Quantum cryptography with a predetermined key, using continuous-variable Einstein-Podolsky-Rosen correlations

M. D. Reid
Physics Department, University of Queensland, Brisbane, Queensland 4072, Australia
(Received 13 January 2000; published 10 November 2000)

Correlations of the type discussed by EPR in their original 1935 paradox for continuous variables exist for the quadrature phase amplitudes of two spatially separated fields. These correlations were first experimentally reported in 1992. We propose to use such EPR beams in quantum cryptography, to transmit with high efficiency messages in such a way that the receiver and sender may later determine whether eavesdropping has occurred. The merit of the new proposal is in the possibility of transmitting a reasonably secure yet predetermined key. This would allow relay of a cryptographic key over long distances in the presence of lossy channels.

PACS number(s): 03.67.Dd, 03.65.Bz

The possibility of using quantum mechanics to transmit signals in a way that any eavesdropping can be detected by the receiver and sender is intriguing. This new field of quantum cryptography [1,2] has attracted much attention.

In the pioneering proposal of Bennett and Brassard [1] the sender (Alice) transmits to the receiver (Bob) photon pulses in one of two orthogonal polarizations (labeled 0 and 1), where the orientation (basis) of polarization randomly shifts between $0°$ and $45°$. The 0,1 choice of polarization represents the bit value. Bob randomly selects a basis ($0°$ or $45°$) for a polarization measurement, and records the resulting bit value. Alice and Bob later compare notes, through a public channel, on the sequence of orientations ($0°$ or $45°$) chosen. The bit sequence where Bob selected the same orientation as Alice forms a key, to be used later to encrypt messages. While classically an eavesdropper could measure with perfect accuracy components of polarization along both directions, quantum mechanics forbids this by way of the uncertainty principle. As a consequence the eavesdropper cannot always regenerate the original state transmitted by Alice. The resulting discrepancy between the results recorded by Alice and Bob gives warning to the interference by the eavesdropper. No discrepancy implies a secure key.

Other proposals [2], such as that suggested by Ekert, propose to use a sequence of two spatially separated photons with correlated polarization, and whose joint polarization measurements are predicted by quantum mechanics to show a violation of a Bell inequality [3]. Such fields have no local hidden variable interpretation. Any measurement, and subsequent state regeneration to mask interference, by an eavesdropper along one of these two channels will alter the statistics so that a Bell inequality is always satisfied. Again a fundamental aspect of quantum mechanics is utilized to alert receiver and sender to eavesdropping.

The majority of proposals so far focus on the use of single photons to transmit information. A significant current limitation to the practicality of such schemes is the poor efficiency of photon counting detectors. This contributes to a significant loss factor which makes direct efficient communication of sequences predetermined by Alice difficult. Photon-based proposals rely in practice on deciphering a sequence (key) *a posteriori* from infrequent detected photons.

Recently Ralph [4] and Hillery [5] have suggested cryptographic schemes based on measurement of (continuous variable) field quadrature phase amplitudes. In their proposals Alice transmits a bit value by way of squeezed signals, which means that the fluctuation in one quadrature phase amplitude is reduced to a level below that corresponding to the standard quantum limit as determined by the uncertainty principle. Security is provided as a result of the uncertainty principle since an eavesdropper (Eve) cannot measure both noncommuting quadrature amplitudes arbitrary accuracy. As a result Bob's signal after Eve's interference will contain extra noise, detectable when Alice and Bob compare the bit values received by Bob with the bit values sent by Alice. In this way, following the example of Bennett and Brassard, a secure key can be established.

In this paper it is suggested to use continuous variable measurements in such a way so as to allow transmission of a predetermined sequence (or key) directly (*a priori*) from sender to receiver. Later, communication through a public channel can check whether eavesdropping has occurred. Security is provided not by comparison of Bob's received with Alice's sent bit values, but by establishing whether Einstein-Podolsky-Rosen correlations [6] between two beams, one retained by Alice and the other transmitted with signal to Bob, are maintained after transmission. In this last respect the proposal is not unlike the photon-based proposal of Ekert where security is based on the confirmation by Alice and Bob of a violation of a Bell inequality.

The scheme involves only quadrature phase amplitude measurements, which can be performed with high efficiency. The predetermined nature of the sequence takes most advantage of this high efficiency, since every bit value sent can contribute to the final message. This contrasts with previous schemes for which part of the sequence, randomly selected after transmission, is used only to establish security by way of the public channel.

The predetermined nature of the sequence could also aid incorporation of special repeaters, where the signal and correlated beams are regenerated to help compensate for transmission loss. This method could potentially secure a single key between a single sender-receiver pair a long distance apart.

Correlations of the type discussed by Einstein, Podolsky and Rosen (EPR) in their original 1935 paradox [6], for continuous variables, exist for the quadrature phase amplitudes of two spatially separated fields [7]. The technology of quadrature phase amplitude measurement is sufficiently advanced that in 1992 these correlations were detected, without detection efficiency problems, by Ou *et al.* [8]. More recently, continuous variable EPR-correlated beams have been generated by Zhang *et al.* [9] and Silberkorn *et al.* [10]. Such EPR correlated beams have recently been utilized to enable quantum state teleportation with continuous variables [11]. Further work [12] has shown that quadrature phase amplitude measurements on certain twin beams can predict violations of Bell inequalities.

Consider the nondegenerate parametric down conversion process, modeled by two field modes with boson operators $\hat{a}$ and $\hat{b}$, with the interaction Hamiltonian $H_I = i\hbar\kappa(\hat{a}^\dagger\hat{b}^\dagger - \hat{a}\hat{b})$. We define the quadrature phase amplitudes $\hat{X}_a = (\hat{a} + \hat{a}^\dagger)$, $\hat{P}_a = (\hat{a} - \hat{a}^\dagger)/i$, $\hat{X}_b = (\hat{b} + \hat{b}^\dagger)$, and $\hat{P}_b = (\hat{b} - \hat{b}^\dagger)/i$. The Heisenberg uncertainty relation for the orthogonal amplitudes of mode $\hat{a}$ is $\Delta^2 X_a \Delta^2 P_a \geqslant 1$. The output quadrature amplitudes are

$$\begin{aligned}
\hat{X}_a(t) &= \hat{X}_a(0)\cosh(\kappa t) + \hat{X}_b(0)\sinh(\kappa t), \\
\hat{X}_b(t) &= \hat{X}_b(0)\cosh(\kappa t) + \hat{X}_a(0)\sinh(\kappa t), \\
\hat{P}_a(t) &= \hat{P}_a(0)\cosh(\kappa t) - \hat{P}_b(0)\sinh(\kappa t), \\
\hat{P}_b(t) &= \hat{P}_b(0)\cosh(\kappa t) - \hat{P}_a(0)\sinh(\kappa t),
\end{aligned} \tag{1}$$

where κ is proportional to the strength of parametric interaction and the $t=0$ operators represent inputs. As κt increases, $\hat{X}_a(t)$ becomes increasingly correlated with $\hat{X}_b(t)$, and $\hat{P}_a(t)$ becomes increasingly correlated with $-\hat{P}_b(t)$, the correlation becoming perfect in the limit $\kappa T \rightarrow \infty$. With output fields $\hat{a}$ and $\hat{b}$ spatially separated, this is the situation [7] of the 1935 EPR correlations.

For imperfect correlation, the degree of correlation may still be sufficient to ensure EPR correlations [7]. The results for measurements $\hat{X}_a(t)$ and $\hat{X}_b(t)$ [or $\hat{P}_a(t)$ and $\hat{P}_b(t)$] can be compared, yielding an estimate of the error in inferring the result of measurement $\hat{X}_a(t)$ on mode $\hat{a}$, based on a measurement $\hat{X}_b(t)$ on mode $\hat{b}$. We calculate $\delta_x = \hat{X}_a(t) - \gamma\hat{X}_b(t)$ and $\delta_p = \hat{P}_a(t) + \gamma\hat{P}_b(t)$, where the factor γ may be modified to give the minimum error. One can calculate the variances associated with the inference of $\hat{X}_a$ from $\gamma\hat{X}_b$, and $\hat{P}_a$ from $\gamma\hat{P}_b$: $\Delta^2_{x,\mathrm{inf}} = \langle\delta_x^2\rangle - \langle\delta_x\rangle^2$ and $\Delta^2_{p,\mathrm{inf}} = \langle\delta_p^2\rangle - \langle\delta_p\rangle^2$. The minimum variance $\Delta^2_{x,\mathrm{inf,min}}$ (and $\Delta^2_{p,\mathrm{inf,min}}$) occurs for a particular value of γ. Finding the turning point with γ yields [with $\gamma = \langle\hat{X}_a(T),\hat{X}_b(T)\rangle/\Delta^2\hat{X}_b(T)$] $\Delta^2_{x,\mathrm{inf,min}} = \Delta\hat{X}_a^2(T)\Delta\hat{X}_b^2(T) - [\langle\hat{X}_a(T),\hat{X}_b(T)\rangle]^2/\Delta\hat{X}_b^2(T)$, where $\langle x,y\rangle = \langle xy\rangle - \langle x\rangle\langle y\rangle$ and one deduces a $\Delta^2_{p,\mathrm{inf,min}}$ in similar fashion.

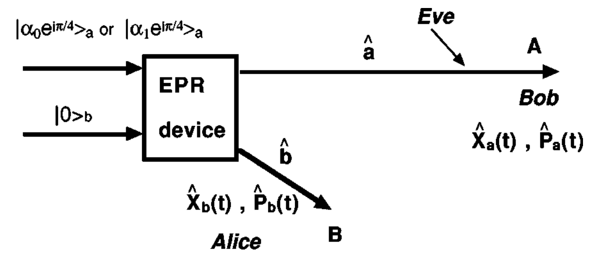

FIG. 1. Schematic representation of the EPR cryptographic scheme. The EPR device generates fields $\hat{a}$ and $\hat{b}$ which are EPR correlated. The bit value is given by Alice's choice of input to $\hat{a}$.

EPR correlations are obtained when the product $\Delta^2_{x,\mathrm{inf}}\Delta^2_{p,\mathrm{inf}}$ drops below the quantum limit given by $\Delta^2 X_a \Delta^2 P_a \geqslant 1$ [7]:

$$\Delta^2_{x,\mathrm{inf}}\Delta^2_{p,\mathrm{inf}} < 1. \tag{2}$$

For arbitrary coherent input states, we predict from Eq. (1) [7] ($\gamma = \tanh 2\kappa t$)

$$\Delta^2_{x,\mathrm{inf,min}} = \Delta^2_{p,\mathrm{inf,min}} = 1/\cosh 2\kappa t. \tag{3}$$

An identical argument and results hold if the measured operators are $X_a - \langle X_a\rangle$, $X_b - \langle X_b\rangle$, $P_a - \langle P_a\rangle$, and $P_b - \langle P_b\rangle$, the fluctuations about the mean, as opposed to X_a, X_b, P_a, and P_b.

With vacuum inputs to $\hat{a}$ and $\hat{b}$, Bob and Alice can secure a random key, using the potentially perfect correlation between quadrature amplitudes. We propose a different scheme, to allow for predetermined sequences, and imperfect correlation. For the purposes of cryptography (Fig. 1), Alice chooses as input to the nondegenerate parametric amplifier one of two possible states: the input for $\hat{a}$ is either a coherent state $|\alpha_0 \exp^{i\pi/4}\rangle_a$ (bit value 1) or a coherent state $|\alpha_1 \exp^{i\pi/4}\rangle_a$ (bit value 0), where α_0 and α_1 are real. The input for $\hat{b}$ is a vacuum state $|0\rangle_b$. The signal is transmitted by spatially separating the two output fields and propagating to Bob the output field of mode $\hat{a}$. Bob can read the message by measuring either $\hat{X}_a(t)$ or $\hat{P}_a(t)$. Suppose Bob chooses to measure $\hat{X}_a(t)$. The probability distribution for his obtaining a result x, given Alice's choice $|\alpha_0 \exp^{i\pi/4}\rangle$, is the Gaussian $\exp[-(x - \sqrt{2}\alpha_0\cosh\kappa t)^2/2\sigma^2]/\sigma\sqrt{2\pi}$ with mean $\sqrt{2}\alpha_0\cosh\kappa t$ and standard deviation $\sigma = \sqrt{\cosh 2\kappa t}$. If Alice chose $|\alpha_1 \exp^{i\pi/4}\rangle$ the probability for Bob's outcome is $\exp[-(x - \sqrt{2}\alpha_1\cosh\kappa t)^2/2\sigma^2]/\sigma\sqrt{2\pi}$, the Gaussian mean shifted by $\sqrt{2}(\alpha_0 - \alpha_1)\cosh\kappa t$. Provided $\sigma \leqslant \sqrt{2}(\alpha_0 - \alpha_1)\cosh\kappa t$, the bit value is clearly determined from Bob's result x (Fig. 2): x near $\sqrt{2}\alpha_0\cosh\kappa t$ implies 1; x near $\sqrt{2}\alpha_1\cosh\kappa t$ implies zero. The bit value can also be determined by a measurement of quadrature phase amplitude $\hat{P}_a(t)$, in this case the input $|\alpha_0 \exp^{i\pi/4}\rangle$ giving a Gaussian distribution about $\sqrt{2}\alpha_0\cosh\kappa t$ (bit value 1), while $|\alpha_1 \exp^{i\pi/4}\rangle$ gives a distribution centered about $\sqrt{2}\alpha_1\cosh\kappa t$ (bit value 0).

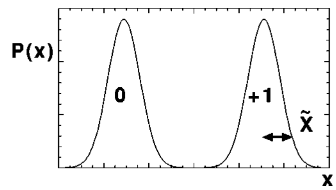

FIG. 2. Schematic plot of the probability distribution $P(x)$ for obtaining a result x upon measurement of the quadrature phase amplitude of a or b, where one Gaussian peak represents input $|\alpha_0 \exp^{i\pi/4}\rangle_a$ (bit value 1) and the other input $|\alpha_1 \exp^{i\pi/4}\rangle_a$ (bit value 0). Bob is able to infer the bit value from x and record, for later communication to Alice, the deviation $\tilde{X}$ of his result from the (known) mean of the distribution as indicated.

Bob records the results of his consecutive quadrature phase measurements, randomly selecting to measure either $\hat{X}_a(t)$ or $\hat{P}_a(t)$, and subtracting from his result either $\sqrt{2}\alpha_0 \cosh \kappa t$ or $\sqrt{2}\alpha_1 \cosh \kappa t$, so that only the fluctuation about the mean of the particular distribution is recorded (Fig. 2). Bob then communicates to Alice, through a public channel, the sequence of recorded fluctuations together with measurements $[\hat{X}_a(t)$ or $\hat{P}_a(t)]$ chosen (the bit value itself is not communicated). Alice also makes a sequence of consecutive measurements $\hat{X}_b(t)$ or $\hat{P}_b(t)$, (preferably) to coincide with Bob's measurement sequence, and records similarly only the fluctuation about the mean (in this case $\sqrt{2}\alpha_0 \sinh \kappa t$ or $\sqrt{2}\alpha_1 \sinh \kappa t$ for X_b, and $-\sqrt{2}\alpha_0 \sinh \kappa t$ or $-\sqrt{2}\alpha_1 \sinh \kappa t$ for P_b). Bob and Alice compare notes, through the public channel, to calculate a $\Delta^2_{x,\mathrm{inf}}\Delta^2_{p,\mathrm{inf}}$. The predicted minimum is, for optimized γ, given by Eq. (3).

Verification by Bob and Alice of the EPR correlations $\Delta^2_{x,\mathrm{inf}}\Delta^2_{p,\mathrm{inf}}<1$ gives an indication of interference by an eavesdropper (Eve). Let us consider various practical options by Eve. To determine the signal Eve's first obvious choice may be to capture the field $\hat{a}$ and measure either $\hat{X}_a$ or $\hat{P}_a$. If she is able to predetermine correctly for each bit value the choice ($\hat{X}_a$ or $\hat{P}_a$) to be made by Bob, Eve can make the same choice and conceal her eavesdropping. However, Bob's choice is delayed until after his detection of $\hat{a}$ forcing errors in Eve's selection. Quantum mechanics makes it impossible for Eve to measure both amplitudes ($\hat{X}_a$ and $\hat{P}_a$) to an uncertainty better than that given by the Heisenberg uncertainty relation. More importantly, Eve cannot regenerate and transmit to Bob a single mode state with both well defined $\hat{X}$ and $\hat{P}$, but is limited by $\Delta^2\hat{X}\Delta^2\hat{P}\geqslant 1$. For example Eve may select to measure $\hat{X}_a$ rather precisely so that the error in the measurement is of order $\Delta^2_m=1/r$, where $r>1$. Eve may then generate, to transmit to Bob, a ''squeezed'' state with this reduced fluctuation in X, so that the new operator describing the quadrature measurement now made by Bob is $\hat{X}^{\mathrm{new}}_a=x_a+\delta\hat{X}_a$ where x_a is the result of Eve's measurement and $\Delta^2\delta\hat{X}_a=1/r$. Quantum mechanics compels an enhanced fluctuation in $\hat{P}$, so that the operator describing the quadrature measurement $\hat{P}_a$ made by Bob on this retransmitted state is $\hat{P}^{\mathrm{new}}_a=p_a+\delta\hat{P}_a$ where at best $\Delta^2\delta\hat{P}=r$ for a minimum uncertainty squeezed state. The variances $\Delta^2_{x,\mathrm{inf,min}}$ and $\Delta^2_{p,\mathrm{inf,min}}$ testing for supposed EPR correlations are now $\Delta^2_{x^{\mathrm{new}},\mathrm{inf,min}}=\Delta^2_{x,\mathrm{inf,min}}+\Delta^2\delta\hat{X}_a$ and $\Delta^2_{p^{\mathrm{new}},\mathrm{inf,min}}=\Delta^2_{p,\mathrm{inf,min}}+\Delta^2\delta\hat{P}$, where here we have $\Delta^2_{x,\mathrm{inf,min}}=\Delta^2_{p,\mathrm{inf,min}}=1/\cosh \kappa t$. This gives $\Delta^2_{x,\mathrm{inf,min}}\Delta^2_{p,\mathrm{inf,min}}\geqslant 1$, and EPR correlations are lost, making a sensitive test for interference on $\hat{a}$. We note that it is possible for Eve to gain access to bit values, but whether this has occurred is later checked by communication between sender and receiver.

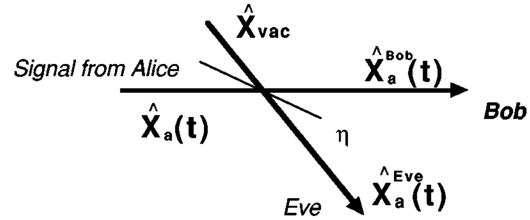

FIG. 3. Schematic representation of Eve's attempt to make measurement of $X_a(t)$ using a partial beam splitter.

To improve her chances, as discussed by Ralph [4], Eve may alternatively opt to make a partial interference of beam a by tapping off only part of the beam using a partially transmitting beam splitter, with a and a_{vac} as inputs, where a_{vac} is a vacuum input (Fig. 3). The outputs are: $\hat{a}_{\mathrm{Bob}}=\sqrt{\eta}\hat{a}+\sqrt{1-\eta}\hat{a}_{\mathrm{vac}}$, the field transmitted and detected by Bob; and $\hat{a}_{\mathrm{Eve}}=\sqrt{1-\eta}\hat{a}-\sqrt{\eta}\hat{a}_{\mathrm{vac}}$, the field detected by Eve to allow her measurement of X_a. Here η gives the fraction of photons transmitted, on to Bob, by the beamsplitter. We define the quadrature amplitudes $\hat{X}^{\mathrm{Bob}}_a=\hat{a}_{\mathrm{Bob}}+\hat{a}^\dagger_{\mathrm{Bob}}$, $\hat{P}^{\mathrm{Bob}}_a=(\hat{a}_{\mathrm{Bob}}-\hat{a}^\dagger_{\mathrm{Bob}})/i$, $\hat{X}^{\mathrm{Eve}}_a=\hat{a}_{\mathrm{Eve}}+\hat{a}^\dagger_{\mathrm{Eve}}$ and $\hat{P}^{\mathrm{Eve}}_a=(\hat{a}_{\mathrm{Eve}}-\hat{a}^\dagger_{\mathrm{Eve}})/i$. For a vacuum input we have $\Delta^2\hat{X}_{\mathrm{vac}}=\Delta^2\hat{P}_{\mathrm{vac}}=1$:

$$\begin{aligned}
\hat{X}^{\mathrm{Bob}}_a(t)&=\sqrt{\eta}X_a(t)+\sqrt{1-\eta}X_{\mathrm{vac}},\\
\hat{X}^{\mathrm{Eve}}_a(t)&=\sqrt{\eta}X_{\mathrm{vac}}-\sqrt{1-\eta}X_a(t),\\
\hat{P}^{\mathrm{Bob}}_a(t)&=\sqrt{\eta}P_a(t)+\sqrt{1-\eta}P_{\mathrm{vac}},\\
\hat{P}^{\mathrm{Eve}}_a(t)&=\sqrt{\eta}P_{\mathrm{vac}}-\sqrt{1-\eta}P_a(t).
\end{aligned} \tag{4}$$

The variances $\Delta^2_{x,\mathrm{inf,min}}$ and $\Delta^2_{p,\mathrm{inf,min}}$ later measured by Alice and Bob, testing for EPR correlations, are now

$$\begin{aligned}
\Delta^2_{x^{\mathrm{new}},\mathrm{inf,min}}&=\eta\Delta^2_{x,\mathrm{inf,min}}+(1-\eta)\Delta^2\hat{X}_{\mathrm{vac}},\\
\Delta^2_{p^{\mathrm{new}},\mathrm{inf,min}}&=\eta\Delta^2_{p,\mathrm{inf,min}}+(1-\eta)\Delta^2\hat{P}_{\mathrm{vac}}.
\end{aligned} \tag{5}$$

With $\eta\rightarrow 1$ the back-action noise ($\sqrt{1-\eta}X_{\mathrm{vac}}$ for measurement X) feeding into Bob's signal as a result of Eve's tapping is decreased. In this limit, the change $(1-\eta)\Delta^2\hat{X}_{\mathrm{vac}}$ and $(1-\eta)\Delta^2\hat{P}_{\mathrm{vac}}$ to the variances $\Delta^2_{x,\mathrm{inf}}$ and $\Delta^2_{p,\mathrm{inf}}$ respectively, as a result of Eve's eavesdropping becomes increasingly undetectable. Eve however pays the price, since she observes a reduced signal $[-\sqrt{1-\eta}X_a(t)$ for the measurement X] with increased noise (due to $\sqrt{\eta}X_{\rm vac}$), limiting her ability to obtain information from the channel. With noise $\sqrt{\eta}X_{\rm vac}$ from the vacuum input increasing as $\eta\rightarrow 1$, a point is reached where she can no longer resolve the two peaks, separated by $\sqrt{2}\sqrt{1-\eta}\cosh \kappa t(\alpha_0-\alpha_1)$, giving the bit value.

In an effort to reduce the feedback noise $(1-\eta)\Delta^2\hat{X}_{\rm vac}$ in Bob's signal, and to allow better resolution of the bit value for larger η, Eve may choose to perform a quantum nondemolition measurement of quadrature amplitude $\hat{X}_a$ (Fig. 3). Such measurements allow accurate determination of $\hat{X}_a$ (to $\Delta^2\hat{X}\leqslant 1$) and have been achieved experimentally [13]. The quantum nondemolition measurement may be performed using the beam splitter as above (Fig. 3) but where $a_{\rm vac}$ is a squeezed vacuum input so that $\Delta^2\hat{X}_{\rm vac}<1$ (suppose $\Delta\hat{X}_{\rm vac}=1/r$). Increased squeezing of the fluctuation in $X_{\rm vac}$ $(\Delta^2\hat{X}_{\rm vac}\rightarrow 0)$ implies that $X_a^{\rm Bob}(t)=\sqrt{\eta}X_a(t)$ and $X_a^{\rm Eve}=-\sqrt{1-\eta}X_a(t)$ and perfect inference of $X_a(t)$ is obtainable by Eve, without any feedback vacuum noise in the value $X_{\rm Bob}(t)$ later measured by Bob. However large fluctuations in $P_{\rm vac}$ (we must have $\Delta\hat{P}_{\rm vac}=r$ to satisfy the uncertainty principle for the squeezed vacuum input state) necessarily create a large noise in $P_a^{\rm Bob}$:

$$P_a^{\rm Bob}(t)=\sqrt{\eta}P_a(t)+\sqrt{1-\eta}P_{\rm vac}. \tag{6}$$

This excess noise, detectable when Bob selects to measure P rather than X, causes an increase in $\Delta^2_{p^{\rm new},{\rm inf,min}}=\eta\Delta^2_{p,{\rm inf,min}}+(1-\eta)\Delta^2\hat{P}_{\rm vac}$, alerting Bob to Eve's interference.

The presence of loss due to transmission will also reduce the EPR correlation. Loss (and detection inefficiencies) may be modeled by a beam splitter which mixes our signal mode $\hat{a}$ with a vacuum field $\hat{a}_{\rm vac}$ to give a new output at Bob's detector: $\hat{a}^{\rm new}=\sqrt{\eta}\hat{a}+\sqrt{1-\eta}\hat{a}_{\rm vac}$. Here η is the overall efficiency factor ($\eta\rightarrow 1$ for no loss). The new noise levels measured by Bob are

$$\begin{aligned}\Delta^2_{x^{\rm new},{\rm inf,min}}&=\eta^2\Delta^2_{x,{\rm inf,min}}+(1-\eta^2),\\ \Delta^2_{p^{\rm new},{\rm inf,min}}&=\eta^2\Delta^2_{p,{\rm inf,min}}+(1-\eta^2).\end{aligned} \tag{7}$$

With $\eta>0$, a partial loss, EPR correlations are still maintained, though decreased. For complete loss we obtain $\Delta^2_{x^{\rm new},{\rm inf,min}}=\Delta^2_{p^{\rm new},{\rm inf,min}}=1$.

In practice, the degree of EPR correlation for a given transmission line and distance would be accurately established. This degree of correlation is independent of Alice's bit value. Any increase of our EPR noise indicator above this previously evaluated level alerts Bob to the additional loss caused by a partial tapping of the channel by Eve.

Security is also provided by comparing individual results of measurements made by Alice and Bob. For a given transmission line and loss along this line, and for a given bit value (based on the choice α) the mean and shape (the shape is predicted to be independent of the bit value) of the measured distribution can also be accurately recorded. A specified result for the measurement (or fluctuation about the mean) X_b made by Alice will imply a conditional probability distribution for the measurement (or fluctuation about mean) X_a made by Bob. In the absence of loss the variance of this conditional distribution is $\Delta^2_{x,{\rm inf,min}}$. Loss increases the variance by the amount given above in Eq. (7). Significant deviation of a result for Bob from this distribution is indication of Eve's presence. Importantly loss acts to increase noise levels in X and P equally. Marked increase, for some of the bit values sent, in the deviation of Bob's measurement from Alice's predicted result for Bob would alert Alice and Bob to the possibility of Eve having performed a quantum nondemolition measurement as discussed above.

Eve's best chance then may be to perform measurement with a partial beam splitter with standard vacuum input, in the hope that the extra noise put back into Bob's channel will not be noticeable over loss. To safeguard against this Alice and Bob must evaluate by measurements the minimum extra noise, or additional loss, for which they would conclude the existence of a potential eavesdropper. With this value of η Eve could have performed a measurement (4) and would be compelled to infer a bit value based on extra noise levels as indicated by Eq. (4). Bob and Alice must select the difference between inputs α_0 and α_1 so that Eve is unable to

Schemes using Bell inequalities [2] can also be proposed in principle for quadrature phase detection, since the failure of local realism has recently [12] been predicted possible for such measurements, for certain types of quantum states. One such state is the pair-coherent state [12]

$$|\Psi\rangle=N\int_0^{2\pi}|r_0e^{i\varsigma}\rangle_a|r_0e^{-i\varsigma}\rangle_b d\varsigma. \tag{8}$$

Here N is a normalization coefficient, we choose $r_0=1.1$ and $|\alpha\rangle_q$ $(q=a,b)$ is a coherent state for the mode $\hat{q}$. Also we might consider the two-mode ''Schrodinger cat'' state undergoing interaction for a time t with a parametric amplifier [10]

$$|\Psi\rangle=N\hat{U}(|\alpha_0\rangle_a|\beta_0\rangle_b+|-\alpha_0\rangle_a|-\beta_0\rangle_b), \tag{9}$$

where $U=\exp[-i\hat{H}_It/\hbar]$, and we choose $\alpha_0=\beta_0=0.9$ and $\kappa t=0.6$ Our protocol is not a direct parallel of Ekert's for spin-1/2 particles, because for states (8) and (9) there is not a perfect correlation between quadrature amplitude measurements on $\hat{a},\hat{b}$.

After generation of the state (8) [or Eq. (9)], the two fields $\hat{a}$ and $\hat{b}$ are spatially separated. Alice may then choose to phase shift the field $\hat{a}$ by 180° or not, this choice of relative phase between $\hat{a}$ and $\hat{b}$ being her signal. The field $\hat{a}$ is then propagated to Bob at a distant location A. The signal is transmitted from Alice to Bob in the form of blocks, consisting of many (N say where N is large) identical states with the same value of phase shift. Bob measures at a location A a quadrature phase amplitude $\hat{X}^A_\theta=\hat{X}_a\cos\theta+\hat{P}_a\sin\theta$ for each state comprising a certain block, where θ randomly varies between $\theta=0,\pi/2,3\pi/2$, for state (8) [or between $\theta=0,0.42\pi,-0.28\pi,1.42\pi,0.72\pi$ for state (9)]. Alice also makes a series of measurements $\hat{X}^B_\phi=\hat{X}_b\cos\phi+\hat{P}_b\sin\phi$ at a location B, where ϕ randomly varies between $\phi=0,-\pi/4,-3\pi/4$, for state (8) [or between $\phi=0,-0.28\pi,0.42\pi$ for state (9)]. Alice then communicates to Bob through a public channel the results for her quadrature phase amplitude measurements.

Bob may build up, for each block, the probability distribution $P(q_a,q_b)$ for getting results q_a and q_b upon measurement of $\hat{X}_a$ at $\hat{a}$ and $\hat{X}_b$ at $\hat{b}$, respectively. This information is given by the $\theta=0$ and $\phi=0$ measurements. The shape of the distribution changes with the choice of phase shift, and gives the bit value. This information is not determinable from the measurements of amplitudes made on $\hat{b}$ alone, and hence cannot be determined by the information passed along the public channel.

To check whether eavesdropping has occurred, Bob tests for a Bell inequality. The result of the measurement is classified as $+1$ if the quadrature phase result x is greater than or equal to zero, and -1 otherwise. We define the probability distributions: $P_+^A(\theta)$ for obtaining $+1$ at $\hat{a}$ upon measurement of $\hat{X}_\theta^A$; $P_+^B(\phi)$ for obtaining $+1$ at $\hat{b}$ upon measurement of $\hat{X}_\phi^B$; and $P_{++}^{AB}(\theta,\phi)$ the joint probability of obtaining a $+1$ result at both $\hat{a}$ and $\hat{b}$. The existence of a local hidden variable theory implies the "strong" Bell-Clauser-Horne inequality [3]:

$$S=\frac{P_{++}^{AB}(\theta,\phi)-P_{++}^{AB}(\theta,\phi')+P_{++}^{AB}(\theta',\phi)+P_{++}^{AB}(\theta',\phi')}{P_+^A(\theta')+P_+^B(\phi)} \leqslant 1. \tag{10}$$

For state (8), a violation of this inequality occurs with $S\approx1.0157$, and with angles given by $\theta=0,\phi=-\pi/4,\theta'=\pi/2,\phi'=-3\pi/4$ [12]. For state (9), violation given by $S=1.008$ is obtained for angles $\theta=0.42\pi,\phi=-0.28\pi,\theta'=0.28\pi,\phi'=0.42\pi$ [12]. The above violations also hold for the states generated by phase shifting $\hat{a}$ by 180°, with the choice of angles for ϕ as before, but replacing θ with $\theta+\pi$ and θ' with $\theta'+\pi$.

Violation of the Bell inequality at the level predicted by quantum mechanics ensures that no interference by Eve has occurred along $\hat{a}$ (see Ekert [2]). Suppose Eve performs a measurement on the field $\hat{a}$, measuring $\hat{X}_{\theta_0}^A$ say to obtain a result x_{θ_0}. She then generates and transmits to Bob a state $|\Phi_{x_{\theta_0},\theta_0}\rangle$. The density operator for the new combined system is $\rho=\rho^B_{x_{\theta_0},\theta_0}\rho^A_{x_{\theta_0},\theta_0}$ where $\rho^B_{x_{\theta_0},\theta_0}=\langle x_{\theta_0}|\Psi\rangle\langle\Psi|x_{\theta_0}\rangle$ is the reduced density matrix for field $\hat{b}$ given the measurement by Eve, $|x_{\theta_0}\rangle$ is the eigenstate of $\hat{X}^A_{\theta_0}$, and $\rho^A_{x_{\theta_0},\theta_0}=|\Phi_{x_{\theta_0},\theta_0}\rangle\langle\Phi_{x_{\theta_0},\theta_0}|$. Bob tests for the Bell inequality using $P_{x,y}^{AB}(\theta,\phi)$, the joint probability for respective results x and y for measurements $\hat{X}_\theta^A$ and $\hat{X}_\phi^B$. With intervention,

$$P_{x,y}^{AB}(\theta,\phi)=\sum_{x_{\theta_0}}\sum_{\theta_0} P(x_{\theta_0},\theta_0)\langle y_\phi|\langle x_{\theta_0}|\Psi\rangle\langle\Psi|x_{\theta_0}\rangle|y_\phi\rangle \times\langle x_\theta|\Phi_{x_{\theta_0},\theta_0}\rangle\langle\Phi_{x_{\theta_0},\theta_0}|x_\theta\rangle, \tag{11}$$

where $P(x_{\theta_0},\theta_0)$ is the probability that Eve obtains a result x_{θ_0} for her measurement. We have the form $P_{x,y}^{AB}(\theta,\phi)=\int\rho(\lambda)\,p_x^A(\theta,\lambda)p_y^B(\phi,\lambda)\,d\lambda$ from which a Bell inequality follows, regardless of the state regenerated by Eve.

In terms of feasibility, the second scheme based on the Bell inequality is more likely to be limited by difficulty of state preparation and susceptibility to loss ($\eta=0.96$ destroys violations [12] and is greatly limited by its use of redundancy). The first scheme, not so limited, may offer advantages over schemes utilizing photon counting. The high detection efficiencies give a very much reduced overall loss factor, which may make it possible to transmit directly and efficiently a predetermined message, later checking providing a means to check security. The generation and detection of EPR correlations with $\Delta^2_{x,\mathrm{inf}}\Delta^2_{p,\mathrm{inf}}=0.7$ has been achieved [8]. The generation of squeezed (where $\Delta^2\hat{X}_\theta^A<1$ for some θ) optical and soliton pulses [10,14] opens up possibilities for transmission of EPR correlated fields. The robustness of squeezing to propagation loss has not been keenly explored, but similar distances should be achievable for EPR correlations. This loss represents the chief limitation to long distance transmission, since loss acts to degrade the EPR correlations which must be kept at $\Delta^2_{x,\mathrm{inf}}\Delta^2_{p,\mathrm{inf}}<1$. Repeated detection and regeneration of the signal with new EPR fields could help combat loss. Security then relies on a set of senders and receivers being able to communicate reliably at a later stage, after the detections.

In recent applications [11] EPR beams have been generated as the two outputs of a beam splitter with squeezed vacuum state inputs. It would be possible to use such EPR beams for our cryptography scheme where the squeezed vacuum is replaced by an amplitude squeezed state.

[1] C. H. Bennett and G. Brassard, in *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, Bangalore, India (IEEE, New York, 1984), p. 175; A. K. Ekert, J. G. Rarity, P. R. Tapster, and G. M. Palma, Phys. Rev. Lett. **69**, 1293 (1992); A. K. Ekert, B. Huttner, G. M. Palma, and A. Peres, Phys. Rev. A **50**, 1047 (1994); C. H. Bennett, F. Bessette, G. Brassard, L. Savail, and J. Smolin, J. Cryptology **5**, 3 (1992); A. Muller, J. Breguet, and N. Gisin, Europhys. Lett. **23**, 383 (1993); P. D. Townsend, Electron. Lett. **30**, 809 (1994); J. D. Franson and H. Ilves, Appl. Opt. **33**, 2949 (1994); W. T. Buttler, R. J. Hughes, and C. M. Simmons, Phys. Rev. Lett. **81**, 3283 (1998).

[2] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991); C. H. Bennett, G. Brassard, and N. D. Mermin, *ibid.* **68**, 557 (1992); S. M. Barnett and S. M. D. Phoenix, J. Mod. Opt. **40**, 1443 (1993).

[3] J. S. Bell, Physics (N.Y.) **1**, 195 (1965); J. F. Clauser and A. Shimony, Rep. Prog. Phys. **41**, 1881 (1978).

[4] T. C. Ralph, Phys. Rev. A **61**, 010303(R) (2000).

[5] M. Hillery, Phys. Rev. A **61**, 022309 (2000).

[6] A. Einstein, B. Podolsky, and N. Rosen, Phys. Rev. **47**, 777 (1935).

[7] M. D. Reid, Phys. Rev. A **40**, 913 (1989); M. D. Reid and P. D. Drummond, Phys. Rev. Lett. **60**, 2731 (1988).

[8] Z. Y. Ou, S. F. Pereira, H. J. Kimble, and K. C. Peng, Phys. Rev. Lett. **68**, 3663 (1992).

[9] Yun Zhang, Hai Wang, Xiaoying Li, Jietai Jing, Changde Xie, and Kunchi Peng, Phys. Rev. A **62**, 023813 (2000).

[10] Ch. Silberkorn, P. K. Lam, G. Wasik, N. Korolhova, and G. Leuchs (private communication).

[11] L. Vaidman, Phys. Rev. A **49**, 1473 (1994); S. Braunstein and H. J. Kimble, Phys. Rev. Lett. **80**, 869 (1998); A. Furasawa, J. Sorensen, S. Braunstein, C. Fuchs, H. Kimble, and E. Polzik, Science **282**, 706 (1998).

[12] A. Gilchrist, P. Deuar, and M. D. Reid, Phys. Rev. Lett. **80**, 3169 (1998); Phys. Rev. A **60**, 4259 (1999); B. Yurke, M. Hillery, and D. Stoler, *ibid.* **60**, 3444 (1999); W. J. Munro and G. J. Milburn, Phys. Rev. Lett. **81**, 4285 (1998); W. J. Munro, Phys. Rev. A **59**, 4197 (1999).

[13] M. D. Levenson, R. M. Shelby, M. D. Reid, and D. F. Walls, Phys. Rev. Lett. **57**, 2473 (1986); S. F. Pereira, Z. Y. Ou, and H. J. Kimble, *ibid.* **72**, 214 (1994).

[14] R. E. Slusher, P. Grangier, A. LaPorta, B. Yurke, and M. J. Potasek, Phys. Rev. Lett. **59**, 2566 (1987); M. Rosenbluh and R. M. Shelby, *ibid.* **66**, 153 (1991).