Special issue: Quantum information technology

Research Paper

Passive preparation of BB84 signal states with coherent light

Marcos CURTY[1], Xiongfeng MA[2], Hoi-Kwong LO[3], and Norbert LÜTKENHAUS[4]
[1]*ETSI Telecomunicación, University of Vigo, Spain*
[2,4]*Institute for Quantum Computing, University of Waterloo, Canada*
[3]*Center for Quantum Information and Quantum Control, University of Toronto, Canada*

ABSTRACT

In a typical optical implementation of the Bennett-Brassard 1984 (so-called BB84) quantum key distribution protocol, the sender uses an active source to produce the required signal states. While active state preparation of BB84 signals is a simple and elegant solution in principle, in practice passive state preparation might be desirable in some scenarios, for instance, in those experimental setups operating at high transmission rates. Passive devices usually involve parametric down-conversion. Here we show that coherent light is also suitable for passive generation of BB84 signal states. Our method does not require any externally-driven element, but only linear optical components and photodetectors. The resulting key rate is similar to the one delivered by an active source.

KEYWORDS

Quantum key distribution, quantum communication, quantum-state engineering, passive transmitter

1 Introduction

Quantum key distribution (QKD) is the first commercial application of quantum information that offers efficient and user-friendly cryptographic systems with an unprecedented level of security [1], [2]. It exploits quantum effects to establish a secure secret key between two distant parties (typically called Alice and Bob) despite the computational and technological power of an eavesdropper (Eve), who interferes with the signals in the channel. This secret key is the essential ingredient of the one-time-pad or Vernam cipher [3], the only known encryption method that can provide information-theoretic secure communications.

Most experimental realizations of QKD are based on the so-called BB84 QKD scheme introduced by Bennett and Brassard in 1984 [4]. In a typical quantum optical implementation of this protocol, Alice sends to Bob phase-randomized weak coherent pulses (WCP) with usual average photon number of 0.1 or higher. Each light pulse may be prepared in a different polarization state, which is selected, independently and randomly for each signal, between two mutually unbiased bases. On the receiving side, Bob measures each incoming signal by choosing at random between two polarization analyzers, one for each possible basis. Once this quantum communication phase is completed, Alice and Bob use an authenticated public channel to process their data and obtain a secure secret key. A full proof of the security of this protocol has been given in Refs. [5], [6]. Its performance can be improved further if the original hardware is slightly modified. For instance, one can use the so-called decoy-state method [7]–[9], where Alice varies the mean photon number of each signal state she sends to Bob. This translates into an enhancement of the achievable secret key rate, which can now basically reach the performance of single photon sources.

The preparation of the BB84 signal states is usually realized by means of an active source. There are two main configurations. In the first one, Alice uses four laser diodes, one for each possible BB84 signal.

Received October 30, 2010; Revised December 20, 2010; Accepted December 27, 2010.
[1] *mcurty@com.uvigo.es,* [2] *xfma@iqc.ca,* [3] *hklo@comm.utoronto.ca,* [4] *nlutkenhaus@iqc.ca*
DOI: 10.2201/NiiPi.2011.8.7

These lasers are controlled by a random number generator (RNG) that decides each given time which one of the four diodes is triggered. The second configuration uses only one single laser diode in combination with a polarization modulator which is controlled by a RNG. This modulator can rotate the state of polarization of the signals produced by the source.

While active state preparation is a simple and elegant solution to implement the BB84 protocol in principle, in practice passive state preparation might be desirable in some scenarios [10]–[15]; for instance, in those experimental setups operating at high transmission rates, since no RNG is required in a passive device. For example, Alice can use one or more light sources to produce different signal states that are sent through a linear optics network. Depending on the detection pattern observed in some properly situated detectors, she can infer which signal states are actually generated. Typical passive schemes involve parametric down-conversion [10], [16]. For instance, Alice and Bob can use a beamsplitter (BS) to passively and randomly select which bases is used to measure each incoming pulse. More recently, it has been shown that phase-randomized weak coherent pulses can be used to passively generate decoy states for QKD [13], [15]. Intuitively speaking, the authors of Refs. [13], [15] exploit the random phases of the different incoming pulses to passively generate states with distinct photon number statistics. This paper follows a similar spirit; in particular we show that phase-randomized coherent light is also suitable for passive generation of BB84 signal states. That is, one does not need a nonlinear optics network preparing entangled states in order to passively generate BB84 signals, but one can exploit the arbitrary phases of the incoming signals to prepare the desired states at random [17]. Our method requires only linear optical elements and photodetectors. In the asymptotic limit of an infinite long experiment, it turns out that the resulting key rate of a passive transmitter is similar to the one delivered by an active source, thus showing the practical interest of the passive setup.

Passive schemes might also be more robust than active systems to side-channel attacks hidden in the imperfections of the optical components. If a polarization modulator is not properly designed, for example, it may distort some of the physical parameters of the pulses emitted by the sender depending on the particular value of the polarization setting selected. This fact could open a security loophole in the active schemes.

2 Passive QKD transmitter

The basic setup is rather simple. It is illustrated in Fig. 1. Suppose two phase-randomized strong coherent pulses prepared, respectively, in +45° and −45° linear polarization, interfere at a polarizing beamsplitter (PBS). These states can be written as

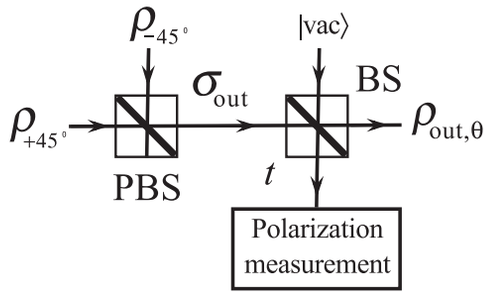

Fig. 1 Basic setup of a passive BB84 QKD source with coherent light.

$$\rho_{\pm 45^\circ} = e^{-\frac{\upsilon}{2}} \sum_{n=0}^{\infty} \frac{(\upsilon/2)^n}{n!} |n_{\pm 45^\circ}\rangle\langle n_{\pm 45^\circ}|, \tag{1}$$

where $|n_{\pm 45^\circ}\rangle$ denote Fock states with n photons in ±45° linear polarization. The mean photon number, $\upsilon/2$, of each signal can be chosen very high; for instance, $\approx 10^6$ photons. This kind of states can be generated, for instance, using a laser diode biased with a DC current far below threshold and directly modulated with a strong radio frequency current [18]. In Ref. [19], for example, Jofre et al. reported recently on an optical source of up 100 MHz repetition rate, which emits phase-randomized strong coherent pulses with mean photon number $\approx 6 \cdot 10^6$ photons centered at 850 nm. Moreover, as emphasized by the authors, this source might be easily scalable to higher repetition rates.

In this scenario, it turns out that the signals σ_{out} at the output port of the PBS (see Fig. 1) can be expressed as [17]

$$\sigma_{\text{out}} = \frac{1}{2\pi} e^{-\upsilon} \sum_{n=0}^{\infty} \frac{\upsilon^n}{n!} \int_\theta |n_\theta\rangle\langle n_\theta| \, \mathrm{d}\theta, \tag{2}$$

where the Fock states $|n_\theta\rangle$ are given by

$$|n_\theta\rangle = \frac{\left[\frac{1}{\sqrt{2}}(a^\dagger_{+45^\circ} + e^{i\theta} a^\dagger_{-45^\circ})\right]^n}{\sqrt{n!}} |vac\rangle. \tag{3}$$

The state $|vac\rangle$ represents the vacuum state, and $a^\dagger_{\pm 45^\circ}$ are the creation operators for the ±45° linear polarizations modes.

Now, to prepare the signal states that are sent to Bob, Alice performs a polarization measurement followed by a post-selection step. By assumption, we have that the intensity υ of the signals σ_{out} is very high. Therefore, Alice can always employ, for instance, a BS of very small transmittance ($t \ll 1$) to split these states into

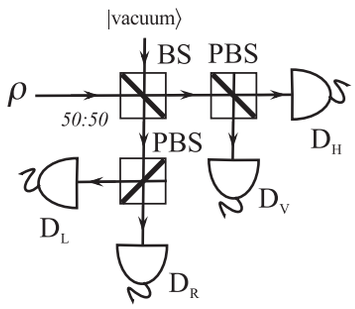

Fig. 2 Example of a polarization measurement based on the passive BB84 detection scheme with classical photodetectors. *H* stands for horizontal polarization, *V* for vertical polarization, *L* for circular left polarization and *R* for circular right polarization. The different intensities observed in the four classical photodetectors determine the value of the angle θ.

two light beams: one very weak suitable for QKD, and one strong. The weak signal is sent to Bob through the quantum channel (see Fig. 1). The strong beam is used to measure its polarization by means of a polarization measurement which, for simplicity, we assume is *perfect*. For each incoming signal, this device provides Alice with a precise value for the measured angle θ. This can be achieved, for example, by means of a passive BB84 detection scheme where the basis choice is performed by a 50 : 50 BS, and on each end there is a PBS and two classical photodetectors. Such a detection device is illustrated for completeness in Fig. 2. From the different intensities observed in each of the four classical photodetectors, Alice can determine the value of the angle θ. In this scenario, the conditional states emitted by the source can be described as

$$\rho_{\text{out},\theta} = e^{-\mu} \sum_{n=0}^{\infty} \frac{\mu^n}{n!} |n_\theta\rangle\langle n_\theta|, \tag{4}$$

where θ denotes the value of the angle obtained by Alice's polarization measurement, and μ is given by $\mu = \upsilon t$.

Note, for instance, that whenever $\theta = 0$, $\pi/2$, π, or $3\pi/2$, Alice can generate one of the four BB84 polarization states perfectly. In practice, however, Alice does not need to restrict herself to only those events where she actually prepares a perfect BB84 state, since the probability associated with these ideal events tends to zero. Instead, she can also accept signals with a polarization sufficiently close to the desired ones. This situation is illustrated in Fig. 3, where Alice selects some valid regions for the angle θ. These regions are marked with gray color in the figure. They depend on an acceptance parameter $\Omega \in [0, \pi/4]$ that we optimize. Specifically, whenever the value of θ lies within any of the intervals $\psi \pm (\pi/4 - \Omega)$ with $\psi \in \{0, \pi/2, \pi, 3\pi/2\}$, then Alice considers the pulse emitted by the source as a valid signal. Otherwise, the pulse is discarded afterwards during the post-processing phase of the protocol, and it does not contribute to the key rate. The probability that a pulse is accepted, p_{acc}, is given by

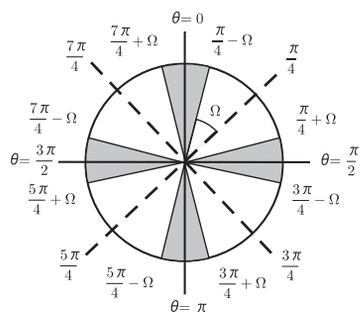

Fig. 3 Graphical representation of the valid regions for the angle θ. These regions are marked in gray.

$$p_{\text{acc}} = 1 - \frac{4\Omega}{\pi}. \tag{5}$$

To increase this probability, one can reduce the value of Ω. Note, however, that this action also results in an increase of the quantum bit error rate (QBER) of the protocol, that we shall denote as E. On the other hand, when Ω increases, we have that both p_{acc} and E decrease. There is a trade-off on the acceptance parameter Ω. A high acceptance probability p_{acc} favors $\Omega \approx 0$, whereas a low QBER favors $\Omega \approx \pi/4$. In the limit where Ω tends to $\pi/4$ we recover the standard BB84 protocol.

3 Lower bound on the secret key rate

We use the security analysis provided by Gottesman-Lo-Lütkenhaus-Preskill in Ref. [6]. It considers that Eve can always obtain full information about the part of the key generated from the multiphoton signals. This pessimistic assumption is also true for the passive transmitter illustrated in Fig. 1 when Alice and Bob use only unidirectional classical communication during the public-discussion phase of the protocol. This result arises from the fact that all the photons contained in a pulse are prepared in the same polarization state and, therefore, no secret key can be distilled with one-way post-processing techniques [20]. Note, however, that such security analysis could still leave room for improvement when Alice and Bob employ two-way classical communication. In this situation, it might be possible to obtain secret key even from the multiphoton pulses since the signal states prepared by the passive

device are already mixed at the source. This last scenario, however, is beyond the scope of this paper.

We further assume the typical initial post-processing step in the BB84 protocol, where double click events are not discarded by Bob, but they are randomly assigned to single click events [21], [22]. The secret key rate formula can be written as [6]

$$R \geq q p_{\rm acc}\Big\{(Q - p_{\rm multi})[1 - H(E_1)] - Q f(E) H(E)\Big\}. \quad (6)$$

The parameter q is the efficiency of the protocol ($q = 1/2$ for the standard BB84 protocol, and $q \approx 1$ for its efficient version [23]); Q is the gain, i.e., the probability that Bob obtains a click in his measurement apparatus when Alice sends him a signal state; $f(E)$ is the efficiency of the error correction protocol as a function of the error rate E, typically $f(E) \geq 1$ with Shannon limit $f(E) = 1$; $H(x)$ is the binary Shannon entropy function defined as

$$H(x) = -x \log_2(x) - (1 - x) \log_2(1 - x); \quad (7)$$

$p_{\rm multi}$ is the multiphoton probability of the source, i.e.,

$$p_{\rm multi} = 1 - e^{-\mu}(1 + \mu); \quad (8)$$

and E_1 denotes an upper bound on the single photon error rate. In the case of the standard BB84 protocol without decoy-states, this last quantity is given by

$$E_1 = \frac{E}{1 - \frac{p_{\rm multi}}{Q}}. \quad (9)$$

3.1 Evaluation

For simplicity, we shall consider that Bob employs an active BB84 detection setup. Moreover, we assume a simple model of a quantum channel in the absence of eavesdropping; it just consists of a BS of transmittance $\eta_{\rm channel}$. This model allows us to calculate the observed experimental parameters Q and E. These quantities are given in an Appendix. Our results, however, can also be straightforwardly applied to any other quantum channel or to the case where Bob uses a detection apparatus with passive basis choice, as they depend only on the observed gain and QBER.

The resulting lower bound on the secret key rate is illustrated in Fig. 4 (dashed line). In our simulation we employ the following experimental parameters: the dark count rate of Bob's detectors is $\epsilon_{\rm B} = 1 \times 10^{-6}$, the overall transmittance of his detection apparatus is $\eta_{\rm B} = 0.1$, and the loss coefficient of the quantum channel is $\alpha = 0.2$ dB/km. We further assume that $q = 1/2$, and $f(E) = 1.22$. With this configuration, it turns out that the optimal value of the mean photon number μ decreases with the distance, while the value of the parameter Ω increases. In particular, μ diminishes from ≈ 0.084 to approximately 4×10^{-3}, while Ω augments from ≈ 0.365 to ≈ 0.76. This result is not surprising. At long distances the gain Q of the protocol is very low and, therefore, it is especially important to keep both the multiphoton probability of the source, and the intrinsic error rate of the signals $\rho_{{\rm out},\theta}$, also low. Fig. 4 includes an inset plot with the optimized parameters μ (dashed line) and Ω (solid line). This figure shows as well a lower bound on the secret key rate for the case of an active source. The cutoff point where the secret key rate drops down to zero is basically the same in both cases. It is given by $l \approx 67.5$ km. This result arises from two main limiting factors: the multiphoton probability of the source, and the dark count rate of Bob's detectors. Note that in these simulations we do not consider any misalignment effect in the channel or in Bob's detection apparatus. From the results shown in Fig. 4 we see that the performance of the passive scheme is similar to the one of an active setup. The (relatively small) difference between the achievable secret key rates in both scenarios is due to two main factors: (a) the probability $p_{\rm acc}$ to accept a pulse emitted by the source, which is $p_{\rm acc} < 1$ in the passive setup, and $p_{\rm acc} = 1$ in the active scheme, and (b) the intrinsic error rate of the signals accepted by Alice, that is zero only in the case of an active source.

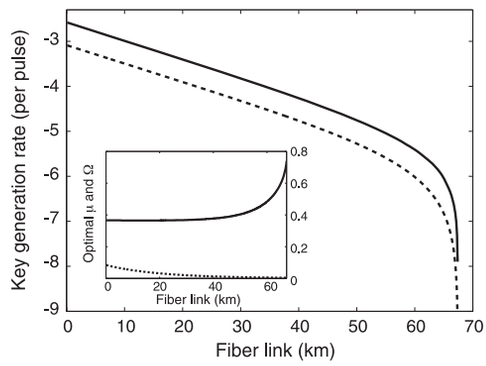

Fig. 4 Lower bound on the secret key rate R given by Eq. (6) in logarithmic scale for the passive source illustrated in Fig. 1 (dashed line). The solid line represents a lower bound on R when Alice employs an active source. The inset figure shows the value for the optimized parameters μ (dashed line) and Ω (solid line) in the passive setup.

4 Alternative implementation scheme

Instead of using the scheme shown in Fig. 1, Alice could as well employ, for instance, the device illustrated in Fig. 5. This setup has only one laser diode, but fol-

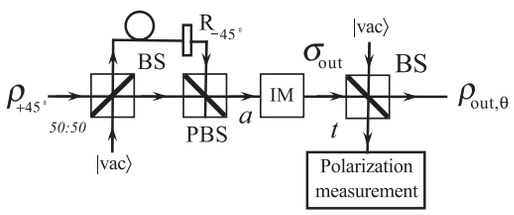

Fig. 5 Alternative implementation scheme with only one pulsed laser source. The delay introduced by one arm of the interferometer is equal to the time difference between two consecutive pulses. The polarization rotator R_{-45° changes the $+45^\circ$ linear polarization of the incoming pulses to -45° linear polarization.

lows a similar spirit like the original scheme shown in Fig. 1, where a polarization measurement is used to determine the polarization of the incoming signals. The main idea is just to replace two single light pulses emitted by two different diodes with two consecutive light pulses generated by only one laser diode.

To keep the analysis simple, the scheme includes as well an intensity modulator (IM) to block either all the even or all the odd pulses in mode a (see Fig. 5). The main reason for blocking half of the incoming pulses is to suppress possible correlations between them. The IM guarantees that the signals that go to Bob are precisely tensor product of states of the form given by Eq. (4). To see this, note that the signal states in mode a (before the IM) can always be written as

$$\rho_{\text{out}} = \frac{1}{(2\pi)^{n+1}} \int_{\phi_0} \int_{\phi_1} \int_{\phi_2} \cdots \int_{\phi_n} |\alpha_{(\phi_0,\phi_1)}\rangle \langle\alpha_{(\phi_0,\phi_1)}| \otimes |\alpha_{(\phi_1,\phi_2)}\rangle\langle\alpha_{(\phi_1,\phi_2)}| \otimes \ldots \otimes |\alpha_{(\phi_{n-1},\phi_n)}\rangle\langle\alpha_{(\phi_{n-1},\phi_n)}| \, \mathrm{d}\phi_0 \mathrm{d}\phi_1 \mathrm{d}\phi_2 \ldots \mathrm{d}\phi_n, \quad (10)$$

where the coherent states $|\alpha_{(\phi_i,\phi_{i+1})}\rangle$ have the form $|\alpha_{(\phi_i,\phi_{i+1})}\rangle = \exp[\sqrt{\nu}(e^{i\phi_i}a_i^\dagger - e^{-i\phi_i}a_i)]|vac\rangle$, and the operators $a_i^\dagger$ are given by

$$a_i^\dagger = \frac{1}{\sqrt{2}}(a_{+45^\circ}^\dagger + e^{i(\phi_{i+1}-\phi_i)}a_{-45^\circ}^\dagger). \quad (11)$$

If now Alice blocks, for instance, all the even pulses in mode a, we obtain that the output state σ_{out} can be written as

$$\sigma_{\text{out}} = \bigotimes_{i=0}^{\lfloor\frac{n-1}{2}\rfloor} \frac{1}{(2\pi)^2} \int_{\phi_{2i}} \int_{\phi_{2i+1}} |\alpha_{(\phi_{2i},\phi_{2i+1})}\rangle \langle\alpha_{(\phi_{2i},\phi_{2i+1})}| \, \mathrm{d}\phi_{2i}\mathrm{d}\phi_{2i+1} = \bigotimes_{i=0}^{\lfloor\frac{n-1}{2}\rfloor} \sigma_{\text{out}}^i, \quad (12)$$

with σ_{out}^i of the form given by Eq. (2). This way we can directly apply the security evaluation provided in Sec. 3. This transmitter requires, therefore, an active control of the functioning of the IM. Note, however, that this configuration might still be much less of a problem than using a polarization modulator to actively generate BB84 signal states at high rates, since no RNG is needed to control the IM. Thanks to the one-pulse delay introduced by one arm of the interferometer, it can be shown that both setups in Fig. 1 and Fig. 5 are completely equivalent, except from the resulting secret key rate. More precisely, the secret key rate in the passive scheme with two lasers is double than that in the setup illustrated in Fig. 5, since half of the pulses are now discarded.

5 Conclusion

We have presented a method to passively generate the signal states of the Bennett-Brassard 1984 QKD protocol with coherent light. It needs only linear optical components and photodetectors, and constitutes an alternative to those active sources that use externally-driven elements. In the asymptotic limit of an infinite long experiment, we have shown that the secret key rate delivered by a passive transmitter is similar to the one provided by an active source, thus showing the practical interest of the passive scheme.

Acknowledgement

This work was supported by CFI, CIPI, the CRC program, CIFAR, MITACS, NSERC, OIT, QuantumWorks, and by Xunta de Galicia (Spain, grant INCITE08PXIB322257PR).

References

[1] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," *Rev. Mod. Phys.*, vol.74, pp.145–195, 2002.

[2] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, "The security of practical quantum key distribution," *Rev. Mod. Phys.*, vol.81, pp.1301–1350, 2009.

[3] G. S. Vernam, "Cipher printing telegraph systems for secret wire and radio telegraphic communications," *J. Amer. Inst. Elec. Eng.*, vol.45, pp.109–115, 1926.

[4] C. H. Bennett and G. Brassard, "Quantum cryptography: public key distribution and coin tossing," in *Proc. IEEE Int. Conference on Computers, Systems and Signal Processing*, Bangalore, India, IEEE Press, New York, pp.175–179, 1984.

[5] H. Inamori, N. Lütkenhaus, and D. Mayers, "Unconditional security of practical quantum key distribution," *Eur. Phys. J. D*, vol.41, no.3, pp.599–627, 2007.

[6] D. Gottesman, H.-K. Lo, N. Lütkenhaus, and J. Preskill, "Security of quantum key distribution with imperfect

devices," *Quantum Inf. Comput.*, vol.4, pp.325–360, 2004.

[7] W.-Y. Hwang, "Quantum key distribution with high loss: toward global secure communication," *Phys. Rev. Lett.*, vol.91, 057901, 2003.

[8] H.-K. Lo, X. Ma, and K. Chen, "Decoy state quantum key distribution," *Phys. Rev. Lett.*, vol.94, 230504, 2005.

[9] X.-B. Wang, "Beating the photon-number-splitting attack in practical quantum cryptography," *Phys. Rev. Lett.*, vol.94, 230503, 2005.

[10] J. G. Rarity, P. C. M. Owens, and P. R. Tapster, "Quantum random-number generation and key sharing," *J. Mod. Opt.*, vol.41, no.12, pp.2435–2444, 1994.

[11] W. Mauerer and C. Silberhorn, "Quantum key distribution with passive decoy state selection," *Phys. Rev. A*, vol.75, 050305(R), 2007.

[12] Y. Adachi, T. Yamamoto, M. Koashi, and N. Imoto, "Simple and efficient quantum key distribution with parametric down-conversion," *Phys. Rev. Lett.*, vol.99, 180503, 2007.

[13] M. Curty, T. Moroder, X. Ma, and N. Lütkenhaus, "Non-Poissonian statistics from Poissonian light sources with application to passive decoy state quantum key distribution," *Opt. Lett.*, vol.34, pp.3238–3240, 2009.

[14] Y. Adachi, T. Yamamoto, M. Koashi, and N. Imoto, "Boosting up quantum key distribution by learning statistics of practical single-photon sources," *New J. Phys.*, vol.11, 113033, 2009.

[15] M. Curty, X. Ma, B. Qi, and T. Moroder, "Passive decoy-state quantum key distribution with practical light sources," *Phys. Rev. A*, vol.81, 022310, 2010.

[16] W. Tittel, J. Brendel, H. Zbinden, and N. Gisin, "Quantum cryptography using entangled photons in energy-time Bell states," *Phys. Rev. Lett.*, vol.84, pp.4737–4740, 2000.

[17] M. Curty, X. Ma, H.-K- Lo, and N. Lütkenhaus, "Passive sources for the Bennett-Brassard 1984 quantum key distribution protocol with practical signals," preprint arXiv:1009.3830.

[18] K. Peterman, *Laser Diode Modulation and Noise*, Kluwer Academic Publishers, New York, 1991. ISBN: 978-0792312048.

[19] M. Jofre, A. Gardelein, G. Anzolin, G. Molina-Terriza, J. P. Torres, M. W. Mitchell, and V. Pruneri, "100 MHz Amplitude and Polarization Modulated Optical Source for Free-Space Quantum Key Distribution at 850 nm," *J. of Lightwave Tech.*, vol.28, no. 17, pp.2572–2578, 2010.

[20] T. Moroder, M. Curty, and N. Lütkenhaus, "One-way quantum key distribution: simple upper bound on the secret key rate," *Phys. Rev. A*, vol.74, 052301, 2006.

[21] N. Lütkenhaus, "Estimates for practical quantum cryptography," *Phys. Rev. A*, vol.59, pp.3301–3319, 1999.

[22] N. J. Beaudry, T. Moroder, and N. Lütkenhaus, "Squashing models for optical measurements in quantum communication," *Phys. Rev. Lett.*, vol.101, 093601, 2008.

[23] H.-K. Lo, H. F. C. Chau, and M. Ardehali, "Efficient quantum key distribution scheme and a proof of Its unconditional security," *J. Cryptology*, vol.18, pp.133–165, 2005.

Appendix. Gain and QBER

In this Appendix we provide a mathematical expression for the observed gain Q and error rate E. In particular, it can be shown that, in the scenario considered, the gain is independent of the actual polarization of the signals $\rho_{\text{out},\theta}$ given by Eq. (4) and the basis used to measure them. After a short calculation, we find that this parameter has the form

$$Q = 1 - (1 - \epsilon_{\text{B}})^2 e^{-\mu\eta_{\text{sys}}}, \tag{13}$$

for all θ, where ϵ_{B} denotes again the dark count rate of Bob's detectors and η_{sys} is the overall transmittance of the system.

The calculation of E is slightly more involved, since the error rate varies depending on the value of the angle θ. By symmetry, however, we can restrict ourselves to investigate the QBER in only one of the valid regions illustrated in Fig. 3; note that the error rate is the same in all of them. For instance, let us consider the case where $\theta \in [7\pi/4 + \Omega, \pi/4 - \Omega]$ (which corresponds to the horizontal polarization interval), and let E_θ denote the error rate of a signal state $\rho_{\text{out},\theta}$ in that region. After a tedious calculation, it can be shown that this quantity can be written as

$$\begin{aligned} E_\theta \;=\; & \frac{1}{2Q}\Big\{\epsilon_{\text{B}}(\epsilon_{\text{B}} - 1) f_{0,\theta} + [2 + \epsilon_{\text{B}}(\epsilon_{\text{B}} - 3)] f_{1,\theta} \\ & + [1 + \epsilon_{\text{B}}(\epsilon_{\text{B}} - 2)] f_{\text{dc},\theta} + \epsilon_{\text{B}}(2 - \epsilon_{\text{B}})\Big\}, \end{aligned} \tag{14}$$

where the parameters $f_{0,\theta}$, $f_{1,\theta}$, and $f_{\text{dc},\theta}$, have the form

$$\begin{aligned} f_{0,\theta} \;&=\; e^{-\eta_{\text{sys}}\mu}\Big[-1 + e^{\frac{1}{2}\eta_{\text{sys}}\mu(1+\cos\theta)}\Big], \\ f_{1,\theta} \;&=\; e^{-\eta_{\text{sys}}\mu}\Big[-1 + e^{\frac{1}{2}\eta_{\text{sys}}\mu(1-\cos\theta)}\Big], \\ f_{\text{dc},\theta} \;&=\; 1 + e^{-\eta_{\text{sys}}\mu} - e^{-\frac{1}{2}\eta_{\text{sys}}\mu(1+\cos\theta)} \\ & \quad - e^{-\eta_{\text{sys}}\mu\sin^2\left(\frac{\theta}{2}\right)}. \end{aligned} \tag{15}$$

The quantum bit error rate E is then given by

$$E = \frac{2}{\pi - 4\Omega} \int_{\frac{7\pi}{4}+\Omega}^{\frac{\pi}{4}-\Omega} E_\theta \, \mathrm{d}\theta, \tag{16}$$

and we solve this equation numerically.

Marcos CURTY

Marcos CURTY received his M.Sc. and Ph.D in Telecommunication Engineering from Vigo University in 1999 and 2004 respectively. In 2001 he joined the Quantum Information Theory Group at the University of Erlangen-Nürnberg and he obtained a Ph.D in Physics (2006) under the supervision of Prof. Norbert Lütkenhaus. After postdoc positions at Toronto University (Prof. Hoi-Kwong Lo) and at the Institute for Quantum Computing, Waterloo University (Prof. Norbert Lütkenhaus), he joined the department of Electronic and Communications Engineering at Zaragoza University as Assistant Professor. Currently he is Associate Professor at the department of Theory of Signal and Communications at Vigo University. His research interest lies in quantum information processing, particularly quantum cryptography.

Xiongfeng MA

Xiongfeng MA is a post-doctoral fellow at the Institute for Quantum Computing, University of Waterloo. He did his PhD in the Department of Physics at the University of Toronto. After earning a BSc in physics at Peking University in 2003, he joined Prof. Hoi-Kwong Lo's group at the University of Toronto as a graduate student. His research interest is in Quantum Information Processing with a special emphasis on Quantum Cryptography.

Hoi-Kwong LO

Hoi-Kwong LO is a Full Professor and a Canada Research Chair at the Center for Quantum Information and Quantum Control (CQIQC), the Department of Physics and the Department of Electrical and Computer Engineering, at the University of Toronto. His research interest lies in quantum information processing, particularly quantum cryptography. He received his B.A. in Mathematics from Trinity College, Cambridge University in 1989 and his M.Sc. and Ph.D. in Physics from Caltech in 1991 and 1994 respectively. Prof. Lo had six years of industrial research experience at Hewlett-Packard Lab., Bristol UK and also as the Chief Scientist and Senior Vice President, R&D, of MagiQ Technologies, Inc., New York. He was a co-founder of a leading journal "Quantum Information and Computation" (QIC). He is a Fellow of the Canadian Institute for Advanced Research (CIFAR).

Norbert LÜTKENHAUS

Norbert LÜTKENHAUS studied at the RWTH Aachen and the LMU Munich, from which he graduated with a thesis in general relativity. Then he changed the field to study quantum optics and quantum cryptography under the supervision of Stephen M. Barnett at the University of Strathclyde, Scotland, UK. In 1996 he obtained his PhD. After postdoc positions in Innsbruck (Peter Zoller and Ignacio Cirac) and the Helsinki Institute of Physics (Kalle-Antti Suominen) he worked for MagiQ Technologies (New York) to initiate the project of commercial realisation of quantum key distribution. Returning to academia in 2001, he build up and lead an Emmy-Noether Research Group at the University of Erlangen-Nürnberg, during which time he did his habilitation (2004). Currently he is an Associate Professor in the Physics Department at the University of Waterloo and a member of the Institute of Quantum Computing.