int d\omega |\phi(\omega)|^2 = 1$. Upon calculating the ensemble average of Eq. (4) with the state $|\Psi\rangle_{\rm cl}$ using the property

$$a(\omega') \bigotimes_{\omega} |\alpha[\lambda(\omega)]\rangle = \lambda(\omega') \bigotimes_{\omega} |\alpha[\lambda(\omega)]\rangle, \tag{8}$$

one obtains the probability density

$$P_M(t_{i,k}; N_i) \propto \prod_{i=1}^{M} \prod_{k=1}^{N_i} |g(t_{i,k})|^2, \tag{9}$$

where $g(t)$ is the Fourier transform of the spectral function $\phi(\omega)$,

$$g(t) = \frac{1}{\sqrt{2\pi}} \int d\omega\, \phi(\omega) e^{-i\omega t}. \tag{10}$$

Notice that the probability $P_M$ factorizes, since in the classical state all the photons are independent. The quantity $|g(t_{i,k})|^2$ is the probability that the $k$th photon is received on the $i$th channel at time $t_{i,k}$. Define $\Delta\tau^2$ as the variance of $|g(t_{i,k})|^2$ (which is independent of $i$ and $k$ since all the photons have the same spectrum). From Eq. (9) it follows that the statistical error relative to the mean time of arrival $\langle t \rangle$ is

$$\Delta t \gtrsim \frac{\Delta\tau}{\sqrt{MN}} \tag{11}$$

with approximate equality for $N \gg 1$.

Now compare this result with the one obtained from a quantum state which combines entanglement and photon-number squeezing. Define the state $|N_\omega\rangle$ the number-

squeezed state of frequency $\omega$ in which all modes are in the vacuum state, except for the mode at frequency $\omega$, which is populated by exactly $N$ photons. The entangled-squeezed state that allows us to achieve the most enhancement over the classical case is given by

$$|\Psi\rangle_{NM}=\int d\omega\ \phi(\omega)|N_\omega\rangle_1\cdots|N_\omega\rangle_M . \tag{12}$$

By choosing the same spectral function $\phi(\omega)$ of the state (7), the spectral characteristics of each of the channels of the state $|\Psi\rangle_{NM}$ (obtained by tracing $|\Psi\rangle_{NM}$ over all the other channels) is the same as the classical state. Notice that $|\Psi\rangle_{NM}$ is a frequency maximally entangled state: a measurement of the frequency of a single one of its photons will have a random outcome weighted by the probability $|\phi(\omega)|^2$, but will determine the frequency of all the other photons. Since the number of photons in each channel is fixed ($N$) and no photons are lost ($\eta=1$), the probability $P_M(t_{i,k};N_i)$ is null for $N_i\neq N$, thanks to its normalization discussed previously. For $N_i=N$, inserting $|\Psi\rangle_{NM}$ in Eq. (4), it follows that

$$P_M(t_{i,k};N)\propto\left|g\left(\sum_{i=1}^{M}\sum_{k=1}^{N}t_{i,k}\right)\right|^2, \tag{13}$$

where the property $[a_i(\omega')]^N|N_\omega\rangle_j=\delta_{ij}\delta(\omega-\omega')\sqrt{N!}|0\rangle$ was employed ($|0\rangle$ being the normalized vacuum state) and $g(t)$ is the same as Eq. (10). Equation (13) shows that the entanglement in frequency translates into the bunching of the times of arrival of the photons of different pulses: although their individual times of arrival are random, the average $T=(1/MN)\Sigma_{i,k}t_{i,k}$ of these times is highly peaked. Indeed, from Eq. (13) it follows that the probability distribution of $T$ is $|g(MNT)|^2$. This immediately implies that the average time of arrival $\langle t\rangle$ is determined to an accuracy

$$\Delta t=\frac{\Delta\tau}{MN}, \tag{14}$$

where $\Delta\tau$ is the same as Eq. (11). This result shows a $\sqrt{MN}$ accuracy improvement over the classical case (11). The Margolus-Levitin theorem [12] implies that a $\sqrt{MN}$ improvement in accuracy is the best that can be obtained [7]. The role of the entanglement and the role of the squeezing in enhancing position measurements are separately addressed in Ref. [7]. It is shown that the $\sqrt{M}$ enhancement derives from the entanglement between the channels and the $\sqrt{N}$ enhancement from the number squeezing within each channel.

Notice that when the state $|\Psi\rangle_{NM}$ is used, the results of the single time-of-arrival measurement are meaningless: it is necessary to make correlation measurements, i.e., in this case one must consider the *sum* of the times of arrival of all the photons as in the quantity $T$. This implies that the geometry of the problem that can be solved depends on the state that can be produced. The state $|\Psi\rangle_{NM}$, which is tailored as to give the least indetermination in the physical quantity $T$, is appropriate for the geometry of the case considered here, where all the detectors are in the same position and the sum of the pulses' time of arrival is needed. Other maximally entangled states have to be tailored for different geometric dispositions of the detectors [7].

In conclusion, the suggested positioning protocol requires: (i) to produce and deploy the maximally entangled state suited for the given disposition of the reference points, (ii) to measure the time of arrival $t_{i,k}$ of the $k$th photon in the $i$th reference point, and (iii) to collect and compare the results in order to have the needed correlation measurement.

### B. Quantum cryptographic positioning

The accuracy enhancement over classical protocols is not the only reason that makes the use of quantum mechanics appealing in the positioning problem. In fact, one is also offered the possibility of employing the ideas of quantum cryptography in this context. In this section two different cryptopositioning protocols based on our scheme will be given. The aim is for Alice to learn her position in space relative to Bob (located at the detectors position), without anybody else gaining *any* information by intercepting neither the photons nor the classical information Alice and Bob exchange.

The first protocol is essentially equivalent to a classical protocol in which Alice sends Bob photons each of which she delayed by a random amount of time, which she does not disclose. From Bob's random times of arrival she may recover her position without anybody else (including Bob) knowing it. In the quantum version given here, however, the accuracy for a fixed number $M$ of photons is increased over the classical version. This protocol allows only Alice to recover her position: nobody else (including Bob) will be able to determine where she is. Consider for simplicity the case of the state $|\Psi\rangle_{NM}$ with one photon per channel ($N=1$), given by

$$|\Psi\rangle_{\mathrm{en}}\equiv\int d\omega\ \phi(\omega)|\omega\rangle_1\cdots|\omega\rangle_M , \tag{15}$$

where $|\omega\rangle\equiv|1_\omega\rangle$. The extension to the general case is straightforward. This protocol is simply implemented by allowing Alice to detect the time of arrival of the photons in one of the $M$ channels. She will send to Bob only the rest $M-1$ photons. When Bob receives and measures them, he will use a public channel to broadcast the measurement result to Alice. As will be shown in Sec. II, the loss of a single photon results in not being able to recover *any* information on Alice's position. Thus if an eavesdropper was to intercept the photons Alice sends to Bob (the eavesdropper need not even bother: he only has to wait for Bob's broadcast), he would obtain no information. Alice, on the other hand, simply has to add the random times of arrival that Bob tells her to the one she herself has measured. This allows her to find her position, with an uncertainty $\Delta t=\Delta\tau/(M-1)$, since she only used $M-1$ photons for the positioning.

The second protocol allows both Alice and Bob to recover their distance without anybody else discovering it. This protocol is analogous to the quantum-cryptographic key exchange BB84 [1]. Alice and Bob share $r$ copies of the state $|\Psi\rangle_{\mathrm{en}}$ of which, as before, Alice retains one photon and

sends Bob the remaining $M-1$. For each of the $r$ copies, Alice and Bob choose randomly (and independently) to measure either the frequency or the time of arrival of *all* the photons. After that they compare which of the two ''observables'' they used on each of the $r$ copies they exchanged: they discard all the cases in which the two observables do not match, namely, Alice measured the frequency and Bob the time of arrival or vice versa. For all the cases in which both of them measured the frequency, they broadcast the measurement results. Since the state is maximally entangled in frequency, their measurement outcomes (though random) must agree. If this is not the case, they know that there is an eavesdropper, who is ruining the states that are transiting between them. If all the frequency-measurement outcomes do agree, they can be confident that no one is measuring the photon time of transit in the channel. Once they have verified that no eavesdropper was present, Alice can broadcast the measurement results for half of the copies in which they both measured the time of arrival and Bob can broadcast the measurement results of the other half. From the information they exchange, which is utterly useless for anybody else, both Alice and Bob may recover Alice's position. Of course an eavesdropper might be measuring the frequency of the exchanged photons without being detected, but this will not give him any information on Alice's position: he may only succeed in ruining Alice and Bob's exchange.

Notice that it is possible to modify this second protocol to include more complicated scenarios, such as the case in which also other trusted persons may be allowed to learn Alice's position, or (by suitably tailoring the entanglement of the exchanged pulses) the case in which some of the trusted persons may learn Alice's position *only* when they meet and exchange their data, or the case in which Alice herself is not allowed to discover her own position, etc.

Finally, it is worth noticing that an implementation of the cryptopositioning schemes described here can be achieved with the state $|\Psi\rangle_{\rm en}$ for $M=2$, the practical realization of which has been recently proposed in Ref. [13].

## II. LOSS ANALYSIS IN THE IDEAL CASE

In this section the problem of the loss is addressed. The loss of a single photon from a maximally entangled state (such as $|\Psi\rangle_{MN}$) makes it completely useless for positioning, since the information is encoded in the entanglement and not in the single photons. On the other hand, the loss of a single photon from a ''classical'' state (such as $|\Psi\rangle_{\rm cl}$) allows us still to recover information on the time of arrival of the remaining photons. Nonetheless, it will be shown that the the gain in accuracy obtained by using entangled photons vs unentangled photons is quite robust against the loss. In Sec. II A the conditions on the channel quantum efficiency that is necessary to obtain an enhancement in the accuracy is derived. First a simple argument is given, then a more rigorous approach is discussed. In Sec. II B the effect of the loss on the state is studied in the density-matrix formalism.

### A. Condition on the quantum efficiency

One can understand the robustness to loss from the following intuitive explanation (the rigorous derivation is given in detail later). For simplicity, consider the case of one photon per channel ($N=1$), comparing the entangled state $|\Psi\rangle_{\rm en}$ given in Eq. (15) with its unentangled analogous (i.e., with one photon per channel) given by

$$|\Psi\rangle_{\rm un}=\bigotimes_{i=1}^{M}\int d\omega_i\phi(\omega_i)|\omega_i\rangle_i, \tag{16}$$

which describes $M$ uncorrelated single-photon pulses each with the same spectral function $\phi(\omega)$ of Eq. (15). Given the channels' quantum efficiency $\eta$ (namely, $1-\eta$ is the probability that one photon is lost), the probability that all $M$ photons reach Alice is given by $\eta^M$. Repeating $r\gg 1$ times the whole experiment, a total number $rM$ of photons is sent. In average only a fraction $\eta^M$ of the experimental runs will not lose any photon. If Alice is employing the entangled states $|\Psi\rangle_{\rm en}$ of Eq. (15) (i.e., the state $|\Psi\rangle_{NM}$ with $N=1$) to evaluate the mean time of arrival $\langle t\rangle$, she must only use the data obtained from the experimental runs where all the $M$ photons of the state reach the detectors. As will be shown, the other cases in which some of the photons are lost are useless. The evaluation of the time-of-arrival accuracy obtained from the $r$ experimental runs through Eq. (14) will then be

$$\Delta t(r)=\frac{\Delta\tau}{M\sqrt{r\,\eta^M}}, \tag{17}$$

where the factor $1/\sqrt{r\,\eta^M}$ stems from the statistical independence of different experimental runs. On the other hand, if Alice employs $r$ copies of the unentangled $M$ photon state $|\Psi\rangle_{\rm un}$ defined in Eq. (16), all of the $\eta rM$ photons that in average reach the detectors may be employed to evaluate the time of arrival with an accuracy

$$\Delta t(r)\gtrsim\frac{\Delta\tau}{\sqrt{\eta rM}}, \tag{18}$$

where the equality holds for $rM\gg 1$. The condition for achieving a greater accuracy through the state $|\Psi\rangle_{\rm en}$ than through $|\Psi\rangle_{\rm un}$ is given by

$$\frac{\Delta\tau}{\sqrt{\eta rM}}>\frac{\Delta\tau}{M\sqrt{r\,\eta^M}}\Rightarrow\ \eta>\left(\frac{1}{M}\right)^{1/(M-1)}. \tag{19}$$

This condition is shown in Fig. 1. It is evident that relatively low values of quantum efficiency $\eta$ are sufficient for obtaining the accuracy-increase feature also for high numbers of entangled photons.

The intuitive reasoning that yields the condition (19) must be taken only as a qualitative demonstration, since Eq. (18) is valid only for $rM\gg 1$. Now the rigorous condition is derived. It turns out to be even more favorable to the entangled case, even though only a small correction to the condition (19) is required. Equation (9) shows that, in the case of no

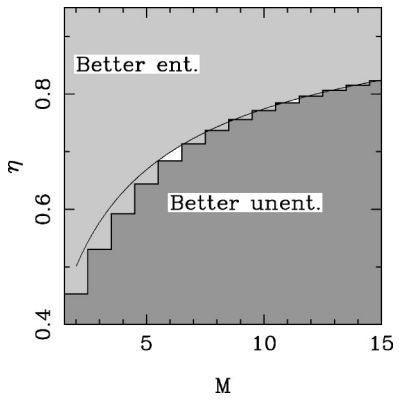


FIG. 1. Graph showing which values of quantum efficiency $\eta$ are needed to achieve an accuracy increase with the entangled state $|\Psi\rangle_{\rm en}$ of $M$ photons over the unentangled state $|\Psi\rangle_{\rm un}$ of $M$ photons. The higher region is where a better accuracy may be obtained using $|\Psi\rangle_{\rm en}$ and the lower region is where a better accuracy is obtained through $|\Psi\rangle_{\rm un}$. The continuous line graphs the condition (19). The histogram is obtained by the more rigorous analysis of Eq. (23). The two conditions coincide for $M \gg 1$.

loss, using an unentangled state $|\Psi\rangle_{\rm un}$, the probability distribution $P_M(t_1,\ldots,t_M)$ of the time of arrival of the $M$ photons is just the product of the probability distributions of the times of arrival of the single photons $|g(t)|^2$. Thus, if each photon has a probability $\eta$ of arriving and a probability $1-\eta$ of being lost, then the probability of retaining $m$ of the initial $M$ photons is given by the binomial distribution

$$P_m(t_1,\ldots,t_m)=\binom{M}{m}\frac{\eta^m(1-\eta)^{M-m}}{1-(1-\eta)^M}\prod_{i=1}^{M}|g(t_i)|^2. \quad (20)$$

In this case, the integral of $P_m$ over all the times of arrival $t_1,\ldots,t_m$ is the probability of retaining $m$ of the $M$ photons, discarding the case in which all the photons are lost—an event that happens with probability $(1-\eta)^M$. In fact, in the latter case no information on time of arrival is acquired and this is the source of the renormalization factor $1/[1-(1-\eta)^M]$ in Eq. (20). In particular, for $\eta=1$ Eq. (20) coincides with Eq. (9), namely, $P_m(t_1,\ldots,t_m)=0$ for $m\neq M$. The accuracy that may be obtained from $|\Psi\rangle_{\rm un}$ is given by the the variance of the distribution given in Eq. (20), i.e.,

$$\Delta t=\left[\sum_{m=1}^{M}\binom{M}{m}\frac{\eta^m(1-\eta)^{M-m}}{m[1-(1-\eta)^M]}\right]^{1/2}\Delta\tau. \quad (21)$$

If the experiment is repeated $r\gg 1$ times, in a fraction $1-(1-\eta)^M$ of the photons at least one photon is received and the accuracy that can be reached in each of these cases is given by Eq. (21). Thus the overall accuracy for the $r$ experiments is

$$\Delta t(r)=\left[\sum_{m=1}^{M}\binom{M}{m}\frac{\eta^m(1-\eta)^{M-m}}{m[1-(1-\eta)^M]^2}\right]^{1/2}\frac{\Delta\tau}{\sqrt{r}}. \quad (22)$$

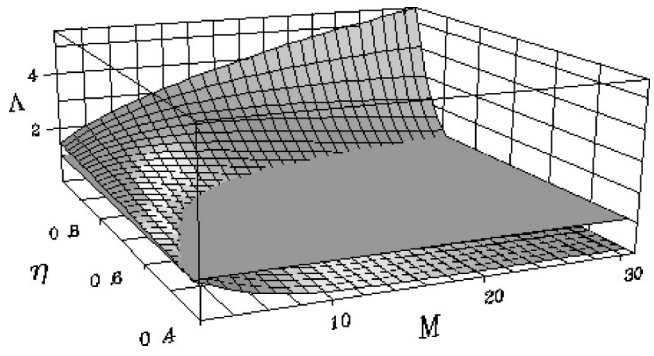


FIG. 2. Three-dimensional graph depicting the gain in accuracy $\Lambda(M,\eta)$ vs the number of photons $M$ and the quantum efficiency $\eta$. The horizontal plane in the figure for $\Lambda=1$ separates the regions where it is better to employ $|\Psi\rangle_{\rm en}$ (over) and $|\Psi\rangle_{\rm un}$ (under). Notice the $\sqrt{M}$ dependence for $\eta=1$, which corresponds to the enhancement discussed in Sec. I A.

Again, by comparing this variance with the one obtained from the entangled case (17), one finds the condition under which it is better to use entangled states with respect to unentangled ones, i.e.,

$$\Lambda\equiv M\left[\sum_{m=1}^{M}\binom{M}{m}\frac{\eta^{M+m}(1-\eta)^{M-m}}{m[1-(1-\eta)^M]^2}\right]^{1/2}>1, \quad (23)$$

which for $M\gg 1$ coincides with condition (19). The condition (23) is plotted in Fig. 2.

### B. Loss dynamical evolution

In this section the evolution of the states introduced previously is analyzed in the presence of loss. Also here, for simplicity, we analyze the case $N=1$ of one photon per channel.

It can be shown [14] that a lossy channel of quantum efficiency $\eta$ (which also takes into account the detection efficiency) can be described by considering a perfect channel and inserting a beam splitter of transmissivity $\eta$. The second input port $b$ of the beam splitter is in the vacuum state $|0\rangle$ and one output port is traced out (refer to Fig. 3).

This allows us to obtain the nonunitary evolution of a lossy channel. It can be shown that starting from the unitary evolution of the beam splitter

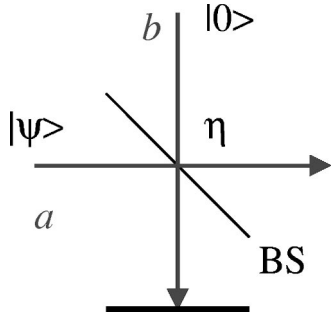


FIG. 3. Description of a lossy channel mode through a beam splitter of transmissivity $\eta$ equal to the channel quantum efficiency.

$$U=\exp[-\arctan(\sqrt{\{1-\eta\}/\eta})(ab^\dagger-a^\dagger b)] \qquad (24)$$

(where the mode definition for $a$ and $b$ is given in Fig. 3), one obtains the following completely positive map for the density-matrix evolution in the presence of loss:

$$\varrho\rightarrow\varrho'=\mathrm{Tr}_b[U\varrho\otimes|0\rangle_b\langle 0|U^\dagger]=\sum_{n=0}^{\infty}V_n\varrho V_n^\dagger, \qquad (25)$$

with

$$V_n=\left(\frac{1-\eta}{\eta}\right)^{n/2}\frac{a^n}{\sqrt{n!}}\eta^{a^\dagger a/2}. \qquad (26)$$

The case of frequency-independent loss is considered. The evolution (25) must be calculated for each mode of the continuum of modes of the entangled and unentangled states given, respectively, by $|\Psi\rangle_{\mathrm{en}}$ defined in Eq. (15) and $|\Psi\rangle_{\mathrm{un}}$ defined in Eq. (16). In the case of the density operator $\varrho_{\mathrm{en}}=|\Psi\rangle_{\mathrm{en}}\langle\Psi|$ corresponding to the state $|\Psi\rangle_{\mathrm{en}}$, it is possible to show

$$\varrho'_{\mathrm{en}}=\eta^M\varrho_{\mathrm{en}}+\sum_{m=0}^{M-1}\eta^m(1-\eta)^{M-m}\int d\omega|\phi(\omega)|^2 \times[|\omega\rangle\langle\omega|\otimes|0\rangle\langle 0|\otimes\cdots+|0\rangle\langle 0|\otimes\cdots], \qquad (27)$$

where $|0\rangle\langle 0|$ is the vacuum state and the term in square brackets is the sum of all the $\binom{M}{m}$ possible combinations of $m$ times the state $|\omega\rangle\langle\omega|$ and $M-m$ times the vacuum $|0\rangle\langle 0|$. The interpretation of Eq. (27) is that none of the photons is lost and the state is unaffected with a probability $\eta^M$, and $m$ photons are lost and the state is left in a mixture of $|\omega\rangle$ and $|0\rangle$ with probability $\binom{M}{m}\eta^m(1-\eta)^{M-m}$. Since the second term of the state (27) contains only density matrices diagonal in the $|\omega\rangle$ representation, it does not contain any information on the time-of-arrival measurement. In fact, the probability $P_M$ defined in Eq. (4) gives a ''constant'' probability if applied to the state $|\omega\rangle\langle\omega|$. Thus post-selection measurements are needed in this case: if Alice is expecting the state $|\Psi\rangle_{\mathrm{en}}$, she must throw away all the data coming from events in which she recorded less than $M$ photons. These events are useless. As shown before, the fragility to loss is only apparent, since the accuracy gain over the unentangled case is high enough so that it is possible to find a wide experimental region in which the accuracy enhancement is preserved.

On the other hand, the evolution of the unentangled state $|\Psi\rangle_{\mathrm{un}}$ defined in Eq. (16), $\varrho_{\mathrm{un}}=|\Psi\rangle_{\mathrm{un}}\langle\Psi|$, is given by

$$\varrho'_{\mathrm{un}}=\sum_{m=0}^{M}\eta^m(1-\eta)^{M-m} \times[\varrho_1\otimes\varrho_2\otimes\cdots+|0\rangle\langle 0|\otimes\varrho_2\otimes\cdots], \qquad (28)$$

where the term in square brackets contains the sum of all possible combinations of $m$ times the states $\varrho_i$ and $M-m$ times the vacuum $|0\rangle\langle 0|$, and where

$$\varrho_i=\int d\omega\, d\omega'\,\phi(\omega)\phi^*(\omega')|\omega\rangle_i\langle\omega'|, \qquad (29)$$

which is a single-photon wave packet with spectral function $\phi(\omega)$ in the $i$th channel, i.e., the state (16) for $M=1$. Starting from the state in Eq. (28) no post selection is necessary (except the obvious case in which Alice does not receive any photon), since all the terms are composed of the states of the form (29), which do retain time-of-arrival information.

The same analysis can be extended to the general case of the state $|\Psi\rangle_{NM}$, showing that the loss of a single photon destroys all the timing information.

## III. TRADE-OFF ENTANGLEMENT vs LOSS RESISTANCE

In this section some strategies for battling the effects of the loss are presented. Instead of using the maximally entangled states employed so far, one may devise strategies for using partially entangled states that turn out to be more robust to the loss. The use of partially entangled states to protect entangled atomic clocks from the effects of decoherence was noted in Ref. [4]. Here we show that partial entanglement can protect against loss while still retaining some of the quantum enhancement. A simple example to illustrate this is first presented and a more sophisticated case is then analyzed in detail.

It is well known (see, for example, [15]) that when more than two systems are entangled, a variety of different effects can occur. Hence, in order to address the relation occurring between the degree of entanglement of a state and its loss resistance, it is useful to start from a simple example. Consider the case of one photon per channel ($N=1$) where the first $Q$ of the $M$ channels are maximally entangled as the ones in the state $|\Psi\rangle_{\mathrm{en}}$ of Eq. (15) and the other $M-Q$ channels are unentangled as in $|\Psi\rangle_{\mathrm{un}}$ of Eq. (16). The parameter $Q$ characterizes the degree of entanglement of this state: bigger values of $Q$ correspond to higher entanglement. Consider first the case of unit quantum efficiency. It is easy to show through Eq. (4) that the accuracy in the determination of $\langle t\rangle$ follows as

$$\Delta t=\frac{\Delta\tau}{\sqrt{M}}\sqrt{\frac{M-Q+1}{M}}. \qquad (30)$$

For $Q>1$ (i.e., at least two of the $M$ channels are entangled), the accuracy achievable is greater than the completely unentangled case, but not as high as the completely entangled case. The loss of performance of this state is balanced by a greater resistance to the effects of photon losses than the maximally entangled state $|\Psi\rangle_{\mathrm{en}}$, for which the loss of a single photon proves fatal. On the contrary, the loss of photons from the partially entangled state still allows us to recover information if a suitable post selection is employed. Namely, one must discard all the times of arrival of the entangled photons if one or more of them is lost, but all the times of arrival of the unentangled photons that do arrive can be safely retained.

This simple example shows how one can increase the resistance to loss by reducing the entanglement, however, at

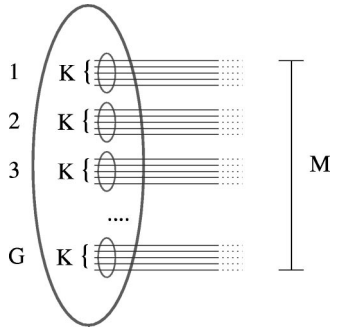


FIG. 4. Quantum fault tolerance applied to the quantum positioning protocol. Each of the $G$ groups of photons (which are frequency entangled) is composed of $K$ frequency maximally entangled photons.

the cost of achieving less accuracy enhancement. Of course much more sophisticated configurations can be introduced for entangling multiple systems [15], in which the different systems share a different degree of entanglement with all the other systems. It is expected that also in the general case, a similar trade-off between the degree of entanglement and resilience to loss holds. Depending on the quantum efficiency of the channel and on the degree of entanglement one is able to produce, different strategies, involving different data processing or post selections, are possible. A better insight on this may be gained by analyzing the following example, where a multistructured entanglement is employed.

A procedure analogous to fault-tolerant quantum computation may be introduced in our scheme. Consider again the simple case of one photon in each of the $M$ channels ($N=1$). Instead of sending the maximally entangled state $|\Psi\rangle_{\rm en}$ of Eq. (15), Alice sends Bob a state in which groups of $K$ photons are maximally entangled and $G=M/K$ groups are entangled together, as depicted in Fig. 4. If no photon is lost, then one will not only be able to use the correlations within all the groups, but also the correlation *between* the groups. In the event of a photon loss, thanks to the structure of the entanglement employed, not all the information will be lost as would happen when using the state $|\Psi\rangle_{\rm en}$. In fact, suppose that the lost photon comes from the $j$th group of photons: as will be shown, the only data that must be discarded is the data relative to the $j$th group photon times of arrival. All the other times of arrival may be retained and employed. The procedure can also be nested, namely, each of the $G$ groups of $K$ photons may be partitioned in maximally entangled subgroups and so on.

The state represented in Fig. 4 is given by

$$|\Psi\rangle_G \equiv \int d\Omega\, \Phi(\Omega)|\Omega\rangle_1|\Omega\rangle_2\cdots|\Omega\rangle_G, \tag{31}$$

where

$$|\Omega\rangle_j \equiv \int d\omega\, \phi(\omega,\Omega)|\omega\rangle_{j1}|\omega\rangle_{j2}\cdots|\omega\rangle_{jK} \tag{32}$$

is the state of the $j$th group of $K$ photons described by the one-photon frequency state $|\omega\rangle_{jl}$ for $j=1,\ldots,G$ and $l=1,\ldots,K$. Consider for simplicity the case of Gaussian spectrum, namely, $|\Phi(\Omega)|^2$ is a Gaussian with variance $\Delta\Omega^2$ and $|\phi(\omega,\Omega)|^2$ is a Gaussian centered around $\Omega$ with variance $\Delta\omega^2$. The state $|\Psi\rangle_{\rm en}$ can be obtained from $|\Psi\rangle_G$ in the limit $\Delta\omega\to 0$. Since $|\Omega\rangle_j$ has the same structure of $|\Psi\rangle_{\rm en}$, if one photon is lost in the $j$th group all the time-of-arrival information of such state must be discarded. Namely, only the $g$ groups in which no photons have been lost can be still employed for the positioning. In this case, using the state $|\Psi\rangle_G$ in the ensemble average of Eq. (4), the probability density of detecting all the $gK$ photons of the $g$ groups at times $t_{j,l}$ is given by

$$P_{gK}(t_{j,l}) \propto \exp\left[ -\left( \sum_{j=1}^{g}\sum_{l=1}^{K} t_{j,l} \right)^2 \Big/ (2\Delta\tau_g^2) \right], \tag{33}$$

where $t_{j,l}$ is the time of arrival of the $l$th photon in the $j$th group and

$$\Delta\tau_g = \frac{\sqrt{g}}{2\Delta\omega}\sqrt{\frac{(G-g)\Delta\Omega^2+\Delta\omega^2}{G\Delta\Omega^2+\Delta\omega^2}}. \tag{34}$$

Notice that Eqs. (33) and (34) for $\Delta\omega\to 0$ and $G=g$ reproduce the result derived previously in Eq. (9) for a Gaussian spectrum with $N=1$. Equation (33) shows that even if $G-g$ groups are discarded because they lost some photons, the remaining $g$ groups still retain some entanglement. In fact, since the $|\Omega\rangle_j$ are not orthogonal for $\Delta\omega>0$, the probability $P_{gK}(t_{j,l})$ does not factorize in parts depending on the single groups. The proportionality constant in Eq. (33) must be chosen so that the integral of $P_{gK}(t_{j,l})$ over all the times gives the probability that only $gK$ photons are detected, namely,

$$\mathcal{P}_g \equiv \binom{G}{g} \frac{(\eta^K)^g(1-\eta^K)^{G-g}}{1-(1-\eta^K)^G}, \tag{35}$$

where $\eta^K$ is the probability that all the photons of a group reach the detectors, and where, analogously as in Sec. II A, the term $1/[1-(1-\eta^K)^G]$ is introduced to take into account the case (to be discarded) in which all the $G$ groups have lost at least one photon.

If $g$ of the $G$ groups do not lose any photon, one may estimate the mean time of arrival by calculating the mean value of $\Sigma_{jl}t_{j,l}/(gK)$. The accuracy may be estimated by using the probability (33) obtaining

$$\Delta t = \frac{1}{2K\Delta\omega}\left[ \sum_{g=1}^{G} \frac{(G-g)\Delta\Omega^2+\Delta\omega^2}{g(G\Delta\Omega^2+\Delta\omega^2)}\mathcal{P}_g \right]^{1/2}. \tag{36}$$

As before—see Eq. (22)—when $r\gg 1$ experimental runs are performed, the accuracy $\Delta t(r)$ that can be achieved is obtained from Eq. (36) by dividing $\Delta t$ by the square root of the number of usable runs, namely, $r[1-(1-\eta^K)^G]$.

In order to compare this result to what one would obtain in the unentangled case or in the maximally entangled case, one must employ the states $|\Psi\rangle_{\rm en}$ and $|\Psi\rangle_{\rm un}$ with the same single-photon spectral characteristics of the photons of

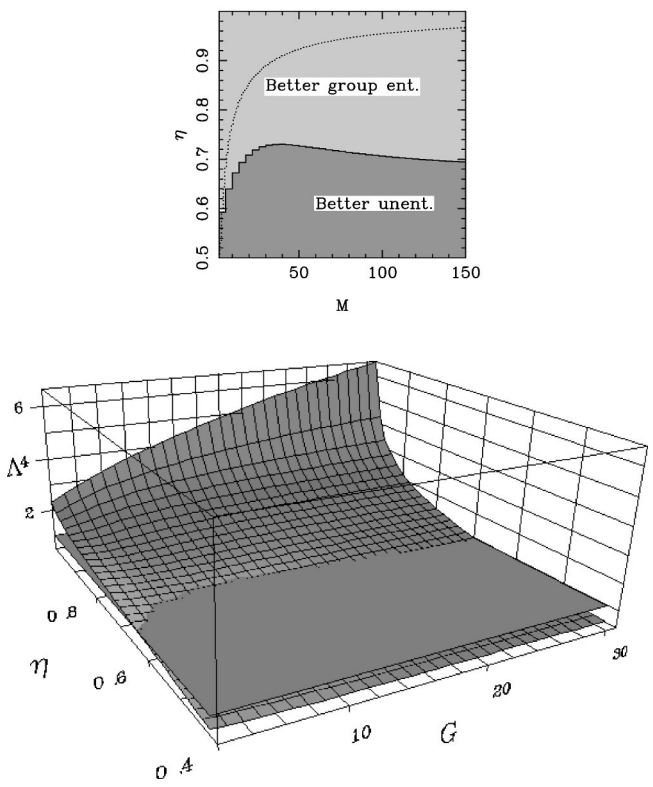


FIG. 5. Robustness to loss of the state (31). Upper graph: The upper part of the graph shows for which values of the quantum efficiency $\eta$ and of the total number of photons $M$ one does better by using the state $|\Psi\rangle_G$ (with $K=4$ and $\Delta\omega^2/\Delta\Omega^2=2$) as compared to the unentangled state $|\Psi\rangle_{\rm un}$. The dotted line is the same as in Fig. 1 and shows the region where it is better to use maximally entangled states $|\Psi\rangle_{\rm en}$ as compared to unentangled ones $|\Psi\rangle_{\rm un}$. Lower graph: The same information as the previous graph is given plotted vs the number of photon groups $G$, but showing also the accuracy gain over the unentangled case.

$|\Psi\rangle_G$. This can be achieved by using in $|\Psi\rangle_{\rm en}$ and $|\Psi\rangle_{\rm un}$ a Gaussian spectrum with variance $\Delta\omega^2+\Delta\Omega^2$: namely, $\Delta\tau=1/(2\sqrt{\Delta\omega^2+\Delta\Omega^2})$. An example of the comparison between the performance of $|\Psi\rangle_{\rm un}$ and $|\Psi\rangle_G$ when using such a coding scheme is given in Fig. 5, where the group-entangled state $|\Psi\rangle_G$ is shown to achieve a better accuracy than a nonentangled state $|\Psi\rangle_{\rm un}$. Notice that the accuracy enhancement feature can be retained also for low quantum efficiency even when a high number $M$ of particles is involved. A comparison between the accuracy enhancement obtainable with the states $|\Psi\rangle_{\rm en}$, $|\Psi\rangle_{\rm un}$, and $|\Psi\rangle_G$ is shown in Fig. 6.

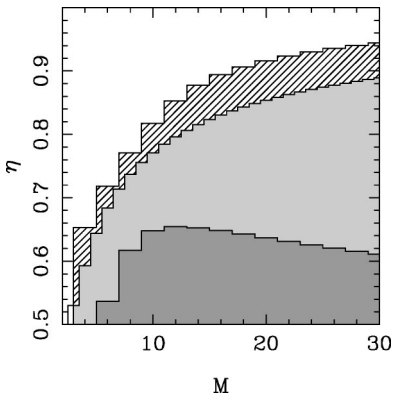


FIG. 6. The upper white region is where the maximally entangled state $|\Psi\rangle_{\rm en}$ achieves a better accuracy than the group-entangled state $|\Psi\rangle_G$ and than the unentangled state $|\Psi\rangle_{\rm un}$ (in brief, $en>G>un$). The striped region is where $G>en>un$, the light-gray region is where $G>un>en$, and the dark-gray region is where $un>G>en$. The parameters for this plot are $K=2$ and $\Delta\omega^2/\Delta\Omega^2=2$.

## CONCLUSION

In this paper, a scheme that employs entanglement and squeezing to achieve a higher accuracy and cryptographic capabilities in position measurement has been analyzed in detail. The positioning quantum-cryptographic protocol described allows only trusted parties (and no one else) to discover their relative positions. The sensitivity to the loss has been addressed by presenting a quantitative analysis of different strategies to contrast it. One finds that, even though the system is, in principle, very sensitive to the loss of a single photon, there are many situations where it may still be employed with an accuracy enhancement over the analogous classical schemes. It has been shown that relaxing the requirements of having maximally entangled states in frequency, one can achieve greater resistance to losses.

An interesting feature, which has been analyzed elsewhere [16], is also present in our proposal. Namely, it is possible to exploit the robustness of the frequency entanglement when the pulses travel through dispersive media [17]. This may be used to achieve positioning and clock synchronization of distant parties without being affected by the intermediate dispersion that would distort any timing signal the parties exchange.

## ACKNOWLEDGMENTS

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

[1] C. H. Bennett, G. Brassard, and N. D. Mermin, Phys. Rev. Lett. **68**, 557 (1992).

[2] C. M. Caves, Phys. Rev. D **23**, 1693 (1981); R. S. Bondurant and J. H. Shapiro, *ibid.* **30**, 2548 (1984); B. Yurke, Phys. Rev. Lett. **56**, 1515 (1986); B. Yurke, S. L. McCall, and J. R. Klauder, Phys. Rev. A **33**, 4033 (1986); M. J. Holland and K. Burnett, Phys. Rev. Lett. **71**, 1355 (1993); J. P. Dowling, Phys. Rev. A **57**, 4736 (1998).

[3] J. J. Bollinger, W. M. Itano, D. J. Wineland, and D. J. Heinzen, Phys. Rev. A **54**, R4649 (1996).

[4] S. F. Huelga, C. Macchiavello, T. Pellizzari, A. K. Ekert, M. B. Plenio, and J. I. Cirac, Phys. Rev. Lett. **79**, 3865 (1997).

[5] A. N. Boto, P. Kok, D. S. Abrams, S. L. Braunstein, C. P. Williams, and J. P. Dowling, Phys. Rev. Lett. **85**, 2733 (2000).
[6] L. K. Grover, Phys. Rev. Lett. **79**, 325 (1997).
[7] V. Giovannetti, S. Lloyd, and L. Maccone, Nature (London) **412**, 417 (2001).
[8] U. M. Titulaer and R. J. Glauber, Phys. Rev. B **140**, B676 (1965); **145**, 1041 (1966).
[9] L. Mandel and E. Wolf, *Optical Coherence and Quantum Optics* (Cambridge University Press, Cambridge, 1995).
[10] A. Peres, *Quantum Theory: Concepts and Methods* (Kluwer, Dordrecht, 1993).
[11] S. S. Schweber, *An Introduction to Relativistic Quantum Field Theory* (Row, Peterson, Evanston, 1961).
[12] N. Margolus and L. B. Levitin, Physica D **120**, 188 (1998).
[13] V. Giovannetti, L. Maccone, J. H. Shapiro, and F. N. C. Wong, e-print quant-ph/0109135.
[14] H. Carmichael, *An Open System Approach to Quantum Optics* (Springer-Verlag, Heidelberg, 1993).
[15] W. Dür, e-print quant-ph/0006105.
[16] V. Giovannetti, S. Lloyd, L. Maccone, and F. N. C. Wong, Phys. Rev. Lett. **87**, 117902 (2001).
[17] A. M. Steinberg, P. G. Kwiat, and R. Y. Chiao, Phys. Rev. A **45**, 6659 (1992); A. M. Steinberg, P. G. Kwiat, and R. Y. Chiao, Phys. Rev. Lett. **68**, 2421 (1992).