Quantum Cryptography Without Switching

Christian Weedbrook,[1] Andrew M. Lance,[1] Warwick P. Bowen,[1] Thomas Symul,[1]
Timothy C. Ralph,[2] 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, University of Queensland, St. Lucia, Queensland 4072, Australia*

(Received 18 May 2004; published 22 October 2004)

We propose a new coherent state quantum key distribution protocol that eliminates the need to randomly switch between measurement bases. This protocol provides significantly higher secret key rates with increased bandwidths than previous schemes that only make single quadrature measurements. It also offers the further advantage of simplicity compared to all previous protocols which, to date, have relied on switching.

DOI: 10.1103/PhysRevLett.93.170504 PACS numbers: 03.67.Dd, 42.50.Dv, 89.70.+c

Quantum cryptography is the science of sending secret messages via a quantum channel. It uses properties of quantum mechanics [1,2] to establish a secure key, a process known as quantum key distribution (QKD) [3]. This key can then be used to send encrypted information. In a generic QKD protocol, a sender (Alice) prepares quantum states which are sent to a receiver (Bob) through a potentially noisy channel. Alice and Bob agree on a set of noncommuting bases with which to measure the states. Using various reconciliation [4] and privacy amplification [5] procedures, the results of measurements in these bases are used to construct a secret key, known only to Alice and Bob. Switching randomly between a pair of noncommuting measurement bases ensures security: in a direct attack, an eavesdropper (Eve) will only choose the correct basis half the time; alternatively, if Eve uses quantum memory and performs her measurements after Bob declares his basis, she is unable to manipulate what Bob measures. It is commonly assumed that randomly switching between measurement bases is crucial to the success of QKD protocols. In this Letter, we show that this is not the case, and in fact greater secret key rates can be achieved by simultaneously measuring both bases.

The original QKD schemes in the discrete variable regime were based on the transmission and measurement of random polarizations of single photon states [2]. Other discrete variable QKD protocols have been proposed [6] and experimentally demonstrated [7] using Bell states. However, the bandwidth of such schemes is experimentally limited by single photon generation and detection techniques. Consequently, in the last few years there has been considerable interest in the field of continuous variable quantum cryptography [8], which provides an alternative to the discrete approach and promises higher key rates. Continuous variable QKD protocols have been proposed for squeezed and Einstein-Podolsky-Rosen entangled states [9]. However, these protocols require significant quantum resources and are susceptible to decoherence due to losses. QKD protocols using coherent states were proposed to overcome these limitations. Originally, such schemes were only secure for line losses less than 50% or 3 dB [10]. This apparent limitation was overcome using the secret key distillation techniques of post-selection [11] and reverse reconciliation [12].

In general, security in discrete variable cryptography protocols is ensured via random switching between measurement bases [2] or random switching of state manipulation [13]. The random switching between measurement bases can be achieved simply via a 50/50 beam splitter, where the selection of the measurement basis is chosen through the random photon transmission and reflection statistics. To date, all continuous variable cryptography protocols have also relied on randomly switching between noncommuting bases. In the continuous variable regime, switching requires precise control of the phase of a local oscillator beam, which is difficult to achieve in practice. This local oscillator switching currently places a serious technical limitation on the bandwidth of cryptography protocols. In this Letter, we introduce a new coherent state protocol that does not require switching. In this

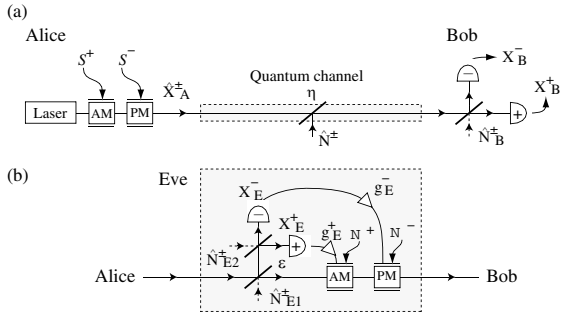

FIG. 1. (a) Schematic of the simultaneous quadrature measurement protocol. $S^{\pm}$: random Gaussian numbers, AM: amplitude modulator, PM: phase modulator, $\hat{X}_A^{\pm}$: quadratures of Alice's prepared state, η: channel transmission, $\hat{N}^{\pm}$: channel noise, $\hat{X}_B^{\pm}$: observables that Bob measures and $\hat{N}_B^{\pm}$: Bob's vacuum noise. (b) Schematic of a possible feed forward attack for Eve. $\hat{X}_E^{\pm}$: observables that Eve measures, $\hat{N}_{E1}^{\pm}$ and $\hat{N}_{E2}^{\pm}$: Eve's vacuum noises, $g_E^{\pm}$: Eve's electronic gains and $\mathcal{N}^{\pm}$: additional Gaussian noise.

protocol, both bases are measured simultaneously, utilizing the quantum channel more effectively and achieving both higher secret key rates and bandwidths compared to previous continuous variable QKD protocols.

The quantum states we consider in this Letter can be described using the field annihilation operator $\hat{a} = (\hat{X}^+ + i\hat{X}^-)/2$, which is expressed in terms of the amplitude $\hat{X}^+$ and phase $\hat{X}^-$ quadrature operators. In this Letter, we denote operators and real numbers with and without ($\hat{}$), respectively, to avoid confusion. Without a loss of generality, the quadrature operators can be expressed in terms of a steady state and fluctuating component as $\hat{X}^\pm = \langle \hat{X}^\pm \rangle + \delta\hat{X}^\pm$, which have variances of $V^\pm = \langle (\delta\hat{X}^\pm)^2 \rangle$. Figure 1(a) shows a schematic of our protocol, which we term the simultaneous quadrature measurement protocol. Our scheme is similar to the continuous variable coherent state quantum cryptography protocols presented in [10]. The protocol goes as follows: Alice draws two random real numbers, S^+ and S^-, from Gaussian distributions with zero mean and a variance of $V_S^\pm$. She then prepares a state by displacing the amplitude and phase quadratures of a vacuum state by S^+ and S^-, respectively. The quadrature operators of Alice's state are therefore given by $\hat{X}_A^\pm = S^\pm + \hat{X}_v^\pm$, where $\hat{X}_v^\pm$ are the quadrature operators of the initial vacuum state. The resulting state has normalized quadrature variances of $V_A^\pm = V_S^\pm + 1$. Alice transmits this state to Bob through a quantum channel with channel transmission efficiency η, which couples in channel noise $\hat{N}^\pm$, where the variances of the channel noise must obey the uncertainty relation $V_N^+ V_N^- \geq 1$. Bob simultaneously measures the amplitude and phase quadratures of the state using a 50/50 beam splitter. The quadrature variances of the state measured by Bob are given by

$$V_B^\pm = \frac{1}{2}[\eta V_A^\pm + (1-\eta)V_N^\pm + 1]. \quad (1)$$

By using secret key distillations protocols [4] and standard privacy amplification techniques [5], Alice and Bob can then distill a common secret key. It is possible to analyze our protocol using either the post-selection, or reverse reconciliation, secret key distillation techniques [11,12]. However, for simplicity, we limit our analysis to the Grosshans and Grangier reverse reconciliation protocol [12]. In this protocol, Alice and Eve both try to infer Bob's measurement results. Alice's inference can be characterized by a conditional variance which is used to calculate the secret key rate. Alice's conditional variance given Bob's measurement can be written as $V_{A|B}^\pm = \min_{g_A^\pm} \langle (\hat{X}_B^\pm - g_A^\pm \hat{X}_A^\pm)^2 \rangle$, where the gain $g_A^\pm$ is optimized to give a minimum conditional variance of

$$V_{A|B}^\pm = V_B^\pm - |\langle \hat{X}_A^\pm \hat{X}_B^\pm \rangle|^2 / V_A^\pm. \quad (2)$$

To calculate a relation between Alice's and Eve's conditional variances of Bob's measurement, $V_{E|B}^\pm$ and $V_{A|B}^\pm$, we define the states that denote Alice's and Eve's inference of Bob's measurement, expressed as: $\hat{X}_{E|B}^\pm = \hat{X}_B^\pm - \alpha\hat{X}_E^\pm$ and $\hat{X}_{A|B}^\mp = \hat{X}_B^\mp - \beta\hat{X}_A^\mp$, where $\beta\hat{X}_A^\pm$ and $\alpha\hat{X}_E^\pm$ are Alice and Eve's optimal estimates with the optimal gains, α and β being real numbers. Finding the commutator of these two equations, and using the fact that different Hilbert spaces commute, we find that $[\hat{X}_{E|B}^+, \hat{X}_{A|B}^-] = [\hat{X}_B^+, \hat{X}_B^-] = 2i$ [12]. This leads to the joint Heisenberg uncertainty relation

$$V_{E|B}^\pm V_{A|B}^\mp \geq 1. \quad (3)$$

Therefore, there is a limit to what Alice and Eve can know simultaneously about what Bob has measured. From this inequality, it is possible to determine the maximum information Eve can obtain about the state in terms of Alice's conditional variances $V_{A|B}^\pm$.

To minimize Alice's conditional variance for one of Bob's measurements, Alice can prepare and send squeezed states instead of coherent states. In this case, the quadrature variance of the states prepared by Alice are given by $V_A^\pm = V_S^\pm + V_{\mathrm{sqz}}^\pm$, where $V_{\mathrm{sqz}}^\pm$ denote the quadrature variances of the squeezed state, and clearly $V_{\mathrm{sqz}}^\pm \geq 1/V_A^\mp$. Using Eqs. (1) and (2), we determine Alice's conditional variance to be

$$V_{A|B}^\pm = \frac{1}{2}[\eta V_{\mathrm{sqz}}^\pm + (1-\eta)V_N^\pm + 1]. \quad (4)$$

To find a lower bound on Eve's conditional variances, we first consider her inference of Bob's state prior to the 50/50 beam splitter in his station. This is given by $V_{E|B'}^\pm = \min_{g_E'^\pm} \langle (\hat{X}_{B'}^\pm - g_E'^\pm \hat{X}_E^\pm)^2 \rangle$, where $\prime$ labels Bob's state prior to the beam splitter, and $g_E'^\pm$ is chosen to minimize $V_{E|B'}^\pm$. Eve's measurement variance after the beam splitter conditioned on Bob's measurement, $V_{E|B}^\pm$, can be expressed in terms of the conditional variance before the beam splitter, $V_{E|B'}^\pm$, as

$$V_{E|B}^\pm = \min_{g_E^\pm} \langle (\hat{X}_B^\pm - g_E^\pm \hat{X}_E^\pm)^2 \rangle = \frac{1}{2}(V_{E|B'}^\pm + 1), \quad (5)$$

where we have used the fact that Eve has no access to the beam splitter in Bob's station, and therefore has no knowledge of the vacuum entering through it. The minimum conditional variance achievable by Alice, prior to the beam splitter in Bob's station, is $V_{A|B'(\min)}^\pm = \eta/V_A^\pm + (1-\eta)V_N^\pm$ [12]. Using this fact, and the conditional variance inequality in Eq. (3), we can establish a lower bound on Eve's inferences of Bob's measurements

$$V_{E|B(\min)}^\pm \geq \frac{1}{2}\left\{\left[\frac{\eta}{V_A^\mp} + (1-\eta)V_N^\pm\right]^{-1} + 1\right\}. \quad (6)$$

The optimal information rate at which a Gaussian signal can be transmitted though a channel with additive Gaussian noise is given by the Shannon formula [14], which can be expressed as $I = (1/2)\log_2(1 + S/N)$ with units of (bits/symbol), where S/N is the standard signal to noise ratio. This optimal net information rate can be used to determine the secret key rate for our simultaneous quadrature measurement protocol, which is given by

$\Delta I = \Delta I^+ + \Delta I^-$, where $\Delta I^\pm = I^\pm_{BA} - I^\pm_{BE}$ with $I_{BA(BE)}$ being the *quadrature* information rates between Bob and Alice (Eve): $I^\pm_{BA} = (1/2)\log_2(V^\pm_B/V^\pm_{A|B})$ and $I^\pm_{BE} = (1/2)\log_2(V^\pm_B/V^\pm_{E|B})$ [12]. From these expressions, the secret key rate for the simultaneous quadrature measurement protocol can be expressed as

$$\Delta I = \frac{1}{2}\log_2\left(\frac{V^+_{E|B}V^-_{E|B}}{V^+_{A|B}V^-_{A|B}}\right), \tag{7}$$

where the generation of a secret key is only possible when ΔI is greater than zero. Substituting Eq. (4) with $V^\pm_{\mathrm{sqz}} = 1$ (Alice maximizes her information rate by using coherent states), and Eq. (6) into Eq. (7), gives a lower bound on the secret key rate of

$$\Delta I \geq \log_2\left(\frac{[\frac{\eta}{V_A} + (1-\eta)V_N]^{-1} + 1}{\eta + (1-\eta)V_N + 1}\right), \tag{8}$$

where we have assumed symmetry between the amplitude and phase quadratures. Figure 2 shows the secret key rate for the simultaneous quadrature measurement scheme as a function of channel efficiency and channel noise. We see that, so long as the channel noise V_N is not excessive, a secret key can be successfully generated between Alice and Bob, even in the limit of very small channel efficiency η. As the channel noise is reduced, or efficiency increased, the rate at which a key can be established is enhanced. Figure 3 compares the information rates of the simultaneous and single quadrature protocols as a function of channel efficiency for varying channel noise. The information rate for simultaneous quadrature measurements is always higher than that for single quadrature measurements, and in the limit of large signal variances and high channel efficiency, it approaches double. The individual secret key rates for the simultaneous and single quadrature measurement protocols can be calculated and are plotted in Fig. 4. It should be noted that in our protocol, Eve must attempt to determine Bob's measurements in both the amplitude and phase quadratures. This introduces an extra penalty to Eve which is not included in the lower bound for her conditional variance in Eq. (6). Therefore, in general, Eve will do even worse than our analysis suggests.

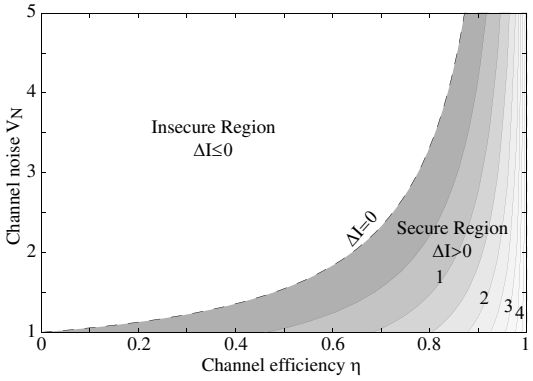

FIG. 2. Contour plot of the information rate for the simultaneous quadrature measurement protocol as a function of channel efficiency η and channel noise V_N in units of (bits/symbol) for $V_A = 100$.

To establish an upper bound on the secret key rate, we now consider the physical implementation of an eavesdropping attack for Eve for our protocol. In the case where Bob measures a single quadrature, Grosshans and Grangier showed that an entangling cloner attack [12] is the optimum attack. However, for simultaneous quadrature measurements, we found a more effective attack to be a simple feed forward attack with no entanglement as shown in Fig. 1(b). The attack goes as follows: Eve taps off a fraction of the beam using a beam splitter with transmission ϵ. She performs simultaneous quadrature measurements on this beam, with measured quadrature variances of

$$V^\pm_E = \frac{1}{2}[(1-\epsilon)V^\pm_A + \epsilon + 1]. \tag{9}$$

She then applies the measured photocurrents back onto the quantum channel using electronic feed forward techniques. The variances of Bob's measurements can then be expressed as

$$V^\pm_B = \frac{1}{2}[(\sqrt{\epsilon} + g^\pm_E\sqrt{(1-\epsilon)/2})^2 V^\pm_A + 1 + \mathrm{V}^\pm_{\mathcal{N}} + g^{2\pm}_E/2 + (\sqrt{1-\epsilon} + g^\pm_E\sqrt{\epsilon/2})^2], \tag{10}$$

where $g^\pm_E$ is the gain of the electric feed forward, and to avoid detection, Eve encodes additional Gaussian noise with a variance $\mathrm{V}^\pm_{\mathcal{N}}$ onto the channel. The gain of Eve's feed forward must be chosen carefully to ensure that the magnitude of the signal detected by Bob remains invariant. The correct gain can be expressed as $g^\pm_E = \sqrt{2}(\sqrt{\eta} - \sqrt{\epsilon})/\sqrt{1-\epsilon}$. Substituting this into Eq. (10) we obtain

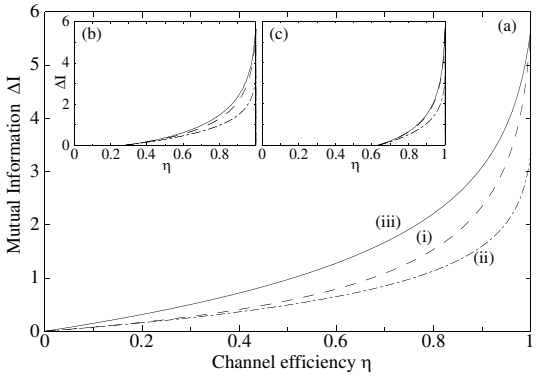

FIG. 3. Net information rates for the simultaneous and single quadrature measurement schemes as a function of channel efficiency. (i) Dashed line, simultaneous quadrature measurement. (ii) Dotted-dashed line, single quadrature measurement. (iii) Solid line, simultaneous quadrature measurement with feed forward attack. For a variance of $V_A = 100$ with varying channel noise: (a) $\mathrm{V}_N = 1$, (b) $V_N = 1.2$, and (c) $V_N = 2$.

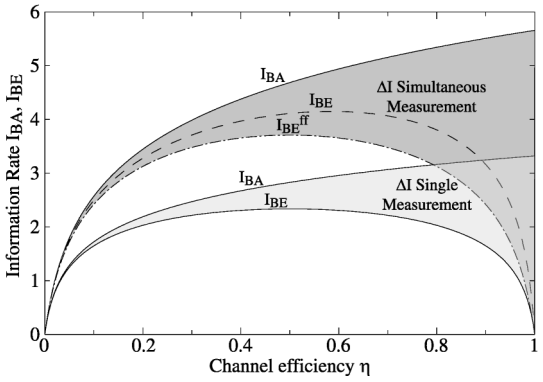

FIG. 4. Information rates for the simultaneous and single quadrature measurement schemes as a function of channel efficiency η, with $V_A^{\pm} = 100$ and $V_N^{\pm} = 1$. The net information rate for both schemes is $\Delta I = I_{BA} - I_{BE}$. In the case of simultaneous quadrature measurements, I_{BE}, the dashed line, denotes maximum information rate obtained by Eve, while I_{BE}^{ff}, the dotted-dashed line, denotes the information rate obtained by Eve using the feed forward attack.

Bob's variance due to the feed forward attack, $V_B^{ff\pm}$. We can now calculate Eve's conditional variance, $V_{E|B}^{ff\pm}$, for the feed forward attack as a function of the beam splitter transmission ϵ. Ideally, Eve would take $\epsilon \to 0$ to gain as much information about Alice's signal as possible. However, in doing so she increases the noise on Alice's inference of Bob's state and consequently alerts them to her presence. She must ensure that her attack does not change the magnitude of this noise. This places both lower $\epsilon_{\min}$ and upper $\epsilon_{\max}$ limits on the beam splitter transmission. We numerically minimize $V_{E|B}^{ff\pm}$ for all ϵ between $\epsilon_{\min}$ and $\epsilon_{\max}$, and hence determine the secret key rate ΔI^{ff}. The secret key rate for the feed forward attack is plotted in Figs. 3 and 4 and compared with the lower bound calculated in Eq. (8). Figure 3 shows that for channel noise of variance $V_N = 1$, the feed forward information rate is higher than our lower bound. However, as the channel noise variance is slightly increased, the feed forward bound asymptotes to the lower bound calculated in Eq. (8).

To summarize, we have proposed a new coherent state QKD protocol based on simultaneous quadrature measurements. We have calculated a lower bound on the secret key rate for this protocol, finding that in the limit of large signal variance and high channel efficiency, it approaches twice that of previous coherent state QKD schemes. We have considered a possible eavesdropping attack in the form of a simple feed forward scheme, which has provided us with an upper bound on the secret key rate. An important advantage of our simultaneous quadrature measurement protocol is the increase in total bandwidth. The absolute information rate, in bits/second, can be expressed as $I = W\log_2(1 + S/N)$ [14], where W is the limiting bandwidth associated with the state preparation or detection. Typically, in continuous variable quantum cryptography schemes, W can be attributed to the switching time for the local oscillator phase. The simultaneous quadrature measurement scheme does not require switching, so that orders of magnitude increases in absolute secret key rates should be achievable.

In conclusion, we have shown that there is no need to randomly switch bases to achieve secure QKD. By performing simultaneous quadrature measurements in a coherent state quantum cryptography protocol, we are able to achieve a significantly larger secret key rate than that obtained by the usual single quadrature measurements. This new QKD protocol will allow simpler and higher bandwidth quantum cryptographic experiments and technological applications.

We would like to acknowledge the support of the Australian Research Council and the Australian Department of Defence. We are grateful to Roman Schnabel for useful discussions.

[1] S. Wiesner, SIGACT News **15**, 78 (1983).
[2] C. H. Bennett and G. Brassard, in *Proceedings IEEE International Conference on Computers, Systems and Signal Proceedings, Bangalore* (IEEE, New York, 1984), pp. 175–179.
[3] N. Gisin *et al.*, Rev. Mod. Phys. **74**, 145 (2002), and references therein.
[4] U. M Maurer, IEEE Trans. Inf. Theory **39**, 733 (1993); G. Brassard and L. Salvail, *Advances in Cryptology-EUROCRYPT93*, Lecture Notes Computer Science Vol. 765 (Springer-Verlag, Berlin, 1994), pp. 411–423.
[5] C. H. Bennett *et al.*, IEEE Trans. Inf. Theory **41**, 1915 (1995).
[6] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).
[7] D. S. Naik *et al.*, Phys. Rev. Lett. **84**, 4733 (2000).
[8] T. C. Ralph, in *Quantum Information Theory with Continuous Variables*, edited by S. L. Braunstein and A. K. Pati (Kluwer, Dordrecht, 2003), and references therein.
[9] M. Hillery, Phys. Rev. A **61**, 022309 (2000); N. J. Cerf, M. Levy, and G. Van Assche, Phys. Rev. A **63**, 052311 (2001); Ch. Silberhorn, N. Korolkova, and G. Leuchs, Phys. Rev. Lett. **88**, 167902 (2002); M. D. Reid, Phys. Rev. A **62**, 062308 (2000); D. Gottesman and J. Preskill, Phys. Rev. A **63**, 022309 (2001).
[10] T. C. Ralph, Phys. Rev. A **62**, 062306 (2000); F. Grosshans and Ph. Grangier, Phys. Rev. Lett. **88**, 057902 (2002).
[11] Ch. Silberhorn *et al.*, Phys. Rev. Lett. **89**, 167901 (2002).
[12] F. Grosshans and Ph. Grangier, quant-ph/0204127; F. Grosshans *et al.*, Nature (London) **421**, 238 (2003).
[13] K. Boström and T. Felbinger, Phys. Rev. Lett. **89**, 187902 (2002).
[14] C. E. Shannon, Bell Syst. Tech. J. **27**, 623 (1948).