Eur. Phys. J. D **18**, 147–153 (2002)
DOI: 10.1140/epjd/e20020018

THE EUROPEAN PHYSICAL JOURNAL D
EDP Sciences

Quantum key distribution using quantum-correlated photon sources

P.J. Edwards[a], G.H. Pollard, and W.N. Cheung

Advanced Telecommunications and Quantum Electronics Research Centre, University of Canberra, Canberra ACT 2601, Australia

Received 14 July and Received in final form 20 November 2001

Abstract. Quantum key exchanges using weak coherent (Poissonian) single-photon sources are open to attack by a variety of eavesdropping techniques. Quantum-correlated photon sources provide a means of flagging potentially insecure multiple-photon emissions and thus extending the secure quantum key channel capacity and the secure key distribution range. We present indicative photon-counting statistics for a fully correlated Poissonian multibeam photon source in which the transmitted beam is conditioned by photon number measurements on the remaining beams with non-ideal multiphoton counters. We show that significant rejection of insecure photon pulses from a twin-beam source cannot be obtained with a detector having a realistic quantum efficiency. However quantum-correlated (quadruplet or octuplet) multiplet photon sources conditioned by high efficiency multiphoton counters could provide large improvements in the secure channel capacity and the secure distribution range of high loss systems such as those using the low earth orbit satellite links proposed for global quantum key distribution.

PACS. 03.67.Dd Quantum cryptography – 02.50.Fz Stochastic analysis – 42.50.Lc Quantum fluctuations, quantum noise, and quantum jumps

1 Introduction

Current quantum key distribution systems commonly employ weak Poissonian laser and light- emitting diodes as quasi single-photon sources. However it is well known that such systems are susceptible to "intercept/resend", "beam-splitter" and "photon number splitting" attacks [1–3]. If the transmitted key bits contain two or more photons, a hypothetical Eve, constrained only by the laws of physics and not by the realities of contemporary technology could gain significant Shannon information without disturbing the quantum channel and so compromise the security of the key.

In lossy systems such as those employing low earth orbit satellites as key couriers, it is generally recognised that the key exchange will be totally insecure if the number of transmitted multiple photon signals exceeds the number of received single photon signals [3]. For the weak coherent (Poissonian) photon sources currently used this leakage of Shannon entropy increases with the mean photon number $\langle n \rangle$, which must therefore be kept small in order to maintain secure key exchange over a lossy channel. In consequence the probability of single photon emission, and therefore the transmission efficiency, will be correspondingly small, most pulses being empty of photons. For example for a multiple-photon "leakage" probability $L = P(n > 1) \approx \langle n \rangle^2/2 < 0.005$, the single photon probability $S = P(n = 1) \approx \langle n \rangle < 0.1$, is unavoidably low, and the "no photon" probability $P(n = 0) \approx (1 - \langle n \rangle) > 0.9$, unavoidably high. This enforced trade between potential entropy leakage (multiple-photon probability) and channel efficiency (single-photon probability) becomes even more unfavourable at low single-photon efficiencies when the bit error rate due to background photons and dark counts further restricts the secure key bit transfer rate.

Improved methods of single-photon generation for which the single photon probability S and the ratio S/L are both higher than for Poissonian sources are currently under active investigation [4–8].

We recently proposed [9] a novel scheme based on an extension of the correlated twin beam concept [10–12] in which one of two quantum-correlated beams formed by parametric down conversion (PDC) is used to condition the other beam [3]. Our conditional single-photon generating scheme requires strong photon number-correlations between a *multiplet* of spatially separated beams each of which is monitored by a high efficiency multiphoton counter capable of differentiating between single-photon and multiple-photon pulses [12–14].

Multiple-photon events are detected and either deleted during the quantum key transmission or else subsequently discarded in the error correction and privacy amplification dialogue following the transmission. Although not yet demonstrated in the laboratory, a possible

[a] paule@ise.canberra.edu.au

realisation might be a tandem array of two or more quantum wells, microcavities, or quantum dot light-emitters [15]. This would represent an extension to the mesoscopic scale of the strong quantum correlation observed between the bright beams emitted from arrays of macroscopic semiconductor junction light-emitting diodes and diode lasers when these are electrically coupled together [15–20].

We first briefly review the limitations of an unconditioned Poissonian photon source. We then obtain indicative statistics for a fully correlated multiplet photon source conditioned by one or more high quantum efficiency noiseless photon counters.

2 Single Poissonian photon beam

Consider an ideal semiconductor light-emitting diode or ideal laser diode driven by a periodic train of identical current pulses. These generate a train of weak light pulses each of which contains a Poisson-distributed number of photons, with the same mean photon number per pulse $\langle n\rangle$. This is a typical realisation of a quasi-single-photon QKD source.

For later comparison with the conditioned multiple beam statistics we note the Poisson probability that a pulse will contain exactly n photons is

$$P(n) = [\langle n\rangle^n/(n!)]\exp(-\langle n\rangle), \tag{1}$$

so that:

$$N_1 = P(0) = \exp(-\langle n\rangle) \approx (1 - \langle n\rangle); \tag{2}$$

$$S_1 = P(1) = \langle n\rangle \exp(-\langle n\rangle) \approx \langle n\rangle; \tag{3}$$

$$L_1 = P(>1) = 1 - (1 + \langle n\rangle)\exp(-\langle n\rangle) \approx \langle n\rangle^2/2; \tag{4}$$

where the approximations refer to small mean numbers, $\langle n\rangle \ll 1$.

Figure 1 shows the variation of N, S, L and L/S with $\langle n\rangle$. Note that while the maximum value of the single photon probability $S = 1/\mathrm{e} = 0.37$ for $\langle n\rangle = 1$, such a high value of $\langle n\rangle$ is unusable because of the correspondingly high leakage probability of multiple photons, $L = 0.26$. Each multiple photon pulse carries a potentially insecure bit which can in principle be intercepted and copied clandestinely. The ratio S/L is therefore one convenient parameter to characterise the quality of a single-photon generator.

A conservative and necessary (but not sufficient) condition for the secure exchange of a key is that the number of multiple bits available for covert copying by an eavesdropper at the transmitter must not exceed the number of single photon reaching the receiver [3].

For single-photon channel transmission probability η_T, this means that $\eta_\mathrm{T}P(n = 1) > P(n > 1)$, or $\eta_\mathrm{T}S/L > 1$. A conservative lower limit for the parameter S/L required for secure key exchange over a lossy channel is then the channel attenuation $(1/\eta_\mathrm{T})$. A convenient figure of merit (Q_s) for a single-photon quantum key source

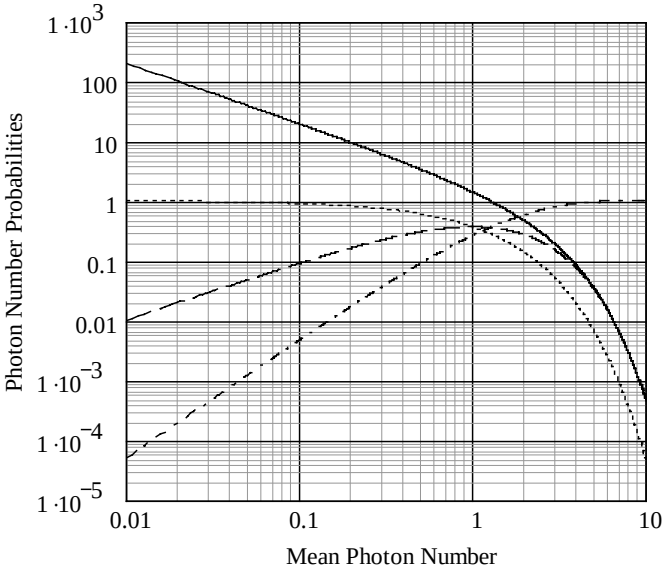

Fig. 1. Unconditioned Poissonian photon source: $S/L = P(1)/P(>1)$ (solid curve); empty pulse probability, $P(0)$ (dotted curve); single photon probability, $P(1)$ (dashed curve); multiple photon probability $P(>1)$ (dot-dashed curve).

is the product of the maximum permissible secure channel loss $(1/\eta_\mathrm{T} = S/L)$ and the single-photon transmitter efficiency, S:

$$Q_\mathrm{s} = S^2/L. \tag{5}$$

Evidently S/L must certainly exceed 1, corresponding to a lossless channel with ideal photon detection. Reference to equations (1–4) and Figure 1 shows that this limits $\langle n\rangle$ to values less than 1.33 for a secure lossless, ideal noiseless Poisson channel. Practical lossy channels necessitate much higher values of S/L. These can only be achieved by greatly reducing the value of $\langle n\rangle$ and so sacrificing transmitter efficiency. In the limit of small $\langle n\rangle \ll 1, S = \langle n\rangle$, $S/L = 2/\langle n\rangle$ and $Q_\mathrm{s} = 2$. A channel loss $(1/\eta_\mathrm{T})$ of greater than 100 (20 decibels) therefore restricts S to less than 0.02. Secure key transfer is thus achieved at the cost of low channel efficiency. The minimum tolerable channel transmission factor is,

$$\eta_\mathrm{T}(\min) = L_1/S_1 = P(n > 1)/P(n_1 = 1) = [\exp(\langle n\rangle) - (1 + \langle n\rangle)]/\langle n\rangle \cdot \tag{6}$$

From equation (6) above, since $L_1/S_1 \approx \langle n\rangle/2$ for small $\langle n\rangle$, the corresponding secure BB84 [21] Poisson channel efficiency is then,

$$\varepsilon(\max) \approx \eta_\mathrm{T}(\min)\langle n\rangle/2 = \langle n\rangle^2/4 = \eta_\mathrm{T}^2(\min). \tag{7}$$

A single-mode fibre QKD channel with an attenuation of, say, 0.5 dB/km (a conservative estimate of the loss encountered in public switched optical networks operating at long wavelengths) can therefore be no longer than

$$R = 20\log_{10}(1/\eta_\mathrm{T}(\min)) = 10\log_{10}(1/\varepsilon), \tag{8}$$

with R in km and $\varepsilon = \langle n \rangle^2/4$, the corresponding secure channel efficiency for noise-free key exchange using the BB84 protocol.

For secure QKD systems operating with $\langle n \rangle = 0.1$, the maximum permissible channel loss is then only 13 dB, corresponding to a noiseless BB84 Poisson channel efficiency, ε of less than 0.0025 bits per transmitted symbol.

It is apparent that this severely limits the efficiency and therefore the (bit rate) capacity of a secure lossy channel. In practice the efficiency and capacity will be significantly lower because of the need to discard erroneous bits and to institute privacy amplification in order to maintain security in the presence of thermal and background photon counting noise.

Earth satellite − based QKD systems have been proposed [23] in which the channel attenuation is typically greater than 30 dB ($\eta_T < 10^{-3}$). The corresponding secure channel efficiency (ε) will then (from Eq. (7)), be less than 10^{-6}, even assuming ideal detection.

It has been argued that the physical security associated with "line of sight" systems of this kind allow the condition expressed in equation (6) to be relaxed [24]. Other authors [3] argue that the security of quantum key systems should be guaranteed by the laws of physics, rather than by physical circumstances and current technology. If this latter view is accepted, the capacity of Poissonian channels will be limited so severely by equations (6–8), that they are unlikely to be useful for any purpose other than low loss, low capacity, short range quantum key distribution. Single photon sources employing single quantum dots, and diamond colour centres are therefore being developed [4–8] with reported S/L ratios approaching 10^2.

3 Conditional single-photon sources

Considerations such as those above indicate the desirability of realising photon transmitters for which the ratio $L/S = P(n > 1)/P(n = 1)$ is much lower and the figure of merit $Q_s = S^2/L$ is much higher than that for Poissonian sources. Ideally such sources should emit only single photons on demand.

In what follows, we shall examine the potential gains in secure channel capacity and range to be had from the use of conditioned single photon sources in a quantum key transmitter. For simplicity we shall assume fully correlated Poissonian photon sources, each with the same mean emission rate. As we shall show, conditioned twin-beam sources suffer from the disadvantage that an unrealistically high quantum detector efficiency is required. However, one can take advantage of the repeated measurement of photon number provided by a larger array to improve the identification (and subsequent rejection) of multiple-photon signals.

In the following sections we discuss one method of achieving this based on quantum- correlated multiple beams. The relative probability (L/S) of insecure multiple-photon signals is strongly suppressed and the figure of merit Q_s is raised above the Poissonian values by a conditioning process, allowing secure quantum keys to be exchanged over longer distances at higher rates.

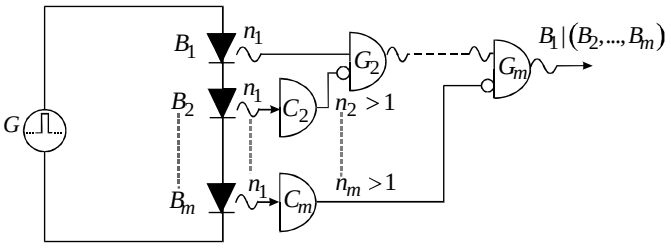

Fig. 2. Representation of conditional single-photon multiplet m-beam source conditioned by $(m-1)$ multiphoton counters C_2, C_3, ...C_m coupled to correlated beams $B_2, B_3, ..., B_m$. Logic gates G_2, G_3, ..., G_m represent the rejection of photon pulses from B_1 if $n_2 > 1$, or $n_3 > 1$, ..., or $n_m > 1$.

The process is shown schematically in Figure 2. Quantum-correlated photon emitters $B_1, ..., B_m$ are shown electrically connected together and driven by repetitive pulse generator G. The transmitter beam, B_1, is coupled to a modulating device before being launched into an optical fibre or free-space. If each transmitted pulse (from B_1) contains n_1 photons then for fully correlated beams the same photon number n_1 will be replicated at $B_2, ..., B_m$ and will be separately counted by the $(m-1)$ noiseless multiphoton counters C_2 through C_m, each with the same quantum efficiency (single-photon counting efficiency), η. For simplicity we assume that n_1 is a Poisson variable. It then follows that photon counts $n_2, n_3, ., n_m$ are also Poissonian with the same mean $\langle n_j \rangle = \eta \langle n_1 \rangle$ for $j = 2, ..., m$.

Figure 2 shows the logic of this conditioning process in which gate G_2 is closed if $n_2 > 1$, gate G_3 is closed if $n_3 > 1$,..., and gate G_m is closed if $n_m > 1$. If any one of the $(m-1)$ independent counts n_2 through n_m exceeds 1, the corresponding pulse is removed from the sequence of photon pulses from B_1, leaving the conditioned sequence $\{B1|(B_2, ..., B_m)\}$ available for the key exchange. A photon pulse from B_1 will pass through all gates and be included in the key transfer only if the counters register either one photon per pulse or none. The logic gates do not necessarily represent physical devices or operations although these are certainly not excluded. Insecure pulses can therefore be identified and removed prior to transmission or subsequently discarded in the post key transmission dialogue.

The multiple beams generated by tandem arrays of macroscopic semiconductor junctions are generally sub-Poissonian [16] while PDC twin beams have excess number variance. In order to simplify the analysis we assume Poissonian source statistics so that the analysis is "worst case" in this respect.

We also assume noiseless detection. This latter assumption is realistic in that a state-of-the-art multiphoton detector such as the visible light photon counter [14] has nanosecond resolution and a dark count of order 10^4 s^{-1}. The noise count in any one detector will then be of order 10 s^{-1} for a pulse repetition rate of 10^6 s^{-1}, typically less than 0.01% of the single photon counting rate. The effects

of noise on both Alice's and Bob's detectors can thus be minimised, as in other single-photon systems, by precise time-gating.

Our third simplifying assumption will be to assume multiphoton counters characterised by a single parameter, the single-photon counting "quantum" efficiency, η. With this assumption the two-photon counting efficiency is η^2, the N-photon counting efficiency is η^N and the photon counts remain Poissonian. Coupling efficiencies will generally be less than 100%. In our calculations we have therefore used external single-photon detection efficiencies as low as 50%. In later examples (shown in Figs. 5 and 6), we have taken $\eta = 0.875$ [13], corresponding to an ideal two-photon counting efficiency of 0.77. This latter figure is somewhat higher than the external two-photon counting efficiency currently achieved [14] so it should be regarded as an upper limit. Note that the correlated photons emitted from different junction in Alice's semiconductor multiplet source may have different wavelengths. Thus, the wavelength of the transmitted photon could be tuned (by choice of band gap) to 1 550 nm to minimise fibre transmission loss, while the wavelength of the conditioning photons could be tuned to 700 nm for maximum detection efficiency using current multiphoton counters.

4 Quantum-correlated photon twin beam

Consider two fully number-correlated pulsed photon beams B_1, B_2 ($m = 2$ in Fig. 2). These might be realised by the use of parametric down conversion [11] or, as suggested, by pulsed electrically coupled mesoscopic light-emitters [15].

For the twin beam case the conditional probabilities $N_2 = P(n_1 = 0|n_2 = 0, 1)$ and $S_2 = P(n_1 = 1|n_2 = 0, 1)$ are then easily found from Bayes' theorem to be :

$$N_2 = [(1/(1 + \eta\langle n_1\rangle)] \exp[-\langle n_1\rangle(1 - \eta)] \quad (9)$$

$$S_2 = [\langle n_1\rangle/(1 + \eta\langle n_1\rangle)] \exp[-\langle n_1\rangle(1 - \eta)]. \quad (10)$$

So that

$$L_2 = P(n_1 > 1|n_2 = 0, 1) = 1 - N_2 - S_2$$
$$= 1 - [(1 + \langle n_1\rangle)/(1 + \eta\langle n_1\rangle)] \exp[-\langle n_1\rangle(1 - \eta)]. \quad (11)$$

The leakage ratio:

$$L_2/S_2 = (D_2 \exp[\langle n_1\rangle(1 - \eta)] - [(1 + \langle n_1\rangle)])/\langle n_1\rangle \quad (12)$$

in which the function $D_2(\langle n_1\rangle, \eta) = (1 + \eta\langle n_1\rangle)$ is plotted in Figure 3 for a range of single-photon counting efficiencies η and mean photon numbers, $\langle n\rangle$. The uppermost curves (for $\eta = 0$), correspond to the unconditioned single beam. Figure 4 shows the conditioned single photon emission probability, $S_2 = P(n_1 = 1)$. It shows the increase in single-photon probability in the higher photon-number regimes made possible by an efficiently conditioned Poissonian source.

It is evident that high quantum efficiency is needed in a conditioned twin beam source to effect a major improvement in either channel efficiency or security against

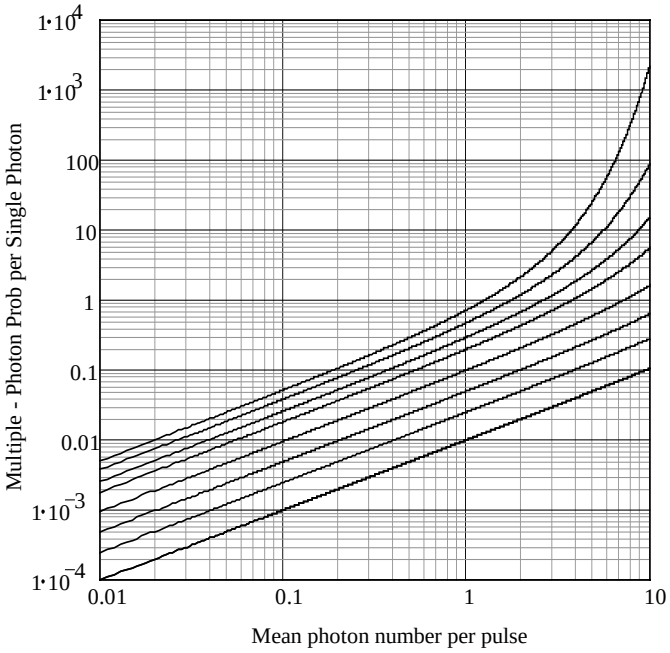

Fig. 3. Mean number of multiple photon signals per single-photon, $L/S = P(n_1 > 1)/P(n_1 = 1)$ for a fully correlated Poissonian twin-beam QKD transmitter conditioned by a noiseless multiphoton counter with quantum efficiencies ranging from 0 (top), through 0.5, 0.7, 0.8, 0.9, 0.95, 0.975 to 0.99 (bottom). The top curve (zero quantum efficiency) gives the unconditional (single beam) Poisson probabilities.

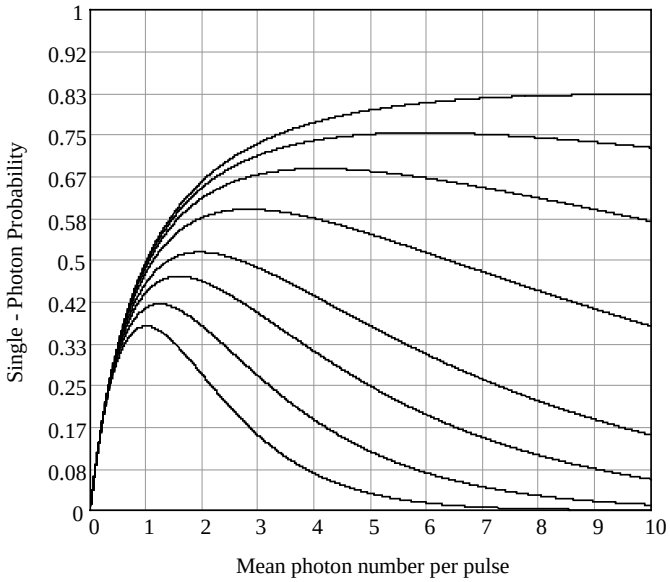

Fig. 4. Single photon emission probability, $S_2 = P(n_1 = 1)$ for a fully correlated Poissonian twin-beam QKD transmitter conditioned by a noiseless multiphoton counter with quantum efficiencies ranging from 0 (bottom), through 0.5, 0.7, 0.8, 0.9, 0.95, 0.975 to 0.99 (top). The bottom curve (zero quantum efficiency) gives the unconditioned (single beam) Poisson probabilities.

a beam-splitter attack. From equation (12), for $\langle n\rangle \ll 1$, $L_2/S_2 \approx \langle n_1\rangle(1-\eta^2)/2$, a factor of $(1-\eta^2)^{-1}$ less than for the unconditioned single beam. For η close to 1, $L_2/S_2 \approx \langle n_1\rangle(1-\eta)$, giving a reduction by a factor of $1/[2(1-\eta)] = 50$ for $\eta = 0.99$. This is a very significant improvement since for the same $\langle n\rangle$ it would permit a fifty fold (17 dB) increase in channel attenuation (corresponding to a 34 km increase in fibre length, or a seven fold increase in free-space range) without any loss of security, albeit with the inevitable reduction in channel capacity. Alternatively, for the same channel loss it would permit a fifty fold increase in channel capacity through increased $\langle n\rangle$. Unfortunately, such a high value of counting efficiency is well beyond the capabilities of current technology and we must look to other means of beam conditioning which make more relaxed demands on detector photon counting efficiency.

5 Quantum – correlated multiplet beam

It has been shown [15–20] that arrays of semiconductor light emitting junctions provide photon "multiplet" beams in which m, the number of correlated beams is not restricted to 2 as for PDC twin beams. We shall show that repeated $(m-1)$ photon number measurements made with such a photon multiplet beam source allows effective conditioning with much lower (and more practical) detector efficiencies. It should be pointed out however that although macroscopic quantum correlations have been demonstrated with bright multiplet beams of this type, successful extension to the single-photon number domain remains to be shown. However, Sumitomo et alia [22] have recently confirmed by Monte Carlo simulation the concept of efficient heralded twin-photon production by a pair of series-coupled array of mesoscopic light-emitting diodes.

Equations (9–12) for the conditioned twin beam source can be extended (Appendix A) to multiplet (m-beam) sources. For the triplet case ($m = 3$), where we identify and reject multiple photon signals if *either one* of two detectors register more than one count, we can rewrite equation (12) as

$$L_3/S_3 = (D_3 \exp[\langle n_1\rangle(1-\eta)^2] - [(1+\langle n_1\rangle)])/\langle n_1\rangle \quad (13)$$

with

$$D_3 = \left[1 + 2\langle n_1\rangle\eta(1-\eta) + \langle n_1\rangle\eta^2\left(1+\langle n_1\rangle(1-\eta)^2\right)\right]. \quad (14)$$

Similarly from Appendix A, for the quad source ($m = 4$),

$$L_4/S_4 = (D_4 \exp[\langle n_1\rangle(1-\eta)^3] - [(1+\langle n_1\rangle)])/\langle n_1\rangle \quad (15)$$

$$\text{with} \quad D_4 = \left[1 + 3\langle n_1\rangle\eta(1-\eta)^2 + 3\langle n_1\rangle\eta^2(1-\eta) \times \left\{1+\langle n_1\rangle(1-\eta)^3\right\} + \langle n_1\rangle\eta^3 \times \left\{1 + 3\langle n_1\rangle(1-\eta)^3 + \langle n_1\rangle^2(1-\eta)^6\right\}\right]. \quad (16)$$

Table 1. Single-photon quantum key transmitter efficiency S, multiple-photon leakage ratio L_m/S_m, and figure of merit $Q_s = S_m^2/L_m$, in the small $\langle n\rangle$ approximation for multiplet (m-beam) sources conditioned by $(m-1)$ noiseless multiphoton counters with quantum efficiencies $\eta = 0.875;\ 0.500$.

M	S	L_m/S_m	$Q_s(\eta)$	$Q_s(0.875)$	$Q_s(0.5)$
1	$<n>$	$<n>/2$	2	2	2
2	$<n>$	$<n>\cdot\left(1-\eta^2\right)/2$	$\frac{2}{\left(1-\eta^2\right)}$	8.53	2.67
3	$<n>$	$<n>\cdot\left(1-\eta^2\right)^2/2$	$\frac{2}{\left(1-\eta^2\right)^2}$	36.4	3.56
4	$<n>$	$<n>\cdot\left(1-\eta^2\right)^3/2$	$\frac{2}{\left(1-\eta^2\right)^3}$	155	4.74
8	$<n>$	$<n>\cdot\left(1-\eta^2\right)^7/2$	$\frac{2}{\left(1-\eta^2\right)^7}$	5.14×10^4	15.0

In the small $\langle n\rangle$ approximation, $L_3/S_3 \approx 2\langle n\rangle(1-\eta)^2$, so that, for example, if two identical detectors were used to monitor two fully correlated beams of the triplet a more realistic quantum efficiency of only 0.93 would be required to obtain the 50 fold suppression of multiple photon signals referred to above. Proceeding further, for the quad beam, $L_4/S_4 \approx 4\langle n\rangle(1-\eta)^3$, allowing the quantum efficiency to be relaxed even further, to $\eta = 0.85$, while for an octuplet beam with seven independent beam counters, the required efficiency is only $\eta = 0.65$.

In general, for the m-fold beam the leakage ratio (to first order in $\langle n\rangle$),

$$L_m/S_m = \langle n\rangle\left(1-\eta^2\right)^{m-1}/2 \quad (17)$$

and the figure of merit of the conditioned source,

$$Q_s = 2(1-\eta^2)^{1-m}. \quad (18)$$

It follows that the leakage continues to drop by the factor $(1-\eta^2) \approx 2(1-\eta)$ for every additional high efficiency conditioning counter used. If we take $\eta = 0.875$, the maximum single-photon counting detector efficiency currently reported [13], the leakage drops by a maximum factor of 4.27 with each additional conditioning beam.

Table 1 summarises these results for the case of small $\langle n\rangle$, with $\eta = 0.875$ and $\eta = 0.5$ as examples. The advantages to be had from using a high order multiplet source conditioned by high efficiency multiphoton counters in a high loss quantum channel are evident.

Figure 5 shows the leakage $L_m = P(>1)$ plotted for $m = 0, 1, 2, 3, 4$, and Figure 6 shows the ratio L_m/S_m for $\eta = 0.875$. It is evident that the leakage suppression is maintained for mean photon numbers close to unity. This permits high values of the figure of merit $Q_s = S_m^2/L_m$ to be achieved. It is also evident from equations (17, 18) that we can profitably trade beam number for detector quantum efficiency to maintain a given degree of suppression. Returning to the previous discussion, a fifty fold reduction in leakage requires either a single 99% (twin beam) detector efficiency, two 93% efficient detectors for a triplet beam, four 79% efficiency detectors for a quintuplet, seven 65% efficiency detectors or nine 59% efficient detectors.

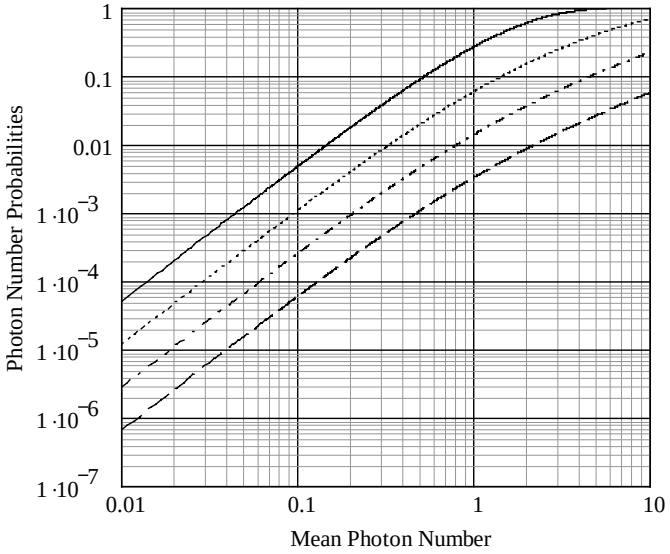

Fig. 5. Multiple photon number probabilities $P(>1)$ for a fully correlated Poissonian multiplet beam source with conditioning by $(m-1)$ noiseless multiphoton counters each with quantum efficiency $\eta = 0.875$. Solid curve ($m = 1$); dotted curve ($m = 2$); dot-dash curve ($m = 3$); dashed curve ($m = 4$).

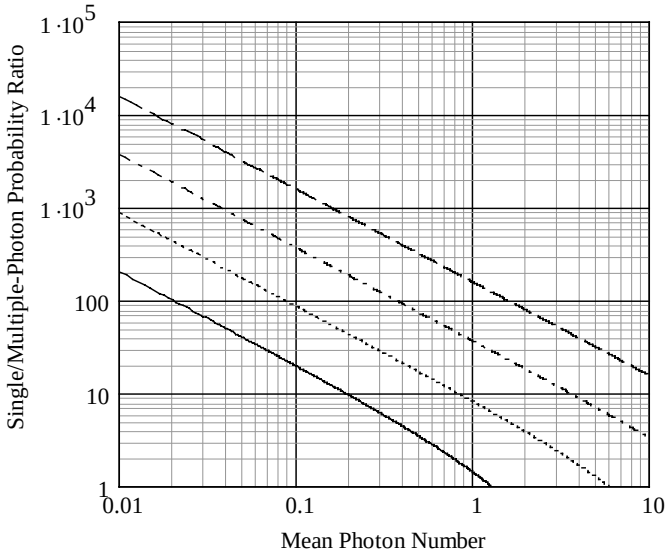

Fig. 6. The photon source parameter $S/L = P(1)/P(>1)$ for a multiplet single-photon source conditioned by $(m-1)$ noiseless multiphoton counters each with quantum efficiency $\eta = 0.875$. Solid curve: $m = 1$; dotted curve: $m = 2$; dot-dash curve: $m = 3$; dashed curve: $m = 4$.

6 Conclusions

The secure QKD outreach can be extended by reducing the occurrence of multiple-photon signals in the key bit sequence. One possible technique, discussed here, is the use of a photon beam conditioning technique using correlated multibeam (multiplet) photon sources monitored by high quantum efficiency multiphoton detectors. In practice, for practical quantum counting efficiencies of less than 90%, multiplet (quadruplet, or even octuplet) beams must be employed. These could provide source parameters $S/L = P(1)/P(>1)$ of 10^4 or more as required for secure quantum key distribution by earth satellite, for reasonable values of transmitter efficiency, $S = P(1) > 0.1$, corresponding to a single-photon source figure of merit $Q_s > 1\,000$. Entangled photon pair systems have been shown to be immune to beam-splitting attacks [25], however it is difficult to see how global key distribution could be implemented by earth satellites using entangled photon twins.

Reasonably efficient multiphoton conditioning counters are currently available. It appears therefore that if quantum-correlated multiple Poissonian photon beams can be realised, then the L/S ratio may be lowered by several orders of magnitude with a commensurate increase in channel capacity and/or permissible secure channel loss using existing detector technology.

However weak photon beams correlated at the single-photon level remain to be demonstrated. Electrically coupled arrays of single-electron/photon turnstile devices such as quantum dot emitters or mesoscale light-emitting semiconductor junctions may provide suitable quantum-correlated multiplet beams [9,15,22].

This work was supported by the Australian Research Council under its Large Research Grants Scheme. The authors acknowledge with thanks the assistance of G. Ganesharajah.

Appendix A

We sketch here the derivation of a general expression for the multiple-photon "leakage" L_m, and the "leakage ratio" L_m/S_m , the ratio of the conditional probabilities $P(n_1 > 1)/P(n_1 = 1)$ given that *none* of the $(m-1)$ noiseless photon counters with single-photon quantum efficiency η register more than a single count.

From Section 3, the probability of a null count in every one of the $(m-1)$ counters,

$$P\{n_2 = 0, n_3 = 0, ..., n_m = 0\} =$$
$$\sum_{j=0}^{\infty} P[n_1 = j \quad \text{and} \quad \{n_2 = 0, n_3 = 0, ..., n_m = 0\}]$$
$$= \sum_{j=0}^{\infty} \left[(\langle n_1\rangle^j \exp(-\langle n_1\rangle))/j!\right] \left[(1-\eta)^{m-1}\right]^j$$
$$= \exp\left(-\langle n_1\rangle \left[1-(1-\eta)^{m-1}\right]\right).$$

Also, the probability of a single count in the mth counter and null counts in every one of the remaining $(m-2)$ counters,

$$P\{n_2 = 0, n_3 = 0, ..., n_{m-1} = 0, n_m = 1\} =$$
$$\sum_{j=1}^{\infty} P[n_1 = j \quad \text{and} \quad \{n_2 = 0, n_3 = 0, ..., n_{m-1} = 0, n_m = 1\}],$$

becomes, after insertion of the Poisson and binomial probability functions, summation and collection of terms:

$$= \left\{E_0(\langle n_1\rangle(1-\eta)^{m-1})\right\}\langle n_1\rangle\eta(1-\eta)^{m-2}\exp(-\langle n_1\rangle),$$

where $E_r(x) = \sum_{j=1}^{\infty}(j^r x^{j-1})/(j-1)!$, so that $E_0(x) = \exp(x)$; $E_1(x) = (1+x)\exp(x)$; etc.

Similarly,

$$P\{n_2=0, n_3=0, ..., n_{m-2}=0, n_{m-1}=1, n_m=1\} = \sum_{j=1}^{\infty} P[n_1=j \text{ and } \{n_2=0, n_3=0, n_{m-2}=0, n_{m-1}=1, n_m=1\}]$$
$$= \{E_1(\langle n_1\rangle(1-\eta)^{m-1})\}\langle n_1\rangle\eta^2(1-\eta)^{m-3}\exp(-\langle n_1\rangle)\cdot$$

Further, proceeding in the same way,

$$P\{n_2=0, n_3=0, ..., n_{m-3}=0, n_{m-2}=1, n_{m-1}=1, n_m=1\} = \sum_{j=1}^{\infty} P[n_1=j \text{ and } \{n_2=0, n_3=0, n_{m-3}=0, n_{m-2}=1, n_{m-1}=1, n_m=1\}]$$
$$= \{E_2(\langle n_1\rangle(1-\eta)^{m-1})\}\langle n_1\rangle\eta^3(1-\eta)^{m-4}\exp(-\langle n_1\rangle)\cdot$$

Hence,

$$P\{n_2=0 \text{ or } 1, n_3=0 \text{ or } 1, ..., n_m=0 \text{ or } 1\} = \{\exp(\langle n_1\rangle(1-\eta)^{m-1}) + \langle n_1\rangle\sum_{j=1}^{m-1}\binom{m-1}{j}\eta^j(1-\eta)^{m-1-j} \times E_{j-1}(\langle n_1\rangle(1-\eta)^{m-1})\}\exp(-\langle n_1\rangle) = C_m,$$

say.

It then follows immediately that the conditional probability of exactly one photon per pulse from B_1,

$$S_m = P\{n_1=1, n_2=0 \text{ or } 1, ..., n_m=0 \text{ or } 1\} \times (P\{n_2=0 \text{ or } 1, ..., n_m=0 \text{ or } 1\})^{-1} = [\langle n_1\rangle\exp(-\langle n_1\rangle)]/C_m,$$

and

$$L_m = 1 - P\{n_1=0 \text{ or } 1/n_2=0 \text{ or } 1, n_3=0 \text{ or } 1, ..., n_m=0 \text{ or } 1\} = 1-(1+\langle n_1\rangle)C_m^{-1}\exp(-\langle n_1\rangle)\cdot$$

Thus, the leakage ratio for the m beam case,

$$L_m/S_m = [C_m\exp(\langle n_1\rangle) - (1+\langle n_1\rangle)]/\langle n_1\rangle = [D_m\exp(\langle n_1\rangle\left(1-\eta\right)^{m-1}) - (1+\langle n_1\rangle)]/\langle n_1\rangle,$$

as in equations (12, 13, 15), where

$$D_m = C_m\exp\langle n_1\rangle\left[1-(1-\eta)^{m-1}\right].$$

References

1. C.H. Bennett *et al.*, J. Cryptology **5**, 3 (1992).
2. H.P. Yuen, Quant. Semiclass. Opt **8**, 939 (1996).
3. G. Brassard, N. Lutkenhaus, T. Mor, B Sanders, Phys. Rev. Lett. **85**, 1330 (2000).
4. J. Kim, O. Benson, H. Kan, Y. Yamamoto, Nature **397**, 500 (1999).
5. J.M. Gerard *et al.*, Phys. Rev. **81**, 1110 (1998).
6. R. Brouri, A. Beveratos, J.-P. Poizat, P. Grangier, Opt. Lett. **25**, 1294 (2000).
7. C. Becher *et al.*, *Heralded single photons from a single quantum dot*, Paper QthE3, QELS 2001, Baltimore Md, Technical Digest, p. 185 (2001).
8. C. Santori, M. Pelton, G. Solomon, Y. Dale, *Triggered single photons from a quantum dot*, Paper QthE4, QELS 2001, Baltimore Md, Technical Digest, p. 186 (2001).
9. P.J. Edwards, W.N. Cheung, H. van Pham, G. Ganesharajah, P. Lynam, L. Barbopoulos, A note on quantum key channel efficiency and security using correlated photon beam transmitters, `quant-ph/0008013` (Aug. 2000).
10. Z. Walton, A.V. Sergienko, M. Atature, B.E.A. Saleh, M.C. Teich, Performance of Photon-Pair Quantum Key Distribution Systems, `quant-ph/0103145` (26 Mar. 2001).
11. A.K. Ekert, J.G. Rarity, P.R. Tapster, G.M. Palma, Phys. Rev. Lett. **69**, 1293 (1992).
12. T.P. Spiller, Proc. IEEE **84**, 1719 (1996).
13. S. Takeuchi, J. Kim, Y. Yamamoto, H. Hogue, Appl. Phys. Lett. **74**, 1063 (1999).
14. J. Kim, S. Takeuchi, Y. Yamamoto, H. Hogue, Appl. Phys. Lett. **74**, 902 (1999).
15. P.J. Edwards, in Quantum Optics VI, *Proceedings of the 6th International Symposium on Quantum Optics*, edited by D.F. Walls, J.D. Harvey (Rotorua, New Zealand, 1994), p. 285.
16. P.J. Edwards, G.H. Pollard, Phys. Rev. Lett. **69**, 1757 (1992).
17. P.J. Edwards, Electron. Lett. **29**, 299 (1993).
18. E. Goobar, A. Karlsson, G. Bjork, P.J. Rigole, Phys. Rev. Lett. **70**, 437 (1993).
19. Y.-q. Li, P.J. Edwards, P. Lynam, W.N. Cheung, Int. J. Optoelectron. **10**, 417 (1996).
20. Y.-q. Li, P.J. Edwards, X. Huang, Y. Wang, J. Opt. B: Quant. Semiclass. Opt. **2**, 292 (2000).
21. C.H. Bennett, G. Brassard, in *Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing*, Bangalore, India (IEEE, New York, 1984), p. 175.
22. H. Sumitomo, M. Yamanishi, Y. Kadoya, Jpn. J. Appl. Phys. **40**, L85 (2001).
23. W.T. Buttler *et al.*, Phys. Rev. Lett. **81**, 3283 (1998).
24. W.T. Buttler *et al.*, Phys. Rev. Lett. **83**, 2476 (1999).
25. G. Ribordy, J. Brendel, J.-D. Gautier, N. Gisin, H. Zbinden, Phys. Rev. A **63**, 12309 (2001).