JOURNAL OF MODERN OPTICS, 2001, VOL. 48, NO. 14, 2055–2063

# Letter

# Performance of photon-pair quantum key distribution systems

Z. WALTON,† A. V. SERGIENKO,†‡ M. ATATÜRE,‡
B. E. A. SALEH,† and M. C. TEICH†‡

† Quantum Imaging Laboratory, Department of Electrical and Computer Engineering, Boston University, 8 Saint Mary's Street, Boston, Massachusetts 02215, USA

‡ Department of Physics, Boston University, 8 Saint Mary's Street, Boston, Massachusetts 02215, USA

(*Received 3 April 2001; revision received 5 May 2001*)

**Abstract.** We analyse the quantitative improvement in performance provided by a novel quantum key distribution (QKD) system that employs a correlated photon source (CPS) and a photon-number resolving detector (PNR). Calculations suggest that given current technology, the CPS/PNR implementation offers an improvement of several orders of magnitude in secure bit rate over previously described implementations.

## 1. Introduction

While much progress has been made in the field of experimental quantum key distribution (QKD) since the first proof-of-principle in 1992 [1], the failure of the experimental community to choose a well-defined scope for the technological power of the eavesdropper has made comparing the competing implementations difficult. Specifically, the mean number of photons per pulse is arbitrarily set at approximately 0.1 photons per pulse by most groups. There are two problems with operating the source at this power. First, since this mean value is not determined by maximizing the appropriate figure of merit (i.e. secure bits per pulse), each implementation must be assumed to be operated at a suboptimal point in the parameter space, making it difficult to quantify the performance advantage enjoyed by one system over another. Second, recent work has shown that the choice of 0.1 photons per pulse makes all existing weak coherent pulse implementations insecure to an eavesdropper armed with foreseeable, though not presently available, technology [2]. Gilbert and Hamrick previously calculated the optimal mean number of photons per pulse in their comprehensive analysis [3] incorporating many practical considerations relevant to experimental weak coherent pulse quantum cryptography.

In this paper, we combine reported experimental results in the literature with a specific scope for the eavesdropper and Lütkenhaus' fully secure version [4] of the BB84 protocol [5] to determine which of three physical implementations provides the best performance for free-space and optical fibre applications. The first two

*Journal of Modern Optics* ISSN 0950–0340 print/ISSN 1362–3044 online © 2001 Taylor & Francis Ltd
http://www.tandf.co.uk/journals
DOI: 10.1080/09500340110067671

implementations, based on weak coherent pulses (WCP) and correlated photon sources (CPS) respectively, have been investigated elsewhere [2]; the third implementation (CPS/PNR) is a new design that combines the perfect photon-number correlation in spontaneous down conversion [6] with photon-number resolving detectors (PNR) [7, 8] to reduce the effect of the multi-photon security loophole. Calculations indicate that this novel design offers a substantial advantage over the competing implementations, mainly because of its closer approximation to the true single-photon state.

Most reports of the performance of specific QKD systems either ignore the vulnerability of the system to eavesdropper attack or provide special-case analyses in which the information accessible to an eavesdropper employing a specific attack is estimated. This runs counter to the fundamental paradigm of quantum cryptography. While conventional public-key cryptosystems are based on unproven propositions of theoretical computer science and can only be used against an adversary who has limited computational power, quantum cryptography promises unconditional security *regardless* of the technological capabilities of the adversary. Thus, candidate QKD systems should be evaluated in this context.

Our analysis places no technological limitations on the eavesdropper (Eve) except that she attacks each pulse individually. Although it is not yet proven, it it widely believed that restricting Eve to individual attacks does not prevent her from performing the optimal attack. The essence of the argument is that Eve's techniques for learning information about any two pulses are in no way restricted by requiring her to gain information from each separately, since the two parties (Alice and Bob) are attempting to share a random bit string in which any two bits are completely uncorrelated.

## 2. The figure of merit: secure bits per pulse

The existence of classical privacy amplification algorithms for distilling arbitrarily secure bits from partially secure bits means that it is not necessary to have complete security for each pulse. As long as a bound on the information leaked to the adversary can be inferred from measurable quantities, such as the observed error rate, Alice and Bob can recover a perfectly secure, shared key by a two-step procedure. They first use traditional error-correcting methods to ensure they have the same key, and then use the technique of generalized privacy amplification [9] to extract a shorter secure key from a longer key. Thus, the crucial figure of merit for QKD implementations is the fraction of the raw bits shared by Alice and Bob that may be kept, such that they are certain that they share the same key and that Eve has negligible information about that key.

This fraction, labelled $G$ for gain, depends on four factors: the observed error rate ($\bar{\epsilon}$), the probability that Alice's detector-triggered source indicates that a valid signal was created ($p_s$), the probability that Alice sends a multi-photon pulse ($S_m$), and the probability that a pulse sent by Alice leads to a successful detection by Bob ($p_{exp}$). The dependence of $G$ on $\bar{\epsilon}$ for the BB84 protocol faced with the aforementioned adversary was determined by C. Fuchs *et al.* in 1997 [10]; however, the more crucial dependence of $G$ on $p_s$, $S_m$, and $p_{exp}$ has only recently been determined by Lütkenhaus [4]. Combining these two analyses, we have

$$G(\bar{\epsilon}, p_s, S_m, p_{exp}) = \tfrac{1}{2} p_s p_{exp} \{ -R_1 \log_2 [\tfrac{1}{2} + 2\bar{\epsilon} R_1 - 2(\bar{\epsilon} R_1)^2] + 1.35 [\bar{\epsilon} \log_2 \bar{\epsilon} + (1 - \bar{\epsilon}) \log_2 (1 - \bar{\epsilon})] \},$$

where $R_1 = (p_{exp} - S_m)/p_{exp}$. It should be noted that for this derivation of $G$, the most conservative approach to the imperfections in Bob's apparatus has been used: Eve has complete control over all of the errors, photon losses, background, and dark counts that occur in the optical channel *and* in Bob's detection unit. If it is assumed that Eve cannot control the imperfections in Bob's apparatus, the fraction $G$ increases; however, it is difficult to prove exactly which aspects of Bob's apparatus Eve may or may not be able to influence. Thus, it seems prudent to assume the worst case, as we have done here.

## 3. Three QKD source designs

A complete QKD implementation consists of the physical apparatus and a protocol which specifies how the apparatus should be operated, and which provides probabilistic statements that characterize the outcome (i.e. with probability $\epsilon$, Eve's guess at the secret key will be correct in more than half of the bits). Since BB84 is the only protocol for which there exists an agreed-upon method for calculating $G(\bar{\epsilon}, p_s, S_m, p_{exp})$ in the face of our adversary [4], we use this protocol exclusively in comparing the performance of the three implementations: WCP, CPS, and CPS/PNR.

The physical apparatus required for the BB84 protocol can be conveniently partitioned into the single-photon source, the optical channel, and the detection unit. Several single-photon source technologies are being considered for use in a complete QKD system. Before presenting the results of our calculations, we summarize the qualitative advantages and disadvantages of the three leading single-photon-source technologies.

### 3.1. *Weak coherent pulse (WCP)*

The simplest and most common method of reducing the probability of a multi-photon pulse is to attenuate a weak coherent pulse (WCP) of light from a laser (see figure 1 (*a*)). Since a partitioned Poisson random variable still exhibits Poisson statistics, Alice must adjust the mean photon number per pulse in order to strike a balance between two undesirable effects: the wasteful zero-photon pulses and the insecure multi-photon pulses. Once the pulse is created, Alice and Bob may use standard optical components to modify, launch, transmit, collect and measure the polarization of the optical pulse. Since the different sources we consider work equally well with the other parts of the complete QKD apparatus, we leave these aspects of the apparatus unspecified and base our calculations on values for optical coupling efficiency, error probabilities, and detector performance reported in the literature [11–13].

### 3.2. *Correlated photon source (CPS)*

In the paper that reveals the complete insecurity of current WCP implementations [2], Brassard *et al.* investigate the ability of a detector-triggered source based on spontaneous parametric down conversion (SPDC) to mitigate the multi-photon security loophole (see figure 1 (*b*)). The perfect correlation in photon

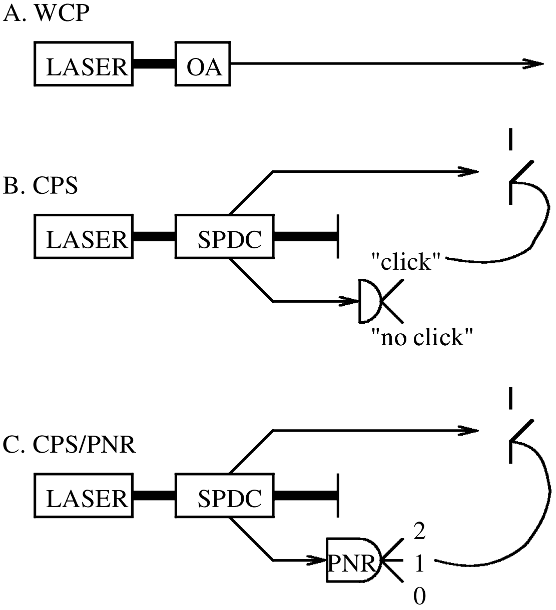

Figure 1. Three QKD source designs. In A, a weak coherent pulse (WCP) from a laser source is optically attenuated (OA) to a mean photon number much less than one (the polarization rotator necessary for implementing the BB84 protocol is not shown). Both B and C are detector-triggered sources based on spontaneous parametric down conversion (SPDC) in which Alice allows the pulse in the signal beam to propagate to Bob only if her detector indicates that one photon arrived in the idler beam. In B the idler beam is monitored with a standard 'click'/'no click' detector. In C, the idler beam is monitored with a photon-number resolving detector (PNR), which can discriminate between single- and double-photon arrivals. By not using the pulses that she determines contain multiple photons, Alice significantly improves the secure bit rate and extends the range of tolerable channel loss.

number in the signal and idler beams allows Alice to run the protocol only when her detectors on the idler beam indicate that one photon was sent to Bob along the signal beam. While this implementation of the correlated photon source (CPS) extends the range of permissible channel losses several orders of magnitude from that allowed in the WCP case [4, 2], the Poisson statistics for the number of pairs per pulse [14] combined with the inability of standard detectors to distinguish single- and multi-photon detection events lead to a persistence of the insecure multi-photon pulses.

### 3.3. *Correlated photon source with a photon-number resolving detector* (*CPS*/*PNR*)

To minimize the chance that Alice registers a valid signal when more than one pair was created, we place a photon-number resolving detector in Alice's laboratory. In our calculations we use the characteristics of the photon-number resolving detector reported in [8], since this device is representative of the state-of-the-art. While this detector has a finite quantum efficiency of approximately 70%, the gain mechanism ensures that the device can distinguish the number of photoelectron-multiplication events with very low error (~0.63%). The relatively high dark count rate ($\sim 10^4$ counts per second) can be effectively mitigated by limiting the detector's exposure time by nanosecond gating. By initiating a pulse transmission only when the detector reports one photon arriving, Alice significantly reduces the fraction of pulses sent to Bob that contain more than one photon.

The difficulties with this approach stem from the extreme conditions necessary for the PNR to provide such high efficiency and low multiplication noise. The actively controlled, bath-type He cryostat required for optimal performance [8] precludes miniaturization of the source and complicates the task of creating a QKD implementation that is reliable, durable, and economically feasibly for real-world applications. Nonetheless, our simulations indicate that, in achieving a closer approximation to the true single-photon source, the CPS/PNR implementation provides an option for obtaining a secure link for certain applications in which existing implementations provide negligible gain.

## 4. Examples

We calculated the performance of the three implementations over both free space and fibre-optic channels using values for optical coupling efficiency, error probabilities, and detector performance reported in the literature [11–13]. In each case the performance was determined by maximizing $G$ over the power of the original laser pulses that are either attenuated (WCP) or down-converted (CPS and CPS/PNR) to create the pulse. It is this crucial step that most experimental groups have ignored, leading to mean photon numbers that are orders of magnitude away from optimality and to unrealistic claims concerning secure bit rates. While the experiments have been performed at specific distances, the predicted gain is extrapolated over a range of distances by reasoning that the dependence of $G$ on distance is dominated by absorption in optical fibres and diffraction in a free-space link.

As graphed in figures 2 and 3, each of the curves stops at a specific distance along the $x$-axis and fails to descend off the bottom of the plot, suggesting that there may be valid operating points with gain beyond the end of the curve. It should be understood that the true shape of these curves is nearly vertical at the cut-off distance—the plot fails to convey this steep drop-off because the numerical sampling algorithm used by the plotting program is not fine enough to show the curves' continuity.

### 4.1. *Free-space QKD*

### *Ground-to-ground link*

Figure 2 (*a*) shows the relative performance of the three implementations along the surface of the Earth under nighttime conditions. The values of the gain at $d = 1$ km (i.e. WCP $\rightarrow 5.6 \times 10^{-4}$, CPS $\rightarrow 1.5 \times 10^{-4}$, and CPS/PNR $\rightarrow 4.2 \times 10^{-3}$) represent the actual values that could be achieved using the experimental apparatus reported by Buttler *et al.* for signal launch, collection, and detection [13]. Thus, using a base repetition rate of 100 MHz, the CPS/PNR implementation offers a 400 kbit/s perfectly secure channel. The rate of this channel is approximately one order of magnitude greater than that offered by the WCP and CPS implementations. The most dramatic feature in figure 2 (*a*) is the precipitous decline of the WCP gain around 2 km. The persistence of the CPS and CPS/PNR curves beyond 10 km suggest

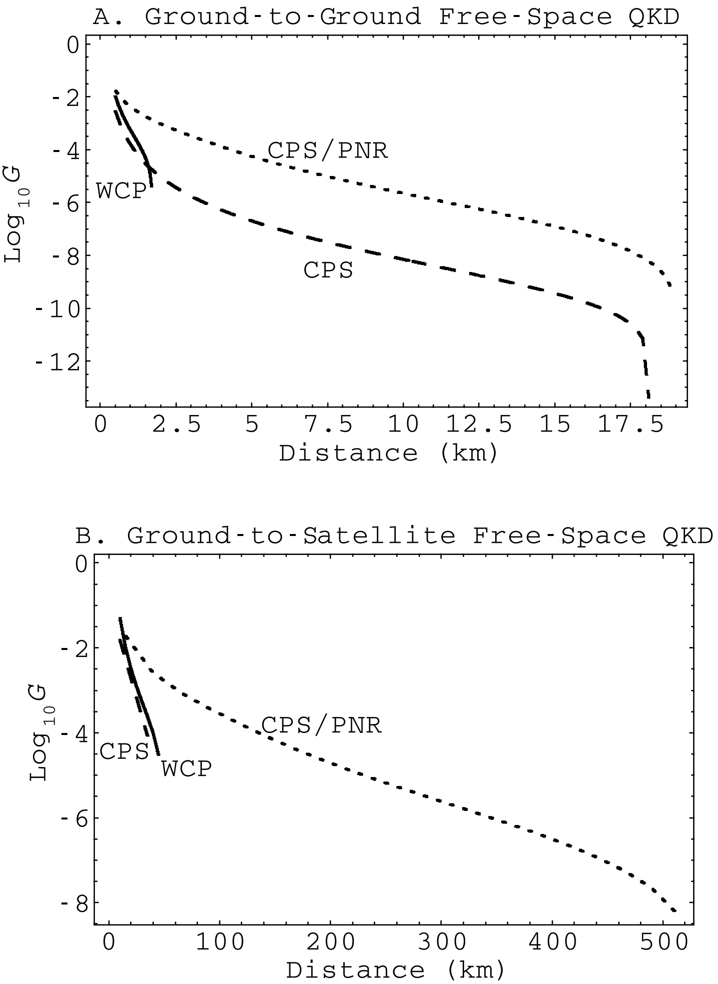

Figure 2. Free-space QKD in ground-to-ground (A) and ground-to-satellite (B) configurations for the three source designs of Section 3. The gain G represents the number of perfectly shared, secure bits, per pulse. Note the different scales in A and B. The values at 1 km in A and 300 km in B are based on the parameters for channel loss, error, and background reported in [13]. The gain at all other distances is calculated by assuming that the optical coupling efficiency varies as $1/d^2$ as a result of beam diffraction, where $d$ is the distance of the transmission.

that a detector-triggered source would be required for secure communications in a metropolitan area or battlefield, while the WCP would be sufficient for close proximity, building-to-building applications.

### *Ground-to-satellite link*

In [13], Buttler *et al.* provide rough estimates of the optical coupling efficiency and background rates in a ground-to-satellite QKD application. Using these estimates, we have simulated the gain achievable with each implementation for a range of low-Earth orbit altitudes (see figure 2(*b*)). The apparent discrepancy between figure 2(*a*) and figure 2(*b*)—both describe free-space implementations,

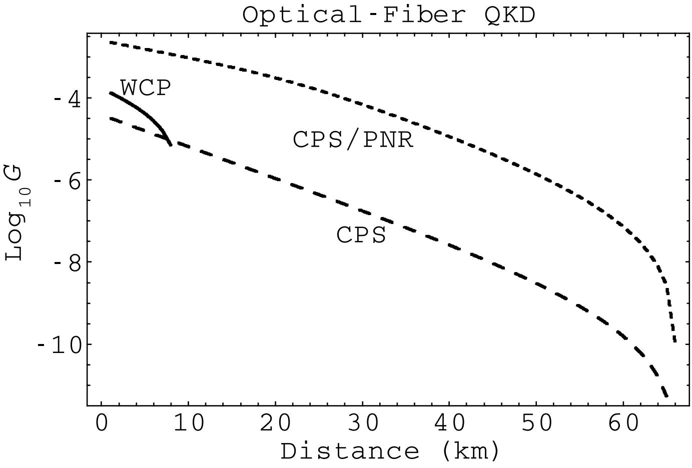

Figure 3. Gain through an optical fibre for the three source designs of section 3. Transmission wavelength is set at the second telecom window (1.3 μm) to achieve low loss (0.38 dB/km) and to optimize detector performance (the detectors used had quantum efficiency 0.11 and $10^{-5}$ dark counts per pulse duration). Detector-triggered sources (i.e. CPS and CPS/PNR) use idler beams at 0.8 μm where detectors have higher efficiency and lower noise. Calculations are based on the experimental values provided in [11, 12]. Note that the scales differ from those in figure 2.

yet figure 2 (*b*) shows gain far past the 20-km cutoff of figure 2 (*a*)—is understood by observing that all but the lowest 2 km of the ground-to-satellite link is turbulence-free vacuum. Our results indicate that while the WCP and CPS implementations offer no secure communication at standard low Earth orbit altitudes (~100 km), the CPS/PNR implementation could enable the exchange of approximately $10^3$ secret bits for each nighttime exchange (assuming a 10 MHz repetition rate, a 300 km orbit, and several minutes line-of-sight exposure between the ground station and the satellite).

A complicating factor in these estimates is that the satellite altitude determines the velocity necessary to remain in orbit. While a very low orbit would allow increased gain, the amount of time that the satellite spends in sight of the ground station would be reduced, decreasing the total number of secret bits shared in one pass. It seems reasonable to delay a determination of the optimal satellite altitude until the exact characteristics of each element in the proposed communication system are established.

### 4.2. *Optical fibre QKD*

Figure 3 confirms the conclusion of [2, 4]: the detector-triggered source offers gain far beyond the ~10 km cutoff distance of the WCP implementation through optical fibre. Unlike these papers which focused entirely on 'click'/'no click' detectors in Alice's source, our results indicate the considerable increase in gain offered by photon-number resolving detectors. Comparing figure 3 to figure 2 (*a*), it is clear that fibre-based QKD offers performance superior to that of free-space QKD, and is the obvious choice for long-distance ground-to-ground applications, as a result of its immunity from diffraction, background light, cloud cover, and temperature-dependent turbulence. However, given current technology, ground-to-satellite free-space QKD with a CPS/PNR source appears to be the preferred option for implementing a global, secure network.

## 5. Discussion

We have calculated the performance currently attainable with QKD systems through free-space and optical fibres, for three different source designs, in the face of an unrestricted adversary who attacks each pulse individually. Results indicate that the implementation based on a correlated photon source (CPS) offers the best performance, as a result of the potentially unlimited precision in identifying the presence of a single photon. Furthermore, while using a detector-triggered source extends the range of a QKD system, exploiting the photon-number resolving capabilities of a photon-number resolving detector (PNR) to decrease the fraction of multi-photon pulses provides a further increase of several orders of magnitude in $G(\bar{\epsilon}, p_s, S_m, p_{exp})$, as seen in figures 2 and 3. It is concluded that future progress in practical QKD will come largely from advances in detector performance and in the attendant improvement in the detector-triggered single-photon source.

A summary of these calculations is as follows. Using a base repetition rate of 100 MHz for the pump laser, the CPS/PNR implementation provides a 400 kbit/s secure channel over 1 km of free space, 100 bit/s over 50 km of optical fibre, and 100 bit/s to a satellite in low earth orbit. The two competing implementations provide at best only 50 kbit/s over 1 km of free space, 1 bit/s over 50 km of optical fibre, and cannot safely communicate with a satellite at any rate.

More accurate estimates of the dependence of free-space QKD performance on source characteristics and on the communication distance $d$ can be obtained by applying existing analyses of atmospheric effects on optical signals [15, 16, 3].

Finally, we mention a subtle issue in quantum cryptography that has not, to our knowledge, been analysed: the role of Alice's and Bob's prior distribution on the error rate ($\bar{\epsilon}$) that Eve effects by her eavesdropping. In their attempts to determine $\bar{\epsilon}$, Alice and Bob can only use the revealed outcome of a subset of the total transmission record to update an *a priori* distribution over $\bar{\epsilon}$ to an *a posteriori* distribution over $\bar{\epsilon}$ via Bayes' rule. While most practical analyses choose the uniform distribution over $\bar{\epsilon}$ as the *a priori* distribution, Eve can obviously use any distribution she likes to choose the value of $\bar{\epsilon}$. Thus, it seems likely that a more sophisticated game-theoretic analysis would be required to plug this '*a priori* distribution loophole'.

## Acknowledgments

Z. W. thanks M. Dusek and N. Lütkenhaus for useful conversations. This work has been supported by DARPA and the National Science Foundation.

## References

[1] BENNETT, C. H., BESSETTE, F., BRASSARD, G., SALVAIL, L., and SMOLIN, J., 1992, *J. Cryptol.*, **5**, 1.
[2] BRASSARD, G., LÜTKENHAUS, N., MOR, T., and SANDERS, B. C., 1999, Eprint quant-ph/9911054.
[3] GILBERT, G., and HAMRICK, M., 2000, Eprint quant-ph/0009027.

[4] Lütkenhaus, N., 1999, *Acta Phys. Slovaca*, **49,** 549; quant-ph/9910093.
[5] Bennett, C. H., and Brassard, G., 1984, in *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing*, Bangalore, India (IEEE, New York), p. 175.
[6] Sergienko, A. V., Atatüre, M., Walton, Z., Jaeger, G., Saleh, B. E. A., and Teich, M. C., 1999, *Phys. Rev.* A, **60,** R2622.
[7] Teich, M. C., Matsuo, K., and Saleh, B. E. A., 1986, *IEEE Trans. Electr. Dev.*, **ED-33,** 1475.
[8] Kim, J., Takeuchi, S., and Yamamoto, Y., 1999, *Appl. Phys. Lett.*, **74,** 902.
[9] Bennett, C. H., Brassard, G., Crépeau, C., and Maurer, U. M., 1995, *IEEE Trans. Inf. Theory*, **41,** 1915.
[10] Fuchs, C. A., Gisin, N., Griffiths, R. B., Niu, C.-S., and Peres, A., 1997, *Phys. Rev.* A **56,** 1163.
[11] Marand, C., and Townsend, P. T., 1995, *Opt. Lett.*, **20,** 1695.
[12] Townsend, P. T., 1998, *IEEE Phot. Tech. Lett.*, **10,** 1048.
[13] Buttler, W. T., Hughes, R. J., Kwiat, P. G., Lamoreaux, S. K., Luther, G. G., Morgan, G. L., Nordholt, J. E., Peterson, C. G., and Simmons, C. M., 1998, *Phys. Rev. Lett.*, **81,** 3283.
[14] Larchuk, T. S., Teich, M. C., and Saleh, B. E. A., 1995, *Ann. N. Y. Acad. Sci.*, **755,** 680.
[15] Diament, P., and Teich, M. C., 1970, *J. Opt. Soc. Am.*, **60,** 1489.
[16] Teich, M. C., and Diament, P., 1989, *J. Opt. Soc. Am.*, A, **6,** 80.