No-Switching Quantum Key Distribution Using Broadband Modulated Coherent Light

Andrew M. Lance,[1] Thomas Symul,[1] Vikram Sharma,[1] Christian Weedbrook,[1,2] 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 31 March 2005; published 28 October 2005)

We realize an end-to-end no-switching quantum key distribution protocol using continuous-wave coherent light. We encode weak broadband Gaussian modulations onto the amplitude and phase quadratures of light beams. Our no-switching protocol achieves high secret key rate via a post-selection protocol that utilizes both quadrature information simultaneously. We establish a secret key rate of 25 Mbits/s for a lossless channel and 1 kbit/s for 90% channel loss, per 17 MHz of detected bandwidth, assuming individual Gaussian eavesdropping attacks. Since our scheme is truly broadband, it can potentially deliver orders of magnitude higher key rates by extending the encoding bandwidth with higher-end telecommunication technology.

DOI: 10.1103/PhysRevLett.95.180503 PACS numbers: 03.67.Dd, 03.67.Hk, 42.50.Dv

Quantum key distribution (QKD) [1] is a technique for generating a shared cryptographic key between two parties, Alice and Bob, where the security of the shared key is guaranteed by the laws of quantum mechanics. QKD based on continuous variables (CV) [2], in particular coherent state QKD [4–9], promises significantly higher secret key rates in comparison to single photon schemes [1,3]. They are relatively simple to implement, in contrast to QKD protocols employing ''nonclassical'' states [10]. Coherent states can be readily produced by a well-stabilized laser and can be detected using high quantum efficiency detectors. Confidence in the practicability of coherent state QKD protocols has increased since it was shown that the security of these protocols can be ensured for channel losses greater than 50% using post-selection [6] or reverse reconciliation [7] procedures. In principle, it is therefore possible to generate a secure key even in the presence of arbitrarily high loss. This development, coupled with potentially high secret key rates, render coherent state QKD protocols viable contenders for real-world cryptographic applications.

Our coherent state QKD protocol builds on previous protocols presented in [5–7] and is an advance on random switching by simultaneously measuring both measurement bases [8]. The QKD protocol operates as follows. Alice draws two random numbers x_A and p_A from two Gaussian probability distributions with zero mean and variances of $V(x_A)$ and $V(p_A)$, respectively. Alice prepares a coherent state $|x_A + ip_A\rangle$ and sends it to Bob. As a result of losses in the quantum channel, vacuum noise is coupled into the transmitted state. On receiving the state, Bob simultaneously measures both the amplitude (x_B) and phase (p_B) quadratures of the state via a 50/50 beam splitter. At this stage, Alice and Bob share correlated random data from which they can generate a secret key. They use post selection [6] to reverse any initial ''information advantage'' a potential eavesdropper (Eve) might have obtained, and perform information reconciliation and privacy amplification to distill a final secret key. Although no-switching coherent state QKD protocols have been demonstrated to be secure against coherent (collective) attacks [11] and progress has been made towards proving the unconditional security of CV coherent state QKD protocols [11,12], we restrict our analysis of Eve here to only incoherent Gaussian attacks [4–9].

The experimental setup is shown in Fig. 1. In our implementation we use a continuous-wave, coherent laser operating at 1064 nm. In contrast to pulsed or temporal encoding schemes, we achieve high secret key rates by exploiting the continuous-wave nature of the laser field to implement a true broadband encoding protocol. We employ standard electro-optic modulators to encode weak broadband modulations onto the quantum states at the sideband frequencies of the electromagnetic field. Using this technique, the transmission rate of coherent states can be arbitrarily increased, limited only by Alice's encoding and Bob's detection bandwidths. To maximize Bob's detection bandwidth, we simultaneously measure both the amplitude and phase quadratures of the electromagnetic

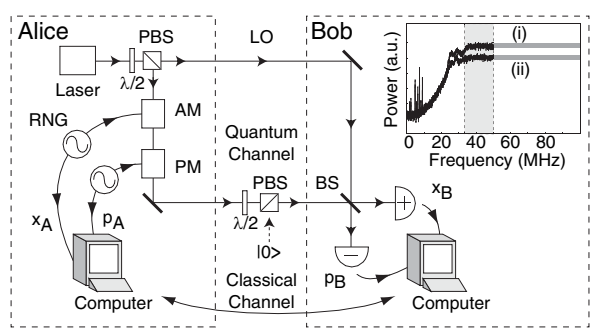

FIG. 1. Schematic of experiment. LO: local oscillator; RNG: random number generators; AM/PM: amplitude/phase modulators; PBS: polarizing beam splitter; $\lambda/2$: half wave plate; BS: 50/50 beam splitter; $|0\rangle$: vacuum state. (inset) (i) Bob's detected noise spectra of the broadband modulation encoding shown with respect to the quantum noise limit (ii). Grey region denotes the 17 MHz sideband frequency spectrum used in our analysis.

 © 2005 The American Physical Society

field at Bob's station, using the no-switching protocol [8]. This protocol has a significantly improved secret key rate and no weakening of security when compared with previous protocols that rely on random switching between measurement bases. This random switching requires the precise and rapid control of the optical phase of a local oscillator field, which is difficult to achieve in practice.

In the experiment we process quantum states encoded on 17 MHz of the sideband frequency spectrum [Fig. 1 (inset)]. As intrinsic classical noise is manifest at low frequencies on the laser beam and our data acquisition system has a maximum sample rate of 50 MHz, we process data from sideband frequencies between 33 MHz and 50 MHz. We verify that the laser field is coherent in this range with both quadrature variances equal to $V(x), V(p) = 1.01 \pm 0.01$, normalized to the quantum noise limit. We digitally filter the data in the identified frequency band, demodulate and resample it at 17 MHz. To improve the statistical correlations between Alice's and Bob's data, we apply a previously characterized transfer function to the data, which correct for the frequency response of Alice's electro-optic modulator and Bob's detectors. After this data processing, Alice and Bob have correlated random data with Gaussian probability distributions which are shown in a scatter-plot diagram [Fig. 2(a)]. Using a random subset of these data they can quantify the quantum channel transmission efficiencies of each quadrature (η_x and η_p), and the variances of Alice's quadrature displacements [$V(x_A)$ and $V(p_A)$] and thereby verify that the channel noise introduced as a result of transmission losses corresponds to a vacuum state. Although here we assume Gaussian attacks, Alice and Bob can check for non-Gaussian attacks by analyzing, prior to post selection, the statistical distribution of the announced set of data. Finally, Alice and Bob can determine the maximum information Eve could have obtained during quantum state transmission.

In our security analysis, we assume that Eve performs a beam splitter attack [6], where she replaces the quantum channel with a perfect lossless line and uses a beam splitter to simulate the channel transmission losses. The security of our protocol relies on the indistinguishability of nonorthogonal pure states [13]. For every transmitted state, Alice publicly announces the absolute values $|x_A|$ and $|p_A|$, thereby requiring Bob (and Eve) to distinguish from one of the four possible coherent states prepared by Alice $|\pm x_A \pm i p_A\rangle$. So that Eve's state after the beam-splitting attack can be expressed as $|\pm\sqrt{1-\eta}x_A \pm i\sqrt{1-\eta}p_A\rangle$. The general solution for the maximum Shannon information for the indistinguishability of four pure states is not known. To calculate Eve's Shannon information, we assume that after the beam splitter attack Eve splits her state on a 50/50 beam splitter, which corresponds to an optimal cloning of the information on the two quadratures, and performs Helstrom measurements [14], denoted H_x and H_p, on the two resulting outputs. For each Helstrom measurement, H_x or H_p, Eve must distinguish between two

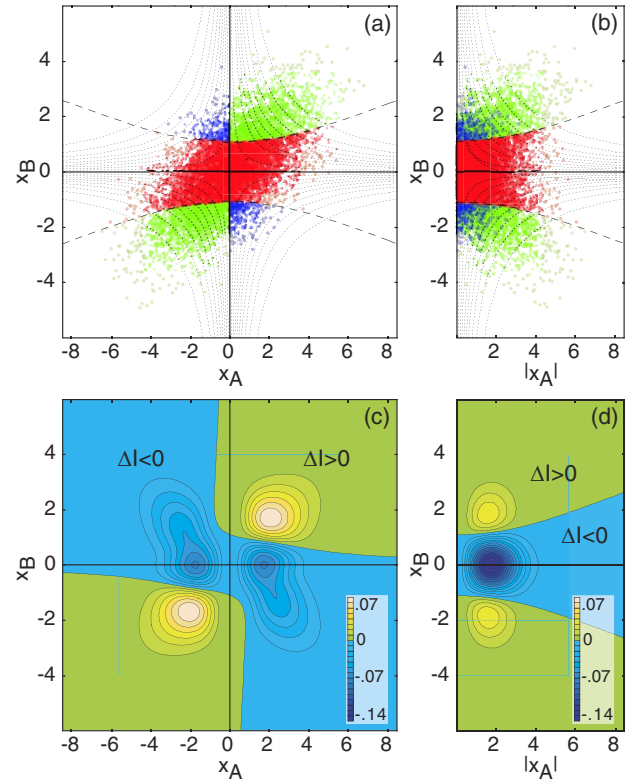

FIG. 2 (color online). (a) The "global" perspective of Alice's (x_A) and Bob's (x_B) data, represented in a scatter-plot diagram, for transmission losses of 54%. Dotted lines: "banded information channels"; green points: data that have error free binary encoding; blue points: data that have bit-flip errors; red points: data that have a negative net information rate. (b) Bob's perspective of his and Alice's data. (c) The global perspective and (d) Bob's perspective of the theoretical net information rate contour plots.

mixed states, each being a mixture of two pure states on either side of the $x, p = 0$ axis. The Shannon information for the distinguishability of two pure states of an equivalent separation is greater than for that of two mixed states, hence giving us an upper bound on Eve's information [15].

$$I_{AE} = \sum_{v=\{x,p\}} \left[\frac{1}{2}(1+\sqrt{1-z_v^2})\log_2(1+\sqrt{1-z_v^2}) + \frac{1}{2}(1-\sqrt{1-z_v^2})\log_2(1-\sqrt{1-z_v^2}) \right], \quad (1)$$

where $z_v = |\langle -v_E | v_E\rangle|^2 = e^{-2|v_E|^2} = e^{-(1-\eta_v)|v_A|^2}$ are Eve's quadrature overlap functions, and $v = \{x, p\}$.

We next calculate the mutual information between Alice and Bob. The scatter-plot diagram of Figs. 2(a) and 2(b) show the "global" perspective of Alice's and Bob's results, and Bob's perspective during the QKD protocol (after Alice publicly announces the absolute value of her data), respectively. To interpret information encoded onto the quantum states, Alice and Bob use a binary encoding system based on the directional displacements of the quadrature measurements, interpreting positive displacements

in phase space as a binary "1" and negative displacements as a binary "0." Hence 2 bits of information are encoded per transmitted state (one bit on each quadrature). From the global perspective of Alice's and Bob's results [Fig. 2(a)], the points in the diagonal quadrants correspond to error-free bits, while the points in the off-diagonal quadrants correspond to bit-flip errors. We encode at approximately the Shannon capacity of the quantum channel [16] by partitioning Alice's and Bob's data into "banded information channels" (BICs). We achieve this by calculating the theoretical probability of error for Alice's and Bob's data given by

$$P_v = (e^{-4|v_A v_B|\sqrt{2\eta_v}})/(1 + e^{-4|v_A v_B|\sqrt{2\eta_v}}) \qquad (2)$$

and allocate the data into BICs with increasing probabilities of error, as shown by the dotted hyperbolas in Figs. 2(a) and 2(b). For each BIC, let the number of error-free points be denoted by N_{good} and the number of bit-flip errors by N_{error}. We calculate the experimental probability of error for each BIC using $P_v = N_{\text{error}}/(N_{\text{error}} + N_{\text{good}})$. Bob's mutual information with Alice summed over n BICs is given by

$$I_{AB} = \sum_{v=\{x,p\}} \sum_{k=1}^{n} [1 + P_{(v,k)} \log_2(P_{(v,k)}) + (1 - P_{(v,k)}) \log_2(1 - P_{(v,k)})], \qquad (3)$$

where $P_{(v,k)}$ is the probability error rate for the kth BIC, of either the amplitude or phase quadrature. The mutual information rate between Alice and Bob [Eq. (3)] approaches the Shannon capacity [16] as the number of BICs is increased. In our analysis we partition the data into 10 BICs by assigning an equal number of data points to each, thereby achieving a mutual information rate, prior to information reconciliation and privacy amplification, of ~99% of the Shannon information limit for a binary symmetric quantum channel [Fig. 3 (inset)].

From his perspective Bob can calculate, for each BIC, the amount of mutual information he has with Alice [Eq. (3)], and Eve has with Alice [Eq. (1)]. The total secret information rate summed over all BICs can be expressed as

$$\Delta I = \sum_{v=\{x,p\}} \sum_{k=1}^{n} \left[I_{AB(v,k)} - \iint_{S_{(v,k)}} I_{AE} \times P(v_A, v_B) dv_A dv_B \right], \qquad (4)$$

where the joint probability distribution of Alice and Bob's measurements is given by $P(v_A, v_B)$, $S_{(v,k)}$ is the area of the kth BIC of either the amplitude or phase quadrature, and Bob's mutual information with Alice for the kth BIC for each quadrature is denoted by $I_{AB(v,k)}$. Figure 2(c) is a contour plot of the theoretical net information rate from a global perspective of Alice's and Bob's results. Alice and Bob cannot directly use Fig. 2(c), as Bob only knows the absolute values of Alice's data. Bob's perspective of the theoretical net information rate is shown in Fig. 2(d). Using

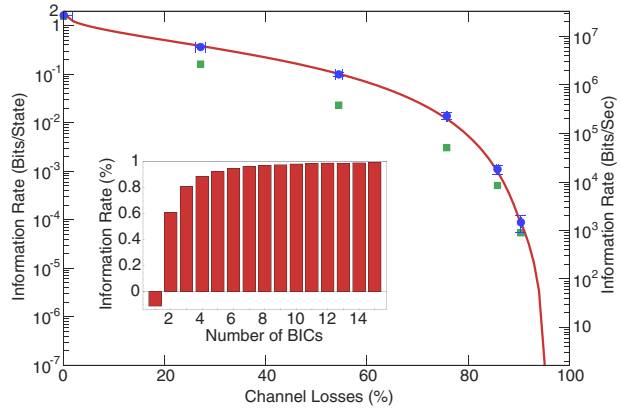

FIG. 3 (color online). Secret key rate for varying channel losses. Solid line: theoretical net Shannon information rate; circle symbols: experimental secret key rate after post selection; square symbols: secret key rate after privacy amplification. (inset) Bob's mutual information with Alice (normalized to the Shannon's capacity) for increasing number of banded information channels with 54% channel loss.

Eq. (4) Bob can post select points about which his mutual information with Alice is greater than Eve's maximum accessible information. Applying this post-selection procedure Alice and Bob gain an "information advantage" over Eve, reversing Eve's possible information advantage prior to post selection [6].

After post selection, we proceed to distill an errorless secret key by performing an information reconciliation procedure. We take advantage of the BICs, each having differing probability error rates, by applying the reconciliation procedure iteratively to each BIC, thereby increasing the overall efficiency of the procedure. To amplify Bob's information advantage, we apply an "n bit repeat code" advantage distillation protocol [17], at the cost of reducing the size of the key. After advantage distillation, we apply the well-known "Cascade" error reconciliation protocol [18] to correct the remaining errors. We distill a final secret key by employing a privacy amplification procedure based on universal hashing functions [19]. Eve's resulting information about the final secret key for each BIC is $2^{-s}/\ln 2$ bits, where s is a security factor. We decrease Eve's total information about the final secret key (summed over all BICs and both quadratures) to less than 1 bit by discarding an additional $s = 5$ bits per BIC.

Table I shows the experimental results for the processes used to distill a final secret key. For 90% channel loss, Eve's probability error rate in the raw data is lower than Bob's error rate with a corresponding negative information rate of $\Delta I = -0.18$ bits/symbol. Using post selection Alice and Bob get a slight information advantage over Eve ($\Delta I = 0.01$ bits/symbol), which is further enhanced through advantage distillation. The cost of these processes is a reduction in the size of the secret key, as can be seen in the bit-rate column in Table I. Alice and Bob reconcile an errorless string using the Cascade protocol, which leaks

TABLE 1. Experimental results for the different stages of the QKD protocol. Each procedural step shows Bob's and Eve's probability error rates (P), the corresponding net information rate (ΔI bits/symbol) and the final secret key rate (bits/second). Eve's total information about the final secret key is less than one bit.

	90% Transmission loss				54% Transmission loss			
	Rate (bits/s)	P Bob (%)	P Eve (%)	ΔI (bits/sym)	Rate (bits/s)	P Bob (%)	P Eve (%)	ΔI (bits/sym)
Raw data	3×10^7	40	24	−0.18	3×10^7	19	16	−0.07
Post selection	6×10^4	29	30	0.01	1×10^7	13	17	0.10
Advantage distillation	9×10^3	10	21	0.27	5×10^6	5	10	0.18
Information reconciliation	9×10^3	∼0	8	0.40	5×10^6	∼0	4	0.24
Privacy amplification	1×10^3	∼0	∼50	1.00	4×10^5	∼0	∼50	1.00

additional information to Eve, decreasing her probability of error to ∼8%. Privacy amplification is performed to reduce Eve's knowledge of the final key to less than 1 bit in total. To ensure the overall security of our protocol is maintained, we attribute Eve in each of the processing stages a level of information that is above the maximum theoretical information that she could have obtained. Figure 3 shows the secret key rate of our QKD protocol as a function of transmission loss. For a lossless quantum channel we achieve a final secret key rate of ∼25 Mbits/s. For transmission losses of 90%, we are still able to generate a final secret key at a rate of ∼1 kbits/s out of only 17 MHz of our broadband spectrum, which represents a major improvement over previous protocols. The solid line in Fig. 3 gives the theoretical curve for transmitting information at the Shannon's limit. For all transmission losses, the experimental secret key rate after post selection is at this limit. The final secret key rate is less than the Shannon's capacity as the information reconciliation procedure discloses more error correction information than Shannon's equivocation limit stipulates [16]. The size of the final secret key that can be extracted after privacy amplification is calculated using Eve's Rènyi entropy (Fig. 3), which is always a lower bound on her Shannon entropy.

In conclusion, we have implemented an end-to-end coherent state QKD protocol for channel losses up to 90% by using weak sideband modulation techniques and simultaneously measuring the amplitude and phase quadratures of the electromagnetic field. In our analysis we only consider 17 MHz of the sideband frequency spectrum. Extending this analysis to a much larger frequency bandwidth will enable orders of magnitude increase in the rate of secret key generation. Our system is not hampered by the technical difficulties of production and detection of single photon states that constrain discrete variable QKD protocols. We show that our protocol is secure against a beam-splitting attack, and in our analysis we always assume maximal estimates of Eve's information. The QKD scheme demonstrated provides a viable platform for the development of real-world cryptographic applications over local area networks, or citywide networks.

We thank W. P. Bowen, T. J. Williams, D. Pulford, Ph. Grangier, and N. J. Cerf for useful discussions. This research is supported by the Australian Research Council and the Australian Department of Defence.

[1] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).
[2] S. L. Braunstein and P. van Loock, Rev. Mod. Phys. **77**, 513 (2005).
[3] C. H. Bennett and G. Brassard, *Proceedings IEEE International Conference on Computers*, Systems and Signal Proceedings (Bangalore) (IEEE, New York, 1984), pp. 175–179.
[4] T. C. Ralph, Phys. Rev. A **61**, 010303(R) (2000).
[5] F. Grosshans and P. Grangier, Phys. Rev. Lett. **88**, 057902 (2002).
[6] Ch. Silberhorn, T. C. Ralph, N. Lutkenhaus, and G. Leuchs, Phys. Rev. Lett. **89**, 167901 (2002).
[7] F. Grosshans *et al.*, Nature (London) **421**, 238 (2003).
[8] C. Weedbrook *et al.*, Phys. Rev. Lett. **93**, 170504 (2004).
[9] S. Lorenz, N. Korolkova, and G. Leuchs, Appl. Phys. B **79**, 273 (2004).
[10] M. Hillery, Phys. Rev. A **61**, 022309 (2000); Ch. Silberhorn, N. Korolkova, and G. Leuchs, Phys. Rev. Lett. **88**, 167902 (2002).
[11] F. Grosshans, Phys. Rev. Lett. **94**, 020504 (2005).
[12] M. Navascues and A. Acin, Phys. Rev. Lett. **94**, 020505 (2005); S. Iblisdir, G. Van Assche, and N. J. Cerf, Phys. Rev. Lett. **93**, 170502 (2004); D. Gottesman and J. Preskill, Phys. Rev. A **63**, 022309 (2001).
[13] M. A. Nielsen and I. L. Chuang, in *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, England, 2000).
[14] C. W. Helstrom, *Quantum Detection and Estimation Theory* (Academic, New York, 1976).
[15] L. B. Levitin, in *Quantum Communications and Measurements*, edited by V. P. Belavkin, O. Hirota, and R. L. Hudson (Plenum, New York, 1995), pp. 439–448.
[16] C. E. Shannon, Bell Syst. Tech. J. **27**, 623 (1948).
[17] U. M. Maurer, IEEE Trans. Inf. Theory **39**, 733 (1993).
[18] G. Brassard and L. Salvail, *Advances in Cryptology-Eurocrypt'93* (Springer-Verlag, Berlin, 1993), pp. 411–423.
[19] C. H. Bennett, G. Brassard, C. Crepeau, and U. M. Maurer, IEEE Trans. Inf. Theory **41**, 1915 (1995); C. Cachin and U. M. Maurer, J. Cryptology **10**, 97 (1997).