Proceedings of the International Conference "Quantum Optics V", Kościelisko, Poland, 2001

Quantum Cryptography with Macroscopic Photon-Number-Correlated Light

M.G. Raymer* and A.C. Funk

Oregon Center for Optics and Department of Physics
University of Oregon, Eugene, Oregon, 97403, USA

We describe a new scheme for performing quantum key distribution. We present two physical implementations for the quantum key distribution system. The first implementation uses a type-II optical-parametric amplifier to generate the optical pulses which contain the key information. The second implementation uses correlated semiconductor emitters to generate the optical pulses.

PACS numbers: 03.67.Dd, 03.67.Hk, 42.50.Dv, 42.50.Lc

1. Introduction: quantum states provide security

Let us consider the following scenario: one person (Alice) wants to send a secret message to a second person (Bob). At the same time, an eavesdropper (Eve) is attempting to obtain the secret message. Alice and Bob can use a One-Time Pad cryptographic protocol in order to securely transmit their secret message. This protocol consists of Alice and Bob having a shared secret key prior to the sending of the secret message. The key will consist of a string of random binary data. The key is used to encode the secret message by a simple binary addition of the secret message with the key. The encoded secret message can then be transmitted over a public channel (i.e. a channel which can be seen by anyone including Eve). As long as the key data is shared by only Alice and Bob and the key is only used once, it is provably impossible for Eve to decode the encoded message.

This would appear to be a very powerful technique for sending secret messages. The catch is that it is hard to create and distribute a key that is shared by Alice and Bob but also remains secret after the distribution procedure. Presum-

*corresponding author; e-mail: raymer@oregon.uoregon.edu

ably Alice and Bob are separated by a large enough distance that is impractical for them to simply meet and exchange envelopes containing the key (in this case, they could pass the secret message in the envelope just as easily). Distributing the key in a secure fashion is however possible. This is due largely to the fact that if the key is intercepted by Eve, she gains no "secret data". She has merely obtained the particular string of random binary data for that particular key. If Alice and Bob are able to determine the extent of Eve's knowledge about the key after the key was distributed, they could then determine whether the key is secure. If the key is secure, it can be used for encoding a secret message. If the key is not secure it will be discarded, and the distribution procedure will be attempted again. Therefore, Eve's goal is to obtain as much information about the key as is possible without alerting Alice and Bob to her presence.

We will now present a brief overview of the general strategy and the underlying principles behind quantum key distribution (QKD) before beginning a more detailed description. In QKD, each key bit is represented by the quantum state of an object (particle or light pulse) which is physically sent from Alice to Bob. The basis of the security for QKD rests on two ideas: (i) the quantum state of an object cannot be tampered with or probed without imparting some disturbance to the state, and (ii) any measurement (or sequence of measurements) on a single quantum object cannot fully reveal its state. The first of these ideas has its basis in the famous uncertainty principle, and the second (proven in [1–3]) is related to the no-cloning theorem [4]. For if we could clone a quantum state many times, we could use quantum-state topography [5, 6] to determine the state of the single original object, an impossibility.

For a general example of this measurement property, we refer to Fig. 1, where a single object can be visualized as being represented by a state Ψ. Information about the state can be accessed only partially by any measurement of the object. If one measures a variable called Q (which can be visualized as "viewing" Ψ from the "front side"), then there can be no information obtained about a conjugate variable P, and vice versa. Referring to Fig. 1, a message (such as "OCO") could

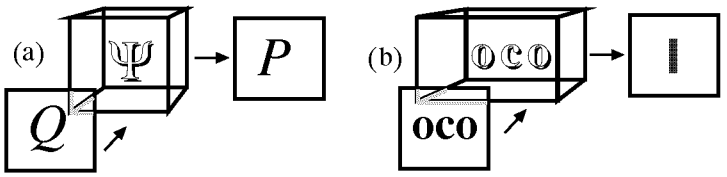

Fig. 1. (a) A state Ψ can be measured in one of two bases either Q or P. (b) If the message "OCO" (which is the abbreviation used for the Oregon Center for Optics), is encoded in the P variable of the quantum state of an object, a measurement along P will read out the message, whereas a measurement along Q will not yield any information about the message.

be stored in Ψ (e.g., in the value of Q), and the object could be sent to a second party. However, only if the second party knows which variable to measure (i.e. which side to "look into") will he/she be able to extract the stored information with certainty. Measurements of the object in the "wrong" basis (i.e. measuring P in the example of Fig. 1b) will not reveal any information about the message and will preclude a measurement in the other (correct) basis. Quantum key distribution exploits these measurement properties of quantum mechanics to keep a secret key secure from unintended (eavesdropping) measurements.

2. BB84: one realization of QKD

In 1984, Charles Bennett and Giles Brassard proposed the first QKD protocol, which has since been named BB84 [7]. The following is a brief review for those readers not familiar with the BB84 QKD protocol. The protocol uses a single photon as the physical object whose state is used to encode each key bit. Following this we will discuss our new proposal for QKD with light pulses containing a macroscopic number of photons.

Alice encodes the key bit in the polarization state of the photon. Alice uses two different polarization bases to accomplish this task. The first basis consists of the vertical and horizontal polarization directions, and the second basis consists of the +45 degree linear polarization and the –45 degree linear polarization directions. A logical 1 is encoded by preparing a photon in either the vertical polarization mode *or* in the +45 degree polarization mode. A logical 0 is encoded by preparing a photon in either the horizontal polarization mode *or* in the –45 degree polarization mode.

Alice chooses at random which basis to use for each bit. Given the bit value, she prepares the photon in the appropriate polarization direction depending on the chosen basis, and then sends the photon to Bob. We will refer to the basis used by Alice for the encoding of the bit as the "correct" basis and the other basis as the "wrong" basis. Bob's measurement procedure consists of splitting the beam sent by Alice on a polarizing beam splitter, which is either aligned to split the vertical and horizontal polarizations *or* to split the +45 degree linear and –45 degree linear polarizations, and then measuring the number of photons (0 or 1) in each of the two polarization modes chosen by the alignment of his beam splitter. Bob does not know a priori which basis Alice used for her encoding of the bit. Bob will simply choose at random whether to make his measurement in the vertical/horizontal basis or in the +/–45 degree basis. In the case where Bob measures in the correct basis, he will always measure exactly one photon in the polarization mode in which Alice encoded the bit, and zero photons in the other polarization mode. In the case where Bob measures in the wrong basis, he will measure one photon in each of the polarization modes for 50% of the measurements. Clearly on any given trial, there will only be one photon in one mode and zero photons in the other mode. However for measurements in the wrong basis, which mode has one photon and

which mode has zero photons will change from trial to trial. Regardless of the bit value encoded by Alice, for measurements made in the wrong basis, Bob will get measurement results corresponding to a logical 1 for 50% of the measurements and results corresponding to a logical 0 for the other 50% of the measurements. Measurements in the wrong basis will thus give Bob the wrong bit value for 50% of the measurements. To eliminate these erroneous measurement results, Bob and Alice communicate after all the bits have been sent via a public channel and tell each other which basis they used for each bit, but they do *not* reveal to each other the actual bit values. The bits are kept only for those cases where both Alice and Bob were using the same basis; all other bits are thrown away. At this point, Bob and Alice will have exact agreement between all of their key bits, assuming no tampering with bits took place during transmission.

We must now consider the possible effects of an eavesdropper on Alice and Bob's protocol. Eve is able to intercept and perform any sort of measurement on the photons sent by Alice. Eve, like Bob, does not know which basis is going to be used for any particular bit. Her measurement strategy will therefore be the same as Bob's. Eve will choose randomly between the two polarization bases in which to make her measurements. Eve will obtain a measurement result which corresponds to a particular bit value in a particular polarization basis. At this point, Eve must send a photon to Bob, for if he does not receive a photon, he immediately knows that an eavesdropper is present, and the key will not be used. Eve will attempt to prepare a photon in the same state that Alice used to encode the bit. If Eve were able to prepare the photon in the same state that Alice used, the results of Bob's measurements would be exactly the same as in the case where there was no eavesdropper. However, as stated earlier based on principles (i) and (ii), it is not possible for Eve to reproduce exactly the state.

For the case of the single photon it is easy to see how this works. Eve makes measurements in the wrong basis for 50% of her measurements. She does not know whether she is measuring in the correct basis or the wrong basis, because the measurement results in the wrong basis appear to be valid measurement results. The state she subsequently prepares and sends to Bob in an attempt to try to fool him, will sometimes be prepared in the wrong basis. In these cases, when Bob makes his measurements (in the correct basis), his measurement results will no longer perfectly agree with Alice's bits. The bit values corresponding to the measurements made by Bob will be incorrect for 50% of the bits sent by Eve, when Eve measures in the wrong basis (which happens for 50% of her measurements). Bob will thus have a 25% bit error rate when his key is compared with Alice's key.

If Alice and Bob sacrifice a small portion of their bits by comparing the actual values publicly, they can determine how many of their bits agree. From this public discussion, they can make an estimate of the overall error rate in their bit values. From this error rate, they can determine the extent to which Eve was

tampering with the photons as they were sent from Alice to Bob. If Alice and Bob determine that Eve obtained enough information to compromise the security of their key, they simply discard the key and attempt the key distribution again.

This rather simplistic analysis of the BB84 protocol hopefully provides a convincing plausibility argument for the security of the protocol and the underlying principles which guarantee the security. One might however question whether Eve might use more sophisticated attacks such as performing quantum non-demolition measurements on the photons which pass from Alice to Bob, or Eve might attempt to entangle the photons with a local system, which she can then measure after the basis information is revealed. It turns out that BB84 is secure against any attack that Eve might perform. There exist several proofs, which prove the security of BB84 [8–10].

Single-photon QKD schemes have been implemented, but are subject to some limitations. It is not technically feasible at the present time to produce single photons on demand. All currently available light sources have a nonzero probability to produce various numbers of photons on a given trial. If more than one photon is unknowingly sent by Alice, Eve might be able to take away one photon and measure it, while letting the other pass on to Bob. In this case, Bob and Alice would be unaware of the information gained by Eve via the extra photon emitted by the light source. In fact the security proofs that exist for BB84 cannot prove security if too many extra photons are emitted. Another problem is that at the single-photon level stray background photons give false results.

3. QKD with macroscopic pulses

We will now consider whether it is possible to encode key bits into macroscopic light pulses and still achieve security that rests on principles (i) and (ii) above. This would offer advantages in the areas of signal creation and immunity to background light. QKD schemes have been proposed using optical fields containing more than one photon [11–13], but none of these schemes appear to be workable at the macroscopic level. By macroscopic we mean (somewhat arbitrarily) a pulse of light containing on the order of one million or more photons.

As in BB84, our scheme for QKD will use the directions of optical polarization as the two bases in which Alice may encode bit values. But in contrast to BB84, each bit will be encoded into a pulse containing many photons. To represent a logical 1 (0), Alice will create an optical pulse having on average $\langle n_{\mathrm{V}}\rangle = N + (-)\delta/2$ photons polarized in the vertical direction and $\langle n_{\mathrm{H}}\rangle = N - (+)\delta/2$ polarized in the horizontal direction, or in the other basis $\langle n_{+45}\rangle = N + (-)\delta/2$ photons polarized in the +45 degree direction and $\langle n_{-45}\rangle = N - (+)\delta/2$ photons polarized in the –45 degree direction. Here N is taken to be a large number of the order 10^6, and δ is taken to be a much smaller number of the order $\sqrt{N} \sim 10^3$. The mean difference number $\langle n\rangle$ for a logical 1 (0) will thus be given by $\langle n\rangle = \langle n_{\mathrm{V}} - n_{\mathrm{H}}\rangle = +(-)\delta$, or in the other basis, $\langle n\rangle = \langle n_{+45} - n_{-45}\rangle = +(-)\delta$.

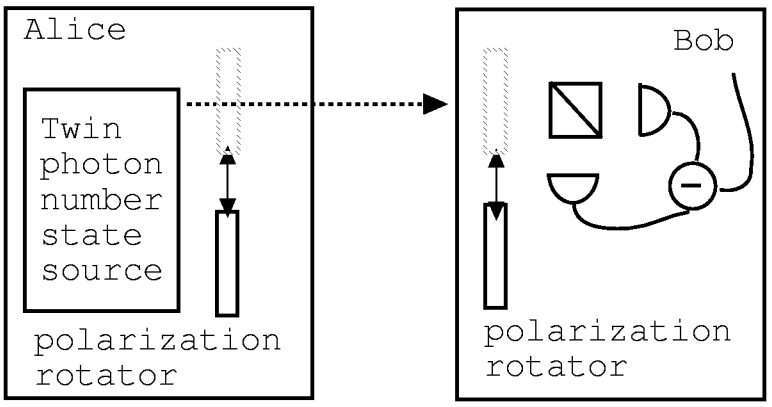

Fig. 2. A schematic of the apparatus used by Alice and Bob to perform QKD. The polarization rotators are used at random by both Alice and Bob.

The protocol for the transmission of the pulses is similar to that of BB84. Figure 2 shows the setup for transmission. Alice first encodes a bit value in the V/H basis and then either rotates or does not rotate the polarization basis by +45 degrees. Neither Bob nor Eve will know whether Alice rotated or not on each pulse. Alice sends the pulses to Bob, who measures the photon difference number n in either the rotated or the unrotated basis, selected at random. After transmission, Alice and Bob reveal publicly whether they rotated each pulse or not, they discard the measurement results for the cases in which they were not using the same basis, and they then compare a certain fraction of their bit values, looking for evidence of tampering.

It was pointed out that such a scheme could be implemented using coherent--state ("classical") pulses from an ordinary laser [14]. The security is guaranteed by setting δ to be very small compared to N. The inherent uncertainty in the number of photons in a coherent state pulse ensures that any measurement by an eavesdropper would be dominated by the noise. The variance of the photon difference number is equal to $\sqrt{N}$, which defines the shot-noise limit for the coherent state pulse, which is set to be larger than δ, making it impossible for the eavesdropper to obtain accurate key information. Unfortunately, Bob (the intended recipient of the key) is also subject to large uncertainties in his measurement results. This requires huge amounts of error correction for Alice and Bob to get good key data agreement. The end result is a very low bit per optical pulse efficiency. In one given example, for each key bit that is to be sent, approximately 500 laser pulses would need to be sent, giving an efficiency of 0.5% (check).

In our scheme the pulses are prepared in "twin-photon-number states" (TPNS). The TPNS are states which consist of two modes where the total photon number can fluctuate, but the difference of the number of photons between the

two modes is very well defined [15–18]. This is the result of correlations which exist between the two modes. The TPNS are quantum mechanical states (i.e. there is no way to describe them using statistical mixtures of classical states), and the TPNS should thus also enjoy the same benefits of security as outlined in principles (i) and (ii). There are however requirements for the actual form of the TPNS (specifically the values of N and δ) to ensure security.

The TPNS have the property of having a very well defined photon difference number between two modes. Thus the distributions for measurements of the difference number are very narrow. They can in fact be narrower than the shot-noise limit (SNL), which is the variance for an equivalent coherent state having the same total number of photons. The sub-SNL photon difference number distributions allow for Alice to encode bits using a value of δ that is significantly smaller than $\sqrt{N}$, yet the uncertainties in the measurement in the correct basis will not be dominated by noise due to the narrow distribution. However, a measurement of the photon difference number in the wrong basis will have a distribution with a width that is given roughly by $\sqrt{N}$.

There are two methods for producing twin-photon-number-state pulses: optical parametric amplification [15, 16, 18] and correlated semiconductor diode lasers [17, 19, 20].

For the optical parametric amplification process, a weak, quasi-monochromatic signal light beam, with two orthogonal polarization modes, is injected into a type-II nonlinear-optical crystal that is also pumped by a strong laser pulse having frequency twice that of the signal beam. As each photon in the pump beam is annihilated, it creates a pair of down-converted photons — exactly one in each of the polarization modes of the signal beam. Let us denote the numbers of photons in the two polarization modes by n_1 and n_2. After a number M of such events, both n_1 and n_2 increase by the addition of the number M. As pointed out by B. Mollow and R. Glauber in 1967, "since the magnitudes of both n_1 and n_2 increase exponentially, ... the relative magnitude of the difference between them becomes exceedingly small" [21]. This is precisely what is needed for efficient QKD.

In Fig. 3 we show for the case of parametric amplification the calculated probability distributions for Bob's observed difference number for a logical 1 measured in the correct basis (solid curve), a logical 0 measured in the correct basis (dotted curve), and for a logical 1 or 0 measured in the wrong basis (dashed curve). The first important thing to note is that the distribution for measurements made in the wrong basis contain no bit information because the distribution is identical for both the logical 1 and the logical 0. The other important thing to note is that for the case of 100% transmission, the distributions for the logical 1 and the logical 0 for measurements in the correct basis are well separated. The fact that the distributions are well separated means that there will be very few measurements results which correspond to a logical 0 (1) when a logical 1 (0) was in fact sent. This will give Alice and Bob a very low systematic bit-error rate.

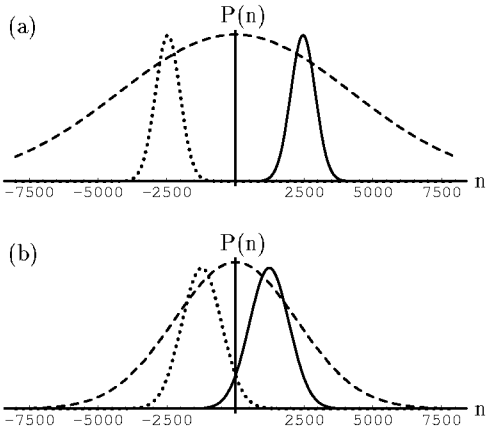

Fig. 3. The unnormalized probability distributions for the measurement of the photon difference number for twin-photon-numberstates produced by an optical parametric amplifier (OPA) for a logical 1 in the correct basis (solid curve), a logical 0 in the correct basis (dotted curve), and a logical 1 or 0 in the incorrect basis (dashed curve), for the cases (a) 100% transmission and (b) 50% transmission.

We define the bit-error rate as the probability for Bob's measurement to yield a negative difference number, when a positive number is expected in the case that Alice sent a logical 1 (or vice versa).

If Eve intercepts and measures the difference number, she will be using the wrong basis half the time. As shown above, measurements in the wrong basis do not reveal any key bit information. Thus Eve will have zero information for the bit value in those cases where she makes a measurement in the wrong basis. Therefore she cannot prepare a TPNS to send to Bob that will give Bob measurement results without adding errors, which are subsequently detectable by Alice and Bob.

We must also consider more sophisticated attacks which Eve might perform in order to obtain some key information. For example, Eve might choose to measure the photon difference number simultaneously in both the vertical/horizontal and +/–45 degree bases. Such an approach would not make much sense in the single photon QKD protocols, because the single photon is not divisible, however one might think that if there are large numbers of photons, there might be some information available by measuring half of the pulse in one basis and the other half of the pulse in the other basis. This strategy does not in fact provide the eavesdropper with enough information to reproduce the state sent by Alice, because simultaneous measurement of non-commuting variable necessarily adds additional noise [22]. This is consistent with the underlying principles governing quantum measurement described earlier.

The relevant distributions governing the measurement results for the case of simultaneous measurements in both of the bases are shown in Fig. 3 for the

case of 50% transmission. There are several features of these distributions which make it impossible for Eve to accurately reproduce the state which was sent by Alice. The results of a given measurement will give a number for the photon difference number n in the vertical/horizontal basis and another number for n in the +/–45 degree basis. As can be seen from the distributions, there is significant overlap between the distribution in the correct basis (for a given logical bit value) and the distribution in the wrong basis. This means that a single measurement result will not be an accurate indicator as to which basis was the correct basis and which basis was the wrong basis. Eve could get lucky and the measurement result for the wrong basis could be in the very tails of the wrong basis distribution. Such a measurement result is unlikely to have come from a measurement in the correct basis. In this case, Eve has a good chance of knowing which basis is correct and which is wrong. However there is significant overlap between the distribution for the logical 1 and the logical 0 for measurements in the correct basis. This overlap will lead to approximately a 10% error in Eve's ability to determine the logical bit value. This error rate is easily detectable by Bob and Alice in their post measurement error check procedure.

Eve could attempt an even more subtle attack in which she samples only a very small portion of the beam using a non-polarizing beam splitter. She can then perform any sort of measurement on this portion of the pulse, letting the rest of the pulse continue on to Bob. Shown in Fig. 4 are the probability distributions for the photon difference number measured in the correct basis, for various values of transmission efficiency of the optical transmission channel. Assuming that Alice sent a logical 1, represented in this case by a mean difference number of +2400 (while –2400 would represent a logical 0), the distribution for zero loss is shown to be rather narrow and centered at +2400. As the loss increases, the distribution broadens and the mean decreases. The broadening is characteristic of sub-shot-noise light statistics, and enhances the detection of an eavesdropper. Any sampling by Eve is equivalent to a loss in transmission. The broadening of the distributions will result in overlap between the distributions for the logical 1 and

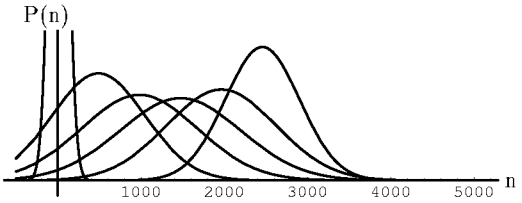

Fig. 4. The unnormalized probability distributions as a function of the photon difference number n for a logical 1 encoded in the correct basis from an OPA for different values of the transmission coefficient. The rightmost distribution is for 100% transmission, the distributions to the left are in order: 80, 60, 40, 20, and 0.1% transmission.

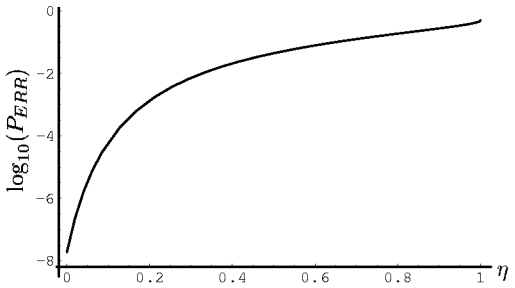

Fig. 5. Bob and Alice's bit error rate as a function of the loss η in the transmission channel for pulses generated by an OPA.

the logical 0. This overlap will lead to errors in Bob's measurement results. The error rate versus loss is shown plotted in Fig. 5. It increases steeply for losses near zero, and approaches unity with total loss of the pulse. Alice and Bob can make an estimate on the amount of eavesdropping (in the absence of other unknown transmission losses) which has occurred based on their error rate.

For the correlated semiconductor laser scheme, a common current is passed in series through two lasers having high quantum efficiency (photon emitted per electron injected). It has been shown in experiments that the difference of the photon fluxes from the two lasers has noise less than that from two independent lasers having Poisson photon number distributions [19, 20]. This is a consequence of the correlation between single electrons passing into a junction and a photon being emitted combined with the regulation of the current throughout the circuit. The intensity noise of each diode laser by itself is at or slightly below the SNL.

In Fig. 6 we show, for the case of correlated laser diodes, the calculated probability distributions for Bob's observed difference number for a 1 or 0 measured in the wrong basis. We use a mean total photon number of 128 with a standard deviation of $\sigma_{\mathrm{TOTAL}} = 12$, a mean photon difference number of ± 10 with a stan-

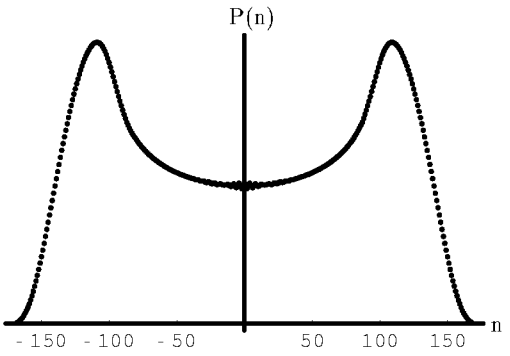

Fig. 6. The probability distribution for the photon difference number n in the wrong basis for pulses generated with correlated laser diodes.

dard deviation of $\sigma_{\mathrm{DIFF}} = 4$. We assume a Gaussian distribution for the total and difference photon numbers in the correct basis. These numbers correspond to a sub-SNL distribution in the photon difference number in the correct basis. We use standard beam splitter theory to determine the form of the distribution in the wrong basis [23, 24].

The features of the distributions for the photon difference number using pulses generated by the correlated laser diodes are similar to the distributions for the pulses generated by parametric amplification. The double-humped nature of the distribution in the wrong basis for the laser diodes does not seriously affect the security of the scheme. What is important is that the distribution in the wrong basis is independent of the bit value and wide compared to the distance between the mean values of the distributions for the different bit values in the correct basis.

4. Conclusions

We have shown that macroscopic pulses of light (containing of order one million photons) prepared in number-correlated states can be used to transmit efficiently key data with security that is enhanced by the quantum properties of light under measurement. The particular number of photons chosen for use depends on detector technology. Linear photodiodes coupled to charge-sensitive amplifiers may be used to detect the total number of photons in a pulse with duration in the ps or ns range with an uncertainty (set by dark noise) of around 200–300. A pulse with 10^6 photons will have a corresponding shot-noise level of 10^3, greater than the detector noise, allowing meaningful measurements to be made at or below the SNL [15]. Photon numbers much greater than a few millions will lead to detector saturation and possibly introduce classical sources of noise.

A challenging question to answer is whether the scheme is robust against all possible attacks by Eve. It seems plausible that a proof of absolute security could be derived for our scheme along the lines of that in Gottesman and Preskill's proof [12].

The technique has advantages relative to single-photon implementations regarding ease of source construction and immunity to low-level background light. A further advantage is the ability to encode more than one bit per pulse by using a multi level bit value represented by various values of photon difference number. Such a possibility has also been proposed in the context of QKD using quadrature-squeezed light, which is distinct from our proposal [11].

A disadvantage is that losses during transmission degrade the sub-SNL number correlations, leading to the need for increased levels of classical error correction, and the corresponding loss of efficiency.

Simple eavesdropping attacks, such as beam sampling or divide-measure-and--resend, have been shown to introduce sufficient noise or error for the legitimate parties to detect the eavesdropping. It remains to study the security against more general attacks.

Acknowledgments

We wish to thank John Preskill and Konrad Banaszek for helpful discussions. This material is based upon work supported by the National Science Foundation under Grant No. 9876608.

References

[1] O. Alter, Y. Yamamoto, *Phys. Rev. Lett.* **74,** 4106 (1995).

[2] O. Alter, Y. Yamamoto, *Quantum Measurement of a Single System*, Wiley, New York 2001.

[3] G. D'Ariano, H. Yuen, *Phys. Rev. Lett.* **76,** 2832 (1996).

[4] W. Wooters, W. Zureck, *Nature* **299,** 802 (1982).

[5] W. Vogel, H. Risken, *Phys. Rev. A* **40,** 2847 (1989).

[6] D. Smithey, M. Beck, M. Raymer, A. Faridani, *Phys. Rev. Lett.* **70,** 1244 (1993).

[7] C.H. Bennett, G. Brassard, in: *Proc. IEEE Int. Conf. on Computers, Systems and Signal Processing, Bangalore 1984*, IEEE, New York 1984, p. 175.

[8] D. Mayers, in: *Advances in Cryptology — Proceeding of Crypto '96*, Ed. N. Koblitz, Springer-Verlag, New York 1996, p. 343.

[9] P.W. Shor, J. Preskill, *Phys. Rev. Lett.* **85,** 441 (2000).

[10] H.-K. Lo, H. Chau, *Science* **283,** 2050 (1999).

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

[12] D. Gottesman, J. Preskill, *Phys. Rev. A* **63,** 022309 (2001).

[13] T.C. Ralph, *Phys. Rev. A* **62,** 062306 (2000).

[14] C.H. Bennett, S.J. Wiesner, U.S. Patent 5,515,438 (1996).

[15] D.T. Smithey, M. Beck, M. Belsey, M.G. Raymer, *Phys. Rev. Lett.* **69,** 2650 (1992).

[16] O. Aytur, P. Kumar, *Phys. Rev. Lett.* **65,** 1551 (1990).

[17] G. Björk, *Phys. Rev. A* **45,** 8259 (1992).

[18] A. Heidmann, R. Horowicz, S. Reynaud, E. Giacobino, C. Fabre, G. Camy, *Phys. Rev. Lett.* **59,** 2555 (1987).

[19] P. Edwards, G. Pollard, *Phys. Rev. Lett.* **69,** 1757 (1992).

[20] E. Goobar, A. Karlsson, G. Björk, *Phys. Rev. Lett.* **71,** 2002 (1993).

[21] B. Mollow, R. Glauber, *Phys. Rev.* **160,** 1097 (1967).

[22] E. Arthurs, J. Kelly, *Bell Syst. Tech. J.* **45,** 725 (1965).

[23] U. Leonhardt, *Measuring the Quantum State of Light*, Cambridge University Press, Cambridge 1997.

[24] R. Campos, B.E.A. Saleh, M.C. Teich, *Phys. Rev. A* **40,** 1371 (1989).