Efficient sharing of a continuous-variable quantum secret

2003 J. Phys. A: Math. Gen. 36 7625

(http://iopscience.iop.org/0305-4470/36/27/314)

INSTITUTE OF PHYSICS PUBLISHING JOURNAL OF PHYSICS A: MATHEMATICAL AND GENERAL

J. Phys. A: Math. Gen. **36** (2003) 7625–7637 PII: S0305-4470(03)58372-X

Efficient sharing of a continuous-variable quantum secret

Tomáš Tyc[1,2], David J Rowe[1,3] and Barry C Sanders[1]

[1] Department of Physics and Centre for Advanced Computing—Algorithms and Cryptography, Macquarie University, Sydney, NSW 2109, Australia
[2] Institute of Theoretical Physics, Masaryk University, Kotlářská 2, 61137 Brno, Czech Republic
[3] Department of Physics, University of Toronto, Toronto, Ontario, M5S 1A7, Canada

Received 15 January 2003, in final form 7 May 2003
Published 25 June 2003
Online at stacks.iop.org/JPhysA/36/7625

Abstract

We propose an efficient scheme for sharing a continuous-variable quantum secret using passive optical interferometry and squeezers: this efficiency is achieved by showing that a maximum of two squeezers is required to extract the secret state, and we obtain the cheapest configuration in terms of total squeezing cost. Squeezing is a cost for the dealer of the secret as well as for the receivers, and we quantify limitations to the fidelity of the extracted secret state in terms of the squeezing employed by the dealer.

PACS numbers: 03.67.−a, 03.67.Dd, 42.50.Dv

1. Introduction

Secret sharing (SS) is an important cryptosystem protocol for dealing secret information to a set of players, not all of whom can be trusted [1]. The encoded secret can only be extracted (or, equivalently, reconstructed[4]) if certain subsets of players collaborate, and these subsets are referred to as the access structure. The remaining subsets comprise the adversary structure, and the protocol denies the adversary structure any information about the secret. The underpinning scheme for arbitrary SS is (k, n)-threshold SS, which involves n players, and any subset of k players constitutes a valid set in the access structure; other SS schemes can be constructed via threshold SS, for example by distributing an unequal number of shares to players. Although quantum secret sharing (QSS) was first introduced as a method of transmitting classical information in a hostile environment with quantum-enhanced security [3], QSS was subsequently established [4] as a quantum analogue to Shamir's secret sharing described above and we use the term QSS to refer to the latter approach. QSS provides a valuable protocol in quantum communication but is also important as an error correction scheme [4].

[4] We use the term 'extraction' of the secret state as the term 'reconstruction' is used in optical homodyne tomography to refer to the process of inferring the wavefunction by subjecting many identical copies of the state to a battery of measurements; see for example [2].

Here we are concerned with continuous-variable (CV) QSS [5]. Quantum information protocols and tasks are now studied both as discrete-variable, qubit-based (or qudit-based) protocols and tasks [6] and as CV realizations [7]. CV quantum information protocols are generally realized in optical systems and exploit advanced quantum optics tools, such as the generation of squeezed light [8] and ability to count single photons [9, 10], as well as the low rate of decoherence for optical systems. The recent demonstration of CV unconditional quantum teleportation [11] is an excellent example of the capabilities of CV quantum information processes in optical systems. Moreover, the technology for this CV quantum teleportation is not very different from the techniques required for CV QSS.

The original proposal for CV QSS [5] established a general method for CV QSS, and for (k, n)-threshold schemes in particular, using interferometry involving passive optical elements (mirrors, beam splitters and phase shifters), active elements (squeezers) and homodyne detectors. A $(2, 3)$-threshold scheme was proposed involving a single squeezer, thereby suggesting an experiment that is within the reach of current technology [12]. The original proposal of how to perform the general (k, n) scheme was complicated, though, by the need for an increasing number of squeezers in the interferometer. A practical realization of threshold-QSS would need to minimize the number of optical squeezers as the number of players increases.

Here we establish that, for any number n of players and any threshold level k for the number of collaborators to be in the access structure, the total number of squeezers needed by the collaborating players does not exceed two. This remarkable result informs us that at most two squeezers are required for an arbitrary number of players n. In particular, to extract the secret state, the collaborating players require access to an interferometer with k channels but only two active components (i.e., squeezers). This analysis also allows us to determine the total amount of squeezing required in a two-squeezer threshold QSS protocol: the analysis is important because the degree of squeezing required for the protocol can be regarded as an effective cost for the procedure [13].

The second major concern of this paper is the extent to which it is possible to achieve the goals of the CV QSS protocol with finite physical resources. For the protocol to work perfectly, the dealer needs access to ancillary states prepared with infinite squeezing; as this is not physically possible, we analyse the effects of finite squeezing, which imposes limitations on the fidelity of the extracted secret state.

The paper is organized as follows: in section 2 we summarize the CV QSS protocol for threshold schemes. In section 3, we describe an efficient extraction of the secret state, which requires the minimal number of squeezing elements and minimal overall squeezing. The total amount of squeezing is discussed in section 4 and we conclude in section 5.

2. Threshold QSS with finite resources

The optical (k, n)-threshold scheme is sketched in figure 1. A dealer holds a pure secret state $|\psi\rangle$ realized in a single mode of the electromagnetic field and encodes the secret as an n-mode entangled state $|\Psi\rangle$ by mixing it with $n-1$ ancillary states in an n-channel active interferometer, where the term active refers to one- or two-mode squeezers [14]. The dealer then sends one output, or 'share', to each of the players, and at least k players must combine their shares in an active interferometer to extract the secret state. However, the no-cloning theorem [15] requires that no threshold scheme exists for $n \geqslant 2k$ [4]. Also any threshold scheme with $n < 2k-1$ can be obtained from the $(k, 2k-1)$ scheme by discarding $2k-1-n$ shares. Therefore, we concentrate on the $(k, 2k-1)$-threshold scheme.

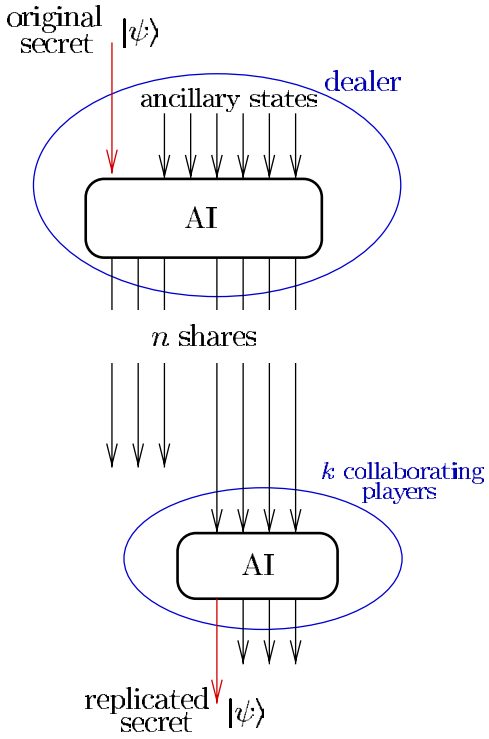

Figure 1. The optical ($k = 4, n = 7$) QSS threshold scheme: the dealer encodes the secret via an interferometer (AI) by mixing it with $n - 1$ ancillary states, transmits the resulting n shares to the players and any k players employ a second interferometer to extract the secret state. The interferometers are active, meaning that they employ both passive optical devices and energy-consuming squeezers.

2.1. Entanglement of the secret state

The secret is a state $|\psi\rangle \in \mathbb{H}^{(1)} \sim \mathcal{L}^2(\mathbb{R})$ with wavefunction $\psi(x) = \langle x|\psi\rangle$. Let $\mathbb{H}^{(n)}$ be the tensor product of $n = 2k - 1$ copies of $\mathbb{H}^{(1)}$, one copy of which is owned by each player.

The basic idea is that the dealer hides the secret wavefunction by entangling it with $k - 1$ very broad Gaussians (of width so large that they are effectively constant over the range in which the secret state is nonzero) and $k - 1$ very narrow Gaussians (of width so narrow that the secret state is effectively constant over a range of its coordinate for which the latter Gaussians are nonzero). To the extent that the required limits are achieved, we will show that the component of the wavefunction that is accessible to every k-dimensional subspace of the full n-dimensional Hilbert space contains full information about the secret state.

The Hilbert space $\mathbb{H}^{(n)}$ is the space $\mathcal{L}^2(\mathbb{R}^n)$ of square integrable wavefunctions on $\mathbb{R}^n$. Thus, if $\mathbb{F}^n$ denotes a real linear space of coordinate functions for $\mathbb{R}^n$, then choosing a system of Euclidean coordinates $(x_1, \ldots, x_n)$ for any vector $\mathbf{x} \in \mathbb{R}^n$ is equivalent to picking an orthonormal basis $(f_1, \ldots, f_n)$ for $\mathbb{F}^n$ such that

$$f_i(\mathbf{x}) = x_i. \tag{1}$$

We denote the inner product of these coordinate functions by $f_i \cdot f_j = \delta_{ij}$.

Suppose the dealer starts with an unentangled tensor product

$$|\Psi\rangle = |\psi\rangle \otimes \underbrace{|\varphi_a\rangle \otimes \cdots \otimes |\varphi_a\rangle}_{k-1} \otimes \underbrace{|\varphi_{1/a}\rangle \otimes \cdots \otimes |\varphi_{1/a}\rangle}_{k-1} \tag{2}$$

of the secret state $|\psi\rangle$, with $k-1$ copies of a state $|\varphi_a\rangle$ and $k-1$ copies of a state $|\varphi_{1/a}\rangle$, where

$$\varphi_a(x) = \langle x|\varphi_a\rangle = (\pi a^2)^{-1/4}\, \mathrm{e}^{-x^2/2a^2}. \tag{3}$$

Write this state

$$|\Psi\rangle = \int \mathrm{d}x^n \Psi(\mathbf{x})|x_1\rangle \otimes \cdots \otimes |x_n\rangle = \int \mathrm{d}x^n \Psi(\mathbf{x})|f_1(\mathbf{x})\rangle \otimes \cdots \otimes |f_n(\mathbf{x})\rangle \tag{4}$$

where

$$\Psi(\mathbf{x}) = \psi(x_1) \prod_{i=2}^{k} \varphi_a(x_i) \prod_{i=k+1}^{n} \varphi_{1/a}(x_i). \tag{5}$$

The dealer then entangles the secret state by a linear canonical point transformation

$$f_i \to g_i = \sum_j g_{ij} f_j \tag{6}$$

in which the orthogonal (Euclidean) coordinate functions $\{f_i\}$ are replaced by a general linear system $\{g_i\}$ for which $g_i(\mathbf{x}) = \sum_j g_{ij} f_j(\mathbf{x}) = \sum_j g_{ij} x_j$. The corresponding unitary transformation of $\mathbb{H}^{(n)}$ then maps the state $|\Psi\rangle$ to

$$|\Psi_g\rangle = |\det g|^{1/2} \int \mathrm{d}x^n \Psi(\mathbf{x})|g_1(\mathbf{x})\rangle \otimes \cdots \otimes |g_n(\mathbf{x})\rangle. \tag{7}$$

To understand the entanglement procedure and the options available to the dealer, it is useful to think geometrically in terms of vectors in the n-dimensional vector space $\mathbb{F}^n$. First observe that the process of entanglement, in which the state $|\Psi\rangle$ is mapped to a state $|\Psi_g\rangle$, is equivalent to expressing the wavefunction Ψ for the state $|\Psi\rangle$ in terms of new coordinates that are linearly related to the original set. In geometrical terms, this corresponds to a linear transformation from the orthonormal basis $\{f_i\}$ for the vector space $\mathbb{F}^n$ to a new basis $\{g_i\}$ defined by a general linear $n \times n$ matrix (g_{ij}). One may suppose that each of the n players is assigned one of the basis vectors $\{g_i\}$. However, the choice of the vectors $\{g_i\}$ is not arbitrary; it must be such that any k players are able to disentangle the secret state but that any lesser number is unable to do so. We shall show that, by choosing the parameter a to be sufficiently large, only the orthogonal projection ζ_i of each vector g_i onto the subspace of $\mathbb{F}^n$ spanned by the vectors $\{f_1, f_2, \ldots, f_k\}$, is important. A set of vectors $\{g_i\}$ must then be chosen which satisfy the following two conditions: (i) every subset of k vectors in the set $\{\zeta_i\}$ is linearly independent, and (ii) the vector f_1 is not a linear combination of any set of less than k of these vectors. As we will see, these conditions guarantee any k players to be able to extract the quantum secret. At the same time, cloning of the quantum secret is not possible [15], which implies that any $k-1$ or less players cannot extract the secret. The two conditions (i) and (ii) can be expressed succinctly as a requirement that any k vectors from the set $\{f_1, \zeta_1, \zeta_2, \ldots, \zeta_n\}$ are linearly independent, which is always possible to achieve [4]. Otherwise the choice of $\{g_i\}$ by the dealer is arbitrary.

2.2. The extraction algorithm

In extracting the secret state, it is convenient to identify three subspaces of coordinates; i.e., express $\mathbb{F}^n$ as a direct sum of three mutually orthogonal subspaces

$$\mathbb{F}^n = \mathbb{X} \oplus \mathbb{Y} \oplus \mathbb{Z} \tag{8}$$

where $\mathbb{X}$ is the one-dimensional space spanned by f_1, and $\mathbb{Y}$ and $\mathbb{Z}$ are the $(k-1)$-dimensional spaces spanned, respectively, by $\{f_2, \ldots, f_k\}$ and $\{f_{k+1}, \ldots, f_n\}$. Thus, we relabel the $\{x_i\}$ coordinates as (x, y_i, z_i) coordinates with

$$x = x_1 \qquad y_i = x_{i+1} \qquad z_i = x_{k+i} \qquad i = 1, \ldots, k-1. \tag{9}$$

The wavefunction Ψ is then

$$\Psi(\mathbf{x}) = \psi(x) \prod_{i=1}^{k-1} \varphi_a(y_i)\varphi_{1/a}(z_i). \tag{10}$$

It will be understood in the following that all n players know the encoding transformation in which $f_i \to g_i$. Without loss of generality, we may suppose that the first k players form the collaborating set. These players are able to make any transformation of the states in the subset of Hilbert spaces accessible to them. However, we will restrict the transformations they can make to those corresponding to general linear coordinate transformations, as defined above. Let us suppose they make the transformation

$$g_i \to \xi_i = \sum_j \xi_{ij} f_j \tag{11}$$

with the understanding that $\xi_i = g_i$ for all $i > k$.

The orthogonal decomposition of $\mathbb{F}^n$ given by equation (8) now defines a corresponding decomposition of every ξ_i vector as a sum of three mutually orthogonal vectors

$$\xi_i = \alpha_i + \beta_i + \gamma_i. \tag{12}$$

Equivalently, we can write

$$\xi_i(\mathbf{x}) = \alpha_i x + \sum_j \beta_{ij} y_j + \sum_j \gamma_{ij} z_j. \tag{13}$$

Provided the vectors $\{g_i\}$ are chosen such that any k vectors from the set $\{f_1, \zeta_1, \zeta_2, \ldots, \zeta_n\}$ are linearly independent, where ζ_i is the orthogonal projection of g_i onto the subspace $\mathbb{X} \oplus \mathbb{Y} \subset \mathbb{F}^n$, it is possible for the collaborating players to design the transformation $g_i \to \xi_i$ such that

$$\alpha_1 = 1 \qquad \beta_1 = 0 \qquad \alpha_{i+1} = \alpha_{k+i} \qquad \beta_{i+1} = \beta_{k+i} \qquad i = 1, \ldots, k-1 \tag{14}$$

(recall that $\xi_i = g_i$ for $i > k$). We then claim that such a transformation extracts the secret for sufficiently large values of the parameter a. We demonstrate this result explicitly for the simple case in which $k = 2$ and $n = 3$.

For the $k = 2, n = 3$ case (ξ_1, ξ_2, ξ_3) will have expansions of the form

$$\xi_1(\mathbf{x}) = x + \gamma_1 z \tag{15}$$

$$\xi_2(\mathbf{x}) = \alpha x + \beta y + \gamma_2 z \tag{16}$$

$$\xi_3(\mathbf{x}) = \alpha x + \beta y + \gamma_3 z \tag{17}$$

and $|\Psi_\xi\rangle$ will be given by

$$|\Psi_\xi\rangle = \frac{|\beta(\gamma_2 - \gamma_3)|^{1/2}}{\pi^{1/2}} \int \psi(x) \exp\left[-\frac{1}{2a^2}y^2 - \frac{a^2}{2}z^2\right] \times |x + \gamma_1 z\rangle \otimes |\alpha x + \beta y + \gamma_2 z\rangle \otimes |\alpha x + \beta y + \gamma_3 z\rangle \, \mathrm{d}x \, \mathrm{d}y \, \mathrm{d}z. \tag{18}$$

By a change of the variable x to $x - \gamma_1 z$, we then have

$$|\Psi_\xi\rangle = \frac{|\beta(\gamma_2 - \gamma_3)|^{1/2}}{\pi^{1/2}} \int \psi(x - \gamma_1 z) \exp\left[-\frac{1}{2a^2}y^2 - \frac{a^2}{2}z^2\right] \times |x\rangle \otimes |\alpha x + \beta y + \gamma_2' z\rangle \otimes |\alpha x + \beta y + \gamma_3' z\rangle \, \mathrm{d}x \, \mathrm{d}y \, \mathrm{d}z. \tag{19}$$

Now observe that if a is sufficiently large that $\psi(x-\gamma_1 z)\approx\psi(x)$ for all values of z for which $\exp[-a^2z^2/2]$ is non-negligible, then

$$\psi(x-\gamma_1 z)\exp\left[-\frac{a^2}{2}z^2\right]\approx\psi(x)\exp\left[-\frac{a^2}{2}z^2\right]. \tag{20}$$

Moreover, this approximation becomes precise to any desired level of accuracy for sufficiently large values of a. By a second change of variables,

$$x\to x \qquad \beta y\to\beta y-\alpha x \tag{21}$$

we also have

$$|\Psi_\xi\rangle=\frac{|\beta(\gamma_2-\gamma_3)|^{1/2}}{\pi^{1/2}}\int\psi(x)\exp\left[-\frac{1}{2a^2}\left(y-\frac{\alpha}{\beta}x\right)^2-\frac{a^2}{2}z^2\right]$$
$$\times|x\rangle\otimes|\beta y+\gamma_2' z\rangle\otimes|\beta y+\gamma_3' z\rangle\,\mathrm{d}x\,\mathrm{d}y\,\mathrm{d}z. \tag{22}$$

Now for every secret $\psi(x)$ decaying fast enough for $|x|\to\infty$, the parameter a can be chosen to be sufficiently large so that $\exp\left[-\frac{1}{2a^2}\left(y-\frac{\alpha}{\beta}x\right)^2\right]\approx\exp\left[-\frac{1}{2a^2}y^2\right]$ for all values of x for which $\psi(x)$ is non-negligible. Then we have

$$|\Psi_\xi\rangle\approx\frac{|\beta(\gamma_2-\gamma_3)|^{1/2}}{\pi^{1/2}}\int\psi(x)\exp\left[-\frac{1}{2a^2}y^2-\frac{a^2}{2}z^2\right]|x\rangle\otimes|\beta y+\gamma_2' z\rangle\otimes|\beta y+\gamma_3' z\rangle\,\mathrm{d}x\,\mathrm{d}y\,\mathrm{d}z$$
$$=|\psi\rangle\otimes|\Phi\rangle \tag{23}$$

where $|\Phi\rangle$ is the entangled state

$$|\Phi\rangle=\frac{|\beta(\gamma_2-\gamma_3)|^{1/2}}{\pi^{1/2}}\int\exp\left[-\frac{1}{2a^2}y^2-\frac{a^2}{2}z^2\right]|\beta y+\gamma_2' z\rangle\otimes|\beta y+\gamma_3' z\rangle\,\mathrm{d}y\,\mathrm{d}z. \tag{24}$$

The generalization of the proof to larger values of k is straightforward.

2.3. Fidelity of the secret sharing scheme

As we have seen, the CV QSS scheme works perfectly only for $a\to\infty$ in equation (3). In this case the dealer has infinitely squeezed ancillary states with which to entangle the secret state $|\psi\rangle$. The situation is similar to CV quantum teleportation [16], where an ideal EPR pair (which is a two-mode infinitely squeezed vacuum) is required for the protocol to work perfectly. However, with some loss of fidelity the scheme can be adapted to a realistic, finite-squeezing situation [17]. In CV QSS, finite squeezing implies that the secret state can only be approximately extracted because there is entanglement between the secret state and the shares in both the access structure and the adversary structure, which limits the fidelity of the extracted state with respect to the original secret state. Also entanglement with the adversarial shares allows some information about the secret state to escape. These compromises to CV QSS are reduced by increasing the degree of squeezing.

A detailed analysis reveals that the reduced density operator $\hat\rho'$ of the extracted secret is related to the original density operator $\hat\rho=|\psi\rangle\langle\psi|$ by

$$\rho'(x,x')\equiv\langle x|\hat\rho'|x'\rangle=\frac{a}{\sqrt{\pi}v}\exp\left[-\frac{u^2(x-x')^2}{4a^2}\right]\int_{\mathbb{R}}\rho(x-y,x'-y)\exp\left[-\frac{a^2y^2}{v^2}\right]\mathrm{d}y \tag{25}$$

(see the appendix for the proof). Here v is the norm of the vector γ_1 in equation (12) and $u^2=\sum_{i=1}^{k-1}u_i^2$, where $\{u_i\}$ are the coefficients of the expansion $\alpha_j=\sum_{i=1}^{k-1}u_i\beta_{ji}$, $j=2,\ldots,k$. The parameters u and v quantify the degree to which the secret state has been degraded for

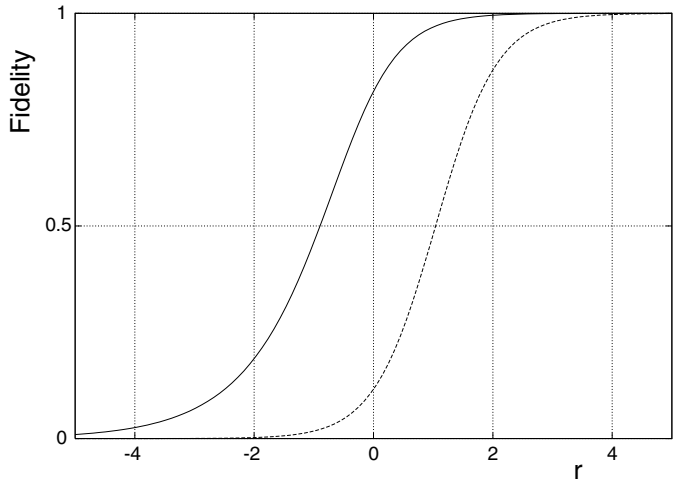

Figure 2. The fidelity $\mathcal{F}$ versus the squeezing parameter $r = \ln a$ for an arbitrary coherent state as the secret. Two cases are presented: (1) $u = 0.5$ and $v = 1$ (solid line) and (2) $u = 3$ and $v = 5$ (dashed line).

a given a by encoding and decoding. The degradation is symmetric under the exchange of $u \leftrightarrow v$. Perfect extraction corresponds to $u = 0$ and $v = 0$, which is in general unachievable for all authorized groups of players. The reason is that the dealer controls n^2 parameters by the encoding process (the coordinates g_{ij} of the vectors g_i), which are insufficient to satisfy the conditions $u = 0$, $v = 0$ for all $n!/k!(k-1)!$ groups of k players.

The *extraction fidelity* of the system can be characterized by evaluating $\mathcal{F} = \langle\psi|\hat{\rho}'|\psi\rangle$ for some standard secret state $|\psi\rangle$. For an arbitrary coherent state as the secret, the fidelity is given by the function

$$\mathcal{F} = [1 + (u^2 + v^2)/2a^2 + u^2v^2/4a^4]^{-1/2}. \tag{26}$$

The dependence of $\mathcal{F}$ on $r = \ln a$ for some particular values of u and v can be seen in figure 2. The fidelity tends to unity for large squeezing ($a \to \infty, r \to \infty$) and to zero for large antisqueezing ($a \to 0, r \to -\infty$). The fidelity for $r = 0$ corresponds to the case when the ancillary states are all vacuum states.

An interesting challenge is to determine the encoding procedure that would maximize the average fidelity for any access group for a given value of r.

3. Efficient extraction

In the previous section we have established an extraction protocol for the access structure; here we seek the most efficient protocol, which minimizes the total number of squeezers (expensive components in an active interferometer) required. In the following we show that by a suitable choice of a particular disentangling transformation, it is possible to reduce the total number of squeezers required in the extraction to not more than two.

Let $\xi_i \to \zeta_i$ denote the orthogonal projection of $\xi_i \in \mathbb{F}^n$ to the subspace $\mathbb{X} \oplus \mathbb{Y} \subset \mathbb{F}^n$ so that

$$\xi_i(\mathbf{x}) = \zeta_i(\mathbf{x}) + \sum_j \gamma_{ij} z_j \qquad \zeta_i(\mathbf{x}) = \alpha_i x + \sum_j \beta_{ij} y_j. \tag{27}$$

Claim. A transformation $g_i \to \xi_i = \alpha_i + \beta_i + \gamma_i$, with $\alpha_i \in \mathbb{X}$, $\beta_i \in \mathbb{Y}$ and $\gamma_i \in \mathbb{Z}$, which leaves the coordinates $\xi_i = g_i$ unchanged for $i = k+1, \ldots, n$ and is such that

$$\alpha_1 = 1 \qquad \beta_1 = 0 \qquad \operatorname{span}(\zeta_2, \ldots, \zeta_k) = \operatorname{span}(\zeta_{k+1}, \ldots, \zeta_n) \tag{28}$$

disentangles the secret state for sufficiently large values of the parameter a.

To prove this claim, we show, by a change of variables that, for sufficiently large values of a, the state

$$|\Psi_\xi\rangle = |\det \xi|^{1/2} \int \mathrm{d}x\, \psi(x) \prod_{i=2}^{k} \frac{1}{(\pi)^{1/2}} \int \mathrm{d}y_i\, \mathrm{d}z_i \exp\left[-\frac{1}{2a^2} y_i^2 - \frac{a^2}{2} z_i^2\right] \times |x + \gamma_1(\mathbf{x})\rangle \otimes |\zeta_2(\mathbf{x}) + \gamma_2(\mathbf{x})\rangle \otimes \cdots \otimes |\zeta_n(\mathbf{x}) + \gamma_n(\mathbf{x})\rangle \tag{29}$$

defined by the transformation $g_i \to \xi_i$, is expressible in the form

$$|\Psi_\xi\rangle = |\psi\rangle \otimes |\Phi\rangle \tag{30}$$

with

$$|\Phi\rangle = |\det \xi|^{1/2} \prod_{i=2}^{k} \frac{1}{(\pi)^{1/2}} \int \mathrm{d}y_i\, \mathrm{d}z_i \exp\left[-\frac{1}{2a^2} y_i^2 - \frac{a^2}{2} z_i^2\right] \times |\beta_2(\mathbf{x}) + \gamma_2'(\mathbf{x})\rangle \otimes \cdots \otimes |\beta_n(\mathbf{x}) + \gamma_n'(\mathbf{x})\rangle. \tag{31}$$

This result is achieved by first changing the variable x to $x - \sum_j \gamma_{1j} z_j$ and noting that, if a is sufficiently large, then $\psi\big(x - \sum_j \gamma_{1j} z_j\big) \approx \psi(x)$ for all values of $\sum_j \gamma_{1j} z_j$ for which $\exp\big[-\frac{a^2}{2} \sum_i z_i^2\big]$ is non-negligible. This shows that

$$|\Psi_\xi\rangle = |\det \xi|^{1/2} \int \mathrm{d}x\, \psi(x) \prod_{i=2}^{k} \frac{1}{(\pi)^{1/2}} \int \mathrm{d}y_i\, \mathrm{d}z_i \exp\left[-\frac{1}{2a^2} y_i^2 - \frac{a^2}{2} z_i^2\right] \times |x\rangle \otimes |\zeta_2(\mathbf{x}) + \gamma_2'(\mathbf{x})\rangle \otimes \cdots \otimes |\zeta_n(\mathbf{x}) + \gamma_n'(\mathbf{x})\rangle. \tag{32}$$

Next observe that, since the vectors $\{\zeta_{k+1}, \ldots, \zeta_n\}$ are linear combinations of the vectors $\{\zeta_2, \ldots, \zeta_k\}$, the change of variables given by the projection $\zeta_i = \alpha_i + \beta_i \to \beta_i$, for $i = 2, \ldots, k$, results in the corresponding projections $\zeta_i \to \beta_i$ for $i = k+1, \ldots, n$. Now, if β^{ij} is defined such that

$$\sum_j \beta^{ij} \beta_{jk} = \delta_{ik} \tag{33}$$

then the projection $\zeta_i \to \beta_i$, for $i = 2, \ldots, k$, corresponds to the coordinate transformation $y_i \to y_i - \big(\sum_j \beta^{ij} \alpha_j\big)x$. Thus, if a is sufficiently large that $\exp\big[-\frac{1}{2a^2}\big(y_i - \big(\sum_j \beta^{ij} \alpha_j\big)x\big)^2\big] \approx \exp\big[-\frac{1}{2a^2} y_i^2\big]$ for all values of x for which $\psi(x)$ is non-negligible, we obtain equation (29).

Now, let the vectors g_i defining the encoded state $|\Psi_g\rangle$ (7) by the linear transformation (6) have decomposition, parallel to that given by equation (27),

$$\begin{aligned} g_i &= \kappa_i + \lambda_i \qquad && i = 1, \ldots, k \\ g_i &= \xi_i = \zeta_i + \gamma_i \qquad && i = k+1, \ldots, n \end{aligned} \tag{34}$$

with $\kappa_i \in \mathbb{X} \oplus \mathbb{Y}$ and $\lambda_i \in \mathbb{Z}$, respectively. And let T denote a transformation

$$g_i \to \xi_i = \sum_{j=1}^{k} T_{ij} g_j \qquad i = 1, \ldots, k \tag{35}$$

such that the vectors

$$\zeta_i = \sum_{j=1}^{k} T_{ij}\kappa_j \qquad i = 1, \ldots, k \tag{36}$$

satisfy the disentanglement criteria (28).

The condition that the vectors $\zeta_2, \ldots, \zeta_k$ span the same subspace of $\mathbb{X} \oplus \mathbb{Y}$ as do $\zeta_{k+1}, \ldots, \zeta_n$ can be satisfied by requiring that both sets are orthogonal to a common vector $v \in \mathbb{X} \oplus \mathbb{Y}$. Thus, if $v \in \mathbb{X} \oplus \mathbb{Y}$ is a vector defined such that

$$v \cdot \zeta_i = 0 \qquad i > k \tag{37}$$

the transformation T is required to satisfy the equation

$$v \cdot \zeta_i = \sum_{j=1}^{k} T_{ij} v \cdot \kappa_j = 0 \qquad \forall i = 2, \ldots, k. \tag{38}$$

To satisfy the first condition of equation (28), T should also be such that

$$\zeta_1 = \sum_{j=1}^{k} T_{1j}\kappa_j = f_1 \tag{39}$$

so that $\zeta_1(\mathbf{x}) = x$.

Equation (39) implies that the first row of the matrix T is the row vector $a = (a_1, a_2, \ldots, a_k)$ whose components are the coefficients in the expansion $f_1 = \sum_{j=1}^{k} a_j\kappa_j$, i.e., $T_{1j} = a_j$. The remaining rows can be defined as a set of orthogonal row vectors $\{T_i; i = 2, \ldots, k\}$, all of which are orthogonal to the unit row vector W_1 whose components are given by

$$W_{1j} = \frac{v \cdot \kappa_j}{\sqrt{\sum_{i=1}^{k} (v \cdot \kappa_i)^2}}. \tag{40}$$

The orthogonality of the vectors $\{T_i; i > 1\}$ to W_1 then ensures that $\sum_{j=1}^{k} T_{ij} W_{1j} = 0$ for $i > 1$ and that condition (38) is satisfied. The norms of the orthogonal vectors $\{T_i; i > 1\}$ are arbitrary and can be chosen to minimize the cost of the transformation. We find (cf section 4) that it is convenient to choose all but one of these vectors (e.g., the vector T_2) to be normalized to unity. Denoting the norm of the vector T_2 by γ, we then have

$$T_{1j} = a_j \qquad T_{2j} = \gamma W_{2j} \qquad T_{ij} = W_{ij} \qquad i > 2 \tag{41}$$

where W_{ij} is an orthogonal matrix.

As remarked above, an orthogonal transformation of the collaborating players' states can be achieved with passive elements. However, the replacement of the first row of W by the vector a, in forming the matrix T, means that the resulting transformation involves squeezing operations and hence a need for active elements. As we now show, the transformation defined by T can be achieved with just two squeezers.

Choose the vector W_2 to lie in the span of the vectors a and W_1. It then follows that a is expandable as $a = \alpha W_1 + \beta W_2$ and

$$T = \left(\begin{array}{cc|ccc} \alpha & \beta & 0 & \ldots & 0 \\ 0 & \gamma & 0 & \ldots & 0 \\ \hline 0 & 0 & & & \\ \vdots & \vdots & & I & \\ 0 & 0 & & & \end{array}\right) W \equiv V W \tag{42}$$

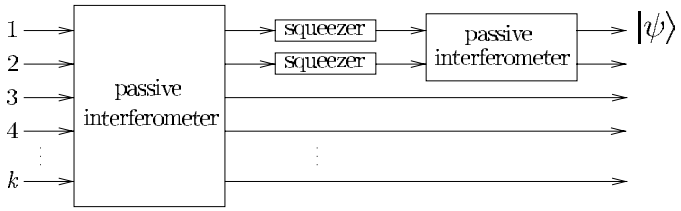

Figure 3. The general scheme of an interferometer used by the players to decode the secret state. The passive k-port interferometer is followed by two independent single-mode squeezers, and the last step is a passive two-mode interferometer that yields the secret at one output port.

with a free parameter $\gamma \neq 0$. This parameter can be adjusted, according to the criteria outlined in section 4 to minimize the demands on the squeezing resources. The $GL(k, \mathbb{R})$ matrix V can now be factored as $V = XV_dY$, with X and Y orthogonal matrices and

$$V_d = \mathrm{diag}(v_1, v_2, 1, 1, \ldots, 1). \tag{43}$$

The complete transformation T then assumes the simple form

$$T = VW = XV_dYW = XV_dZ \tag{44}$$

with both X and Z orthogonal matrices.

The disentangling transformation represented by the matrix T is now achieved by a sequence of three transformations: the first transformation, represented by the orthogonal matrix Z, is achieved by a passive interferometer consisting of only beam splitters and phase shifters; the transformation represented by the diagonal matrix V_d is given by single-mode $Sp(1, \mathbb{R})$ squeezers on the first two modes, with squeezing parameters $r_1 = \ln v_1$ and $r_2 = \ln v_2$; finally, the transformation corresponding to the matrix X is given by a two-mode beam splitter (see figure 3). Hence the number of active optical elements (squeezers) is reduced to two.

4. Total amount of squeezing

It is of interest not only to consider the number of active optical elements necessary for the extraction part of QSS, but also the total amount of squeezing R. It is natural to define this quantity as the sum of magnitudes of squeezing parameters corresponding to the two squeezers, i.e.,

$$R = |r_1| + |r_2| = |\ln v_1| + |\ln v_2| \tag{45}$$

which can be minimized by a judicious choice of γ in equation (42).

We can express R as $R = \frac{1}{2}(|\ln \lambda_1| + |\ln \lambda_2|)$, where $\lambda_{1,2}$ are the eigenvalues of the symmetric matrix $V'\tilde{V}'$ with $V' = \left(\begin{smallmatrix} \alpha & \beta \\ 0 & \gamma \end{smallmatrix}\right)$, and $\tilde{V}'$ the transpose of V'. A simple calculation shows that the eigenvalues are

$$\lambda_{1,2} = \tfrac{1}{2}\left[\alpha^2 + \beta^2 + \gamma^2 \pm \sqrt{(\alpha^2 + \beta^2 + \gamma^2)^2 - 4\alpha^2\beta^2}\,\right]. \tag{46}$$

Depending on γ, the total amount of squeezing R is either (i) $R = \frac{1}{2}|\ln(\lambda_1\lambda_2)|$ (if both $\ln \lambda_1$ and $\ln \lambda_2$ have the same sign) or (ii) $R = \frac{1}{2}|\ln(\lambda_1/\lambda_2)|$ (if $\ln \lambda_1$ and $\ln \lambda_2$ have different signs). We seek γ that minimizes R, which can occur for either case (i) or (ii), so both must be checked. We define the quantity $\kappa \equiv (1 - \alpha^2 - \beta^2)/(1 - \alpha^2)$ and have

(i) The minimum value of $R(\gamma)$ is $R_{\min} = |\ln(\kappa\alpha)|$ and occurs for $\gamma_0 = \sqrt{\kappa}$ in the following situations:

$$\alpha^2 + \beta^2 < 1 \qquad \text{and} \qquad \alpha^2 + \beta^2 < \kappa$$
$$\alpha^2 + \beta^2 > 1 + \beta^2/\alpha^2 \qquad \text{and} \qquad \alpha^2 + \beta^2 > \kappa$$

(ii) The minimum value of $R(\gamma)$ is $R_{\min} = \ln[(\sqrt{\alpha^2 + \beta^2} + |\beta|)/|\alpha|]$ and occurs for $\gamma_0 = \sqrt{\alpha^2 + \beta^2}$ in the following situations:

$$1 \leqslant \alpha^2 + \beta^2 \leqslant 1 + \beta^2/\alpha^2$$
$$\kappa \leqslant \alpha^2 + \beta^2 \leqslant 1$$
$$1 + \beta^2/\alpha^2 \leqslant \alpha^2 + \beta^2 \leqslant \kappa.$$

The strategy for a collaborating group of players to minimize the squeezing resources for the extraction of the secret state is the following: for given α and β, the players calculate the value of κ and decide which of the two cases (i) or (ii) occurs. Then they find the value γ_0 and construct the matrix T in equation (42) and from this, the corresponding active interferometer that contains only two squeezers with a minimum total amount of squeezing equal to $R_{\min}$.

5. Conclusion

We have shown that the extraction procedure in optical continuous-variable quantum secret sharing can be achieved with a small number (at most two) of squeezing elements for any authorized group of players. In particular, we have demonstrated this for the QSS threshold schemes. We have quantified the total amount of squeezing defined as the sum of absolute values of the single-mode squeezing parameters, and found its minimum value analytically. We have also seen that in the realistic situation when the dealer has only finite squeezing resources available, the density operator of the extracted secret becomes a Gaussian convolution of the original secret state.

Acknowledgments

We would like to thank Martin Rowe for assistance with calculations of total squeezing. This project has been supported by a Macquarie University Research Grant and by an Australian Research Council Large Grant.

Appendix A. Density operator of the extracted secret

The total density operator $\hat{\rho}_T$ of all shares after the extraction procedure reads

$$\hat{\rho}_T = \int_{\mathbb{R}^{2n}} \rho(x, x')|\xi_1(\mathbf{x})\rangle_1\langle\xi_1(\mathbf{x}')| \otimes |\xi_2(\mathbf{x})\rangle_2\langle\xi_2(\mathbf{x}')| \otimes \cdots \otimes |\xi_n(\mathbf{x})\rangle_n\langle\xi_n(\mathbf{x}')| \times \exp\left\{-\sum_{i=1}^{k-1}\left[\frac{y_i^2 + y'^2{}_i}{2a^2} + \frac{a^2\left(z_i^2 + z'^2{}_i\right)}{2}\right]\right\} \mathrm{d}^n\mathbf{x}\,\mathrm{d}^n\mathbf{x}' \tag{A1}$$

up to a normalization factor (we will neglect such factors throughout the appendix). Here the share is indicated by a subscript and the product $\psi(x)\psi^*(x')$ is written as the density operator element $\rho(x, x')$ of the original secret.

The density operator $\hat{\rho}'$ of the extracted secret is obtained by tracing $\hat{\rho}_T$ over shares $2, 3, \ldots, n$. In the following we will calculate the density operator element $\rho'(w, w') \equiv \langle w|\hat{\rho}'|w'\rangle$. Using the special form (13), (14) of the vectors ξ_i and employing the fact

that $\langle x|x'\rangle = \delta(x - x')$, we get

$$\rho'(w, w') = \int_{\mathbb{R}^{4k-4}} \rho(w - \gamma_1\mathbf{z}, w' - \gamma_1\mathbf{z}')] \exp\left\{-\sum_{i=1}^{k-1}\left[\frac{y_i^2 + y_i'^2}{2a^2} + \frac{a^2\left(z_i^2 + z_i'^2\right)}{2}\right]\right\}$$
$$\times \prod_{i=2}^{k} \delta[\alpha_i(w - w') + \beta_i(\mathbf{y} - \mathbf{y}') + \gamma_i(\mathbf{z} - \mathbf{z}')]$$
$$\times \prod_{i=2}^{k} \delta[\alpha_i(w - w') + \beta_i(\mathbf{y} - \mathbf{y}') + \gamma_{k-1+i}(\mathbf{z} - \mathbf{z}')]$$
$$\times \mathrm{d}^{k-1}\mathbf{y}\, \mathrm{d}^{k-1}\mathbf{y}'\, \mathrm{d}^{k-1}\mathbf{z}\, \mathrm{d}^{k-1}\mathbf{z}'. \tag{A2}$$

The integration over x, x' has been performed. Now, in the following we will use the property of the δ-function

$$\prod_{i=1}^{r} \delta(a_i) = \|T\| \prod_{i=1}^{r} \delta\left(\sum_{j=1}^{r} T_{ij} a_j\right) \tag{A3}$$

where $T = (T_{ij})$ is a real non-singular matrix and $\|T\|$ its Jacobian (the magnitude of determinant of T). Using the special case of equation (A3), $\delta(x)\delta(y) = \delta(x)\delta(x - y)$, we can rewrite equation (A2) as

$$\rho'(w, w') = \int_{\mathbb{R}^{4k-4}} \rho(w - \gamma_1\mathbf{z}, w' - \gamma_1\mathbf{z}')] \exp\left\{-\sum_{i=1}^{k-1}\left[\frac{y_i^2 + y_i'^2}{2a^2} + \frac{a^2\left(z_i^2 + z_i'^2\right)}{2}\right]\right\}$$
$$\times \prod_{i=2}^{k} \delta[\alpha_i(w - w') + \beta_i(\mathbf{y} - \mathbf{y}') + \gamma_i(\mathbf{z} - \mathbf{z}')]$$
$$\times \prod_{i=2}^{k} \delta[(\gamma_{k-1+i} - \gamma_i)(\mathbf{z} - \mathbf{z}')]\, \mathrm{d}^{k-1}\mathbf{y}\, \mathrm{d}^{k-1}\mathbf{y}'\, \mathrm{d}^{k-1}\mathbf{z}\, \mathrm{d}^{k-1}\mathbf{z}'. \tag{A4}$$

To express the product $\prod_{i=2}^{k} \delta[(\gamma_{k-1+i} - \gamma_i)(\mathbf{z} - \mathbf{z}')]$ of δ-functions, we employ equation (A3) to obtain

$$\prod_{i=2}^{k} \delta[(\gamma_{k-1+i} - \gamma_i)(\mathbf{z} - \mathbf{z}')] = \prod_{i=1}^{k-1} \delta(z_i - z_i') \tag{A5}$$

up to a multiplicative factor provided that the square matrix Γ composed of the coefficients of the $k - 1$ vectors $\gamma_{k-1+i} - \gamma_i (i = 2, \ldots, k)$ is non-singular. This is indeed the case as we can see if we consider the transformation $x_i \to \eta_i$, where $\eta_i = \xi_i$ for $i = 1, \ldots, k$ and $\eta_i = \xi_i - \xi_{i-k+1}$ for $i = k+1, \ldots, n$. This transformation is clearly non-singular and therefore the subdeterminant of the matrix of partial derivatives $\partial\eta_i/\partial x_j$, $i, j = k+1, \ldots, n$, which is precisely the matrix Γ, is nonzero.

Inserting equation (A5) into equation (A4) and integrating over $z_1', \ldots, z_{k-1}'$, we obtain a multiple convolution of $\rho(w, w')$ with a Gaussian. Using the associative properties of convolutions and making the convolution of the $k - 1$ Gaussians first, we obtain

$$\rho'(w, w') = \int_{\mathbb{R}} \rho(w - vz, w' - vz)\, \mathrm{e}^{-a^2z^2}\, \mathrm{d}z \int_{\mathbb{R}^{2k-2}} \exp\left(-\sum_{i=1}^{k-1} \frac{y_i^2 + y'^2{}_i}{2a^2}\right)$$
$$\times \prod_{i=2}^{k} \delta[\alpha_i(w - w') + \beta_i(\mathbf{y} - \mathbf{y}')]\, \mathrm{d}^{k-1}\mathbf{y}\, \mathrm{d}^{k-1}\mathbf{y}' \tag{A6}$$

where $v^2 = \sum_{i=1}^{k-1} \gamma_{1i}^2$.

Next we express α_i as the sum $\alpha_j = \sum_{i=1}^{k-1} u_i \beta_{ji}$, $j = 2, \ldots, k$. This is possible as the vectors β_i, $i = 1, \ldots, k-1$ are linearly independent for a similar reason as was explained above for the vectors $\gamma_{k-1+i} - \gamma_i$ and therefore the matrix composed of β_{ij} is non-singular. Now we can re-express the δ-function product in equation (A6) as

$$\prod_{i=2}^{k} \delta[\alpha_i(w - w') + \beta_i(\mathbf{y} - \mathbf{y}')] = \prod_{i=2}^{k} \delta \left\{ \sum_{j=1}^{k-1} \beta_{ij}[u_j(w - w') + (y_j - y'_j)] \right\}$$
$$= \prod_{i=2}^{k} \delta \left\{ \sum_{j=1}^{k-1} \beta_{ij}(Y_j - Y'_j)] \right\} = \prod_{i=1}^{k-1} \delta(Y_i - Y'_i) \tag{A7}$$

where $Y_i = y_i + u_i w$, $Y'_i = y'_i + u_i w'$.

Rewriting the integral over $\mathbf{y}, \mathbf{y}'$ in equation (A6) using equation (A7), integrating over $\mathbf{y}'$, and changing the variables of the remaining integral from $\mathbf{y}$ to $\mathbf{Y}$ we obtain

$$\int_{\mathbb{R}^{k-1}} \exp \left\{ -\sum_{i=1}^{k-1} \frac{(Y_i - u_i w)^2 + (Y_i - u_i w')^2}{2a^2} \right\} \mathrm{d}^{k-1}\mathbf{Y} = \exp \left\{ -\sum_{i=1}^{k-1} \frac{u_i^2}{4a^2}(w - w')^2 \right\}. \tag{A8}$$

Combining now equations (A6) and (A8), changing the integration variable z to $y = vz$, switching from w, w' to x, x' and properly normalizing, we obtain finally equation (25):

$$\rho'(x, x') = \frac{a}{\sqrt{\pi} v} \exp \left[-\frac{u^2(x - x')^2}{4a^2} \right] \int_{\mathbb{R}} \rho(x - y, x' - y) \exp \left[-\frac{a^2 y^2}{v^2} \right] \mathrm{d}y. \tag{A9}$$

References

[1] Shamir A 1979 *Commun. ACM* **22** 612
[2] Lvovsky A I, Hansen H, Aichele T, Benson O, Mlynek J and Schiller S 2001 *Phys. Rev. Lett.* **87** 050402
[3] Hillery M, Bužek V and Berthiaume A 1999 *Phys. Rev.* A **59** 1829
[4] Cleve R, Gottesman D and Lo H-K 1999 *Phys. Rev. Lett.* **83** 648
[5] Tyc T and Sanders B C 2002 *Phys. Rev.* A **65** 42310
[6] Nielsen M A and Chuang I L 2000 *Quantum Computation and Quantum Information* (Cambridge: Cambridge University Press)
[7] Braunstein S L and Pati A K 2003 *Quantum Information with Continuous Variables* (Dordrecht: Kluwer)
[8] Loudon R and Knight P L 1987 *J. Mod. Opt.* **34** 702
[9] Bartlett S D and Sanders B C 2002 *Phys. Rev.* A **65** 042304
[10] Kim J, Takeuchi S and Yamamoto Y 1999 *Appl. Phys. Lett.* **74** 902
[11] Furusawa A *et al* 1998 *Science* **282** 706
[12] Lance A, Symul T, Bowen W, Tyc T, Sanders B C and Lam P K 2002 *Preprint* quant-ph/0210188
[13] Braunstein S L 1999 *Preprint* quant-ph/9904002 v2
[14] Schumaker B L and Caves C M 1985 *Phys. Rev.* A **31** 3093
[15] Wootters W K and Zurek W H 1982 *Nature* **299** 802
[16] Vaidman L 1994 *Phys. Rev.* A **49** 1473
[17] Braunstein S L and Kimble H J 1998 *Phys. Rev. Lett.* **80** 869
[18] Smith A D 2000 *Preprint* quant-ph/0001087
[19] Kim M S and Sanders B C 1996 *Phys. Rev.* A **53** 3694
[20] Walls D F and Milburn G J 1994 *Quantum Optics* (Berlin: Springer)