HIGH-RATE STRONG-SIGNAL QUANTUM CRYPTOGRAPHY

Horace P. Yuen
Department of Electrical Engineering and Computer Science
Department of Physics and Astronomy
Northwestern University, Evanston, IL 60208

Abstract

Several quantum cryptosystems utilizing different kinds of nonclassical lights are described which can accommodate high intensity fields and high data rate. However, they are all sensitive to loss and both the high rate and the strong-signal character rapidly disappear. A squeezed light homodyne detection scheme is proposed which, with present-day technology, leads to more than two orders of magnitude data rate improvement over other current experimental systems for moderate loss.

The following is the second half of my talk "Squeezing, vacuum fluctuation, and all that" given at the Fourth International Conference on Squeezed States and Uncertainty Relations held in Taiyuan, China, June 1995. The first half consists of a brief review of sqeezing, a discussion of its coherence properties, the reality of vacuum fluctuation, and a treatment of the photon localization problem. At least two of these topics require a quantum field treatment that I cannot go into here, so I will just concentrate on quantum cryptography.

Quantum cryptography [1] -[7] is a very interesting and novel approach to secure communication with eigenstates of noncommuting observables as carriers of information to assure secrecy. In all the concrete optical realizations of such systems which have been studied theoretically or experimentally so far [2] -[7], either single-photon eigenstates orweak coherent states with less than one average photon per mode are employed to provide security [8]. Such systems not only face serious practical limitations in their detection, they are also inherently data-rate limited, especially after large transmission attenuation in possible applications such as the INTERNET. However, from an abstract point of view, two sets of states having the same linear geometry in the Hilbert space of states have the same security in principle. Thus, it is quite possible to describe *strong-signal* quantum cryptosystems, i.e., systems with quantum states that are *macroscopically distinguishable*, which are as secure as the ones that have been proposed. In the following we will describe several such systems involving nonclassical lights [9]. Unfortunately, such equivalent sets of states behave very differently in loss depending on the field intensity. In all the following systems, one cannot maintain either the strong-signal or the high-rate characteristics in the presence of the usual linear loss. Although a general proof is not yet available, the evidence indicates that there is no strong-signal quantum cryptosystem that would function properly in loss, for the same kind of reasons as the difficulties in generating and observing macroscopic superpositions of quantum states. This feature also leads to serious obstacles in transmitting more than $\frac{1}{2}$ bit per mode securely, although it is not clear what the fundamental rate limit is. As a small compensation, a currently implementable system is proposed which may be of practical importance.

Consider the following standard quantum cryptosystem [2] with a single polarized photon in four different possible polarization states,

$$| 1 >_1 | 0 >_2, \quad | 0 >_1 | 1 >_2 \tag{1}$$

$$\frac{1}{\sqrt{2}} (| 1 >_1 | 0 >_2 \pm | 0 >_1 | 1 >_2) \tag{2}$$

where $| 1 >_1$ is the photon number = 1 eigenstate of a vertically polarized light mode, $| 0 >_2$ the vacuum state of the horizontally polarized light mode, so that the two states of (2) are the single photon eigenstates of the corresponding diagonally polarized light modes. A sender, Adam, picks the basis (1) or (2) at random for transmitting a single bit to the legitimate user, Babe, who would choose to measure (1) or (2) also randomly. After comparison in another public channel to match basis, they would succeed in communicating on the average $\frac{1}{2}$ bit per use. An eavesdropper, Eve, cannot duplicate a copy of the transmitted state and wait for the public measurement announcement, because the four possible states in (1) and (2) are nonorthogonal [10]. Similarly, Eve cannot use a quantum measurement to determine without large error which state was transmitted; thus any state she re-sends after measurement would induce large error in the otherwise perfect bit correlations between Adam and Babe, who could therefore detect the eavesdropping via various public forms of comparison. Apart from the practical difficulty of generating and detecting single photons, the data rate of this system is reduced to $\frac{\eta}{2}$ after suffering an energy loss $1 - \eta$ due to transmission attenuation, detection quantum efficiency, and whatever. If the optical system has bandwidth W, i.e., a total number of W adjacent frequency modes per polarization per second, the data rate becomes $\frac{\eta W}{2}$ bits per second assuming perfect detection. In the coherent-state realizations of this scheme with energy $S < 1$, the data rate is further reduced to $\eta SW/2$. Because of the smallness of this rate in practice, especially when the loss is large, it is important to investigate the possibility of rate increase for a single mode.

Clearly, the state vectors

$$| \psi >_1 | \phi >_2, \ | \phi >_1 | \psi >_2 \ ; \ \frac{1}{\sqrt{2}} (| \psi >_1 | \phi >_2 \pm | \phi >_1 | \psi >_2) \tag{3}$$

where $< \psi \mid \phi >= 0$ in each mode 1 and 2 have the same Hilbert space geometry as (1)-(2) in the sense of equal inner products, and hence the same security in principle. A strong-signal scheme can be obtained, say, by using photon number eigenstates $| \psi >= | n >$, $| \phi >= | 0 >$ or more generally $| \psi >= | n_1 >$, $| \phi >= | n_2 >$ with $(n_1 - n_2) >> 1$ for macroscopic distinguishability. Note that $\frac{1}{\sqrt{2}} (| n >_1 | 0 >_2 \pm | 0 > | n >_2)$ are not the number eigenstates of the diagonally polarized light for $n > 1$. In a single pair of modes, one can increase the data rate by utilizing $| \psi_n >= | n + \Delta n >$, $| \phi_n >= | n >$ while keeping $\Delta n >> 1$. If $N >> 1$ is the upper bound on the photon numbers that can be used in a mode, such a scheme would have a data rate of $\frac{W}{2} log_2 (1 + N - \Delta n)$ bits per second. Such high rate can also be obtained for a lossless system via conjugate coding [1], in which the first basis contains N orthogonal states and each state in the second basis is some linear combination of all the N states in the first. While it is possible to suggest concrete optical realizations for certain number state superpositions, it is not clear how the N-state superpositions in conjugate coding may be generated. In any case, all such superpositions degenerate quickly in loss as presently demonstrated.

It is well known [11]-[12] that linear combinations of macroscopically distinguishable coherent states are very sensistive to loss: they degenerate into a mixture of the states very readily. In a way, number states fare even worse. In the present context, this means the cryptosystem would be incapacitated entirely as the second basis degenerates into the first. Let the lossy system be represented by [13]-[14]

$$b = \eta^{\frac{1}{2}} a + (1-\eta)^{\frac{1}{2}} c \tag{4}$$

where c is the photon annihilation operator of a vacuum mode, a and b the input and output mode operators. For a pair of independent modes suffering the same loss $1-\eta$, each would be represented by (4) with different a, b, c . For $\mid \psi >= \mid n >$, $\mid \phi >= \mid 0 >$, the difference $\Delta\rho$ between the two density operators resulting from passing the two superposed states of (3) through (4) can be conveniently calculated via eqns (6)-(7) of ref [15], with the result

$$\Delta\rho = \eta^n (\mid n >_1 \mid 0 >_2 \; {}_1 < 0 \mid \; {}_2 < n \mid + \mid 0 >_1 \mid n >_2 \; {}_1 < n \mid \; {}_2 < 0 \mid) \tag{5}$$

which goes to zero exponentially in η. If $\mid \psi >= \mid n_1 >$, $\mid \phi >= \mid n_2 >$ in (3), a similar but more complicated result is obtained with the eigenvalues of $\Delta\rho = \pm 2\eta^{n_1+n_2}$. For the single-mode system

$$\mid n_1 >, \mid n_2 > ; \; \frac{1}{\sqrt{2}} (\mid n_1 > \pm \mid n_2 >) \tag{6}$$

the eigenvalues of the superposed state difference $\Delta\rho$ in loss are $\pm\sqrt{\eta^{n_1+n_2}}$. Since two equiprobable states can only be discriminated with probability equal to the positive eigenvalue of $\Delta\rho$ from quantum detection theory [16], such superposed number state schemes are useless with even a tiny amount of loss.

The coherent-state superpositions in the following 4-state scheme

$$\mid \alpha >, \mid -\alpha >, \; \frac{(\mid \alpha > \pm \mid -\alpha >)}{\sqrt{2\,[1 \pm exp(-2 \mid \alpha \mid^2)]}} \tag{7}$$

can, at least in principle, be obtained from a Kerr medium [17]. For large $|\alpha|, < \alpha \mid -\alpha >= \exp(-2 \mid \alpha \mid^2)$ is nearly zero and the states (7) would perform in practice like an orthogonal scheme such as (6). For the general coherent-state superpositions in the following scheme

$$\mid \alpha_1 >, \mid \alpha_2 > ; \; \mathcal{N}_{\pm} (\mid \alpha_1 > \pm \mid \alpha_2 >) \tag{8}$$

where $\mathcal{N}_{\pm}$ are normalization factors, the resulting density operator difference $\Delta\rho$ in loss is proportional to $< \sqrt{1-\eta}\,\alpha_1 \mid \sqrt{1-\eta}\alpha_2 >$ which goes to zero exponentially in $(1-\eta)^{\frac{1}{2}} \mid \alpha_1 - \alpha_2 \mid$. To avoid this sensitivity to loss, $|\alpha_1 - \alpha_2|$ has to be chosen small and the resulting data rate for (7) or (8) would be comparable to coherent-state sysytems such as $\{|\pm\alpha >\}$ or $\{|\pm\alpha >; |\pm i\alpha >\}$, although (7) or (8) may be more secure because of their similarity to the single-photon scheme [7]. If one increases the rate in such systems by displacing the amplitude with $(m \pm in)\alpha_0$ for integers m, n and a real α_0 with $\eta\alpha_0^2 \geq 10$ to assure near orthogonality of the displaced states, which can be readily accomplished experimentally, the resulting rate is increased to $\sim \frac{\alpha^2 W}{2} \log(\eta S)$ for large available energy $S >> \alpha_0^2$. However, Eve can split off a small fraction of the signal and determine m, n fairly closely, thus obtaining many bits of information probabilistically so that such systems do not truly have a high secure rate.

Consider the following 4-state cryptosystem with two 2-state bases given by two-photon coherent states (TCS) [13] or pure squeezed coherent states which can readily be generated over a considerable range of parameters [18],

$$|\mu,\ \nu\ ; \pm\alpha > ;\ |\mu, -\nu; \pm i\alpha > \tag{9}$$

where $|\ \mu, \nu; \alpha >$ is the $|\ \beta; \mu, \nu >$ of ref [13] with mean field $\alpha = \mu^*\beta - \nu\beta^*$ and μ, ν, α are all chosen real. In (9), the signal is in the small noise quadrature. As an approximate form of conjugate coding for the two conjugate field quadrature operators whose eigenstates have infinite energy, consider the extension of (9) to the scheme

$$|\mu,\ \nu\ ; \pm m\alpha > ;\ |\mu, -\nu\ ; \pm im\alpha >,\ \ m = 1, 3, 5, \cdots \tag{10}$$

From eqn (3.25) of ref [13], $|< \mu,\ \nu;\ \pm\alpha\ |\ \mu, -\nu;\ \pm\beta >|^2 = \exp(-|\alpha - \beta|^2)$ and

$$|< \mu,\ \nu;\ m\alpha\ |\ \mu, -\nu;\ ni\alpha >|^2 = (\mu^2 + \nu^2)^{-1} \exp\{-(n^2 + m^2)\alpha^2/(\mu^2 + \nu^2)\} \tag{11}$$

Thus $(\mu^2 + \nu^2)$ cannot be too large from (11), and α also cannot be too large or else Eve can determine the state by a phase insensitive linear amplifier followed with beamsplitting or by heterodyne detection with the following signal-to-noise ratio in the quadrature containing the signal [19]

$$SNR_{het} = \frac{4\eta\alpha^2}{\eta(\mu - \nu)^2 + 2 - \eta} \tag{12}$$

In general, one has to assume that Eve may tap at $\eta = 1$.

When the correct quadrature is detected with homodyne detection, the signal-to-noise ratio is [13],[19]

$$SNR_{hom} = \frac{4\eta\alpha^2}{\eta(\mu - \nu)^2 + 1 - \eta} \tag{13}$$

One must also require that at $\eta = 1$, the homodyne SNR obtained by Eve with a beamsplitter of transmittance ϵ is sufficiently small so that she cannot quite resolve the state even after the measurement announcement with a probability larger than, say, $P_e^E = 0.25$, while the induced reduction in the SNR_{hom} for Babe from (13) to

$$SNR_{hom}^B = \frac{4(1 - \epsilon)\eta\alpha^2}{\eta(1 - \epsilon)(\mu - \nu)^2 + \epsilon\eta + (1 - \eta)} \tag{14}$$

is already sufficiently large that Babe can detect the eavesdropping from the increase in her error rate. However, even for small ϵ Eve can locate to within a few states among one basis of (10) quite well, unless α is so small that the data rate is strongly affected. Thus, a large number of secure bits cannot be derived from the use of (10). Nevertheless the potential of homodyne systems can be seen from the following two examples.

Consider (9) with $\alpha^2 = 0.8$, $\nu = 0$, $\eta = 1$. The homodyne detection probability of error [19] is $P_e = erfc(\sqrt{SNR}) \sim 0.037$. If Eve tries to resolve the four states with optimized heterodyne detection, it is readily shown from classsical detection theory that the resulting error probability is ≥ 0.2 which is easily detected by Babe. Amplification and beamsplitting would lower Babe's SNR too much at the present signal level. If Eve taps off just a fraction ~ 0.089 of the field

to wait for measurement announcement so that the resulting optimum quantum receiver [16] for binaray coherent states yields an error probability of 0.25, that would already change Babe's error rate to 0.044 via (10), a 25% increase. With 10^4 transmissions, this means an increase of 3.64 standard deviations of error in an asymptotic standard Gaussian distrubution , which occurs with only a probability $\sim 10^{-4}$. Comparing to the photon detection system [5], [6] with $\alpha^2 \sim 0.1$ and considering the fact that close to an order of magnitude improvement in the photodetector quantum efficiency can be obtained from high efficiency photodiode for homodyme detection, this yields almost two orders of magnitude improvement in the data rate. For the TCS system (10) with $m = \pm 1, \pm 3$, $\alpha^2 = 1$, $(\mu + \nu)^2 = 4$, $\eta = 0.5$, and with the homodyne error probability among the four states in one basis still given by $P_e = erfc(\sqrt{SNR})$, Eve cannot exclude the possibility of any state with $\epsilon = 0.04$ which already induces a 3-standard deviation difference in Babe's error rate for 10^4 transmissions, and $\epsilon = 0.1$ is required for $P_e^E = 0.25$. The data rate is now increased by a factor of ~ 400. The disadvantage of these schemes is that by raising the signal level, the initial beamsplitter attack puts a limit on the transmittance η below which the eavesdroppping cannot be detected. This can be amended by setting the threshold of the binary decision at a higher level and making no decision below it, which of course reduces the data rate, or by decreasing α which would also lower the data rate. Apart from the sensitivity of homodyne detection versus photon counting technology, part of the above improvement is due to more elaborate signal processing which can also be adopted in photon counting systems. Note that as in the direct detection case, the presence of a small error probability for Babe would reduce the information rate from the original data rate by a small fraction. Also, Eve could obtain some probabilistic information without being detected, which can be eliminated by Babe via "privacy amplification" [5] that would further lower the information rate. However, for sufficiently long keys there is no need to eliminate Eve's probabilistic information. A detailed study of the various possibilities will be given elsewhere.

Acknowledgment

This work was supported by the Office of Naval Research and the Advanced Research Project Agency.

References

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

[2] C. H. Bennett, G. Brassard, and A. K. Ekert, Scientific American, Oct. 1992, pp. 50-57.

[3] C. H. Bennett, Phys. Rev. Lett. 68, 3121 (1992).

[4] A. K. Ekert, J. G. Rarity, P. R. Tapster, and G. M. Palma, Phys. Rev. Lett. 69, 1293 (1992).

[5] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, J. Cryptol. 5, 3 (1992).

[6] P. D. Townsend, J. G. Rarity, and P. R. Tapster, Electron. Lett. 29, 1291 (1993).

[7] B. Huttner, N. Imoto, N. Gisin and T. Mor, Phys. Rev. A51, 1863 (1995).

[8] Along with all the other papers in the literature, the fundamental question of security will not be addressed here: What is the robustness level of the system against all possible eavesdropping methods consistent with the laws of physics. Only certain specific eavesdropping approaches will be discussed.

[9] H. P. Yuen, in Photons and Quantum Fluctuations, E. R. Pike and H. Walther, eds., (Hilger, London, 1988), p. 1.

[10] H. P. Yuen, Phys. Lett. 113A, 405 (1986).

[11] A. O. Caldeira and A. J. Leggett, Phys. Rev. A31, 1059 (1985).

[12] D. F. Walls and G. J. Milburn, Phys. Rev. A31, 2403 (1985).

[13] H. P. Yuen, Phys. Rev. A13, 2226 (1976).

[14] H. P. Yuen and J. H. Shapiro, IEEE Trans. Inform. Theory 26, 78 (1980).

[15] H. P. Yuen, Phys. Lett. 113A, 401 (1986).

[16] C. W. Helstrom, Quantum Detection and Estimation Theory, Academic Press, 1976.

[17] B. Yurke and D. Stoler, Phys. Rev. Lett. 57, 13 (1986).

[18] H. J. Kimble, Phys. Repts. 219, 227 (1992)

[19] J. H. Shapiro, H. P. Yuen and J. A. Machado Mata, IEEE Trans. Inform. Theory 25, 179 (1979). Note that eqn(3.49) is too small by a factor of 2, which is not important for large SNR but crucial for our present applications.