How to share a continuous-variable quantum secret by optical interferometry

Tomáš Tyc* and Barry C. Sanders

Department of Physics, Macquarie University, Sydney, New South Wales 2109, Australia
(Received 13 July 2001; published 1 April 2002)

We develop the theory of continuous-variable quantum secret sharing and propose its interferometric realization using passive and active optical elements. In the ideal case of infinite squeezing, a fidelity $\mathcal{F}$ of unity can be achieved with respect to reconstructing the quantum secret. We quantify the reduction in fidelity for the (2,3) threshold scheme due to finite squeezing and establish the condition for verifying that genuine quantum secret sharing has occurred.

I. INTRODUCTION

Classical secret sharing introduced by Shamir [1] is an important primitive of protection of secret classical information. It involves a dealer who distributes a secret amongst a group of n parties (players) in a way that prevents all unauthorized subsets of players (referred to as the adversary structure) from reconstructing this state and permits authorized subsets (referred to as the access structure) to successfully reconstruct the state.

In quantum information theory, where the quantum state itself is a repository of information, protection of this state is of paramount importance. The quantum version of secret sharing (QSS) [2–4] will likely play a key role in protecting secret quantum information, e.g., in secure operations of distributed quantum computation, sharing difficult-to-construct ancilla states and joint sharing of quantum money, as examples of the versatility of QSS [3]. Other examples of quantum security include quantum key distribution [5], protection of a classical secret by quantum means in the presence of eavesdroppers [6,7], and quantum bit commitment [8].

Whereas quantum secret sharing has been developed for discrete variables [2–4], here we develop continuous-variable (CV) quantum secret sharing and show how it can be implemented using optical interferometry and squeezed light sources [9]. Both the theory and the proposed experimental realization are quite different from their discrete variable counterparts, yet serve the same goal: sharing secret quantum states. CV quantum information theory has achieved enormous success in quantum teleportation [10] and quantum computation [11], and continuous-variable quantum secret sharing can be expected to play a key role in future integrated CV quantum information systems. The recent explosion of work going into linear optical quantum computation is an example of the importance of interferometric approaches to quantum information [12], and our proposal fits well with this rapidly growing subfield of quantum information research.

We develop the (2,2) threshold quantum secret sharing

protocol for passive linear interferometry, and our protocols for higher threshold QSS schemes require squeezed light. We show that finite squeezing limits the fidelity of the reconstructed secret quantum state, and we establish a lower bound on fidelity for the (2,3) threshold scheme. This lower bound is a criterion for establishing that genuine QSS (as opposed to classical secret sharing) has been achieved. Finally we discuss the extension of our protocol to nonthreshold QSS schemes.

In contrast to the case of discrete-variable QSS [2–4], continuous-variable QSS involves states in infinite-dimensional Hilbert spaces. Quantum information theory in infinite-dimensional Hilbert spaces is a feature of working with continuous variables [10,11]. In the QSS scheme discussed here, the secret state ψ from an infinite-dimensional Hilbert space $\mathcal{H}$ is encoded into an entangled state $\Phi \in \mathcal{H}^{\otimes n}$ as n shares, one for each player. The entanglement is designed so that entanglement swapping operations [13] by authorized groups of players can recover the secret state, and unauthorized groups recover no information whatsoever about the secret state.

II. THRESHOLD SCHEMES

We will consider first the threshold quantum secret sharing scheme for CV. Whereas secret sharing is concerned with general adversary and access structures, threshold secret sharing considers a particular access structure. For n players, the access structure for (k,n) threshold secret sharing [2] is the set consisting of all groupings of k or more players, and the adversary structure is the set of all groupings consisting of fewer than k players. We will discuss in detail the $(k,2k-1)$ threshold scheme. The general (k,n) scheme, with $n \leq 2k-1$, can be achieved from the $(k,2k-1)$ scheme by having the dealer discard $2k-n-1$ shares prior to dealing the state Φ, and threshold schemes with $n \geq 2k$ are not possible due to the noncloning theorem [2,14]. In the $(k,2k-1)$ threshold scheme, the dealer's state Φ may be operated on by k collaborators to produce the output state $\Phi_{\text{out}} \in \mathcal{H}^{\otimes 2k-1}$. Ideally, Φ_{out} is a product of the original secret state ψ and $k-1$ pairwise entangled states, each in the Hilbert space $\mathcal{H}_i \otimes \mathcal{H}_j$, where the ith and jth player is a collaborator and adversary (or noncollaborating player), respectively. This entanglement of states between collaborator and

———
*On leave from Institute of Theoretical Physics, Masaryk University, Kotlářská 2, 61137 Brno, Czech Republic; email address: tomtyc@physics.muni.cz
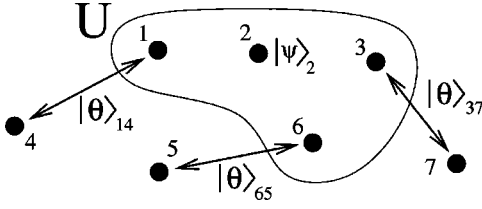
FIG. 1. The reconstruction of the secret for $k=4$ corresponding to the permutation $(r_i)=(2136475)$. In order to reconstruct the secret ψ, the players 2, 1, 3, and 6 perform the unitary operation U from Eq. (2.5) on their shares. This results in the second share left in the state ψ, while the shares 1, 3, and 6 form EPR states with the shares 4, 7, and 5, respectively.

adversary ensures that adversaries do not acquire any information whatsoever about ψ.

We introduce a continuous-variable representation for the secret state $|\psi\rangle$ as $\psi(x)=\langle x|\psi\rangle$ for $|x\rangle$ the eigenstate of the canonical position operator $\hat{x}$, and the eigenvalue spectrum is $x\in\mathbb{R}$. The eigenstates of $\hat{x}$ are not normalizable but satisfy the orthogonality relation

$$\langle x'|x\rangle=\delta(x-x').\tag{2.1}$$

In an optical system, this is the quadrature-phase representation, which can be measured via optical homodyne detection [15].

For $\mathbf{x}\equiv(x_1,\ldots,x_k)^{\mathrm{T}}$ a vector from the k-dimensional vector space $\mathbb{R}^k$ for the canonical positions of k players, the dealer implements a particular linear mapping

$$L:\mathbb{R}^k\to\mathbb{R}^{2k}:\mathbf{x}\mapsto L(\mathbf{x})=[x_1,L_1(\mathbf{x}),\ldots,L_{2k-1}(\mathbf{x})]^{\mathrm{T}}.\tag{2.2}$$

The linear mapping L is constrained by the requirement (which can always be satisfied [2]) that the components of any k-element subset of $\{x_1,L_1,\ldots,L_{2k-1}\}$ are linearly independent. The mapping L is used by the dealer to encode ψ into the entangled state

$$|\Phi\rangle=\int_{\mathbb{R}^k}\psi(x_1)|L_1(\mathbf{x})\rangle_1\cdots|L_{2k-1}(\mathbf{x})\rangle_{2k-1}d^k\mathbf{x}\tag{2.3}$$

(which is not normalizable for the same reason that $|x\rangle$ is not normalizable).

The encoding (2.3) enables ψ to be reconstructed from any k shares as follows. Let $(r_1,\ldots,r_{2k-1})$ be an arbitrary permutation of indices $(1,2,\ldots,2k-1)$. As both sets $\{L_{r_1},L_{r_2},\ldots,L_{r_k}\}$ and $\{x_1,L_1,\ldots,L_{2k-1}\}$ are linearly independent, there exists a non-singular $k\times k$ matrix T such that

$$T\begin{pmatrix}L_{r_1}\\L_{r_2}\\\vdots\\L_{r_k}\end{pmatrix}=\begin{pmatrix}x_1\\L_{r_{k+1}}\\\vdots\\L_{r_{2k-1}}\end{pmatrix}.\tag{2.4}$$

Given T, there exists a unitary operator $U(T)$ such that

$$U(T)|L_{r_1}\rangle_{r_1}|L_{r_2}\rangle_{r_2}\cdots|L_{r_k}\rangle_{r_k}=||T||^{1/2}|x_1\rangle_{r_1}|L_{r_{k+1}}\rangle_{r_2}\cdots$$
$$\times|L_{r_{2k-1}}\rangle_{r_k}\tag{2.5}$$

with $||T||=||\det T||$. The matrix elements of U in the continuous basis

$$\{|\mathbf{x}'\rangle\equiv|x_1'\rangle_{r_1}\cdots|x_k'\rangle_{r_k}\}\tag{2.6}$$

are

$$\langle\mathbf{x}'|U|\mathbf{x}''\rangle=||T||^{1/2}\prod_{i=1}^{k}\delta\left(\sum_{j=1}^{k}T_{ij}x_j''-x_i'\right),\tag{2.7}$$

with $\{T_{ij}\}$ the matrix elements of T.

The collaborators with shares indexed by $r_1,r_2,\ldots,r_k$ reconstruct the secret by transforming their shares via U, which results in the total state of all shares

$$U|\Phi\rangle=J||T||^{1/2}\int_{\mathbb{R}^k}\psi(x_1)\,|x_1\rangle_{r_1}|L_{r_{k+1}}\rangle_{r_2}\cdots$$
$$\times|L_{r_{2k-1}}\rangle_{r_k}|L_{r_{k+1}}\rangle_{r_{k+1}}\cdots|L_{r_{2k-1}}\rangle_{r_{2k-1}}$$
$$\times dx_1dL_{r_{k+1}}\cdots dL_{r_{2k-1}}$$
$$=J||T||^{1/2}|\psi\rangle_{r_1}|\Theta\rangle_{r_2,r_{k+1}}|\Theta\rangle_{r_3,r_{k+2}}\cdots|\Theta\rangle_{r_k,r_{2k-1}},\tag{2.8}$$

with J the Jacobian for the transformation from $\mathbf{x}$ to $(x_1,L_{r_{k+1}},\ldots,L_{r_{2k-1}})$ and

$$|\Theta\rangle_{ij}\equiv\int_{\mathbb{R}}|x\rangle_i|x\rangle_j\,dx.\tag{2.9}$$

Equation (2.8) shows that the r_1th share is the secret state ψ and shares $r_2,\ldots,r_k$ are maximally entangled with the shares of the adversaries (see Fig. 1). Thus the quantum secret is reconstructed from any k shares via a unitary transformation, and any $k-1$ shares produces no information about ψ whatsoever as tracing over the remaining k shares yields a multiple of the identity operator.

Important components of the state (2.8) are the (unnormalized and ideal) Einstein-Podolski-Rosen (EPR) states [16] $|\Theta\rangle_{ij}$ [see Eq. (2.9)] such that $_{ij}\langle x\,x'|\Theta\rangle_{ij}=\delta(x-x')$. These states can be approximated by the strongly squeezed two-mode vacuum states [17] $|\eta\rangle_{ij}$ that have the representation

$$_{ij}\langle x\,x'|\eta\rangle_{ij}\equiv(1-\eta^2)^{1/2}\sum_{n=0}^{\infty}\eta^n u_n(x)u_n(x')\tag{2.10}$$

for $-1\leq\eta\leq1$ and $u_n(x)\equiv\langle x|n\rangle$ with $|n\rangle$ the Fock state. As

$$\sum_{n=0}^{\infty}u_n(x)u_n(x')=\delta(x-x'),\tag{2.11}$$

the relation

$$\lim_{\eta \to 1} (1 - \eta^2)^{-1/2} \langle xx' | \eta \rangle = \delta(x - x') \qquad (2.12)$$

holds; hence $|\eta \to 1\rangle = |\Theta\rangle$. The share i of $|\eta\rangle_{ij}$, after tracing over the share j, behaves locally as a thermal state ϱ_T with temperature $T = -\hbar \omega / (2 k_B \ln|\eta|)$, where k_B denotes the Boltzmann constant; the limit $\eta \to 1$ corresponds to $T \to \infty$.

III. EXPERIMENTAL REALIZATION

Now we show how to implement the above reconstruction procedure experimentally. Given T in Eq. (2.4), there exists $S \in \mathrm{Sp}(2k, \mathbb{R})$ corresponding to T mapping the canonical position and $(T^{\mathrm{T}})^{-1}$ mapping the corresponding canonical momenta, for T the transpose. The symplectic transformation S can be decomposed into a sequence of SU(2) and SU(1,1) transformations [18] that perform passive and active (squeezing) operations on the shares. Physically, such transformations can be realized by the combined SU(2) and SU(1,1) interferometry [19] that uses beam splitters, mirrors, phase shifters, and squeezers. The secret and shares are then distinct spatial modes of light, and an interferometer can be designed by any group of k collaborators to yield the secret at one output port when the shares are injected to the input ports.

The encoding of the secret by the dealer can also be performed via (active) interferometry (again a symplectic transformation). For a chosen permutation of indices, the dealer creates the state (2.8) and employing a suitable interferometer applies $U^{\dagger}$ to this state in order to obtain Φ. In summary, the dealer can encode the secret state ψ in a $2k - 1$ mode entangled state Φ via interferometry which can be decoded by any k collaborators also by interferometry. As has been mentioned at the start, the general (k,n) threshold scheme can be achieved by having the dealer discard $2k - 1 - n$ shares.

IV. EXAMPLE: (2,3) THRESHOLD SCHEME

We will give an example of the (2,3) threshold scheme. The dealer chooses

$$L_1 = \frac{x_2 + x_1}{\sqrt{2}}, \quad L_2 = \frac{x_2 - x_1}{\sqrt{2}}, \quad L_3 = x_2, \qquad (4.1)$$

and constructs the corresponding interferometer with a 50/50 beam splitter (BS) as shown in Fig. 2(a). This interferometer transforms the initial state $|\psi\rangle_1 |\Theta\rangle_{23}$ to the three-mode entangled state

$$|\Phi\rangle = \int_{\mathbb{R}^2} \psi(x_1) \left| \frac{x_2 + x_1}{\sqrt{2}} \right\rangle_1 \left| \frac{x_2 - x_1}{\sqrt{2}} \right\rangle_2 |x_2\rangle_3 \, \mathrm{d}x_1 \, \mathrm{d}x_2 . \tag{4.2}$$

The secret can then be reconstructed from any two shares. By combining shares 1 and 2 on a 50/50 BS [Fig. 2(b)], thereby transforming the canonical positions of the two shares via
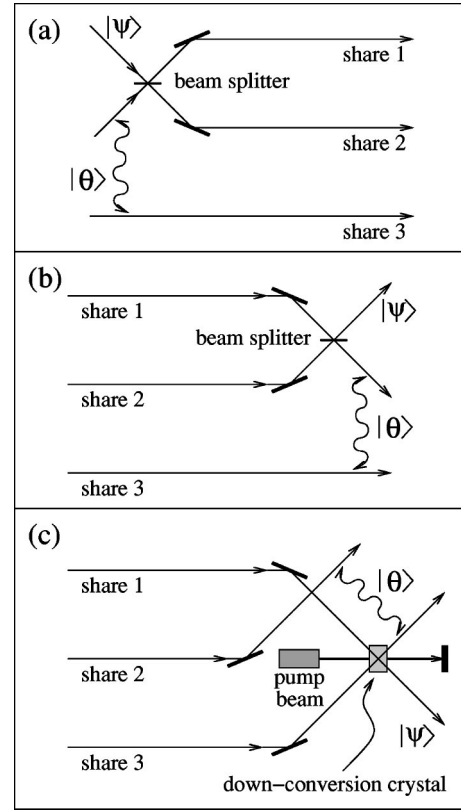

FIG. 2. Encoding and reconstruction procedures for a (2,3) threshold scheme. (a) For the encoding process, the dealer creates the state $|\psi\rangle_1 |\Theta\rangle_{23}$ and combines modes 1 and 2 on a 50/50 BS; (b) players 1 and 2 combine their shares on a 50/50 BS to obtain ψ at one output; (c) players 1 and 3 combine their shares at a nondegenerate parametric down converter which is pumped by a coherent beam of doubled frequency to obtain ψ at one output. In both cases (a) and (b) the remaining output forms an EPR state with the share of the adversary.

$$T_{12} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}, \qquad (4.3)$$

the first share is left in the secret state ψ. Similarly by combining the first and third shares on a nondegenerate parametric down-conversion crystal, pumped by a coherent field [see Fig. 2(c)], that transforms the canonical positions via

$$T_{13} = \begin{pmatrix} \sqrt{2} & -1 \\ -1 & \sqrt{2} \end{pmatrix}, \qquad (4.4)$$

the first share is left in the secret state ψ. A similar procedure can be employed for shares 2 and 3 to reconstruct the secret.

A surprisingly simple (2,2) quantum secret sharing threshold scheme can be derived from the previous (2,3) scheme by discarding the third share. The (unnormalized) reduced density operator of the first two shares after tracing over the last share is

$$\rho_{12} = U^{\dagger} (|\psi\rangle_1 \langle \psi| \otimes 1_2) U, \qquad (4.5)$$
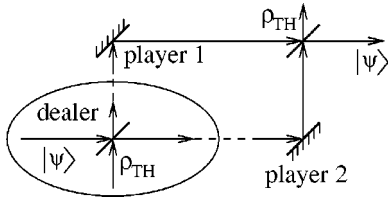
FIG. 3. The (2,2) threshold scheme: the dealer encodes the secret by combining it with a thermal state of an infinite temperature on a 50/50 BS. The two players can then reconstruct the secret by combining their beams on another 50/50 BS.

for U the unitary operator induced by T_{12} according to Eqs. (2.5) and (2.7), and $\mathbb{1}$ the unit operator. As the thermal state $\varrho_{T\to\infty}$ is a multiple of the unit operator, the state of the two shares can be also obtained by mixing the secret ψ with a thermal state of infinite temperature on a 50/50 BS (see Fig. 3). The encoding of the secret is thus performed by simply mixing it with a thermal state on a BS, whereas the reconstruction is accomplished via recombining the two shares on another 50/50 BS. As a result, the players obtain the secret state as well as the thermal state from the two BS output ports.

V. THE CASE OF FINITE SQUEEZING

Whereas infinite temperature is necessary for ideal (2,2) quantum secret sharing threshold scheme, $\varrho_{T\to\infty}$ contains on average an infinite number of photons so any finite error in the encoding or reconstruction process will produce infinitely many photons from output port 1 of the BS and thereby destroy the secret completely. Therefore a finite-temperature ϱ_T must be employed instead, and in the general case of the (k,n) threshold scheme, finitely squeezed two-mode vacuum states must replace EPR states for the same reason. This will generally compromise the secret sharing fidelity, i.e., the overlap of the reconstructed state and the original secret state

$$\mathcal{F}=\langle\psi|\rho|\psi\rangle, \tag{5.1}$$

where ρ is the (generally mixed) state obtained as the result of reconstruction. Consider a dealer using an interferometer as in Fig. 2(a) for the encoding process, where a two-mode squeezed vacuum state $|\eta=\tanh r\rangle$ replaces the EPR state at the two inputs. Clearly, players 1 and 2 can still reconstruct the secret perfectly while players 1 and 3 or players 2 and 3 cannot. If the secret is a coherent state, the fidelity for players 1 and 3 is

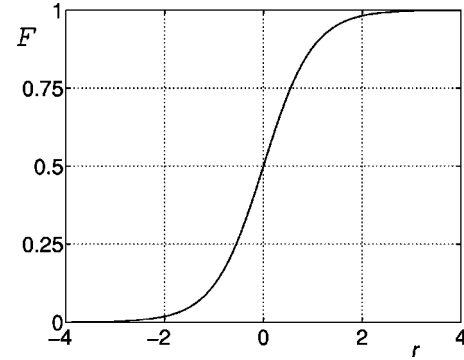$$\mathcal{F}=\frac{1}{1+e^{-2r}}=\frac{1+\eta}{2} \tag{5.2}$$

FIG. 4. The fidelity $\mathcal{F}=\langle\psi|\rho|\psi\rangle$ for the scheme in Figs. 2(a),(c) with squeezing parameter r used by the dealer and the secret ψ a coherent state.

(see Fig. 4). If $r=0$ (no squeezing), the players can still achieve $\mathcal{F}=1/2$. This fidelity threshold can be used to verify whether a genuine quantum secret sharing has taken place in this particular (2,3) threshold scheme.

VI. CONCLUSION

To conclude, we have developed a theory of quantum secret sharing using CV and shown how encoding and reconstruction processes could be achieved via (active) multimode interferometry for the (k,n) threshold scheme. The (2,3) and (2,2) schemes have been presented in detail, including an allowance for finite squeezing and a minimum fidelity necessary to demonstrate that genuine secret sharing has been performed. The (2,2) threshold scheme is achievable with current technology.

The (k,n) threshold scheme is readily generalized to an arbitrary adversary structure $\mathcal{A}$ by analogy with the discrete-variable schemes based on monotone span programs [4]. For any adversary structure $\mathcal{A}$, there exists a self-dual structure $\mathcal{A}'$ ($\mathcal{A}'$ is self-dual if, for any division of the set of all players into two disjoint groups, exactly one group is able to reconstruct the secret), from which $\mathcal{A}$ can be obtained by discarding some shares [4]. For the self-dual adversary structure $\mathcal{A}'$, the encoding procedure of the dealer and decoding procedures of the collaborating players can again be realized by linear mappings of the canonical positions by employing a suitable interferometer. For a total of n players, the initial state of the dealer consists of the secret ψ and $n-1$ single-mode infinitely squeezed vacuum states [9].

[1] A. Shamir, Commun. ACM **22**, 612 (1979).
[2] R. Cleve *et al.*, Phys. Rev. Lett. **83**, 648 (1999).
[3] D. Gottesman, Phys. Rev. A **61**, 042311 (2000).
[4] A.D. Smith, e-print quant-ph/0001087.

[5] C.H. Bennett and G. Brassard, in *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India* (IEEE, New York, 1984), p. 175.
[6] M. Hillery *et al.*, Phys. Rev. A **59**, 1829 (1999).

[7] W. Tittel *et al.*, Phys. Rev. A **63**, 042301 (2001).

[8] Although quantum bit commitment cannot be unconditionally secure [H.-K. Lo and H.F. Chau, Phys. Rev. Lett. **78**, 3410 (1997); D. Mayers, *ibid.* **78**, 3414 (1997)], nontrivial bounds on cheating by either sender or receiver have been established (R.W. Spekkens and T. Rudolph, e-print quant-ph/0106019 and e-print quant-ph/0107042). These bounds are significant, as bit commitment, along with secret sharing, is an important primitive in data security.

[9] D.F. Walls, Nature (London) **324**, 210 (1986).

[10] L. Vaidman, Phys. Rev. A **49**, 1473 (1994); S.L. Braunstein and H.J. Kimble, Phys. Rev. Lett. **80**, 869 (1998); A. Furusawa *et al.*, Science **282**, 706 (1998).

[11] S. Lloyd and S.L. Braunstein, Phys. Rev. Lett. **82**, 1784 (1999).

[12] E. Knill *et al.*, Nature (London) **409**, 46 (2001).

[13] M. Żukowski *et al.*, Phys. Rev. Lett. **71**, 4287 (1993).

[14] W.K. Wootters and W.H. Zurek, Nature (London) **299**, 802 (1982).

[15] H.P. Yuen and J.H. Shapiro, IEEE Trans. Inf. Theory **IT-25**, 179 (1979); **IT-26**, 78 (1980).

[16] A. Einstein *et al.*, Phys. Rev. **47**, 777 (1935).

[17] B.L. Schumaker and C.M. Caves, Phys. Rev. A **31**, 3093 (1985).

[18] S.D. Bartlett *et al.*, Phys. Rev. A **63**, 042310 (2001).

[19] B. Yurke *et al.*, Phys. Rev. A **33**, 4033 (1986).