New Journal of Physics
An Institute of Physics and Deutsche Physikalische Gesellschaft Journal

Continuous variable (2, 3) threshold quantum secret sharing schemes

Andrew M Lance[1], Thomas Symul[1], Warwick P Bowen[1], Tomáš Tyc[2,3], Barry C Sanders[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 and the Centre for Advanced Computing—Algorithms and Cryptography, Macquarie University, Sydney, NSW 2109, Australia
[3] Institute of Theoretical Physics, Masaryk University, 61137 Brno, Czech Republic
E-mail: andrew.lance@anu.edu.au

New Journal of Physics **5** (2003) 4.1–4.13 (http://www.njp.org/)
Received 22 October 2002
Published 17 January 2003

Abstract. We present two schemes to perform continuous variable (2, 3) threshold quantum secret sharing (QSS) on the quadrature amplitudes of bright light beams. Both schemes require a pair of entangled light beams. The first scheme utilizes two phase sensitive optical amplifiers, whilst the second uses an electro-optic feedforward loop for the reconstruction of the secret. We examine the efficacy of QSS in terms of fidelity, as well as the signal transfer coefficients and the conditional variances of the reconstructed output state. We show that both schemes in the ideal case yield perfect secret reconstruction.

PII: S1367-2630(03)55109-6

Contents

1. Introduction

Quantum secret sharing (QSS) is concerned with the transmission of a secret quantum state (which includes classical information) from a dealer to a set of players such that the secret can only be decoded by specific subsets of players (the access structure), and the complementary subsets (the adversary structure) obtain no information about the secret state. Originally proposed [1, 2] and demonstrated experimentally [3] as a cryptographic protocol in the presence of eavesdropping where the access structure was exclusively the entire set of players, QSS was later developed as a quantum analogue of Shamir's powerful threshold secret sharing protocol [4, 5].

Whereas the experimental realization of full QSS may require GHZ states [6], continuous variable QSS can be achieved with squeezed light sources. A continuous variable (2, 3) QSS threshold scheme has been proposed by Tyc and Sanders [7]. In this paper, we extend the original proposal by Tyc and Sanders and introduce another more practical scheme that utilizes an electro-optic feedforward technique. Ideally the dealer would employ a perfectly entangled pair of beams. This is in practice impossible; however, improvement over classical schemes can still be achieved with finite amounts of entanglement. Moreover, we will show that the introduction of large Gaussian noise above the standard quantum limit on the shares by the dealer can further improve the efficacy of QSS.

Similar to quantum teleportation, QSS involves the reconstruction of an original input state at a remote location from transmitted information and available quantum resources. We point out, however, that they differ from each other in two respects. Firstly, in quantum teleportation the input state is destroyed during the measurement process. The reconstruction of the original state is subsequently performed. Only classical information and a pair of entangled beams is shared between the sender and the receiver. In QSS, however, direct linkages of optical beam paths containing the encoded secret *from* the dealer *to* all players are permissible. The dealer therefore is not required to make destructive measurement of the input secret. Secondly, in quantum teleportation the ideal reconstruction of the input state can only be uniquely carried out by one single party as a consequence of the no-cloning theorem. In QSS, on the other hand, multiple reconstruction protocols exist within the access structure.

In spite of the differences, the performance of the QSS scheme can still be quantified using figures of merit similar to those used in quantum teleportation. For the purpose of characterizing the QSS schemes, we consider the secret to be encoded on the sideband frequency quadrature amplitudes of a coherent light beam. We therefore analyse and quantify the performances of the QSS schemes in terms of available input entanglement using two established teleportation measures. We use the fidelity between input and output states as a measure for the quality of state reconstruction. We also characterize QSS in terms of the signal transfer coefficients and the conditional variances of both conjugate quadrature amplitudes of the secret. Although our analysis specifically considers the dealing of coherent states, QSS is primarily concerned with encoding and decoding quantum states. A demonstration of QSS with coherent states is therefore applicable to any arbitrary quantum state in general.

The paper is organized in the following manner. In section 2 we present the dealer protocol to generate three shares. We outline, in section 3, the central role of the optical parametric processes in the QSS schemes. We then present the two secret sharing schemes in section 4 and characterize these schemes in section 5.

2. (2, 3) threshold scheme

Figure 1 shows the dealer protocol of a (2, 3) threshold QSS scheme as proposed by Tyc and Sanders [7]. The dealer employs a pair of entangled beams to encode the secret by interfering one of them with the secret state on a 1:1 beam splitter. We let $\hat{a}_\psi$, $\hat{a}_{\mathrm{EPR1}}$ and $\hat{a}_{\mathrm{EPR2}}$ denote the annihilation operators corresponding to the secret and the two entangled beams, respectively. We express the annihilation operator as $\hat{a}(t) = \alpha + \delta\hat{a}(t)$ where α and $\delta\hat{a}(t)$ denote the steady state component and zero-mean value fluctuations of the annihilation operator, respectively. Provided that the variance of the field fluctuations $V(\delta a)$ is small compared to the field strength $|\alpha|^2$, the dynamics can be treated in the linearized regime for which we can approximate all higher order fluctuation terms to zero. The amplitude and phase quadrature operators are denoted as $\hat{X}^+ = \hat{a}^\dagger + \hat{a}$ and $\hat{X}^- = \imath(\hat{a}^\dagger - \hat{a})$, whilst the variance of these operators is expressed in the frequency domain as $V^\pm(\omega) = \langle[\delta\hat{X}^\pm(\omega)]^2\rangle$. The annihilation operators corresponding to the three shares are then given by

$$\hat{a}_1 = \frac{\hat{a}_\psi + \hat{a}_{\mathrm{EPR1}}}{\sqrt{2}} \tag{1}$$

$$\hat{a}_2 = \frac{\hat{a}_\psi - \hat{a}_{\mathrm{EPR1}}}{\sqrt{2}} \tag{2}$$

$$\hat{a}_3 = \hat{a}_{\mathrm{EPR2}}. \tag{3}$$

Players 1 and 2 (henceforth denoted by $\{1, 2\}$) only need to complete a Mach–Zehnder interferometer with the use of a 1:1 beam splitter to retrieve the secret state. The output beams of the Mach–Zehnder are described by

$$\hat{a}_1' = \frac{\hat{a}_1 + \hat{a}_2}{\sqrt{2}} = \hat{a}_\psi \tag{4}$$

$$\hat{a}_2' = \frac{\hat{a}_1 - \hat{a}_2}{\sqrt{2}} = \hat{a}_{\mathrm{EPR1}}. \tag{5}$$

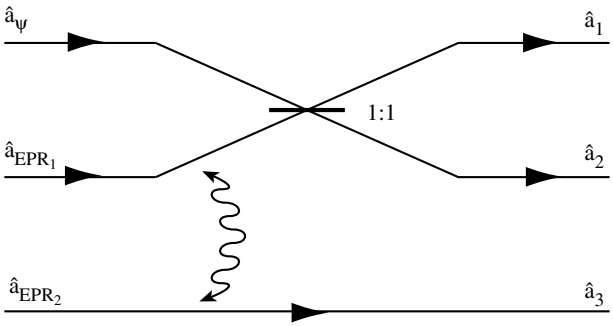

Figure 1. Dealer protocol for the production of three shares in a (2, 3) threshold QSS scheme.

Equation (4) clearly shows that the secret is perfectly reconstructed. In contrast, secret reconstructions for $\{2, 3\}$ or $\{1, 3\}$ require more complex protocols. The paper now focuses on experimental alternatives for the implementation of this reconstruction process.

3. Optical parametric gain and entanglement

3.1. Phase sensitive parametric amplifier

One of the important elements for QSS is the phase sensitive parametric amplifier (PSA). The PSA involves an optical parametric down-conversion process. In this process a pump photon is converted into a pair of twin photons following the simple scheme $\hbar\omega_{\text{pump}} \rightarrow \hbar\omega_{\text{s}} + \hbar\omega_{\text{i}}$, where the signal and idler modes are denoted ω_{s} and ω_{i}, respectively.

The down-conversion process can be achieved in a bulk type II second order non-linear crystal in a travelling wave configuration [8]. In this configuration the signal and idler modes are orthogonally polarized with respect to each other. Assuming that all the power is carried in the mode linearly polarized at 45° with respect to the signal and idler modes, it can be shown that the output mode exhibits phase sensitive parametric amplification.

Another way of achieving down-conversion is in a type I crystal in a continuous wave configuration, where the crystal is in a cavity. An example of this is an optical parametric oscillator (OPO) operating below threshold as a PSA [9]. It can be shown that the output mode from such a system also exhibits phase sensitive parametric amplification similar to the type II case.

The amplitude quadratures of output mode for both the type I and type II systems, X^{+}_{out} and X^{-}_{out}, exhibit amplification and deamplification respectively, relative to the input mode. They can be expressed in the frequency domain as

$$\delta X^{+}_{\text{out}} = \sqrt{G}\delta X^{+}_{\text{in}} \tag{6}$$

$$\delta X^{-}_{\text{out}} = \frac{1}{\sqrt{G}}\delta X^{-}_{\text{in}} \tag{7}$$

where the gain, G, is dependent on the pump power, and on the relative phase between the pump and the input mode, and where the general operator $Z = Z(\omega)$ is the Fourier transform of the time operator $\hat{Z} = \hat{Z}(t)$.

3.2. Production of entangled beams

For type II systems, the signal and idler output modes generated by a single PSA exhibit quadrature entanglement [10, 11]. Since the two modes are orthogonally polarized, the entangled beams can be spatially separated using a polarizing beam splitter. Meanwhile, for type I systems, quadrature entangled beams can be produced by interfering a pair of squeezed beams produced by two OPAs on a 1:1 beam splitter [12]. The output beams from the beam splitter will also exhibit quadrature entanglement.

The entanglement between the X^+ and X^- quadratures of the output modes in both systems can be characterized by using the inseparability criterion proposed by Duan *et al* [13]. For symmetric inputs, Duan's inseparability criterion is given by

$$\langle(\delta X_s^+ + \delta X_i^+)^2\rangle + \langle(\delta X_s^- - \delta X_i^-)^2\rangle < 2 \tag{8}$$

where subscripts s and i denote the two entangled beams. Since $\langle(\delta X_s^+ + \delta X_i^+)^2\rangle = \langle(\delta X_s^- - \delta X_i^-)^2\rangle = 1/\cosh 2r$ for both configurations, the beams show quadrature entanglement when $r > 0$ (where r is the squeezing parameter of the input beams for type I, or the interaction parameter for type II).

4. Proposed experimental set-ups

In this section, we analyse how $\{2, 3\}$ can reconstruct the secret sent by the dealer. The method described here can also be applied unchanged to $\{1, 3\}$, and so we will not cite this case explicitly in the following paragraphs.

First, one can remark that by performing homodyne measurement on $\hat{a}_2$ and $\hat{a}_3$, and then by combining their results with a well chosen gain, $\{2, 3\}$ can get a measure of the amplitude or the phase of the secret, but they cannot measure both at the same time. This scheme can be used for practical applications which require only classical information of a single quadrature to be transferred between the dealer and the players. Since the secret is not reconstructed, nor quantum information of both quadratures transferred, this protocol does not qualify as QSS.

Let us now concentrate on schemes which effectively reconstruct both the amplitude and phase of the secret at the same time.

4.1. The 2PSA scheme

This scheme follows the original idea of Tyc and Sanders [7]. To reconstruct the secret using two PSAs, $\{2, 3\}$ first combine $\hat{a}_2$ and $\hat{a}_3$ on a 1:1 beam splitter, producing two beams $\hat{a}$ and $\hat{b}$, as depicted in figure 2. They pass each of these beams though separate PSAs, denoted by $\mathrm{PSA_a}$ and $\mathrm{PSA_b}$ respectively. Both the PSAs are adjusted so that the output of $\mathrm{PSA_a}$ is amplified in the X^+ quadrature and deamplified in the X^- quadrature whilst the $\mathrm{PSA_b}$ output is deamplified in the X^+ quadrature and amplified in the X^- quadrature. The gains of the two PSAs are assumed to be equal. The final step required for reconstruction of the secret is to combine both PSA outputs on another 1:1 beam splitter. We denote these outputs as $\hat{a}_{\mathrm{out}_1}$ and $\hat{a}_{\mathrm{out}_2}$.

The PSAs can be used in both configurations discussed in section 3. We find the output quadrature amplitudes for both configurations to be of the form

$$X_{\mathrm{out}_1}^{\pm} = \frac{1}{2\sqrt{2}} X_{\psi}^{\pm}\left(\sqrt{G} + \frac{1}{\sqrt{G}}\right) + \frac{\alpha^{\pm}}{\sqrt{2}} + \frac{\beta^{\pm}}{\sqrt{2}}. \tag{9}$$

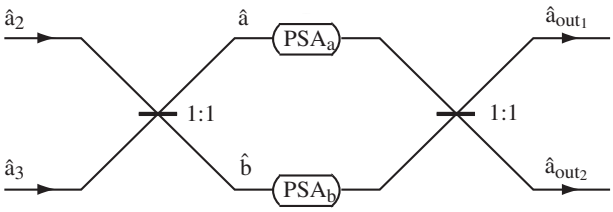

Figure 2. Reconstruction of the secret for $\{2, 3\}$ using the 2PSA scheme.

It is obvious that if output 1 is used to construct the secret, then output 2 will in the limit of perfect QSS contain no relevant information. We will therefore not analyse output 2. For the type II configuration, the $\alpha^{\pm}$ and $\beta^{\pm}$ parameters are dependent on the interaction parameters of the parametric process

$$\alpha^{\pm} = \left[\sqrt{G}\left(\frac{1}{\sqrt{2}}\sinh r - \frac{1}{2}\cosh r\right) - \frac{1}{\sqrt{G}}\left(\frac{1}{2}\cosh r + \frac{1}{\sqrt{2}}\sinh r\right)\right]X^{\pm}_{s,\mathrm{in}} \quad (10)$$

$$\beta^{\pm} = \left[\sqrt{G}\left(\frac{1}{\sqrt{2}}\cosh r - \frac{1}{2}\sinh r\right) - \frac{1}{\sqrt{G}}\left(\frac{1}{2}\sinh r + \frac{1}{\sqrt{2}}\cosh r\right)\right]X^{\pm}_{i,\mathrm{in}}. \quad (11)$$

For the type I configuration, they are dependent on the amount of squeezing of both squeezed state inputs. We therefore obtain

$$\alpha^{\pm} = \frac{X^{\mp}_{\mathrm{sqz1}}}{\sqrt{G}}(-1 \mp \sqrt{2}) + \sqrt{G}(-1 \pm \sqrt{2}) \quad (12)$$

$$\beta^{\pm} = \frac{X^{\pm}_{\mathrm{sqz2}}}{\sqrt{G}}(-1 \pm \sqrt{2}) + \sqrt{G}(-1 \mp \sqrt{2}). \quad (13)$$

In the case of perfect entanglement (i.e. $r \to \infty$), setting the parametric gain to

$$G = \frac{\sqrt{2}+1}{\sqrt{2}-1} \quad (14)$$

will completely eliminate the contribution of the input entanglement modes. We are therefore left with the original secret. With imperfect entanglement, we find for the type II configuration

$$X^{\pm}_{\mathrm{out}_1} = X^{\pm}_{\psi} - \mathrm{e}^{-r}X^{\pm}_{s,\mathrm{in}} + \mathrm{e}^{-r}X^{\pm}_{i,\mathrm{in}}. \quad (15)$$

Similarly, the output quadrature amplitudes for the type I configuration are given by

$$X^{+}_{\mathrm{out}_1} = X^{+}_{\psi} - \sqrt{2}X^{+}_{\mathrm{sqz}_2} \quad (16)$$

$$X^{-}_{\mathrm{out}_1} = X^{-}_{\psi} - \sqrt{2}X^{+}_{\mathrm{sqz}_1} \quad (17)$$

where it is assumed that $X^{+}_{\mathrm{sqz}_{1,2}}$ are the squeezed quadratures. The results above demonstrate that with finite entanglement, $\{2, 3\}$ are able to reconstruct the secret $\hat{a}_{\psi}$ with added noise variance of $2\mathrm{e}^{-2r}$. In addition to the parametric processes required for the generation of a pair of entangled beams, the QSS scheme described above requires two additional PSAs. This is experimentally very challenging. Since non-linear effects in optics are small, methods have been used to increase optical intensities in experiments to enhance the parametric process. One such example is the utilization of high peak power pulsed light sources, either in Q-switched or mode-locked set-ups, to single pass light beams through the non-linear media to achieve the required phase sensitive

amplification. A common difficulty found in such systems is the distortion of optical wavefronts due to the non-linear medium. This would result in poor optical interference and losses. Another method of increasing optical intensity in non-linear processes is the use of optical resonators. In this situation, the resonators also act as mode cleaners to the beams, thus ensuring better beam quality. However, impedance matching of the resonators, which is not required for single-pass phase sensitive amplification, is difficult to achieve. Imperfect impedance matching again leads to losses. It is therefore interesting to find an alternative scheme which does not require additional parametric processes for the reconstruction of the secret. In the next section, we will present a QSS scheme that requires only an electro-optic feedforward loop for $\{2, 3\}$ in secret reconstruction.

4.2. Feedforward loop scheme

Electro-optic feedforward loops have been widely used in many continuous variable experiments. The feedforward set-up has been demonstrated to be useful in noiseless control of light beams [14] and has recently been used in teleportation experiments [15, 16]. In our feedforward QSS scheme, the dealer introduces additional noise above the standard quantum limit on the entangled beams, with a Gaussian distribution. The purpose of this additional noise will be discussed in the characterization section 5. This can be achieved using a pair of phase modulators on the constituent amplitude squeezed beams as shown in figure 3. This results in the two entangled beams having anticorrelated Gaussian noise in the amplitude quadratures and correlated Gaussian noise in the phase quadratures. Due to the 1:1 beam splitter ratio, both beams have an equal amount of added noise. The shares can then be expressed as

$$\hat{a}_1 = \frac{\hat{a}_\psi + \hat{a}_{\mathrm{EPR1}} + \delta\hat{a}_{m1}}{\sqrt{2}} \tag{18}$$

$$\hat{a}_2 = \frac{\hat{a}_\psi - \hat{a}_{\mathrm{EPR1}} - \delta\hat{a}_{m1}}{\sqrt{2}} \tag{19}$$

$$\hat{a}_3 = \hat{a}_{\mathrm{EPR2}} + \delta\hat{a}_{m2} \tag{20}$$

where $\delta\hat{a}_{m1,2} = (\pm\delta\hat{X}_m^+ + \mathrm{i}\delta\hat{X}_m^-)/2$ represent the additional Gaussian noise introduced by the two phase modulators. The strength of these additional modulations is given by $V_m^\pm = \langle(\delta\hat{X}_m^\pm)^2\rangle = \mathrm{e}^{2s}$.

Similar to the previous dealer protocol, $\{1, 2\}$ can retrieve the secret by completing a Mach–Zehnder interferometer. To reconstruct the secret, $\{2, 3\}$ can interfere beams $\hat{a}_2$ and $\hat{a}_3$ on a 2/3 reflective beam splitter as shown in figure 3[4]. The beam splitter outputs are given by

$$X_b^+ = \frac{1}{\sqrt{3}}(X_{\mathrm{sqz}_2}^- - X_{\mathrm{sqz}_1}^- + X_\psi^+ - 2X_m^+) \tag{21}$$

$$X_b^- = \frac{1}{\sqrt{3}}(X_{\mathrm{sqz}_1}^+ - X_{\mathrm{sqz}_2}^+ + X_\psi^-) \tag{22}$$

$$X_c^+ = \frac{[(X_{\mathrm{sqz}_1}^- - X_{\mathrm{sqz}_2}^-) - 3(X_{\mathrm{sqz}_1}^+ + X_{\mathrm{sqz}_2}^+) + 2(X_\psi^+ + X_m^+)]}{\sqrt{24}} \tag{23}$$

[4] In this paper, a 2:1 beam splitter ratio is adopted for the analysis of the secret reconstruction between $\{2, 3\}$ for all situations. We note that in general, both the beam splitter ratio and the feedforward gain can be optimized depending on the amount of input entanglement.

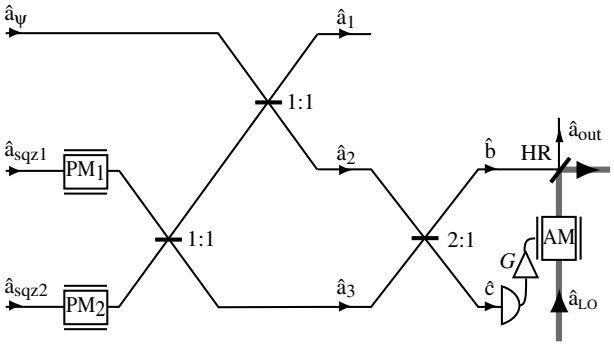

Figure 3. Dealer protocol and the reconstruction of the secret for $\{2, 3\}$ using an electro-optic feedforward loop. 2:1 is a 2/3 reflective beam splitter and HR is an HR beam splitter. $PM_{1,2}$ are phase modulators on the respective amplitude squeezed beams.

$$X_c^- = \frac{[(X^+_{\mathrm{sqz}_2} - X^+_{\mathrm{sqz}_1}) - 3(X^-_{\mathrm{sqz}_1} + X^-_{\mathrm{sqz}_2}) + 2(X^-_{\psi} - 3X^-_m)]}{\sqrt{24}}. \tag{24}$$

Since $V^+_{\mathrm{sqz}1,2} \ll 1$ in the limit of large squeezing, we note that the 2/3 reflective beam splitter ensures that the phase quadrature of the secret is already faithfully reconstructed in X_b^-. By measuring the amplitude fluctuations X_c^+ and applying them to X_b^+, it is possible to eliminate the remaining anti-squeezed fluctuations, $X^-_{\mathrm{sqz}1,2}$, and the added amplitude noise X_m^+ on the same beam. This can be done simply by directly detecting beam $\hat{c}$ and then electro-optically feeding the detected signal to the amplitude of beam $\hat{b}$ with the right gain. Due to optical losses, however, better efficiency can be achieved by divorcing the modulators from beam $\hat{b}$ as shown in figure 3. Instead, the detected signal from beam $\hat{c}$ is encoded off line on a strong local oscillator beam, a_{LO}. The signal on the local oscillator can then be mixed back onto beam $\hat{b}$ using a highly reflective (HR) beam splitter as shown in figure 3. The resulting output quadratures are given by $X^{\pm}_{\mathrm{out}} = \sqrt{1-\epsilon}X^{\pm}_b + \sqrt{\epsilon}X^{\pm}_{\mathrm{LO}}$. In the limit of high beam splitter reflectivity, $\epsilon \to 0$, we obtain

$$\begin{aligned} X^+_{\mathrm{out}} &\simeq X^+_b + K(\omega)\delta I \\ X^-_{\mathrm{out}} &\simeq X^-_b \end{aligned} \tag{25}$$

where $K(\omega)$ is a gain transfer function which takes into account the response of the electro-optic feedforward circuit and the loss due to the HR beam splitter. δI is the detected photocurrent of the amplitude quadrature fluctuations of beam $\hat{c}$ given by

$$\begin{aligned} \delta I = \sqrt{\eta}\langle X_c^+\rangle \Bigg[\frac{1}{2}\sqrt{\frac{1}{3}}\sqrt{\eta}\Big(\frac{1}{\sqrt{2}}(\delta X^-_{\mathrm{sqz}_1} - \delta X^-_{\mathrm{sqz}_2}) - \frac{3}{\sqrt{2}}(\delta X^+_{\mathrm{sqz}_1} + \delta X^+_{\mathrm{sqz}_2}) \\ + \sqrt{2}(\delta X^+_m + \delta X^+_{\psi})\Big) + \sqrt{1-\eta}\delta X^+_d \Bigg] \end{aligned} \tag{26}$$

where η and δX^+_d are, respectively, the detection efficiency and the vacuum fluctuations due to an imperfect detector. The output quadrature fluctuations can be re-expressed as

$$\delta X^+_{\mathrm{out}} = \Big(\frac{1}{\sqrt{3}} + \frac{G}{\sqrt{6}}\Big)\delta X^+_{\psi} + \Big(\frac{G}{2\sqrt{6}} - \frac{1}{\sqrt{3}}\Big)(\delta X^-_{\mathrm{sqz}_1} - \delta X^-_{\mathrm{sqz}_2})$$

$$-\frac{G}{2}\sqrt{\frac{3}{2}}(\delta X^{+}_{\mathrm{sqz}_1}+\delta X^{+}_{\mathrm{sqz}_2})+G\sqrt{\frac{1-\eta}{\eta}}\delta X^{+}_{d}+\Big(\frac{2}{\sqrt{3}}-\frac{G}{\sqrt{6}}\Big)\delta X^{+}_{m} \tag{27}$$

$$\delta X^{-}_{\mathrm{out}}=\sqrt{\frac{1}{3}}\delta X^{-}_{\psi}+\sqrt{\frac{1}{3}}(\delta X^{+}_{\mathrm{sqz}_1}-\delta X^{+}_{\mathrm{sqz}_2}) \tag{28}$$

where $G=\eta K(\omega)\langle X^{+}_{\mathrm{c}}\rangle$ is the total gain of the feedforward loop. By setting $G=2\sqrt{2}$, it is clear that the anti-squeezing and added noise terms of equation (27) are cancelled. In the limit of perfect detection efficiency and large squeezing, we obtain

$$\delta X^{+}_{\mathrm{out}}=\sqrt{3}\delta X^{+}_{\psi} \tag{29}$$

$$\delta X^{-}_{\mathrm{out}}=\frac{1}{\sqrt{3}}\delta X^{-}_{\psi}. \tag{30}$$

Hence $\{2,3\}$ can reproduce a symplectically transformed version of the secret, $\hat{a}_{\psi}$. We note that since symplectic transformations are local unitary operations, no quantum information contained in the secret state is lost. Thus, the feedforward scheme works equally well when compared with the 2PSA scheme in terms of quantum information transfer. In order to reconstruct the quantum state of the secret, however, a single PSA is required on the output beam. Even so, the feedforward scheme is still technically less demanding than the 2PSA scheme introduced in the earlier section. In the next section, we will introduce experimental measures to characterize both QSS schemes.

5. Characterization

In teleportation experiments *fidelity*, $\mathcal{F}=\langle\psi_{\mathrm{in}}|\rho_{\mathrm{out}}|\psi_{\mathrm{in}}\rangle$, is conventionally used to quantify the efficacy of a teleporter [15]. Fidelity can also be adopted to characterize QSS as it is a protocol that reconstructs input quantum states. Whilst the secret state can be arbitrary, we simplify the characterization of our schemes by assuming that the secret is a coherent state. This demonstrates the encoding–decoding process that would, in general, be applicable for any dealt secret state. Assuming that all input noise sources are Gaussian, the fidelity of the QSS schemes is then given by [16]

$$\mathcal{F}=2\mathrm{e}^{-(k^{+}+k^{-})}\sqrt{\frac{V^{+}_{\psi}V^{-}_{\psi}}{(V^{+}_{\psi}+V^{+}_{\mathrm{out}})(V^{-}_{\psi}+V^{-}_{\mathrm{out}})}} \tag{31}$$

where $k^{\pm}=\langle X^{\pm}_{\psi}\rangle^2(1-\langle X^{\pm}_{\psi}\rangle/\langle X^{\pm}_{\mathrm{out}}\rangle)^2/(4V^{\pm}_{\psi}+4V^{\pm}_{\mathrm{out}})$. Assuming an ideal detector ($\eta=1$), we obtain from the analysis of section 4 the theoretical limits of fidelity for the 2PSA scheme as a function of squeezing

$$\mathcal{F}_{\{1,2\}}=1 \tag{32}$$

$$\mathcal{F}_{\{1,3\}}=\mathcal{F}_{\{2,3\}}=\frac{1}{1+\mathrm{e}^{-2r}} \tag{33}$$

where the subscripts i and j in $\mathcal{F}_{\{i,j\}}$ denote the collaborating players (CPs). We note that $\mathcal{F}_{\{1,2\}}$ is always unity since the reconstruction of the secret only requires a simple Mach–Zehnder. In the limit of perfect entanglement, $r\to\infty$, the fidelity of equation (33) also approaches unity. In the case of the feedforward QSS scheme, however, we obtain

$$\mathcal{F}_{\{1,2\}}=1 \tag{34}$$

$$\mathcal{F}_{\{1,3\}} = \mathcal{F}_{\{2,3\}} = \mathrm{e}^{-\Gamma}\sqrt{\frac{3}{(2+\mathrm{e}^{-2r})(2+3\mathrm{e}^{-2r})}} \tag{35}$$

where Γ is dependent on the quadratures of the secret, $\langle X_{\psi}^{\pm}\rangle$, and the squeezing of the input states r, and is given by

$$\Gamma = \frac{2-\sqrt{3}}{12}\left[\langle X_{\psi}^{+}\rangle^2 \frac{1}{(2+3\mathrm{e}^{-2r})} + \langle X_{\psi}^{-}\rangle^2 \frac{9}{(2+\mathrm{e}^{-2r})}\right]. \tag{36}$$

Equation (35) does not tend to unity even in the limit of infinite input squeezing. In fact, it quickly degrades to zero for finite squeezing and large secret sideband modulations. The reason for this is the symplectically transformed secret output state $\hat{a}_{\mathrm{out}}$. We point out, however, that no information is lost. Indeed $\{2, 3\}$ can locally transform the output to get back the original secret state via a single parametric process. The fidelity given in equation (35) after the parametric correction then becomes equal to that of equation (33).

An alternative measure that is invariant to symplectic transformations is the T–V graph proposed by Ralph *et al* [17], and used to characterize quantum teleportation [16]. This graph plots the product of the conditional variances of both conjugate observables $V_q = V_{cv}^{+}V_{cv}^{-}$ against the sum of the signal transfer coefficients $T_q = T^{+} + T^{-}$. Here the conditional variances are given by

$$V_{cv}^{\pm} = V_{\mathrm{out}}^{\pm} + \frac{|\langle \delta X_{\psi}^{\pm}\delta X_{\mathrm{out}}^{\pm}\rangle|}{V_{\psi}^{\pm}} \tag{37}$$

and the signal transfer coefficients are defined as

$$T^{\pm} = \frac{\mathrm{SNR}_{\mathrm{out}}^{\pm}}{\mathrm{SNR}_{\psi}^{\pm}}. \tag{38}$$

In contrast to fidelity which measures the quality of the state reconstruction, the T–V graph emphasizes the transfer of quantum information [16, 18]. V_q is a measure of the amount of added noise on the output state. In an ideal QSS scheme the CP would obtain $V_q = 0$. This suggests perfect quantum correlations between the output and the original input states. T_q is a measure of the amount of transmitted signal on both conjugate quadrature amplitudes of the output state. In an ideal QSS scheme, the access structure would obtain $T_q = 2$. This suggests that the signals on both quadrature amplitudes are perfectly transmitted.

Using these measures, the CPs using the 2PSA scheme can obtain

$$T_q = \frac{2}{1+2\mathrm{e}^{-2r}} \tag{39}$$

$$V_q = 2\mathrm{e}^{-2r} \tag{40}$$

whilst for the feedforward scheme the collaborating players, which we will now denote as (CP), can obtain

$$T_q^{\mathrm{CP}} = \frac{1}{1+2\mathrm{e}^{-2r}} + \frac{(1+\frac{G}{\sqrt{2}})^2}{(1+\frac{G}{\sqrt{2}})^2 + (\frac{G}{2}-\sqrt{2})^2\mathrm{e}^{2r} + (\frac{3G}{2})^2\mathrm{e}^{-2r} + (2-\frac{G}{\sqrt{2}})^2\mathrm{e}^{2s} + \frac{3G^2(1-\eta)}{\eta}} \tag{41}$$

$$V_q^{\mathrm{CP}} = \frac{\mathrm{e}^{-2r}}{18}\left[9G^2\mathrm{e}^{-2r} + \mathrm{e}^{2r}(G-2\sqrt{2})^2 + 2\mathrm{e}^{2s}(G-2\sqrt{2})^2 + 12G^2\left(\frac{1-\eta}{\eta}\right)\right] \tag{42}$$

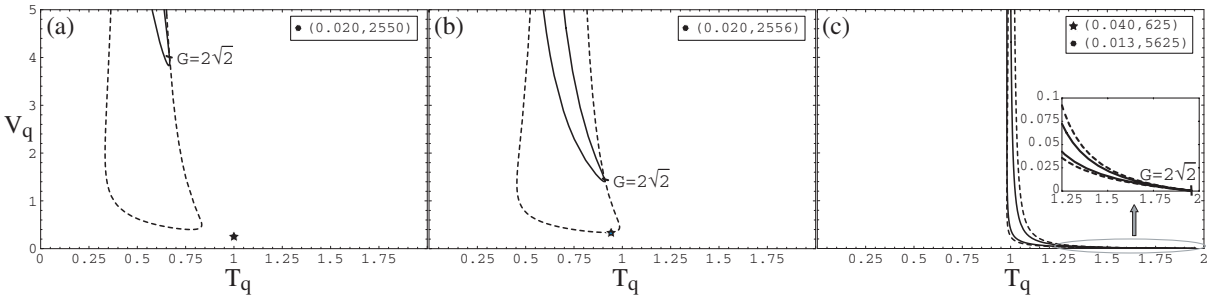

Figure 4. T–V graphs for the feedforward scheme with (a) no squeezing, (b) 40% squeezing and (c) 99% squeezing. The curves represent the information retrieved by $\{2, 3\}$ with varying feedforward gain, and the points represent the information retrieved by $\{1\}$ or $\{2\}$ alone. The dashed curves and stars correspond to the absence of added modulations, whilst the solid curves and circles correspond to 20 dB above the quantum noise of added *Gaussian noise*. We have assumed perfect detector efficiency for the feedforward loop. The coordinates of the points which are outside the plotted region are displayed in the inset of each graph.

where e^{2s} is the power of the added noise. Before analysing these results, we first determine the amount of information the single players (SPs), i.e. the adversary structure, can learn about the secret if they measure their shares directly. In this situation, T_q^{SP} and V_q^{SP} for the SPs are found to be

$$T_q^{\mathrm{SP}} = \frac{2}{1 + \cosh 2r + e^{2s}} \tag{43}$$

$$V_q^{\mathrm{SP}} = \frac{(\cosh 2r + e^{2s})^2}{4}. \tag{44}$$

Figure 4 shows the results of the feedforward QSS scheme for three different amounts of input squeezing. The dotted curves represent the results obtained by $\{2, 3\}$ in the absence of added noise when feedforward gain is varied. The star points represent the maximum information retrievable by $\{1\}$ or $\{2\}$ alone in the corresponding situations. Results for the addition of Gaussian noise, 20 dB above the quantum noise limit, are depicted by solid curves for the CPs and by circles for the SPs. In the limit of infinite input squeezing, the CPs can reconstruct the secret perfectly, with $T_q^{\mathrm{CP}} \to 2$ and $V_q^{\mathrm{CP}} \to 0$. This is achieved with an optimum, feedforward gain of $G = 2\sqrt{2}$ where the influence of both the anti-squeezing quadratures (and the added noise) are completely cancelled as discussed in section 4.2, whilst SPs in the same limit obtain no information about the secret, with $T_q^{\mathrm{SP}} \to 0$ and $V_q^{\mathrm{SP}} \to \infty$, due to the dominant effect of the anti-squeezing quadratures (and the added noise). These results are shown in the plots of figure 4(c).

In the case of finite squeezing and no added noise, however, the optimum feedforward gain for the CPs is always less than $2\sqrt{2}$ as shown in both figures 4(a) and (b). Further, SPs forming the adversary structures can obtain some quantum information about the secret. In the case of weak entanglement (see figures 4(a) and (b)) a single player obtains more information about the secret than the access structure using the feedforward scheme. In this situation, the CPs should optimize the beam splitter ratio based on the amount of entanglement. The optimal beam splitter

Table 1. Summary of the performances of the feedforward QSS schemes with (quant) and without (class) optical entanglement; and with (n) and without added noise ($\bar{n}$). Parameters listed are the best achievable (T_q, V_q) values for the 2:1 beam splitter.

(T_q, V_q)		Class, $\bar{n}$	Class, n	Quant, $\bar{n}$	Quant, n
Adversary	1	$(1, 1/4)$	$(0, \infty)$	$(0, \infty)$	$(0, \infty)$
structure	2	$(1, 1/4)$	$(0, \infty)$	$(0, \infty)$	$(0, \infty)$
	3	$(0, 1)$	$(0, \infty)$	$(0, \infty)$	$(0, \infty)$
Access	$\{1, 2\}$	$(2, 0)$	$(2, 0)$	$(2, 0)$	$(2, 0)$
structure	$\{1, 3\}$	$(1, 1/4)$	$(2/3, 4)$	$(2, 0)$	$(2, 0)$
	$\{2, 3\}$	$(1, 1/4)$	$(2/3, 4)$	$(2, 0)$	$(2, 0)$

reflectivity varies between 66% (for perfect entanglement) and 100% for no entanglement. An alternative way to prevent the SPs from obtaining more information about the secret than the access structure is to have the dealer introduce phase quadrature noise on both input amplitude squeezed beams. The phase noise translates to added noise in both the amplitude and phase quadratures of the entangled beams, $\delta X_m^{\pm}$. For large modulations, say 20 dB above the quantum noise limit, the SPs obtain virtually no information about the secret, thus making $T_q^{\mathrm{SP}} \to 0$ and $V_q^{\mathrm{SP}} \to \infty$ even in the absence of input squeezing. CPs, on the other hand, obtain a zero-squeezing classical limit of $T_q^{\mathrm{CP}} \to 2/3$ and $V_q^{\mathrm{CP}} \to 4$.

Another consequence of the added noise for the CPs is that the optimum gain for maximum information transfer again approaches $2\sqrt{2}$. This results in the CPs obtaining less information about the secret with increasing amounts of added noise. Nonetheless, the CPs can now obtain much more information than the SPs for all levels of input squeezing. Any amount of input squeezing will now differentially increase the amount of information the access structure has over the adversary structure. These results are illustrated by the solid curves and the circles of figure 4.

6. Conclusion

In this paper, we have presented two experimental (2, 3) threshold QSS schemes. The first one requires a pair of optically entangled beams and two phase sensitive amplifiers for the reconstruction of the secret state, whilst the second utilizes a pair of optically entangled beams and an additional electro-optic feedforward loop. We have shown that the latter scheme produces output states that are symplectic transforms of the original secret states. Nevertheless, all quantum information is retained in the reconstructed output state in the limit of perfect entanglement. We show that by introducing added Gaussian noise on the entangled beams, it is possible to guarantee security against attacks from individual players. Table 1 summarizes the performances of our proposed feedforward QSS scheme for both classical (without entanglement), and quantum (with perfect entanglement) regimes. They are also calculated for situations with and without added noise.

Acknowledgments

This research is supported by the Australian Research Council. We thank Ben Buchler and Stephen Bartlett for useful discussions. This work is a part of EU QIPC project no IST-1999-13071 (QUICOV).

References

[1] Hillery M, Buzek V and Bethiaume A 1999 *Phys. Rev.* A **59** 1829
[2] Karlsson A, Koashi M and Imoto N 1999 *Phys. Rev.* A **59** 162
[3] Tittel W, Zbinden H and Gisin N 2001 *Phys. Rev.* A **63** 042301
[4] Shamir A 1979 *Commun. ACM* **22** 612
[5] Cleve R, Gottesman D and Lo H-K 1999 *Phys. Rev. Lett.* **83** 648
[6] Greenberger D M, Horne M A, Shimony A and Zeilinger A 1990 *Am. J. Phys.* **58** 1131
[7] Tyc T and Sanders B C 2002 *Phys. Rev.* A **65** 42310
[8] Levenson J A, Abram I, Rivera T and Grangier P 1993 *J. Opt. Soc. Am.* B **10** 2233
[9] Lam P K, Ralph T C, Buchler B C, McClelland D E, Bachor H-A and Gao J 1999 *J. Opt. B: Quantum Semiclass. Opt.* **1** 469
[10] Reid M 1989 *Phys. Rev.* A **40** 913
[11] Bencheikh K, Symul T, Jankovic A and Levenson J A 2001 *J. Mod. Opt.* **48** 1903
[12] Ou Z Y, Pereira S F, Kimble H J and Peng K C 1992 *Phys. Rev. Lett.* **68** 3663
[13] Duan L-M *et al* 2000 *Phys. Rev. Lett.* **84** 2722
[14] Lam P K, Ralph T C, Huntington E H and Bachor H-A 1997 *Phys. Rev. Lett.* **79** 1471
Ralph T C 1997 *Phys. Rev.* A **56** 4187
Huntington E H, Lam P K, Ralph T C, McClelland D E and Bachor H-A 1998 *Opt. Lett.* **23** 540
[15] Furusawa A *et al* 1998 *Science* **282** 706
[16] Bowen W P, Treps N, Buchler B C, Schnabel R, Ralph T C, Bachor H-A, Symul T and Lam P K 2002 *Preprint* quant-ph/0207179
[17] Ralph T C, Lam P K and Polkinghorne R E S 1999 *J. Opt. B: Quantum Semiclass. Opt.* **1** 483
[18] Ralph T C and Lam P K 1998 *Phys. Rev. Lett.* **81** 5668