A complete quantum cryptographic system using a continuous wave laser

Vikram Sharma\textsuperscript{a} Andrew M. Lance\textsuperscript{a} Thomas Symul\textsuperscript{a} Christian Weedbrook\textsuperscript{b} Timothy C. Ralph\textsuperscript{b} and Ping Koy Lam\textsuperscript{a}

\textsuperscript{a}Quantum Optics Group, Department of Physics, Faculty of Science, Australian National University, ACT 0200, Australia;
\textsuperscript{b}Department of Physics, University of Queensland, St Lucia, Queensland 4072, Australia

ABSTRACT

We experimentally demonstrate a complete, end-to-end, quantum key distribution system using a continuous wave laser and standard optical components. Our implementation encodes random bits as weak Gaussian modulations onto the phase and amplitude quadratures of the laser beam. We process data from the quantum channel using a post-selection procedure and subsequently apply information reconciliation and privacy amplification procedures to generate an absolutely secure secret key. The maximum information that an eavesdropper may have obtained about this secret key, from the quantum channel and classical communications, is bounded to below one bit. Under the assumption of individual Gaussian eavesdropping attacks, we achieve a secret key generation rate of 25 Mbits/s for a lossless channel and 1 kbit/s for 90\% channel loss, per 17 MHz of detected bandwidth.

Keywords: Quantum key distribution, quantum cryptography, quantum information, no-switching protocol, post-selection, broadband gaussian modulation, information reconciliation, privacy amplification

1. INTRODUCTION

Quantum key distribution (QKD)\textsuperscript{1,2} 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. In a generic QKD protocol, a sender (Alice) prepares quantum states which are sent to a receiver (Bob) through a quantum channel. Alice and Bob agree on a set of non-commuting bases with which to measure the states. Switching randomly between a pair of non-commuting measurement bases ensures security: in a direct attack, an eavesdropper (Eve) will only choose the correct basis half the time and will inevitably be revealed; alternatively, if Eve uses a passive attack simulating losses of the quantum channel and a quantum memory to perform her measurements after Bob declares his basis, her attack will be indistinguishable from the quantum channel, however the maximum information she can obtain is known and can be bounded. Using various reconciliation\textsuperscript{3} and privacy amplification\textsuperscript{4,5} procedures, the results of Alice’s and Bob’s measurements in the bases are used to construct a secret key, known only to them.

The original QKD schemes in the discrete variable regime were based on the transmission and measurement of random polarizations of single photon states.\textsuperscript{1,2} Other discrete variable QKD protocols have been proposed\textsuperscript{6} and experimentally demonstrated\textsuperscript{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\textsuperscript{8} quantum cryptography, 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.\textsuperscript{9-11} Such protocols have been shown to be unconditionally secure.\textsuperscript{12} However, these protocols require significant quantum resources and are susceptible to decoherence due to losses.

Further author information: (Send correspondence to Ping Koy Lam)
E-mail: ping.lam@anu.edu.au, Telephone: +61 2 6125 8378
towards proving the unconditional security of these schemes.\textsuperscript{19–21} They are relatively simple to implement, in contrast to QKD protocols employing “non-classical” states\textsuperscript{9,11,22–24} such as squeezed or entangled states. 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\textsuperscript{10} or reverse reconciliation\textsuperscript{15} 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.

As alluded to in the preceding, it has commonly been assumed that randomly switching between measurement bases is crucial to the success of QKD protocols.\textsuperscript{1,2} In general, security in discrete variable cryptography protocols is ensured via random switching between measurement bases\textsuperscript{2} or random switching of state manipulation.\textsuperscript{25} In the discrete variable case, 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 non-commuting bases. In the continuous variable regime however, this requires sophisticated optics and electronics which places a technical limitation on the bandwidth of these protocols. In the following we describe our work that shows that the assumption about the necessity of switching bases in QKD is not correct and that, in fact, a more efficient scheme results if both bases are simultaneously measured.

\section{THE NO-SWITCHING PROTOCOL}

\begin{figure}[h]
\centering
\includegraphics[width=\textwidth]{fig1.png}
\caption{(a) Schematic of the simultaneous quadrature measurement protocol. $x_S$ and $p_S$: random Gaussian numbers, AM: amplitude modulator, PM: phase modulator, $\hat{x}_A$ and $\hat{p}_A$: Alice's amplitude and phase quadratures, $\hat{x}_B$ and $\hat{p}_B$: Bob's amplitude and phase quadratures. $\eta$: channel transmission and $\delta\hat{v}_{1x,p}$, $\delta\hat{v}_{2x,p}$: vacuum noise. (b) Schematic of a possible beam splitter attack for Eve. $H_{x,p}$: Eve's Helstrom measurements corresponding to the mixed states $\rho_1/\rho_2$ and $\rho_1'/\rho_2'$, $\eta$: channel transmission and $\delta\hat{v}_{3x,p}$, $\delta\hat{v}_{4x,p}$: vacuum noise.}
\end{figure}

In this section we detail a new coherent state protocol that does not require switching, which we term the non-switching protocol. The protocol was theoretically proposed in\textsuperscript{16} and experimentally demonstrated in\textsuperscript{18} In this protocol, both bases are measured simultaneously, utilizing the quantum channel more effectively and achieving higher secret key rates compared to previous continuous variable QKD protocols.

The quantum states we consider in this paper can be described using the field annihilation operator $\hat{a} = (\hat{x} + i \hat{p})/2$, which is expressed in terms of the amplitude $\hat{x}$ and phase $\hat{p}$ quadrature operators. We denote
operators and real numbers with and without \( \hat{\cdot} \), 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 \( \hat{x} = \langle \hat{x} \rangle + \delta \hat{x} \) and \( \hat{p} = \langle \hat{p} \rangle + \delta \hat{p} \), which have quadrature variances of \( V(x) = \langle (\delta x)^2 \rangle \) and \( V(p) = \langle (\delta p)^2 \rangle \) respectively.

Figure 1(a) shows a schematic of our protocol. Our scheme is an advancement on previous continuous variable coherent state quantum cryptography protocols\(^{13}\). The protocol goes as follows: Alice draws two random real numbers \( S_x \) and \( S_p \) from Gaussian distributions with zero mean and a variance of \( V(S_x) \) and \( V(S_p) \). She then prepares a state by displacing the amplitude and phase quadratures of a vacuum state by \( S_x \) and \( S_p \), respectively. The quadrature operators of Alice’s state are given by \( \hat{x}_A = S_x + \delta \hat{x} \) and \( \hat{p}_A = S_p + \delta \hat{p} \), where \( \delta \hat{x} \) and \( \delta \hat{p} \) are the quadrature operators of the initial vacuum state. The resulting state has normalized quadrature variances of \( V(x_A) = V(S_x) + 1 \) and \( V(p_A) = V(S_p) + 1 \). Alice transmits this state to Bob through a quantum channel with channel transmission efficiency \( \eta \) that couples in vacuum noise as a result of channel loss. 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

\[
V(x_B) = \frac{1}{2} \eta \left( V(x_A) - 1 \right) + 1
\]

and

\[
V(p_B) = \frac{1}{2} \eta \left( V(p_A) - 1 \right) + 1
\]

It is possible to analyse data from the no-switch protocol using either post-selection, or reverse reconciliation data processing techniques\(^{10,14}\). Here we consider the post-selection protocol. Subsequently, a common secret key can be extracted using secret key distillation protocols\(^3\) and standard privacy amplification methods\(^4,5\).

### 3. Transmission protocol and information rate

In our security analysis, we assume that Eve performs a beam splitter attack (Fig. 1(b)), where she replaces the quantum channel with a perfect lossless line and uses a beam splitter to simulate the channel transmission losses. This is a common assumption in previous QKD protocols where a vacuum state is coupled in as a result of channel loss\(^{10,13-18}\). The security of our protocol relies on the indistinguishability of non-orthogonal pure states\(^{26}\). For every transmitted state, Alice publicly announces the absolute values \( |S_x| \) and \( |S_p| \), thereby requiring Bob (and Eve) to distinguish from one of the four possible coherent states prepared by Alice \( | \pm S_x \pm i S_p \rangle \). So that Eve’s state after the beam splitting attack can be expressed as \( | \pm \sqrt{1 - \eta} S_x \pm i \sqrt{1 - \eta} S_p \rangle \). 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\(^{27}\), 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 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\(^{28}\), hence giving us an upper bound on Eve’s information. Therefore the upper bound on Eve’s Shannon information\(^{29}\) is given by

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

where \( z_v = |\langle v \mid v_E \rangle|^2 = e^{-2|v_E|^2} = e^{-(1-\eta_v)|S_v|^2} \) are Eve’s quadrature overlap functions, and \( v = \{ x, p \} \) is the amplitude or phase quadrature.

We calculate the mutual information between Alice and Bob as follows. The scatter-plot diagrams of Fig. 2(a) and (b) respectively 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); while the plots are for the amplitude quadrature, there are corresponding plots for the phase quadrature which are not shown. 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 two 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, whilst the points in the off-diagonal quadrants correspond to bit-flip errors. We encode at approximately the Shannon capacity of the quantum channel\textsuperscript{30} by partitioning Alice’s and Bob’s data into “banded information channels” (BICs). This is achieved by calculating the theoretical probability of error for Alice’s and Bob’s data given by\textsuperscript{10}

\[ P_v = \frac{e^{-4|S_v,B|\sqrt{\eta}}}{1 + e^{-4|S_v,B|\sqrt{\eta}}} \]

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

\[
I_{AB} = \sum_{v={x,p}} \sum_{k=1}^{n} \left[ 1 + P(v,k) \log_2(P(v,k)) 
+ (1 - P(v,k)) \log_2(1 - P(v,k)) \right] 
\]

where \( P(v,k) \) is the probability error rate for the \( k \)th BIC, of either the amplitude or phase quadrature. The mutual information rate between Alice and Bob (Eq. (5)) approaches the Shannon capacity\(^{30} \) 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 \( \sim 99\% \) 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. (5)), and Eve has with Alice (Eq. (3)). The total secret information rate summed over all BICs can be expressed as

\[
\Delta I = \sum_{v={x,p}} \sum_{k=1}^{n} \left( I_{AB}(v,k) - \int_{R_{(v,k)}} I_{AE} \times P(S_v,v_B) \, dS_v \, dv_B \right) 
\]

where the joint probability distribution of Alice and Bob’s measurements is given by \( P(S_v,v_B) \).\(^{10} \) \( R_{(v,k)} \) is the area of the \( k \)th BIC of either the amplitude or phase quadrature, and Bob’s mutual information with Alice for the \( k \)th 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 Eq. (6) Bob can post-select points about which his mutual information with Alice is greater than Eve’s maximum accessible information (corresponding to the green regions in Fig. 2(d), where \( \Delta I > 0 \)). Applying this post-selection procedure Alice and Bob gain an “information advantage” over Eve, reversing Eve’s possible information advantage prior to post-selection.\(^{10} \)
4. EXPERIMENTAL RESULTS

The experimental set-up is shown in Fig. 4. 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 field at Bob’s station, using the no-switching protocol.\[^{16}\]

In the experiment we process quantum states encoded on 17 MHz of the sideband frequency spectrum (Fig. 4 (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 side-band frequencies between 33 MHz and 50 MHz which represents a region where the noise spectrum was homogeneous in our experiment. We verify that the laser field is coherent in this range with both quadrature variances equal to $V(\delta v_{1x}) = V(\delta v_{1p}) = 1.01 \pm 0.01$, normalized to the quantum noise limit. We digitally filter the data in the identified frequency band, demodulate and re-sample 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 corrects 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 the scatter-plot at Fig. 2(a).

Using a random subset of this data they can quantify the quantum channel transmission efficiencies of each quadrature ($\eta_x$ and $\eta_p$), and the variances of Alice’s quadrature displacements ($V(S_x)$ and $V(S_p)$) 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 as bounded by Eq. (3).

Using Eq. (6) for each of the data points received, Alice and Bob post-select a subset of points where they expect to have a higher information rate than Eve - a process over which Eve has no control. As discussed in the
previous section, this results in an information advantage for Alice and Bob over Eve and \( \Delta I \), which is negative in the raw data for transmission losses exceeding 50\%, now turns positive in the post-selected subset.

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 error rate probability bounds, by applying the reconciliation procedure iteratively to each BIC, thereby increasing the overall efficiency of the procedure. This is achieved by allowing the processing algorithms to optimise run time parameters for the error rate corresponding to each BIC. In the high transmission loss regime, the \( \Delta I \) achieved after post-selection is only marginally positive and insufficiently large to enable the subsequent processing steps to successfully extract a secret key. This is principally due to inefficiency of the information reconciliation protocol, Cascade,\(^3\) which we used. Cascade, while algorithmically elegant, is not an optimal information reconciliation procedure and discloses significantly more information than the equivocation limit suggested by Shannon. We therefore found that, prior to information reconciliation, we needed to further increase Bob’s information advantage by applying an “n-bit repeat code” advantage distillation protocol.\(^31\) This further increased \( \Delta I \) at the cost of reducing the size of the key. After advantage distillation, we apply the Cascade error reconciliation protocol to correct the remaining errors. This protocol locates and corrects errors in Bob’s bit string through the exchange, with Alice, of parities of subsets of their bits. Wherever a mismatch is detected, the search is progressively narrowed until the error is located and corrected.

We distill a final secret key by employing a privacy amplification procedure based on universal hashing functions.\(^4,5\) The procedure we use is based on the multiplication of two very high order polynomials over a Galois field. The first polynomial is constructed by using bits from Alice’s or Bob’s (now identical) bit strings as the binary coefficients of each term in the polynomial and the second polynomial, which may be known to Eve, is selected at random. The result of this multiplication operation is that any differences that Eve has between her data and that of Alice and Bob are now blended through her entire data set. The size of the final secret key that can be extracted after privacy amplification is calculated using Eve’s Rényi entropy, which is always a lower bound on her Shannon entropy. 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 one bit by discarding an additional \( s = 5 \) bits per BIC.

<table>
<thead>
<tr>
<th>Advantages</th>
<th>Bits/s</th>
<th>( P_{\text{Bob}} (%) )</th>
<th>( P_{\text{Eve}} (%) )</th>
<th>( \Delta I ) (b/sym)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Raw Data</td>
<td>( 3 \times 10^4 )</td>
<td>40</td>
<td>24</td>
<td>-0.18</td>
</tr>
<tr>
<td>Post-Selection</td>
<td>( 6 \times 10^4 )</td>
<td>29</td>
<td>30</td>
<td>0.01</td>
</tr>
<tr>
<td>Advantage Distill</td>
<td>( 9 \times 10^3 )</td>
<td>10</td>
<td>21</td>
<td>0.27</td>
</tr>
<tr>
<td>Info Reconciliation</td>
<td>( 9 \times 10^3 )</td>
<td>( \sim 0 )</td>
<td>8</td>
<td>0.40</td>
</tr>
<tr>
<td>Privacy Amp</td>
<td>( 1 \times 10^3 )</td>
<td>( \sim 0 )</td>
<td>( \sim 50 )</td>
<td>1.00</td>
</tr>
</tbody>
</table>

Table 1. Experimental results for the different stages of the QKD protocol used to distill the final secret key. Results shown for 90\% and 54\% transmission loss. Each procedural step shows the key translation rate (bits/second), Bob’s and Eve’s probability error rates \( (P) \) and the corresponding net information rate \( \Delta I \) bits/symbol. Eve’s total information about the final secret key is less than one bit.

Table 1 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 \( (\Delta I = 0.01 \text{ bits/symbol}) \), 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 1. Alice and Bob reconcile an errorless string using the Cascade protocol, which leaks additional information to Eve, decreasing her probability of error to \( \sim 8\% \). 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 greater than the maximum theoretical limit that she could have obtained.

Figure 5 provides a graphical representation of the data in Table 1 for the case of 90% loss. The images in the figure are obtained as a result of using the intermediate keys for Bob and Eve at the various stages of key distillation to encrypt the bits of the original bitmap image (Fig. 5 (top) - often referred to as the plaintext message) using the technique of the one-time pad. In practice, of course, only the final key generated after privacy amplification would actually be used. The key used for Bob is constructed from actual experimental data and that for Eve is simulated using an upper bound on the maximum information that she could have obtained by eavesdropping on both the quantum channel and classical communications. As the images obtained from encryption using raw data from the quantum channel show (Fig. 5 (leftmost column)), Eve initially has a considerably higher level of information. Applying the post-selection process, Bob’s manages to eke out a slight information advantage (Fig. 5 (second column)) which is only marginal and is not readily apparent from the images. He then uses advantage distillation to increase his information level vis-a-vis Eve (Fig. 5 (third column)). After information reconciliation, Bob now has an errorless key, however Eve has also gained additional information (Fig. 5 (fourth column)). Finally, privacy amplification reduces Eve’s total information to less than one bit, a snowflake pattern, while preserving Bob’s information (Fig. 5 (rightmost column)). The gain for Bob in each of these steps comes at the expense of a reduced key rate.

![Figure 5](image-url)

**Figure 5.** Bob’s and Eve’s intermediate keys at the various stages of key distillation. Graphic shows the use of raw keys from the quantum channel to encrypt an image and illustrates their subsequent evolution through each of the four stages of key distillation (in practice only the key from the final stage would be used). The data for Bob is actual experimental data for a transmission with 90% loss and Eve’s data has been simulated based on the theoretic maximal information she could have obtained at each step.

The secret key rate of our QKD protocol as a function of transmission loss is shown in Figure 3. 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 using only 17 MHz of our broadband spectrum, which represents a major improvement over previous protocols both in terms of bandwidth and loss. 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.
5. CONCLUSION

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. We have also implemented a multi-stage key distillation processes to extract an absolutely secure final key from the quantum data such that Eve’s total information of this final key is less than one bit. The QKD scheme demonstrated provides a viable platform for the development of real-world cryptographic applications over local area networks, or city-wide networks.

6. FURTHER RESEARCH

Given the encouraging results for the experiment to date, the group is in the process of developing the next generation of the experiment that will employ a coherent laser operating at 1550 nm, a frequency compatible with commercial optic fibre networks. The modulation bandwidth, which was 50MHz (of which 17 MHz was usable spectrum), is expected to be increased to 100MHz, which will result in usable bandwidth several factors higher than previously. We will also be deploying mode-preserving optic fibre as the conduit for the quantum channel. Finally, a number of enhancements are being made to the post-processing algorithms which are expected to result in efficiency gains for the key distillation process.

ACKNOWLEDGMENTS

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.

REFERENCES

28. C. Weedbrook et al., article in preparation.