PHYSICAL REVIEW A **87**, 020303(R) (2013)

Security of continuous-variable quantum cryptography with Gaussian postselection

Nathan Walk,[1,2,*] Timothy C. Ralph,[1,2] Thomas Symul,[1,3] and Ping Koy Lam[1,3]
[1]*Centre for Quantum Computation and Communication Technology*
[2]*School of Mathematics and Physics, University of Queensland, St. Lucia, Queensland 4072, Australia*
[3]*Department of Physics, Faculty of Science, Australian National University, Acton, ACT 0200, Australia*
(Received 20 July 2011; revised manuscript received 10 June 2012; published 21 February 2013)

We extend the security analysis of continuous variable quantum-key-distribution protocols using a family of post selection schemes to account for arbitrary eavesdropping attacks. We show that the postselection protocol is equivalent to a virtual entanglement-based protocol including a distillation stage. We introduce a particular 'Gaussian' post selection and demonstrate that the security can be calculated using only experimentally accessible quantities. Finally, we explicitly evaluate the performance for the case of a noisy Gaussian channel in the limit of unbounded key length and find improvements over all pre-existing continuous variable protocols in realistic regimes.

DOI: 10.1103/PhysRevA.87.020303 PACS number(s): 03.67.Dd, 03.67.Hk

Quantum key distribution (QKD) is the process of generating a common random key between two parties using a quantum communications protocol. The power of this method is that the security of the key distribution, and the subsequent communication via a one time pad, is established while making no assumptions about the technological capabilities of an eavesdropper. This procedure also has the distinction of being the most developed quantum information technology [1].

There are two main flavors of QKD, discrete variable (DV) and continuous variable (CV), which are realized by encoding and then detecting single photons [2] and the quadrature variables of the optical field [3], respectively. The latter kind, which we consider here, has the advantage of higher raw bit rates due to the high efficiency and high bandwidth of homodyne detection and ease of integration with the existing communications infrastructure. CV protocols that employ postselection [4]—a classical filtering of the measurement results—enjoy additional advantages in terms of versatility and reconciliation efficiency. Asymptotic (in the sense of string length) unconditional security for protocols that do not employ postselection is achieved by first noting the equivalence of an experimentally implemented prepare and measure (P&M) scheme to an entanglement-based (EB) version [5], originally proposed in the DV context [6]. This is followed by the result that, for collective attacks, security may be bounded from below by assuming that the entangled state at the end of the protocol is Gaussian [7,8] and, finally, a proof that collective attacks are asymptotically optimal [9]. However, for protocols using post-selection (PS) this analysis cannot be straightforwardly applied as an equivalent entanglement based picture has yet to be constructed, with security only shown under the assumption of a Gaussian eavesdropping attack [10].

Here we fill this gap and hence demonstrate unconditional security for postselected CVQKD following the proof method used in [8]. In particular, we construct an EB scheme in which the postselection is replaced by equivalent heralded state transformations. We show we are able to straightforwardly construct the necessary parameters of this EB scheme from experimental data providing a realistically obtainable bound for the case of collective attacks and hence asymptotically unconditional security. This extension only holds automatically if the postprocessing is independent under permutations of Alice and Bob's subsystems. This is the case for the protocol considered here, as the postselection decision for an individual measurement depends only upon that measured value and an ensemble average, with the order of measurements being immaterial.

Security of CVQKD. In general one equates each protocol in which the sender (Alice) prepares an ensemble of quantum states based upon a classical random probability distribution and sends it through the domain of the eavesdropper (Eve) to the recipient (Bob), to an entanglement based scheme in which Alice prepares an entangled state one half of which is kept and used for a projective measurement and the other transmitted to Bob again through Eve's domain. The proper choice of the initial entangled state and the projective measurement by Alice allows us to rigorously express any prepare and measure schemes [5].

Bob performs a quadrature measurement upon his received states and then Alice and Bob engage in a reconciliation procedure to correct the errors in their shared classical string. The secret key rate for the entire protocol is then given by [1]

$$K = \beta I(a:b) - I(E:X), \quad X \in \{a,b\} \tag{1}$$

where $I(a:b)$ is the Shannon mutual information between classical strings belonging to Alice and Bob at the end of the protocol, β is the efficiency of their reconciliation procedure, and $I(E:X)$ is the quantum mutual information between either Eve and Bob, if considering reverse reconciliation protocols, or Eve and Alice, if considering direct reconciliation.

Eve's mutual information is given by the purification of the entangled state before and after Alice or Bob's measurement. For example, the direct reconciliation expression is [7,8]

$$I(E:a) = S(\rho_E) - S(\rho_E|a) = S(\rho_{AB}) - S(\rho_B|a) \tag{2}$$

with the von Neumann entropy given by $S(\rho) = -\mathrm{tr}(\rho \log \rho)$, and for the second equality we have used the fact that the overall tripartite state $|ABE\rangle$ is pure. This quantity is not easy to calculate in general but it has been shown that we may bound Eq. (1) from below by analyzing a Gaussian [7,8], symmetric [11] state with the same first and second moments. For Gaussian states, the von Neumann entropy is obtained

*walk@physics.uq.edu.au

straightforwardly and thus the security of the entire protocol can be characterizsed entirely by the covariance matrix of the entangled state shared by Alice and Bob.

Equivalent postselection scheme. While reverse reconciliation can be shown to be secure for arbitrary losses in the absence of noise, for any nonzero amount of excess noise the secure distance is inevitably finite. One could attempt to address this by increasing the input signal modulation, however, any imperfection in the reconciliation process ($\beta < 1$) means that optimizing the modulation can also only lead to a finite improvement. On the other hand, direct reconciliation is significantly more tolerant to excess noise but only successful when the channel loss is below 50% or 3 dB.

All of these detrimental effects can be improved using postselection [4], a technique in which values in the space of Bob's possible quadrature measurement results and Alice's quadrature encoding are probabilistically reweighted and only these new distributions are kept to form the key. Intuitively one would expect this strategy to yield an advantage, as the eavesdropper is effectively shut out of Alice and Bob's postmeasurement collaboration. This improved performance comes at the price of not being able to directly apply Eq. (2), as this would not allow for Eve's knowledge of Alice and Bob's postselection. This can be accounted for as long as one can keeps track of the way postselection by one party influences the state of the other in the equivalent EB scheme which we now demonstrate.

In general, one postselects by applying a weighting function to achieve a new probability distribution in the chosen measurement basis, $p(x) \xrightarrow{\text{PS}} w(x)p(x) = p'(x)$. The normalization of $p'(x)$ gives the amount of data retained while transitioning from the initial to the postselected ensemble. Alternatively, one could apply an appropriate transformation consisting of a unitary acting on the mode in question together with an auxiliary mode(s) which is(are) subsequently traced out. A useful postselection will correspond in the EB scheme to achieving some amount of distillation of the virtual entanglement, inevitably along with some additional noise. This setting is represented in Fig. 1. The probabilistic nature of the postselection corresponds to Bob's first operation being a nondeterministic but heralded distillation operation (U_D) followed by appropriate deterministic unitary interactions corresponding to the noise addition and Bob's final measurement.

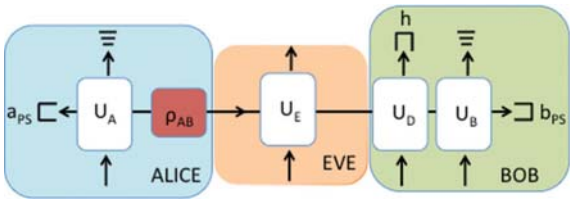

FIG. 1. (Color online) Equivalent entanglement-based version of a postselected protocol. Alice distributes one arm of an entangled state through Eve's domain to Bob and makes a projective measurement U_A (giving classic output a) corresponding to an ensemble of states sent in a prepare-and-measure scheme. Bob passes his arm first through a device that probabilistically distills entanglement, U_D, and then makes a potentially noisy measurement, U_B, giving classical output b_{PS}. The heralding signal of U_D (h) is given to Eve but the remaining ancillae are kept within the stations of Alice and Bob.

In this picture Eve's additional knowledge gained when Alice and Bob apply a postselection is reflected by the state ρ_{AB} in Eq. (2) being identified with the state conditioned on successful heralding of Bob's first operation, i.e., given the result of U_D but not U_B. After all ancillae are traced over, the outputs of U_A and U_B give classical strings a and b_{PS} which exactly match the experimental results for the postselected ensemble. Note that, as usual, we consider the secure station scenario where the ancillae remaining within the laboratories of Alice and Bob are not attributed to the eavesdropper.

The worst-case scenario would correspond to the final state being Gaussian [7,8] so if one is able to uniquely identify a Gaussian collection of unitaries and ancillae that result in the same measurement statistics, then the key rate of that state will provide a lower bound for the postselected protocol. Furthermore, this necessitates that the distillation operation itself produces a Gaussian output, which leads us to conclude that the distillation appearing in the EB scheme used for bounding the key rate should be the noiseless linear amplifier of [12] and [13]. Denoting s a successful run of the distillation, we can think of the whole postselection as $U_{\text{PS}} = U_D U_B$ and the resultant state as $\rho_{\text{PS}} = \frac{(U^s_{\text{PS}})^\dagger \rho_{AB} U^s_{\text{PS}}}{\text{tr}[(U^s_{\text{PS}})^\dagger \rho_{AB} U^s_{\text{PS}}]}$. One may then write Eve's information on the postselected ensemble for direct reconciliation as

$$I_{\text{PS}}(E:a) = S(\rho_{\text{PS}}) - S(\rho_{\text{PS}}|a) \leqslant S\big(\rho^G_{\text{PS}}\big) - S\big(\rho^G_{\text{PS}}|a\big), \quad (3)$$

where ρ^G_{PS} is a Gaussian state with the same covariance matrix. If the postselection is perfectly Gaussian, then there will be an exact equivalence between the EB scheme and the protocol as carried out and these bounds should be tight. If the postselection is non-Gaussian, the two schemes will only be effectively equivalent to the extent of having the same covariance matrix and the same (loose) lower bound for the key rate. This method is thus applicable to highly non-Gaussian postselection, however, demonstrating that the covariance matrix of the equivalent Gaussian setup can be obtained from measured data is nontrivial and may be more or less experimentally demanding, depending upon the particular form of the postselection.

Gaussian postselection. We consider a particular P&M scheme [Fig. 2(a)], in which Alice draws values (x_A, p_A) from a bivariate Gaussian of 0 mean and variance V_A and uses these numbers to displace the vacuum to create an ensemble of coherent states of the form $|x_A + ip_A\rangle$, which she sends to Bob through a quantum channel. Bob uses homodyne detection on his received states, randomly switching between amplitude and phase quadratures given by $\hat{x} = \hat{a} + \hat{a}^\dagger$ and $\hat{p} = i(\hat{a}^\dagger - \hat{a})$, where we have normalized the shot-noise limit to unity. Bob then filters his results with the goal of selecting an ensemble which is a Gaussian distribution with a certain target variance V_{PS}. For the most common case of a Gaussian channel Bob's input distribution is another Gaussian of variance V_B and the appropriate weighting function would look like $w(x) = \sqrt{V_B/V_{\text{PS}}}\exp(-x^2(1/V_{\text{PS}} - 1/V_B))$. In the relevant case $V_{\text{PS}} > V_B$ this function is convex, so in order to obtain a proper probability distribution we choose some end points $\pm\Delta$, renormalize the function to the value at this point, and set all values outside this range to unity. For a Gaussian

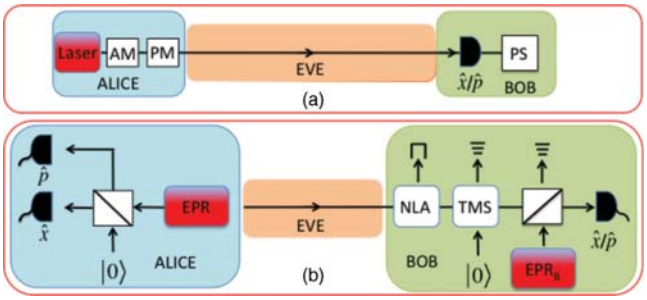

FIG. 2. (Color online) Prepare-and-measure (P&M) and effective entanglement-based versions of a protocol using Gaussian postselection. (a) P&M scheme: Alice uses two classical Gaussian strings (x_A, p_A) to prepare and transmit an ensemble of coherent states to Bob, who homodyne detects and then applies a Gaussian weighting function. (b) Effective EB scheme: Alice distributes one arm of an EPR pair and makes a heterodyne measurement, obtaining measurement results equivalent to (x_A, p_A). Bob first passes his arm through an NLA, classically amplifies via a vacuum-seeded two-mode squeezer (TMS), then mixes his mode with one arm of another entangled pair (EPR_B) on a beamsplitter. He finally homodyne detects and obtains exactly the measurement results from the P&M scheme. The heralding signal of the NLA is given to Eve but the unmeasured ancillae are kept within Bob's station.

input state the exact filter function is

$$W(x) = N\left[1 + \left(\frac{w(x)}{w(\Delta)} - 1\right)[\Theta(x+\Delta) - \Theta(x-\Delta)]\right], \tag{4}$$

where $\Theta(x)$ is the Heaviside step function and the fraction of data kept is the renormalization N. When Δ is 0 this operation is the identity. As $\Delta \to \infty$ it results in a Gaussian distribution of variance V_{PS} and in between it gives a slightly non-Gaussian state with variance $V_B < V < V_{\mathrm{PS}}$. Finally, Alice and Bob publicly announce a subset of their data to characterize the covariance matrix on both the initial and the postselected ensemble and, if secure, engage in reconciliation and privacy amplification to distill a completely secure key. Notice that although the weight function is smooth instead of hard edged, it is determined entirely by Bob and the only information he sends to Alice is a "keep or reject" signal.

The equivalent entanglement-based scheme [Fig. 2(b)] involves Alice preparing a two-mode squeezed vacuum or EPR state, one mode of which she keeps and measures, the other being transmitted to Bob. Alice's makes a heterodyne detection, whereas Bob's measurement, depending upon the target variance, decomposes into a combination of a noiseless amplification/distillation followed by classical amplification and, finally, some additional noise. The necessary Gaussian entanglement distillation is achieved via the noiseless linear amplifier (NLA) [12,13], with the classical amplifier and additional noise corresponding to a two-mode squeezer with vacuum ancilla and a beamsplitter with an EPR pair ancilla, respectively. If we can uniquely characterize Gaussian operations that perform the necessary transformations from the transmitted to the postselected ensemble at the level of the covariance matrix, then we can apply the above proof and determine the security.

To illustrate this method we evaluate the performance for the noisy Gaussian channel, completely parametrized by transmission T and excess noise ξ [14]. One can calculate the action of an NLA on an EPR state sent through a general Gaussian channel [15,16], with the result being an effective protocol for which stronger entanglement was distributed through a channel with less loss but greater excess noise, leading to an overall advantage. Inverting the expression between the gain of the NLA and the effective entanglement generated gives the relationship

$$g = 1 + \frac{2\left(V_A^{\mathrm{PS}} - V_A\right)}{T\left(V_A\left(2 + V_A^{\mathrm{PS}} - \xi\right) + V_A^{\mathrm{PS}}\xi\right)}, \tag{5}$$

where V_A^{PS} is the effective variance that uniquely identifies the gain of the NLA based only upon Alice's modulation variance before (V_A) and after (V_A^{PS}) postselection of the measured channel parameters.

Bob and Alice's other operations are just beamsplitters and two-mode squeezing, their effect on the covariance matrix being given by the appropriate symplectic transformations [17]. Given Alice and Bob's measurement of the covariance matrix before and after the postselection, straightforward algebra allows us to characterize all parameters in Fig. 2 and thus unconditionally bound Eve's information via Eq. (3). The crucial trade-off in this scheme is between a large postselection

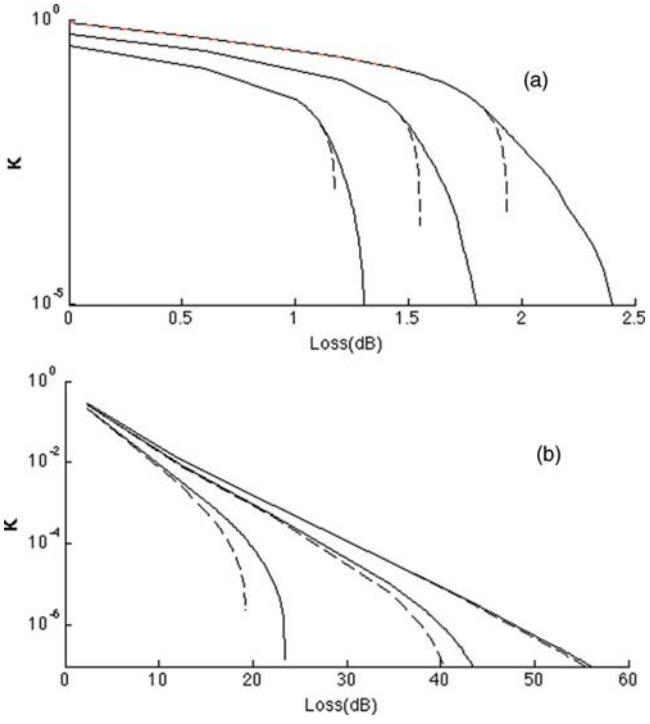

FIG. 3. (Color online) Improvement in secret key rates due to Gaussian postselection. (a) Direct reconciliation with postselection (solid lines) and without postselection (dashed lines) as a function of loss for $\xi = \{0.1, 0.2, 0.3\}$ with decreasing key rate. (b) Reverse reconciliation with postselection (solid lines) and without postselection (dashed lines) as a function of loss for $\xi = \{0.02, 0.03, 0.05\}$ with decreasing key rate. For all plots $\beta = 0.9$ and the modulation variance is numerically optimized [15].

to improve the effective channel and the proportion of measurement results that are discarded.

We plot the actual key rate (that is, the key multiplied by N to account for symbols thrown away in the postselection) as a function of the distance of a coherent-state homodyne protocol (Fig. 3) for both direct and reverse reconciliation, along with the case without postselection for comparison. In all plots the reconciliation efficiency is taken to be a constant value of $\beta = 0.9$ and for each point Alice's modulation variance is independently optimised for each protocol along with the parameters (Δ, V_{PS}) for the postselected scheme. For these realistic experimental parameters the postselection protocol allows for secure key generation over long distances (in combination with RR) and for greater excess noise (in combination with DR) than any previous coherent-state protocol. Finally, the presence of an NLA in the effective Gaussian circuit leads one to compare these results with those in [16]. We find that almost all of the improvements shown there are recovered by our classical postprocessing scheme. This leads one to conclude that an NLA placed just before Bob's detectors will not lead to a benefit for QKD over and above that of postselection.

Conclusion. In conclusion, we have shown how the security of postselection-based CVQKD can be analyzed for arbitrary collective attacks and asymptotically extendable to all attacks if invariant under subsytem permutation. This was achieved by identifying an entanglement-based scheme that correctly reflects the postselected ensemble that is used in the final key generation. Results for a particular Gaussian form of postselection show improvements in performance over all previous coherent-state protocols for certain relevant combinations of loss and noise. Avenues for further work include the investigation of other postselection filters, with a view to proving which is optimal, the incorporation of finite-size effects, and the combination of postselection with other protocols.

Note added. Recently, we were made aware of an independent work showing the equivalence between Gaussian PS and NLA for heterodyne measurements [18].

Acknowledgments. The authors would like to thank Norbert Lütkenhaus, Christian Weedbrook, Anthony Leverrier, Remi Blandino, and Andrew Lance for helpful discussions. This research was conducted by the Australian Research Council Centre of Excellence for Quantum Computation and Communication Technology (Project No. CE11000102).

[1] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, Rev. Mod. Phys. **81**, 1301 (2009).

[2] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).

[3] N. J. Cerf and P. Grangier, JOSA B **24**, 324 (2007).

[4] C. Silberhorn, T. C. Ralph, N. Lütkenhaus, and G. Leuchs, Phys. Rev. Lett. **89**, 167901 (2002).

[5] F. Grosshans, N. J. Cerf, P. Grangier, J. Wenger, and R. Tualle-Brouri, Quantum Inf. Comput. **3**, 535 (2003).

[6] H.-K. Lo and H. F. Chao, Science **283**, 2050 (1999).

[7] M. Navascúes, F. Grosshans, and A. Acín, Phys. Rev. Lett. **97**, 190502 (2006).

[8] R. García-Patrón and N. J. Cerf, Phys. Rev. Lett. **97**, 190503 (2006).

[9] R. Renner and J. I. Cirac, Phys. Rev. Lett. **102**, 110504 (2009).

[10] M. Heid and N. Lütkenhaus, Phys. Rev. A **76**, 022313 (2007).

[11] A. Leverrier, E. Karpov, P. Grangier, and N. J. Cerf, New J. Phys. **11**, 115009 (2009).

[12] T. C. Ralph and A. P. Lund, in *Quantum Communication Measurement and Computing Proceedings of 9th International Conference* (American Institute of Physics, Calgary, Canada, 2009), p. 155.

[13] G. Xiang, T. C. Ralph, A. P. Lund, N. Walk, and G. J. Pryde, Nat. Photon. **4**, 316 (2010).

[14] Note that this is the excess noise referred to the input (injected by Eve), as opposed to the quantity $T\xi$ that would be directly measured by Bob at the channel output.

[15] See Supplemental Material at http://link.aps.org/supplemental/10.1103/PhysRevA.87.020303 for more details on calculations.

[16] R. Blandino, A. Leverrier, M. Barbieri, J. Etesse, P. Grangier, and R. Tualle-Brouri, Phys. Rev. A **86**, 012327 (2012).

[17] C. Weedbrook, S. Pirandola, R. García-Patrón, N. J. Cerf, T. C. Ralph, J. Shapiro, and S. Lloyd, Rev. Mod. Phys. **84**, 621 (2012).

[18] J. Fiurášek and N. J. Cerf, Phys. Rev. A **86**, 060302(R) (2012).