PHYSICAL REVIEW A, VOLUME 61, 010303(R)

Continuous variable quantum cryptography

T. C. Ralph*
Department of Physics, Faculty of Science, The Australian National University, ACT 0200 Australia
(Received 22 July 1999; published 8 December 1999)

We propose a quantum cryptographic scheme in which small phase and amplitude modulations of cw light beams carry the key information. The presence of Einstein-Podolsky-Rosen type correlations provides the quantum protection.

PACS number(s): 03.67.Dd, 42.50.Dv

Quantum cryptographic schemes use fundamental properties of quantum mechanics to ensure the protection of random number keys [1,2]. In particular, the act of measurement in quantum mechanics inevitably disturbs the system. Furthermore, for single quanta, such as a photon, simultaneous measurements of noncommuting variables are forbidden. By randomly encoding the information between noncommuting observables of a stream of single photons any eavesdropper (Eve) is forced to guess which observable to measure for each photon. On average, half the time Eve will guess wrong, revealing herself through the back action of the measurement to the sender (Alice) and receiver (Bob). There are some disadvantages in working with single photons, particularly in free space, where scattered light levels can be high. Also it is of fundamental interest to quantum information research to investigate links between discrete-variable, single-photon phenomena and continuous variable, multiphoton effects. This motivates a consideration of quantum cryptography using multiphoton light modes. In particular, we consider encoding key information as small signals carried on the amplitude and phase quadrature amplitudes of the beam. These are the analogues of position and momentum for a light mode and hence are continuous, conjugate variables. Although simultaneous measurements of these noncommuting observables can be made in various ways, for example, splitting the beam on a 50:50 beam splitter and then making homodyne measurements on each beam, the information that can be obtained is strictly limited by the generalized uncertainty principle for simultaneous measurements [3,4]. If an ideal measurement of one quadrature amplitude produces a result with a signal to noise of

$$(S/N)^{\pm}=\frac{V_s^{\pm}}{V_n^{\pm}}, \tag{1}$$

then a simultaneous measurement of both quadratures cannot give a signal-to-noise result in excess of

$$(S/N)^{\pm}_{sim}=\left(\frac{\eta^{\pm}V_s^{\pm}}{\eta^{\pm}V_n^{\pm}+\eta^{\mp}V_m^{\pm}}\right)S/N^{\pm}. \tag{2}$$

Here $V_s^{\pm}$ and $V_n^{\pm}$ are, respectively, the signal and noise power of the amplitude $(+)$ or phase $(-)$ quadrature at a particular rf frequency with respect to the optical carrier. The quantum noise that is inevitably added when dividing the mode is $V_m^{\pm}$. The splitting ratio is $\eta^{\pm}$ and $\eta^{+}=1-\eta^{-}$ (e.g, a 50:50 beam splitter has $\eta^{+}=\eta^{-}=0.5$). The spectral powers are normalized to the quantum noise limit (QNL) such that a coherent beam has $V_n^{\pm}=1$. Normally the partition noise will also be at this limit ($V_m^{\pm}=1$). For a classical light field, i.e., where $V_n^{\pm}\gg 1$ the penalty will be negligible. However, for a coherent beam a halving of the signal-to-noise ratio for both quadratures is unavoidable when the splitting ratio is a half. The Hartley-Shannon law [5] applies to Gaussian, additive-noise, communication channels such as we will consider here. It shows, in general, that if information of a fixed bandwidth is being sent down a communication channel at a rate corresponding to the channel capacity and the signal-to-noise ratio is reduced, then errors will inevitably appear at the receiver. Thus, under such conditions, any attempt by an eavesdropper to make simultaneous measurements will introduce errors into the transmission. In the following we will first examine what level of security is guaranteed by this uncertainty principle if a coherent state mode is used. We will then show that the level of security can in principle be made as strong as for the single quanta case by using a special type of two-mode squeezed state. The question of optimum protocols and eavesdropper strategies is complex and has been studied in detail for the single quanta case [6]. Here we only examine the most obvious strategies and do not attempt to prove equal security for all possible strategies.

Consider the setup depicted in Fig. 1. A possible protocol is as follows. Alice generates two independent random strings of numbers and encodes one on the phase quadrature and the other on the amplitude quadrature of a bright coherent beam. Bob uses homodyne detection to detect either the amplitude or phase quadrature of the beam when he receives

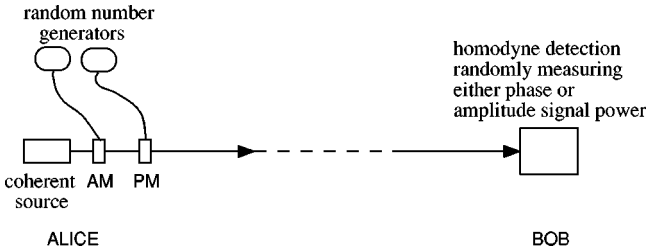

FIG. 1. Schematic of the coherent light cryptographic setup. AM is an amplitude modulator while PM is a phase modulator.

*FAX: +61 7 3365 1242.
Electronic address: ralph@physics.uq.edu.au

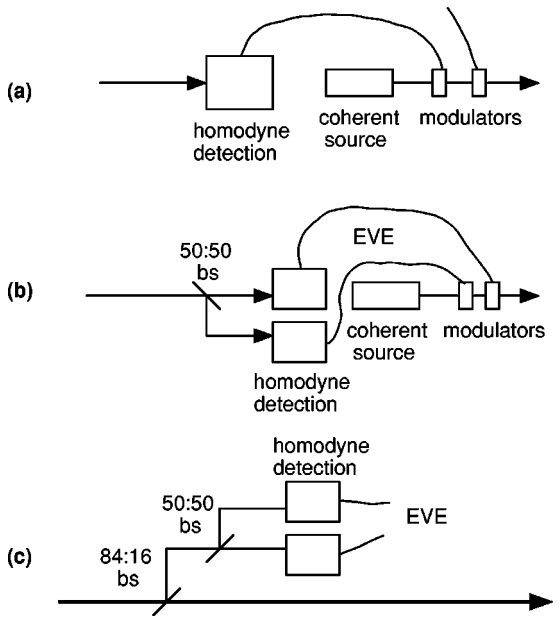

FIG. 2. Schematics of three eavesdropper strategies. Only (a) is available in single quanta schemes.

it. He swaps randomly which quadrature he detects. On a public line Bob then tells Alice at which quadrature he was looking at any particular time. They pick one quadrature to be the test and the other to be the key. For example, they may pick the amplitude quadrature as the test signal. They would then compare results for the times that Bob was looking at the amplitude quadrature. If Bob's results agreed with what Alice sent, to within some acceptable error rate, they would consider the transmission secure. They would then use the undisclosed phase quadrature signals, sent while Bob was observing the phase quadrature, as their key. By randomly swapping which quadrature is key and which is test throughout the data comparison an increased error rate on either quadrature will immediately be obvious.

To quantify our results we will consider the specific encoding scheme of binary pulse code modulation, in which the data is encoded as a train of 1 and 0 electrical pulses that are impressed on the optical beam at some rf frequency using electro-optic modulators. The amplitude and phase signals are imposed at the same frequency with equal power. Let us now consider what strategies Eve could adopt (see Fig. 2). Eve could guess which quadrature Bob is going to measure and measure it herself [Fig. 2(a)]. She could then reproduce the digital signal of that quadrature and impress it on another coherent beam that she would send on to Bob. She would learn nothing about the other quadrature through her measurement and would have to guess her own random string of numbers to place on it. When Eve guesses the right quadrature to measure, Bob and Alice will be none the wiser; however, on average 50% of the time Eve will guess wrong. Then Bob will receive a random string from Eve unrelated to the one sent by Alice. These will agree only 50% of the time. Thus Bob and Alice would see a 25% bit error rate in the test transmission if Eve were using this strategy. This is analogous to the result for single quanta schemes in which this type of strategy is the only available.

However, for bright beams it is possible to make simultaneous measurements of the quadratures, with the caveat that there will be some loss of information. So a second strategy that Eve could follow would be to split the beam in half, measure both quadratures, and impose the information obtained on the respective quadratures of another coherent beam that she sends to Bob [Fig. 2(b)]. How well will this strategy work? Suppose Alice wishes to send the data to Bob with a bit error rate (BER) of about 1%. For bandwidth limited transmission of binary pulse code modulation [7] the BER is given by

$$\mathcal{B}=\frac{1}{2}\mathrm{erfc}\frac{1}{2}\sqrt{\tfrac{1}{2}S/N}. \tag{3}$$

Thus Alice must impose her data with a S/N ratio of about 13 dB. For simultaneous measurements of a coherent state the signal-to-noise ratio obtained is halved [see Eq. (2)]. As a result, using Eq. (3), we find the information Eve intercepts and subsequently passes on to Bob will only have a BER of 6%. This is clearly a superior strategy and would be less easily detected. Furthermore, Eve could adopt a third strategy of only intercepting a small amount of the beam and doing a simultaneous detection on it [Fig. 2(c)]. For example, by intercepting 16% of the beam, Eve could gain information about both quadratures with a BER of 25%, while Bob and Alice would observe only a small increase of their BER to 1.7%. In other words, Eve could obtain about the same amount of information about the key that she could obtain using the ''guessing'' strategy, while being very difficult to detect, especially in the presence of losses.

The preceding discussion has shown that a cryptographic scheme based on coherent light provides much less security than single quanta schemes [8]. We now consider whether squeezed light can offer improved security. For example, amplitude squeezed beams have the property $V_n^+<1<V_n^-$. Because the amplitude quadrature is sub-QNL, greater degradation of S/N than the coherent case occurs in simultaneous measurements of amplitude signals [see Eq. (2)]. Unfortunately the phase quadrature must be super-QNL; thus there is less degradation of S/N for phase signals. As a result the total security is in fact less than for a coherent beam. However, in the following we will show that by using two squeezed light beams, security comparable to that achieved with single quanta can be obtained.

The setup is shown in Fig. 3. Once again Alice encodes her number strings digitally, but now she impresses them on the amplitude quadratures of two, phase locked, amplitude squeezed beams a and b, one on each. A $\pi/2$ phase shift is imposed on beam b and then they are mixed on a 50:50 beam splitter. The resulting output modes c and d are given by

$$\begin{aligned} c&=\sqrt{\tfrac{1}{2}}(a+ib),\\ d&=\sqrt{\tfrac{1}{2}}(a-ib). \end{aligned} \tag{4}$$

These beams are now in an entangled state that will exhibit Einstein-Podolsky-Rosen (EPR) type correlations [9,10]. Local oscillator beams (LO's) of the same power as, and with

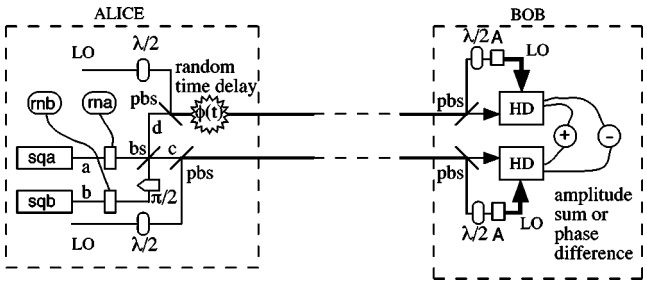

FIG. 3. Schematic of squeezed light cryptographic setup. Sqza and sqzb are phase-locked squeezed light sources. Rna and Rnb are independent random number sources. Bs and pbs are nonpolarizing and polarizing beam splitters, respectively. Half-wave plates to rotate the polarizations are indicated by λ/2 and optical amplification by *A*. The $\pi/2$ phase shift is also indicated. HD stands for homodyne detection system.

their polarizations rotated to be orthogonal to, *c* and *d* are then mixed with the beams on polarizing beam splitters. A rapidly varying random time delay is imposed on one of the beams. Both mixed beams are then transmitted to Bob, who uses polarizing beam splitters to extract the local oscillator from each beam. Bob *cannot* remix the signal beams (*c* and *d*) to separate *a* and *b* because the random time delay introduced between the beams has destroyed their coherence at the signal frequency. However, because each beam has a corresponding local oscillator that has suffered the same time delays, Bob *can* make individual, phase-sensitive measurements on each of the beams and extract either the information on *a* or the information on *b* by amplifying the local oscillators and using balanced homodyne detection. Note that the noise of the LO's is increased by amplification, but balanced homodyne detection is insensitive to LO noise. He randomly chooses to either (i) measure the amplitude quadratures of each beam and add them together, in which case he obtains the power spectrum

$$V^+ = \langle |(\tilde{c}^\dagger + \tilde{c}) + (\tilde{d}^\dagger + \tilde{d})|^2 \rangle = V_{s,a} + V^+_{n,a}, \tag{5}$$

where the tildes indicate Fourier transforms (thus he obtains the data string impressed on beam $a, V_{s,a}$, imposed on the sub-QNL noise floor of beam $a, V^+_{n,a}$); or (ii) measure the phase quadratures of each beam and subtract them, in which case he obtains the power spectrum

$$V^- = \langle |(\tilde{c}^\dagger - \tilde{c}) - (\tilde{d}^\dagger - \tilde{d})|^2 \rangle = V_{s,b} + V^+_{n,b}, \tag{6}$$

i.e., he obtains the data string impressed on beam $b, V_{s,b}$, imposed on the sub-QNL noise floor of beam $b, V^+_{n,b}$. Thus the signals lie on conjugate quadratures but *both* have sub-QNL noise floors. This is the hallmark of the EPR correlation [11].

Consider now eavesdropper strategies. First, like Bob, Eve cannot remix *c* and *d* optically to obtain *a* and *b* due to the randomly varying phase shift $[\phi(t)]$ introduced by the time delay. For small phase shifts beam *c* becomes $c' = (a + ib)(1 + i\phi)$. Mixing c' and *d* on a beam splitter will produce outputs with amplitude power spectra

$$V_{c'+d} = V_{s,a} + V^+_{n,a} + \alpha^2 V_\phi, \qquad V_{c'-d} = V_{s,b} + V^+_{n,b} + \alpha^2 V_\phi, \tag{7}$$

where α^2 is proportional to the intensity of beams *a* and *b* and V_ϕ is the power spectrum of the phase fluctuations. If $\phi(t)$ has a white power spectrum over frequencies from well below to well above the signal frequency, the signals will be obscured. It is not possible to directly control the phase shifts without similarly suppressing the signals. However, the phase shifts are also present on the LO copropagating with c'. Mixing the two LO's will produce an output with amplitude power spectra

$$V_{+LO} = 1 + E^2 V_\phi, \tag{8}$$

where E^2 is proportional to the intensity of the LO's and the ''one'' is from the quantum noise of the LO's. It is possible to use this output to control the phase noise on the mixed signal beams, giving (ideally) the amplitude power spectra

$$V^C_{c'+d} = V_{s,a} + V^+_{n,a} + \frac{\alpha^2}{E^2}, \qquad V^C_{c'-d} = V_{s,b} + V^+_{n,b} + \frac{\alpha^2}{E^2}, \tag{9}$$

where the remaining penalty arises from the quantum noise of the LO's. If $E^2 \gg \alpha^2$ (as is normally the case for a LO) then this penalty can be made negligible, thus retrieving the signals. This is why it is essential that the LO's have the same power as the signal beams at the point where the phase fluctuations are imposed. This makes the ratio of the correlated phase noise to the independent quantum noise the same for the LO and the signal beam. This cannot be changed by Eve. With $E^2 = \alpha^2$ the penalty is at the quantum limit. As we shall see in a moment this is sufficient to reveal Eve.

Eve can still adopt the guessing strategy by detecting a particular quadrature of both beams and then using a similar apparatus to Alice's to resend the beams. As before she will only guess right half the time, thus introducing a BER of 25%. Suppose instead she tries the second strategy of simultaneous detection of both quadratures on each beam. She will obtain the following power spectra for the summed amplitude quadratures and the differenced phase quadratures:

$$V^+ = \frac{1}{2}(V_{s,a} + V^+_{n,a} + 1), \qquad V^- = \frac{1}{2}(V_{s,b} + V^+_{n,b} + 1). \tag{10}$$

The signal-to-noise ratio is reduced as predicted by Eq. (2), but where the noise power for both quadrature measurements is sub-QNL [12]. This leads to improved security. For example, with 10-dB squeezing ($V_{n,a} = V_{n,b} = 0.1$) the signal-

to-noise ratio in a simultaneous measurement will be reduced by a factor of 0.09. As a result, assuming initial S/N of 13 dB and using Eq. (3), we find the information Eve intercepts and subsequently passes on to Bob will now have a BER of about 24%. In other words, the security against an eavesdropper using simultaneous measurements is now on a par with the guessing strategy. The third strategy is also now of no use to Eve, as small samples of the fields carry virtually no information. For example, with 10-dB squeezing, intercepting 16% of the field will give Eve virtually no information (a BER of 49.5%) while already producing a 5% BER in Bob and Alice's shared information.

In any realistic situation losses will be present. Losses tend in general to reduce security in quantum cryptographic schemes [13]. The problem for our system is that losses force Alice to increase her initial S/N in order to pass the information to Bob with a low BER. Eve can take advantage of this by setting up very close to Alice. Nevertheless, reasonable security can be maintained with sufficiently high levels of squeezing. For example, with 10-dB squeezing and 10% loss, strategy two will result in a 15% BER in the shared information. Also Eve must intercept 29% of the light to obtain a 25% BER using the third strategy that will cause a 20% BER in Alice and Bob's information. With 6-dB squeezing and 20% loss the second strategy penalty is reduced to a BER of 7.5%, similar to that of the coherent state scheme. However, for the third strategy, Eve must still intercept 29% of the light to obtain a BER of 25% and this will cause an 11% BER in Alice and Bob's shared information, much larger than for the coherent case. Although these results demonstrate some tolerance to loss for our continuous variable system it should be noted that single quanta schemes can tolerate much higher losses [14] making them more practical from this point of view.

In summary we have examined the quantum cryptographic security of two continuous variable schemes, one based on coherent light, the other based on two-mode squeezed light. While the coherent light scheme is clearly inferior to single quanta schemes, the squeezed light scheme offers, in principle, equivalent security. The quantum security is provided by the generalized uncertainty relation. It is also essential that the coherence between the two squeezed modes is destroyed. More generally this system is an example of a new quantum information technology based on continuous variable, multiphoton manipulations [15]. Such technologies may herald a new approach to quantum information.

[1] S. Wiesner, SIGACT News **15**, 78 (1983).

[2] C.H. Bennett and G. Brassard, in *Proceedings IEEE International Conference on Computers, Systems and Signal Processing (Bangalore)* (IEEE, New York, 1984), pp. 175–179.

[3] Y. Yamamoto and H.A. Haus, Rev. Mod. Phys. **58**, 1001 (1986).

[4] E. Arthurs and M.S. Goodman, Phys. Rev. Lett. **60**, 2447 (1988).

[5] C.E. Shannon, Bell Syst. Tech. J. **27**, 623 (1948).

[6] C.A. Fuchs and A. Peres, Phys. Rev. A **53**, 2038 (1996); C.A. Fuchs, N. Gisin, R.B. Griffiths, C.-S. Niu, and A. Peres, *ibid.* **56**, 1163 (1997); I. Cirac and N. Gisin, Phys. Lett. A **229**, 1 (1997).

[7] A. Yariv, *Optical Electronics in Modern Communications*, 5th ed. (Oxford University Press, 5th Edition, New York, 1997).

[8] Another strategy Eve could use is to do homodyne detection at a quadrature angle half-way between phase and amplitude. This fails because the signals become mixed. Thus Eve can tell when both signals are 0 or both are 1 but she cannot tell the difference between 1,0 and 0,1. This again leads to a 25% BER.

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

[10] G. Yeoman and S.M. Barnett, J. Mod. Opt. **40**, 1497 (1993); T.C. Ralph and P.K. Lam, Phys. Rev. Lett. **81**, 5668 (1998).

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

[12] The signal to noise properties of Eq. (9) are the same as those of Eq. (10).

[13] S.M. Barnett and S.J.D. Phoenix, Philos. Trans. R. Soc. London, Ser. A **354**, 793 (1996).

[14] W.T. Buttler *et al.*, Phys. Rev. A **57**, 2379 (1998).

[15] Other examples include: S.L. Braunstein, Nature (London) **394**, 47 (1998); A. Furusawa *et al.*, Science **282**, 706 (1998); S. Lloyd and S.L. Braunstein, Phys. Rev. Lett. **82**, 1784 (1999); R.E.S. Polkinghorne and T.C. Ralph, *ibid.* **83**, 2095 (1999).