Experimental demonstration of post-selection-based continuous-variable quantum key distribution in the presence of Gaussian noise

Thomas Symul,[1] Daniel J. Alton,[1] Syed M. Assad,[1,2] Andrew M. Lance,[1] Christian Weedbrook,[1,3] Timothy C. Ralph,[3] and Ping Koy Lam[1]

[1]*Quantum Optics Group, Department of Physics, Faculty of Science, Australian National University, ACT 0200, Australia*
[2]*Department of Physics, National University of Singapore, Singapore*
[3]*Department of Physics, University of Queensland, St Lucia, Queensland 4072, Australia*

(Received 12 March 2007; published 14 September 2007)

In realistic continuous-variable quantum key distribution protocols, an eavesdropper may exploit the additional Gaussian noise generated during transmission to mask her presence. We present a theoretical framework for a post-selection-based protocol which explicitly takes into account excess Gaussian noise. We derive a quantitative expression of the secret key rates based on the Levitin and Holevo bounds. We experimentally demonstrate that the post-selection-based scheme is still secure against both individual and collective Gaussian attacks in the presence of this excess noise.

DOI: 10.1103/PhysRevA.76.030303 PACS number(s): 03.67.Dd, 42.50.Dv, 89.70.+c

Continuous-variable quantum key distribution (CV QKD) [1] was introduced as an alternative to the original discrete variable single photon schemes [2]. CV QKD promises to offer higher secret key rates, better detection efficiencies, and higher bandwidths than its single photon counterpart and is easily adapted to current communication systems. Currently the two main protocols in CV QKD are post-selection (PS) [3] and reverse reconciliation (RR) [4]. These protocols are based on the random Gaussian modulation of coherent states using either homodyne [4] or heterodyne [5] detection and both have been experimentally demonstrated [6–10]. At present PS-based CV QKD has practical advantages in terms of key distillation and has been demonstrated experimentally for up to 90% channel loss [7].

Reverse reconciliation CV QKD, due to its inherent nature, easily incorporates excess noise into the protocols, and security proof has been demonstrated in the case of individual Gaussian attacks [4,5], non-Gaussian attacks [11], collective attacks [12,13] (with their Gaussian optimality [14]), and coherent states using homodyne detection [15]. For PS CV QKD, the addition of excess noise into the analysis is quite difficult. The original protocol [3] only considered pure or vacuum states in its scheme, and as yet all post-selection protocols have concentrated on the unrealistic case of zero excess noise [7,16,17]. Recently however, excess noise using a hybrid protocol, consisting of both post-selection and either direct or reverse reconciliation, was considered for the case of collective attacks [18].

In this paper, we present a protocol for calculating the effect of excess Gaussian noise (EGN) on post-selection where two-way classical communication is permitted, and show its security when considering either individual or collective attacks. We apply our analysis to an experimental demonstration and conclude that good key rates can be obtained under the realistic condition of a channel with loss and excess Gaussian noise (Fig. 1).

We extend the original PS CV QKD protocol [3] as follows. The sender, Alice, draws two random numbers S_A^x and S_A^p from Gaussian distributions of variances V_A^x and V_A^p, respectively, which she encodes on the amplitude (x) and phase (p) of a coherent beam. Each encoding (S_A^x, S_A^p) represents a pair of bits whose value is fixed by the sign of the encoding. The modulated Gaussian beam is then transmitted to the receiver, Bob, through a lossy and noisy Gaussian channel with transmission η and variance of EGN ξ. Bob receives a Gaussian mixed state $\hat{\rho}_B$ with variance $V_B^{x,p}=\eta V_A^{x,p}+1+\xi$, and then randomly measures either the amplitude m_B^x or phase m_B^p quadratures of this mixed state. As both amplitude and phase play the same role, we will only explicitly consider one quadrature for the rest of this paper, and denote Alice's encoding and Bob's measurement as S_A and m_B, respectively. The probability that Bob measures a particular value m_B given that Alice used a particular encoding S_A is given by the conditional probability,

$$p(m_B|S_A) = \frac{e^{-(m_B - \sqrt{\eta}S_A)^2/[2(1+\xi)V_V]}}{\sqrt{2\pi(1+\xi)V_V}}, \tag{1}$$

where V_V is the variance of the vacuum noise. Note that in this paper the vacuum noise is normalized to $V_V=1$. The error rate in Bob deciding whether Alice encoded positively or negatively is thus given by

$$P_e = \frac{1}{1+e^{2\sqrt{\eta}|S_A m_B|/[(1+\xi)V_V]}}. \tag{2}$$

The mutual information rate between Alice and Bob is given as a function of this error probability using the Shannon formula [19] $I_{AB}=\Phi(1-2P_e)$, where

$$\Phi(x) = \tfrac{1}{2}[(1+x)\log_2(1+x)+(1-x)\log_2(1-x)]. \tag{3}$$

Bob then informs Alice over a public channel which quadrature he measured and at what time interval. Alice and Bob then both announce the absolute values of their encodings $|S_A|$ and measurement results $|m_B|$, respectively. This is in contrast to previous zero excess noise protocols where only Alice announces her absolute value [3,7]. Alice and Bob then post-select information for which they have a mutual information advantage over Eve and discard information for which they do not. Alice and Bob also choose a random subset of data to characterize the channel loss η, the EGN ξ, and check that the statistics are Gaussian. Finally Alice and

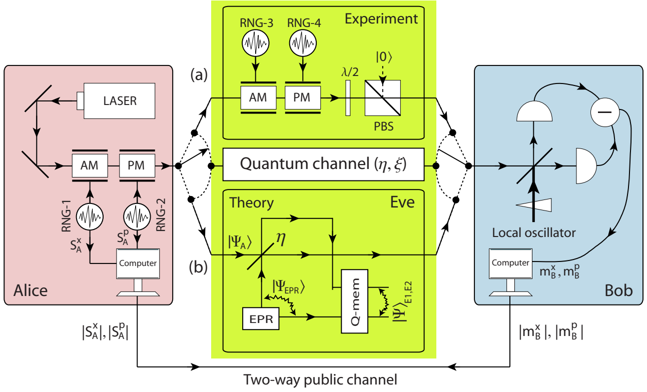

FIG. 1. (Color online) Schematic of setup. Quantum channel of transmission η and excess noise ξ is simulated experimentally (a) and analyzed theoretically for the entangling cloner attack (b). λ/2, half-wave-plate; PBS, polarizing beam-splitter; AM (PM), amplitude (phase) modulators; RNG, independent white noise generators; EPR, entanglement source; Q-mem, quantum memory.

Bob use a two-way reconciliation algorithm to reconcile their data.

As with any type of eavesdropping attack, we assume any EGN on the quantum channel is always attributed to, and controlled by, the eavesdropper, Eve. The fact that there exists excess noise on the channel allows Eve to be entangled to Bob. There exists a known upper bound $\xi < 2\eta$ [16] to the amount of EGN ξ that can be added on a channel of transmission η above which Alice's and Bob's quantum correlation cease to exist [4]. We consider here the entangling cloner attack which has been shown optimal for PS CV QKD with collective attacks in the presence of EGN [18]. The entangling cloner attack [see Fig. 1(b)] consists of Eve replacing the lossy line by a beam splitter of transmission η where one of the inputs is Alice's initial state in a quadrature basis given by

$$|\psi_A\rangle = (2\pi)^{-1/4} \int dx_1 e^{-(1/4)(x_1 - S_A)^2} |x_1\rangle \tag{4}$$

and the second input is one arm of an entangled state Eve has created given by

$$|\psi_{\text{EPR}}\rangle = \frac{1}{\sqrt{2\pi}} \int\int dx_2 dx_3 e^{(1/4)(-V_s x_2^2 - x_3^2/V_s)} \left| \frac{1}{\sqrt{2}}(x_2 + x_3) \right\rangle \times \left| \frac{1}{\sqrt{2}}(x_2 - x_3) \right\rangle, \tag{5}$$

where $\frac{1}{2}(V_s + 1/V_s) = (1-\eta+\xi)/(1-\eta)$ is the variance of the entangled beam she injects to simulate the EGN ξ. Eve keeps one of the entangled beams (denoted E_1) and one of the outputs of the beam splitter (denoted E_2) while she sends the remaining output to Bob (denoted B) through a perfect noiseless and lossless line. When Bob performs his homodyne measurement and announces its absolute value $|m_B|$, Eve's state collapses to one of the four possible pure states given by $|\psi_b^a\rangle_{E_1,E_2}$, where the superscript $a=0,1$ refers to Alice's encoded bit and the subscript $b=0,1$ to Bob's measured bit,

$$|\psi_b^a\rangle_{E_1,E_2} = \frac{1}{\sqrt{\eta}(2\pi)^{3/4}} \int\int dx_2 dx_3 e^{-(1/4)\{[(-1)^b(|m_B|/\sqrt{\eta}) - (-1)^a|S_A| - \sqrt{(1-\eta)/2\eta}(x_3 - x_2)]^2 + x_2^2 V_s + x_3^2/V_s\}} \times \left| -(-1)^b \sqrt{\frac{1-\eta}{\eta}} |m_B| - \sqrt{\frac{1}{2\eta}}(x_2 - x_3) \right\rangle_{E_2} \left| \frac{1}{\sqrt{2}}(x_2 + x_3) \right\rangle_{E_1}. \tag{6}$$

Note that this state is not normalized, $\langle\psi|\psi\rangle = p_{m_B|S_A}$ given by Eq. (1). The amount of secure bits that Alice and Bob can extract for each transmission is given by $\max\{0, I_{AB} - \max\{I_{AE}, I_{BE}\}\}$. Eve chooses to maximize her information with either Alice or Bob depending on which will give her the greater information. If Eve decides to attack Alice, she needs to distinguish between the states $\rho_{AE}^a = |\psi_0^a\rangle\langle\psi_0^a| + |\psi_1^a\rangle \times \langle\psi_1^a|$. To attack Bob, she needs to distinguish between the states $\rho_{BE}^b = |\psi_b^0\rangle\langle\psi_b^0| + |\psi_b^1\rangle\langle\psi_b^1|$.

The inner products between these states can be computed explicitly by performing the Gaussian integrations in Eq. (6). For example, the four terms that distinguish Eve's input for attacking Alice from her inputs for attacking Bob are

$$\langle\psi_0^0|\psi_0^1\rangle = \langle\psi_1^1|\psi_1^0\rangle = \frac{\exp\left(-\frac{m_B^2 + (1+\xi)S_A^2}{2(1+\xi)}\right)}{\sqrt{2\pi(1+\xi)}}, \tag{7}$$

$$\langle\psi_0^0|\psi_1^0\rangle = \langle\psi_1^1|\psi_0^1\rangle = \frac{\exp\left(-\frac{(1+\xi)^2 m_B^2 + \eta S_A^2}{2(1+\xi)}\right)}{\sqrt{2\pi(1+\xi)}}. \tag{8}$$

We see that at the critical value of $m_B^c = \sqrt{1+\xi-\eta/(1+\xi)^2-1}\,S_A$, all of the above inner products are equal. Eve's input state for attacking Alice is unitarily equivalent to that for attacking Bob, and hence her accessible information with Alice is exactly the same as with Bob: $I_{AE} = I_{BE}$. When $m_B > m_B^c$, Eve would gain more information by attacking Bob while below this line she stands to gain more by attacking Alice.

Given Eve's two input states, we need to find her accessible information. If this is smaller than I_{AB}, Alice and Bob keep the bit and distill a key from it. Our task now is to find Eve's accessible information for such states. We bound this information from above for both individual and collective attacks.

A bound on Eve's accessible information $I_E^{(i)}$ in the case of individual attacks is calculated by providing her with the knowledge on whether Alice's and Bob's bit values match or not. With this information, Eve's input is reduced to two pure states. Her accessible information is bounded by

$$I_E^{(i)} = p_1 \Phi(\sqrt{1-f_1^2}) + p_2 \Phi(\sqrt{1-f_2^2}), \qquad (9)$$

where p_1 is the probability that Alice and Bob obtain the same bits and p_2 is the probability that their bits differ, and

$$f_1 = \frac{\langle \psi_0^0 | \psi_1^1 \rangle}{\langle \psi_0^0 | \psi_0^0 \rangle} \quad \text{and} \quad f_2 = \frac{\langle \psi_1^0 | \psi_0^1 \rangle}{\langle \psi_1^0 | \psi_1^0 \rangle} \qquad (10)$$

are the normalized inner products between the states that Eve distinguishes [20]. We note that this bound corresponds to the Levitin bound as given in [3] for the case of no added noise.

We apply Holevo's theorem [21] on Eve's input states, ρ_E, to bound Eve's information in terms of the von Neumann entropy, $S(\rho)$, and obtain the amount of information $I_E^{(c)}$ accessible by Eve when performing collective attacks,

$$I_E^{(c)} = S(\rho_E^0 + \rho_E^1) - S(2\rho_E^0)/2 - S(2\rho_E^1)/2. \qquad (11)$$

Figure 2 shows the difference in mutual information from Bob's point of view when Alice announces S_A for a fixed value of η and ξ. For each η and ξ, Alice then chooses the value of V_A^{opt} such that the weighted integral over the positive information region Ω given below is maximized,

$$\Delta I^{(i,c)} = \int_\Omega p(S_A, m_B)(I_{AB} - I_E^{(i,c)}) dm_B dS_A. \qquad (12)$$

In principle, as long as the post-selection region is nonempty, Alice and Bob can always distill a finite amount of key. At a certain noise threshold however, we expect that there will be no more post-selectable region. This is clear for $\xi=2\eta$ [16], since then the state between Alice and Bob becomes separable. In this case, Eve can do an intercept and resend attack in which $I_E > I_{AB}$ for all values of S_A and m_B.

But even before the separability limit is reached, the post-selectable region may become empty. To analyze this, we consider the case when S_A is large. In such a case, Alice and Bob would share the same bits with a high probability. Eve's accessible information then tends to $\Phi(\sqrt{1-f_1^2})$. In this limit, Eve's input becomes ever closer to being just two classical pure states and so Holevo's bound would tend to the same limiting information. Equating this with I_{AB}, we obtain two solutions for $m_B^{l\pm}$,

$$m_B^{l\pm} = \frac{\sqrt{\eta}(1+\xi) \pm \sqrt{\eta(1+\xi)^2 - \xi(\xi+2)(\xi+1-\eta)}}{\xi(2+\xi)} S_A. \qquad (13)$$

In other words, the region of post-selectibility asymptotes to these two lines as S_A increases (see Fig. 2). The noise threshold ξ_0 over which the quantum channel is insecure is obtained when the two lines m_B^{l+} and m_B^{l-} coincide such that there is no more region of post-selectibility. This occurs when $\eta(1+\xi_0)^2 = \xi_0(\xi_0+2)(\xi_0+1-\eta)$.

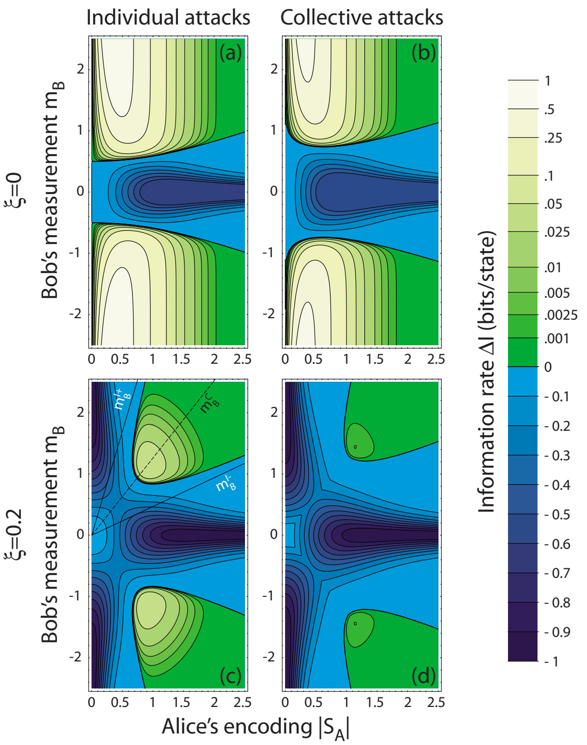

FIG. 2. (Color online) Post-selection regions at $\eta=0.5$ are shown in red. (a) and (b) show the information rates $\Delta I = I_{AB} - I_E$ with no excess noise for individual and collective attacks. (c) and (d) is when $\xi=0.2$. On the dashed line m_B^c in (c), Eve can obtain the same amount of information from Alice as she can from Bob. The post-selection region asymptotes to the lines $m_B^{l\pm}$.

Figure 1(a) shows the schematic of our experiment. In this setup we encoded keys on the amplitude quadrature and simulated the loss of the line by using a variable attenuator and the added noise by adding a random Gaussian signal onto the amplitude quadrature on Alice's amplitude modulator. The transmitted light is detected using a homodyne detection setup at Bob's station. The two sets of time series, Alice's encoding S_A and Bob's measurement m_B were analyzed using the tools developed in [7]. We note that extraction of the final key can be performed using the methods described in [7] with an average efficiency of 2% to 4% for all data sets with positive raw information rates ΔI.

Figure 3 shows experimental results superimposed onto theoretical bounds of total post-selected information rates $\Delta I = I_{AB} - I_E$ at channel transmission $\eta=47\%$ for individual and collective attacks, as a function of channel EGN ξ. The experimental mutual information rate between Alice and Bob I_{AB} is calculated by comparing the two signal-processed time series S_A^x and m_B^x. This quantity is less than the theoretical calculation due to experimental imperfections associated with the encoding (e.g., nonoptimum encoding variance), detection (e.g., homodyne inefficiency), and signal processing. Experimental uncertainty is calculated for I_{AB} due to the finite number of data points. The information rate for Eve I_E is calculated theoretically, with error bars in I_E calculated using the uncertainties in channel transmission, EGN, and Alice's variance V_A.

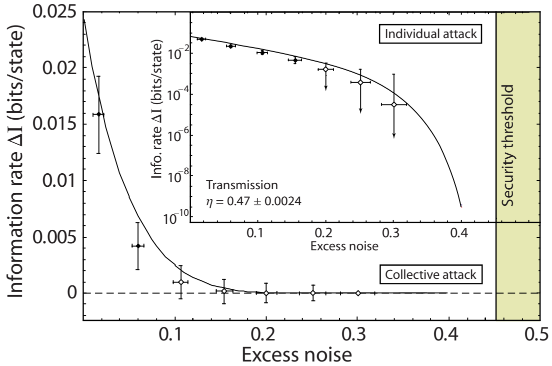

FIG. 3. (Color online) Experimental results superimposed on theoretical lower bounds of secure key rates at transmission $\eta = 0.47 \pm 0.002$ when Eve does a collective attack and an individual attack (inset). Unfilled data points with arrows have error bars going to negative ΔI. The shaded region indicates the noise threshold for secure keys. The experimental results were obtained using an encoding variance optimized for the individual attack bound.

The experimental data points ΔI_{exp} are in good agreement with the theoretical results. For some of the higher EGN cases, the error bars extend towards the negative region. It should be emphasized however, that this is mainly due to the finite number of collected data that results in statistical uncertainties. In our experiment, 2.4 Mbits of data were taken per run. The theoretical curves for ΔI in Fig. 3 monotonically decreases until they reach exactly zero at the security threshold line. No secure keys can be generated in the shaded region.

Figure 4 shows the experimental results superimposed on contour plots of ΔI as a function of η and ξ. Three sets of experimental runs were taken for $\eta \approx 0.2, 0.5, 0.8$. Filled and unfilled data points indicate $\Delta I_{\text{exp}} > 0$ and $\Delta I_{\text{exp}} \leq 0$, respectively. We obtained positive information rates for $\eta = 0.2$ and $\xi = 0.1$. In principle, lower η is attainable; the experimental demonstration for such cases is left for future work.

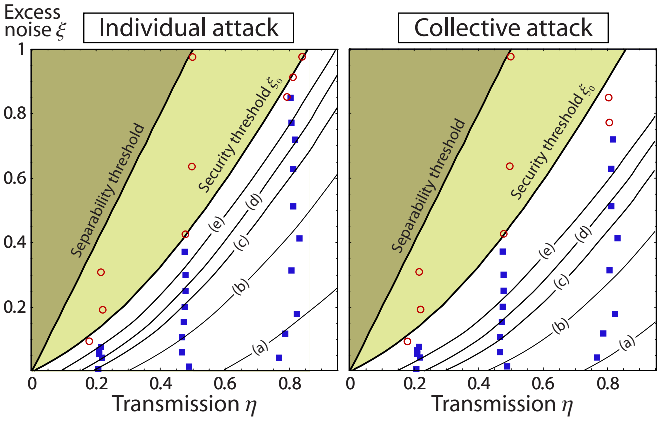

FIG. 4. (Color online) Experimental results superimposed on theoretical contour plots of information rate after post-selection (ΔI) as a function of channel transmission η and EGN ξ. (a),(b),(c),(d),(e) indicates $\Delta I = 10^{-1}, 10^{-2}, 10^{-3}, 10^{-4}, 10^{-7}$ (bits/state). Filled (unfilled) data points indicate $\Delta I_{\text{exp}} > 0$ ($\Delta I_{\text{exp}} \leq 0$). No secure keys can be generated in the shaded regions. Dark shade indicates separability between Alice's and Bob's states.

In conclusion, we have extended the original post-selection protocol [3] to take into account the effect of channel EGN for individual and collective Gaussian attacks by an eavesdropper. In both cases, we find that the scheme is still secure. We have also presented an experimental demonstration, which verifies that continuous-variable quantum cryptography using post-selection is secure in the presence of channel loss as well as EGN. This is important since realistic laser sources and optical fibers [8] inevitably inherit EGN. Reanalyzing our results from [7] using the theory presented in this paper we conclude that the small amount of EGN present in that experiment would have had negligible effect on the key rates if properly accounted for.

The authors thank Ch. Silberhorn and N. Lutkenhaus for useful discussions and acknowledge financial support from the Australian Research Council and the Department of Defense.

[1] *Quantum Information Theory with Continuous Variables*, edited by S. L. Braunstein and A. K. Pati (Kluwer, Dordrecht, 2003).
[2] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).
[3] Ch. Silberhorn, T. C. Ralph, N. Lutkenhaus, and G. Leuchs, Phys. Rev. Lett. **89**, 167901 (2002).
[4] F. Grosshans, N. J. Cerf, J. Wenger, R. Tualle-Brouri, and Ph. Grangier, Quantum Inf. Comput. **3**, 535 (2003).
[5] C. Weedbrook *et al.*, Phys. Rev. Lett. **93**, 170504 (2004).
[6] F. Grosshans*et al.*, Nature (London) **421**, 238 (2003).
[7] A. M. Lance, T. Symul, V. Sharma, C. Weedbrook, T. C. Ralph, and P. K. Lam, Phys. Rev. Lett. **95**, 180503 (2005).
[8] J. Lodewyck, T. Debuisschert, R. Tualle-Brouri, and P. Grangier, Phys. Rev. A **72**, 050303(R) (2005).
[9] J. Lodewyck *et al.*, Phys. Rev. Lett. **98**, 030503 (2007).
[10] S. Lorenz, J. Rigas, M. Heid, U. L. Andersen, N. Lutkenhaus, and G. Leuchs, Phys. Rev. A **74**, 042326 (2006).
[11] F. Grosshans and N. J. Cerf, Phys. Rev. Lett. **92**, 047905 (2004).
[12] F. Grosshans, Phys. Rev. Lett. **94**, 020504 (2005).
[13] M. Navascues and A. Acin, Phys. Rev. Lett. **94**, 020505 (2005).
[14] M. Navascues, F. Grosshans, and A. Acin, Phys. Rev. Lett. **97**, 190502 (2006); R. Garcia-Patron and N. J. Cerf, *ibid.* **97**, 190503 (2006).
[15] S. Iblisdir, G. Van Assche, and N. J. Cerf, Phys. Rev. Lett. **93**, 170502 (2004).
[16] R. Namiki and T. Hirano, Phys. Rev. Lett. **92**, 117901 (2004).
[17] R. Namiki and T. Hirano, Phys. Rev. A **74**, 032302 (2006).
[18] M. Heid and N. Lütkenhaus, e-print arXiv:quant-ph/0608015.
[19] C. E. Shannon, Bell Syst. Tech. J. **27**, 623 (1948).
[20] L. B. Levitin, in *Quantum Communication Measurements*, edited by V. P. Belavkin, O. Hirota, and R. L. Hudson (Plenum, New York, 1995).
[21] A. S. Holevo, Probl. Peredachi Inf. **9**, 311 (1973).