Is Quantum Secret Sharing different to the Sharing of a Quantum Secret?

Andrew M. Lance[a], Thomas Symul[a], Warwick P. Bowen[a], Tomáš Tyc[b,c], Barry C. Sanders[c] and Ping Koy Lam[a]

[a]Quantum Optics Group, Department of Physics, Faculty of Science, Australian National University, ACT 0200, Australia
[b]Institute of Theoretical Physics, Masaryk University, 61137 Brno, Czech Republic
[c]Department of Physics and the Centre for Advanced Computing - Algorithms and Cryptography, Macquarie University, Sydney, NSW 2109, Australia

ABSTRACT

We present an experimental scheme to perform continuous variable (2,3) threshold quantum secret sharing on the quadratures amplitudes of bright light beams. It requires a pair of entangled light beams and an electro-optic feedforward loop for the reconstruction of the secret. We examine the efficacy of quantum secret sharing in terms of fidelity, as well as the signal transfer coefficients and the conditional variances of the reconstructed output state. We show that, in the ideal limit, perfect secret reconstruction is possible. We discuss two different definitions of quantum secret sharing: the sharing of a quantum secret and the sharing of a classical secret with quantum resources.

1. INTRODUCTION

Secret sharing (SS), first introduced by Shamir,[1] is a cryptographic protocol for distributing secret information to a group of *players*, some of whom cannot be trusted. A particular subset of SS schemes is the (k, n) threshold scheme where at least k players among the n total players have to collaborate to reconstruct the secret. The ensemble of all the subsets of k players, called the *access structure*, are able to reconstruct the secret while the remaining players, called the *adversary structure*, are unable to obtain any information about the secret.

The term *quantum secret sharing* (QSS) was first introduced by Hillery *et al.*.[2] In their proposal, QSS was introduced as a protocol for sharing a classical secret, in the presence of eavesdroppers, to many parties. The protection of the secret is achieved using quantum resources. More explicitly, the protocol is the quantum sharing of a classical secret. This idea was first experimentally demonstrated by Tittel *et al.*[3] using single photons pseudo-GHZ states based on energy-time entanglement.

A stronger quantum analogue to Shamir's classical SS scheme was proposed by Cleve *et al.*[4] where the secret being shared is a quantum state. Similar to the scheme of Hillery *et al.*, the integrity of the quantum state is also protected using quantum resources. In the scheme of Cleve *et al.*, the quantum state is divided into n shares where any k shares are required to reconstruct the quantum state. The remaining shares, however, cannot extract any information about the quantum secret. In this sense, QSS describes the quantum sharing of a quantum secret. Assuming that the protocol is fair to all players, a direct consequence of the no-cloning theorem then dictates that $k > n/2$, ensuring that majority is reached before any secret can be revealed.

Both the Hillery *et al.* and Cleve *et al.* proposals have a number of potential applications. Both schemes have applications as a key distribution scheme for multi-partite quantum cryptographic protocols, whilst the scheme of Cleve *et al.* has further application in quantum information processing. For example, it can be used to facilitate the robust transport and storage of quantum states in quantum computation. By dividing a quantum state into n shares, the state can be reconstructed at a later stage using k or more shares.

More recently, QSS has been extended to the continous variable domain.[5,6] These protocols are used to share quantum secret states implemented using Einstein-Podolsky-Rosen (EPR) entangled light beams and optical interferometers.

In this paper we present a continous variable $(2, 3)$ threshold QSS scheme.[7] The quantum state, denoted $|\psi_{\text{in}}\rangle$, is encoded using EPR entangled beams which are generated by mixing two bright squeezed beams on a beam splitter with a relative phase shift of $\pi/2$. The secret is encoded on the sideband frequency quadrature amplitudes of a light beam. Ideally

Quantum Communications and Quantum Imaging, edited by Ronald E. Meyers, Yanhua Shih,
Proc. of SPIE Vol. 5161 (SPIE, Bellingham, WA, 2004) · 0277-786X/04/$15 · doi: 10.1117/12.505349

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 show that the introduction of classical noise by the dealer can further improve the QSS scheme. We compare and quantify the performance of the scheme in terms of available input entanglement using two measures; we measure the fidelity between the input and output states and we also measure the signal transfer coefficients and the conditional variances of both conjugate quadrature amplitudes of the secret.

2. (2,3) THRESHOLD SCHEME

2.1. Dealer protocol

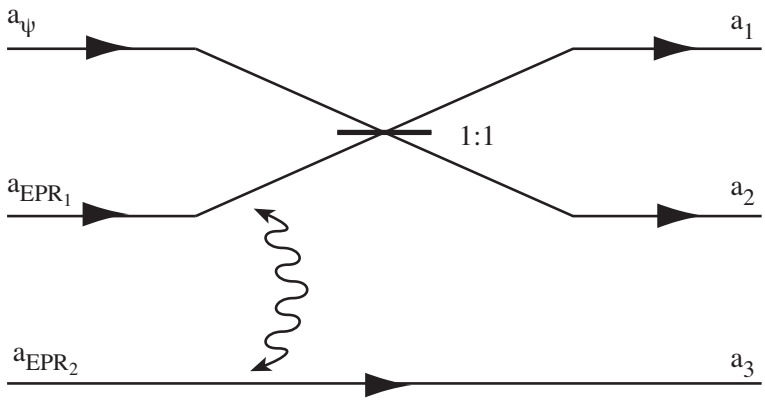

Figure 1. Dealer protocol for the production of three shares in a (2,3) threshold QSS scheme.

Figure 1 shows the dealer protocol of a (2,3) threshold QSS scheme as proposed by Tyc and Sanders. [5] 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 $\hat{a}_\psi$, $\hat{a}_{\rm EPR1}$ and $\hat{a}_{\rm EPR2}$ denote the annihilation operators corresponding to the secret and the two entangled beams, respectively. The linearized expression for the annihilation operator is given by $\hat{a}(t) = \alpha + \delta\hat{a}(t)$ where α and $\delta\hat{a}(t)$ denote the steady state component and zero mean value fluctuations of the annihilation operator, respectively. The amplitude and phase quadrature operators are denoted as $\hat{X}^+ = \hat{a}^\dagger + \hat{a}$ and $\hat{X}^- = \imath\left(\hat{a}^\dagger - \hat{a}\right)$, 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

$$\hat{a}_1 = \frac{\hat{a}_\psi + \hat{a}_{\rm EPR1}}{\sqrt{2}} \quad (1)$$

$$\hat{a}_2 = \frac{\hat{a}_\psi - \hat{a}_{\rm EPR1}}{\sqrt{2}} \quad (2)$$

$$\hat{a}_3 = \hat{a}_{\rm EPR2} \quad (3)$$

2.2. {1,2} protocol

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

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

$$\hat{a}_2' = \frac{\hat{a}_1 - \hat{a}_2}{\sqrt{2}} = \hat{a}_{\rm EPR1} \quad (5)$$

Eq. (4) clearly shows that the the secret is perfectly reconstructed whilst player {3} obtains no information about the secret. In contrast, the secret reconstructions for {2,3} or {1,3} requires a more complex protocol. The next section focuses on the implementation of an experimentally achievable reconstruction protocol for these access structures.

2.3. {2,3} protocol

In this section, we analyze 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 explicitly this case in the following paragraphs.

By encoding correlated classical noise on the amplitude and phase quadratures of the EPR beams it is possible for the dealer to enhance the security of a QSS scheme. This is achieved by using a pair of phase modulators on the constituent amplitude squeezed beams as shown in Fig. 2. This results in the two entangled beams having anticorrelated classical noise in the amplitude quadratures and correlated classical noise in the phase quadratures. The quantum component allows for the reconstruction of the quantum features of the input state whilst the classical component enhances the security of the QSS scheme. The shares can then be expressed as

$$\hat{a}_1 = \frac{\hat{a}_\psi + \hat{a}_{\mathrm{EPR1}} + \delta\hat{a}_{m1}}{\sqrt{2}} \tag{6}$$

$$\hat{a}_2 = \frac{\hat{a}_\psi - \hat{a}_{\mathrm{EPR1}} - \delta\hat{a}_{m1}}{\sqrt{2}} \tag{7}$$

$$\hat{a}_3 = \hat{a}_{\mathrm{EPR2}} + \delta\hat{a}_{m2} \tag{8}$$

where $\delta\hat{a}_{m1,2} = (\pm\delta\hat{X}_m^+ + i\delta\hat{X}_m^-)/2$ are the additional classical noise introduced by the two phase modulators. The strength of these additional modulations is given by $V_m^\pm = \langle(\delta\hat{X}_m^\pm)^2\rangle = e^{2s}$. Similar to the previous dealer protocol, {1,2}

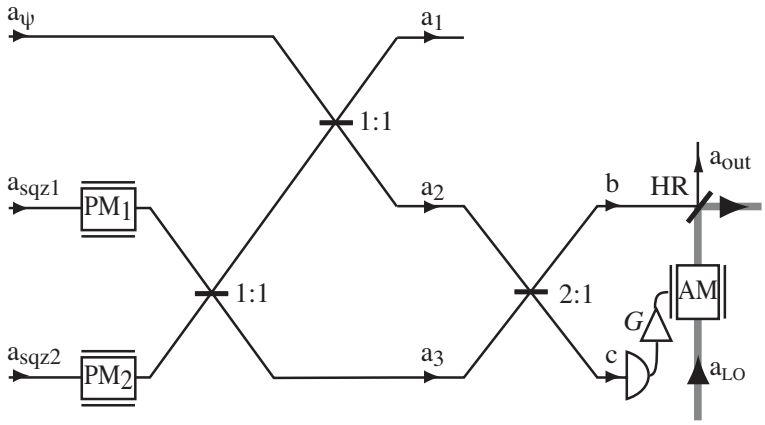

Figure 2. Dealer protocol and the reconstruction of secret for {2,3} using an electro-optic feedforward loop. 2:1 is a $2/3$ reflective beam splitter and HR is a highly reflective beam splitter. $\mathrm{PM}_{1,2}$ are phase modulators on the respective amplitude squeezed beams.

can retrieve the secret by completing a Mach-Zehnder interferometer. To reconstruct the secret, {2,3} interfere beams $\hat{a}_2$ and $\hat{a}_3$ on a $2/3$ reflective beam splitter as shown in Fig. 2 *. The beams splitter outputs are given by

$$X_b^+ = \frac{1}{\sqrt{3}}(X_{\mathrm{sqz}_2}^- - X_{\mathrm{sqz}_1}^- + X_\psi^+ - 2X_m^+) \tag{9}$$

$$X_b^- = \frac{1}{\sqrt{3}}(X_{\mathrm{sqz}_1}^+ - X_{\mathrm{sqz}_2}^+ + X_\psi^-) \tag{10}$$

$$X_c^+ = \frac{[(X_{\mathrm{sqz}_1}^- - X_{\mathrm{sqz}_2}^-) - 3(X_{\mathrm{sqz}_1}^+ + X_{\mathrm{sqz}_2}^+) + 2(X_\psi^+ + X_m^+)]}{\sqrt{24}} \tag{11}$$

$$X_c^- = \frac{[(X_{\mathrm{sqz}_2}^+ - X_{\mathrm{sqz}_1}^+) - 3(X_{\mathrm{sqz}_1}^- + X_{\mathrm{sqz}_2}^-) + 2(X_\psi^- - 3X_m^-)]}{\sqrt{24}} \tag{12}$$

*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 optimised depending on the amount of input entanglement.

Since $X^{+}_{\mathrm{sqz}1,2} \ll 1$ 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 classical 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 Fig. 2. 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 beam splitter as shown in Fig. 2. 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

$$\begin{aligned} X^{+}_{\mathrm{out}} &\simeq X^{+}_{b} + K(\omega)\delta I \\ X^{-}_{\mathrm{out}} &\simeq X^{-}_{b} \end{aligned} \tag{13}$$

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

$$\delta I = \sqrt{\eta}\langle X^{+}_{c}\rangle\left[\frac{1}{2}\sqrt{\frac{1}{3}}\sqrt{\eta}\left(\frac{1}{\sqrt{2}}\left(\delta X^{-}_{\mathrm{sqz}_1} - \delta X^{-}_{\mathrm{sqz}_2}\right) - \frac{3}{\sqrt{2}}\left(\delta X^{+}_{\mathrm{sqz}_1} + \delta X^{+}_{\mathrm{sqz}_2}\right) + \sqrt{2}\left(\delta X^{+}_{m} + \delta X^{+}_{\psi}\right)\right) + \sqrt{1-\eta}\delta X^{+}_{d}\right] \tag{14}$$

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

$$\begin{aligned} \delta X^{+}_{\mathrm{out}} &= \left(\frac{1}{\sqrt{3}} + \frac{G}{\sqrt{6}}\right)\delta X^{+}_{\psi} + \left(\frac{G}{2\sqrt{6}} - \frac{1}{\sqrt{3}}\right)\left(\delta X^{-}_{\mathrm{sqz}_1} - \delta X^{-}_{\mathrm{sqz}_2}\right) \\ &\quad - \frac{G}{2}\sqrt{\frac{3}{2}}\left(\delta X^{+}_{\mathrm{sqz}_1} + \delta X^{+}_{\mathrm{sqz}_2}\right) + G\sqrt{\frac{1-\eta}{\eta}}\delta X^{+}_{d} + \left(\frac{2}{\sqrt{3}} - \frac{G}{\sqrt{6}}\right)\delta X^{+}_{m} \end{aligned} \tag{15}$$

$$\delta X^{-}_{\mathrm{out}} = \sqrt{\frac{1}{3}}\delta X^{-}_{\psi} + \sqrt{\frac{1}{3}}\left(\delta X^{+}_{\mathrm{sqz}_1} - \delta X^{+}_{\mathrm{sqz}_2}\right) \tag{16}$$

where $G = \eta K(\omega)\langle X^{+}_{c}\rangle$ is the total gain of the feedforward loop. By setting $G = 2\sqrt{2}$, it is clear that the anti-squeezing and classical noise terms of Eq. (15) are cancelled. In the limit of perfect detection efficiency and large squeezing, we obtain

$$\delta X^{+}_{\mathrm{out}} = \sqrt{3}\ \ \delta X^{+}_{\psi} \tag{17}$$

$$\delta X^{-}_{\mathrm{out}} = \tfrac{1}{\sqrt{3}}\ \ \delta X^{-}_{\psi} \tag{18}$$

Hence $\{2,3\}$ can reproduce a symplectically transformed version of the secret, $\hat{a}_{\psi}$. We point out, however, that no quantum information contained in the secret state is lost. For example, entanglement swapping using a QSS scheme. In this case since entanglement is invariant to local unitary operations the entanglement will be preserved. To reconstruct the original form of the quantum state, $\{2,3\}$ can perform a local squeezing operation on the output using a phase sensitive amplifier.

3. CHARACTERIZATION

3.1. Fidelity

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.[8] Fidelity can also be adopted to characterize QSS as it is a protocol that reconstructs input quantum states at a distance. If we assume that all input noise sources are Gaussian and that the secret is a coherent state, the fidelity of a QSS scheme is given by[9]

$$\mathcal{F} = \frac{2e^{-(k^{+}+k^{-})}}{\sqrt{(1+V^{+}_{\mathrm{out}})(1+V^{-}_{\mathrm{out}})}} \tag{19}$$

where $k^{\pm} = \langle X_{\psi}^{\pm}\rangle^2(1-\langle X_{\psi}^{\pm}\rangle/\langle X_{\rm out}^{\pm}\rangle)^2/[4(1+V_{\rm out}^{\pm})]$. Assuming an ideal detector ($\eta = 1$), we obtain from the analysis of Section 2.3 the theoretical limits of fidelity for the (2,3) threshold quantum secret sharing scheme as a function of squeezing

$$\mathcal{F}_{\{1,2\}} = \quad 1 \tag{20}$$

$$\mathcal{F}_{\{1,3\}} = \quad \mathcal{F}_{\{2,3\}} = \quad e^{-\Gamma}\sqrt{\frac{3}{(2+e^{-2r})\,(2+3e^{-2r})}} \tag{21}$$

where the subscripts i and j in $\mathcal{F}_{\{i,j\}}$ denote the collaborating players, and Γ is dependent on the amplitude components of the amplitude and phase quadratures of the secret, $\langle X_{\psi}^{\pm}\rangle$, and the squeezing of the input states r, and is given by

$$\Gamma = \frac{2-\sqrt{3}}{12}\left[\langle X_{\psi}^{+}\rangle^2\frac{1}{(2+3e^{-2r})} + \langle X_{\psi}^{-}\rangle^2\frac{9}{(2+e^{-2r})}\right] \tag{22}$$

We note that $\mathcal{F}_{\{1,2\}}$ is always unity since the reconstruction of the secret only requires a simple Mach-Zehnder. Equation (21) does not tend to unity even in the limit of infinite input squeezing ($r \to \infty$). In fact, it quickly degrades to zero for finite squeezing and large secret sideband modulations. The reason for this is due to the symplectically transformed secret output state $\hat{a}_{\rm out}$. To measure the state reconstruction we infer a local transformation on the output state described by the equation $\delta X_{\psi_{\rm infer}}^{\pm} = (\sqrt{3})^{\mp 1}\delta X_{\psi_{\rm out}}^{\pm}$. The fidelity given in Eq. (21) after the inferred transformation then becomes equal to

$$\mathcal{F}_{\{1,3\}}^{\rm infer} = \mathcal{F}_{\{2,3\}}^{\rm infer} = \frac{1}{1+e^{-2r}} \tag{23}$$

3.2. T-V graph

An alternative measure that is invariant to symplectic transformations is the T-V graph proposed by Ralph and Lam, [10] used to characterize quantum teleportation.[9] 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

$$V_{cv}^{\pm} = V_{\rm out}^{\pm} + \frac{|\langle \delta X_{\psi}^{\pm}\delta X_{\rm out}^{\pm}\rangle|^2}{V_{\psi}^{\pm}} \tag{24}$$

and the signal transfer coefficients are defined as

$$T^{\pm} = \frac{SNR_{\rm out}^{\pm}}{SNR_{\psi}^{\pm}} \tag{25}$$

In contrast to fidelity which measures the quality of the state reconstruction, the T-V graph emphasizes the transfer of quantum information.[9] In an ideal QSS scheme, collaborating players would obtain $T_q = 2$ and $V_q = 0$. Using these measures the collaborating players, which we will now denote as (CP), can obtain

$$T_q^{\rm CP} = \frac{1}{1+2e^{-2r}} + \frac{(1+\frac{G}{\sqrt{2}})^2}{\left(1+\frac{G}{\sqrt{2}}\right)^2 + \left(\frac{G}{2}-\sqrt{2}\right)^2 e^{2r} + \left(\frac{3G}{2}\right)^2 e^{-2r} + \left(2-\frac{G}{\sqrt{2}}\right)^2 e^{2s} + \frac{3G^2(1-\eta)}{\eta}} \tag{26}$$

$$V_q^{\rm CP} = \frac{e^{-2r}}{18}\left[9G^2e^{-2r} + e^{2r}(G-2\sqrt{2})^2 + 2e^{2s}(G-2\sqrt{2})^2 + 12G^2\left(\frac{1-\eta}{\eta}\right)\right] \tag{27}$$

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

$$T_q^{\rm SP} = \frac{2}{1+\cosh 2r + e^{2s}} \tag{28}$$

$$V_q^{\rm SP} = \frac{(\cosh 2r + e^{2s})^2}{4} \tag{29}$$

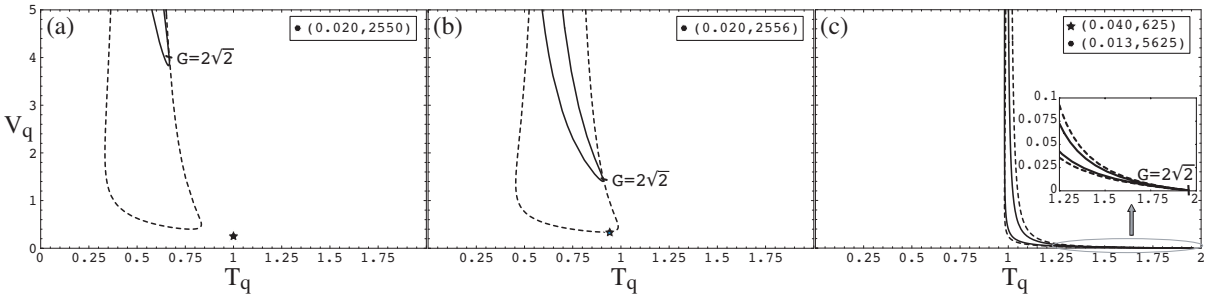

Figure 3. T-V graphs for the feedforward scheme with (a) no squeezing, (b) 40% of squeezing, and (c) 99% of squeezing. The lines represent the information retrieved by $\{2,3\}$ with varying feedforward gain, and the points represent the information retrieved by $\{1\}$ or $\{2\}$ alone. The dashed lines and stars correspond to the absence of added modulations, whilst the solid lines and circles correspond to 20dB above the quantum noise of added modulations. We have assumed perfect detector efficiency for the feedforward loop. The coordinates of the points which are not outside of the plotted region are displayed in the inset of each graph.

Figure 3 shows the results of the feedforward QSS scheme for three different amounts of input squeezing. The dotted lines represent the results obtained by $\{2,3\}$ in the absence of added classical 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 classical noise, 20 dB above the quantum noise limit, are depicted by solid lines for the collaborating players and by circles for the single players. In the limit of infinite input squeezing, the collaborating players can reconstruct the secret perfectly, with $T_q^{\rm CP} \rightarrow 2$ and $V_q^{\rm CP} \rightarrow 0$. 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 classical noise) are completely cancelled. Single players in the same limit obtain no information about the secret, with $T_q^{\rm SP} \rightarrow 0$ and $V_q^{\rm SP} \rightarrow \infty$, due to the dominant effect of the anti-squeezing quadratures (and the added classical noise). These results are shown in the plots of Fig. 3(c). In the case of finite squeezing and no added classical noise, however, the optimum feedforward gain for the collaborating players is always less than $2\sqrt{2}$ as shown in both Fig. 3(a) and (b). Further, single players forming the adversary structures can obtain some quantum information about the secret. When the amount of input squeezing is less than 42%, single players obtain more quantum information than the access structures using the feedforward protocol. In this situation, the collaborating players should directly measure their shares containing the secret. The classical limit obtained when there is no input squeezing and no added classical noise is then $T_q^{\rm SP} = T_q^{\rm CP} = 1$ and $V_q^{\rm SP} = V_q^{\rm CP} = 1/4$, as shown by the star point of Fig. 3(a).

In order to prevent the single players from obtaining information about the secret, the dealer can 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 single players obtain virtually no information about the secret, thus making $T_q^{\rm SP} \rightarrow 0$ and $V_q^{\rm SP} \rightarrow \infty$ even in the absence of input squeezing. Collaborating players on the other hand, obtain a zero squeezing classical limit of $T_q^{\rm CP} \rightarrow 2/3$ and $V_q^{\rm CP} \rightarrow 4$.

Another consequence of the added classical noise for the collaborating players is that the optimum gain for maximum information transfer again approaches $2\sqrt{2}$. This results in the collaborating players obtaining less information about the secret with increasing classical noise. Nonetheless, the collaborating players can now obtain much more information than the single players 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 lines and the circles of Fig. 3.

4. CONCLUSION

In this paper, we presented a (2,3) threshold QSS scheme utilizing a pair of optically entangled beams and an additional electro-optic feedforward loop. We have shown that the reconstructed secret state is a sympletic transform of the original quantum state, however, all quantum information is retained in the reconstructed output state in the limit of perfect entanglement. We show that by introducing controlled classical modulations on the entangled beams, it is possible to insure

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 classical noise. To date we have experimentally demonstrated (2,3) threshold

		(T_q, V_q)				$\mathcal{F}^{\text{infer}}$			
		clas,$\bar{n}$	clas,n	quan,$\bar{n}$	quan,n	clas,$\bar{n}$	clas,n	quan,$\bar{n}$	quan,n
Adversary Structure	1	(1,1/4)	(0,∞)	(0,∞)	(0,∞)	1/2	0	0	0
	2	(1,1/4)	(0,∞)	(0,∞)	(0,∞)	1/2	0	0	0
	3	(0,1)	(0,∞)	(0,∞)	(0,∞)	0	0	0	0
Access Structure	{1,2}	(2,0)	(2,0)	(2,0)	(2,0)	1	1	1	1
	{1,3}	(1,1/4)	(2/3,4)	(2,0)	(2,0)	1/2	1/2	1	1
	{2,3}	(1,1/4)	(2/3,4)	(2,0)	(2,0)	1/2	1/2	1	1

Table 1. Summary of the performances of the feedforward QSS schemes with (quan) and without (clas) optical entanglement; and with (n) and without added noise ($\bar{n}$). Parameters listed are the best achievable (T_q, V_q) values, and inferred fidelity values.

QSS, the results of which will appear in a future publication.[11] This research is supported by the Australian Research Council. We thank Ben Buchler and Stephen Bartlett for useful discussions.

REFERENCES

1. A. Shamir, Comm. of the ACM **22**, 612 (1979).
2. M. Hillery et al, Phys. Rev. A **59**, 1829 (1999).
3. W. Tittel, H. Zbinden and N. Gisin, Phys. Rev. A **63**, 042301 (2001).
4. R. Cleve et al, Phys. Rev. Lett. **83**, 648 (1999).
5. T. Tyc, and B. C. Sanders, Phys. Rev. A **65**, 42310 (2002).
6. T. Tyc,D. J. Rowe, and B. C. Sanders, J. Phys. A:Math. Gen. **36**, 7625 (2003).
7. A. M. Lance, T. Symul, W. P. Bowen, T. Tyc, B. C. Sanders and P. K. Lam, New J. of Phys. **5**, 4.1 (2003).
8. A. Furusawa *et al.*, Science **282**, 706 (1998).
9. W. P. Bowen, N. Treps, B. C. Buchler, R. Schnabel, T. C. Ralph, H-A. Bachor, T. Symul and P. K. Lam, quant-ph/0207179.
10. T. C. Ralph, P. K. Lam and R. E. S. Polkinghorne, J. Opt. B **1**, 483 (1999).
11. A. M. Lance, T. Symul, W. P. Bowen, B. C. Sanders and P. K. Lam, *to be published.*