Relativistic (2,3)-threshold quantum secret sharing

Mehdi Ahmadi,[1,2,*] Ya-Dong Wu,[2,†] and Barry C. Sanders[2,3,4,5,‡]

[1]*Department of Mathematics and Statistics, University of Calgary, Calgary, Alberta T2N 1N4, Canada*
[2]*Institute for Quantum Science and Technology, University of Calgary, Calgary, Alberta T2N 1N4, Canada*
[3]*Program in Quantum Information Science, Canadian Institute for Advanced Research,*
Toronto, Ontario M5G 1Z8, Canada
[4]*Hefei National Laboratory for Physical Sciences at Microscale,*
University of Science and Technology of China, Hefei, Anhui 230026, China
[5]*Shanghai Branch, CAS Center for Excellence and Synergetic Innovation Center in Quantum Information*
and Quantum Physics, University of Science and Technology of China, Shanghai 201315, China

In quantum secret sharing protocols, the usual presumption is that the distribution of quantum shares and players' collaboration are both performed inertially. Here we develop a quantum secret sharing protocol that relaxes these assumptions wherein we consider the effects due to the accelerating motion of the shares. Specifically, we solve the (2,3)-threshold continuous-variable quantum secret sharing in noninertial frames. To this aim, we formulate the effect of relativistic motion on the quantum field inside a cavity as a bosonic quantum Gaussian channel. We investigate how the fidelity of quantum secret sharing is affected by nonuniform motion of the quantum shares. Furthermore, we fully characterize the canonical form of the Gaussian channel, which can be utilized in quantum-information-processing protocols to include relativistic effects.

I. INTRODUCTION

Continuous-variable quantum secret sharing is experimentally feasible [1]; however, a comprehensive theory of continuous-variable quantum error correction is still missing; Gaussian states cannot be protected against Gaussian errors using Gaussian operations [2]. In previous studies [1,3,4], the effect of noninertial motion during the transmission of quantum shares has been ignored. Here we solve continuous-variable quantum secret sharing wherein the quantum shares move nonuniformly in Minkowski spacetime and our results show how acceleration affects the fidelity of quantum secret sharing.

In (k, n)-threshold quantum secret sharing, the dealer encodes a quantum secret in n quantum systems (or quantum shares), which he then distributes to n players. Each player receives exactly one share, where any subsets of k or more players form the access structure to retrieve the secure key while any subsets of fewer than k players, i.e., the adversarial structure, cannot learn any information whatsoever about the key. Continuous-variable threshold quantum secret sharing still faces the challenge that information about the quantum secret can be leaked into the adversarial structure [5,6]. Various models of secret sharing exist with quantum or classical channels that can be public or private and a graph-state formalism was proposed to unify these models [7]. Here we consider the scenario

wherein the dealer shares quantum channels with each player, and also the players share quantum channels between each other, which is known as the QQ case [7].

We focus on a relativistic variant of a (2,3)-threshold quantum secret sharing protocol which is the smallest-sized nontrivial protocol. We take into account the relativistic motion of the quantum shares in Minkowski spacetime during the distribution and collaboration and how it influences the success of the protocol. In our relativistic protocol, similar to the nonrelativistic case [8], a dealer encodes the quantum secret into several quantum shares and distributes them to all the players. The players are located at different regions in the Minkowski spacetime and the dealer and the players are all stationary. Under such circumstances, during the dealer's distribution, the quantum shares experience nonuniform motion, as they are transmitted to spacetime points in the future light cone of the dealer (Fig. 7). Then, a subset of players within the access structure collaborate to retrieve the quantum secret by sharing their individual shares. However, to reach the same spacetime point, the shares go through phases of accelerating and decelerating motion while being transmitted. We analyze the possible collaboration scenarios between the players; i.e., players 1 and 2 collaborate (Fig. 8) or players 2 and 3 collaborate (Fig. 12). In each scenario, we investigate how the noninertial motion of the shares affects the fidelity of the quantum secret sharing protocol.

In (2,3)-threshold quantum secret sharing, the dealer encodes the quantum secret in three quantum shares in a localized manner; hence, we need to be able to analyze the

*mehdi.ahmadi@ucalgary.ca
†yadong.wu@ucalgary.ca
‡sandersb@ucalgary.ca

effect of relativity on such systems. The relativistic effects on the state of localized quantum systems has been studied using different setups [9–15]. We find the framework of accelerating cavities a suitable choice for this purpose, as it can be adapted to study the effect of nonuniform motion on localized quantum fields [9,10]. Accelerating cavities have been employed in the past to study the relativistic effects on quantum clocks [16], quantum teleportation [17], and to estimate proper acceleration [18,19] to name a few. However, we develop a different approach from the previous studies for accelerating cavities; we formulate the evolution of the quantum field inside an accelerating cavity as a bosonic quantum Gaussian channel (BQGC) which we then use to include the effects of nonuniform motion of the quantum shares. Furthermore, this approach enables us to compute physical quantities, such as the average number of produced thermal particles and transmissivity of the relativistic channel.

This paper is organized as follows. In Sec. II, we provide a brief review of how a quantum field inside a cavity is affected due to relativistic motion. In Sec. III, we formulate the change in the state of the quantum field as a BQGC and utilize the canonical form of the BQGC to study particle creation inside the cavity and transmissivity of the channel. In Sec. IV, we employ the channel to study the effect of relativity on the (2,3)-threshold continuous-variable quantum secret sharing for different collaboration scenarios and also for different quantum Gaussian secret states. Finally, in Sec. V, we discuss our results and provide future lines of research. Throughout this paper, we use units in which $c = \hbar = 1$.

II. BACKGROUND

In this section, we briefly review the effect of acceleration on the evolution of a quantum field inside a cavity, which is a well-studied topic (we refer the interested reader for more details to [10]). We focus on a simple trajectory which is known in the literature as the basic building block (BBB), since it enables studying any arbitrary nonuniform trajectory [10]. As depicted in Fig. 1, the BBB employs three steps. Initially, in region I, the cavity is at rest. Then, it accelerates for some time in region II and finally, in region III, it goes back to being inertial again. We note that, for the cavity to remain rigid,[1] different parts of it need to accelerate at different rates [10] (as shown in Fig. 1).

The inertial to uniformly accelerated transition can be modeled as a unitary linear transformation of the mode operators [10]. As there is a unique correspondence between any such unitary and a symplectic transformation on the phase space [20], we represent the transformation of the quantum field inside the cavity from region I to region II
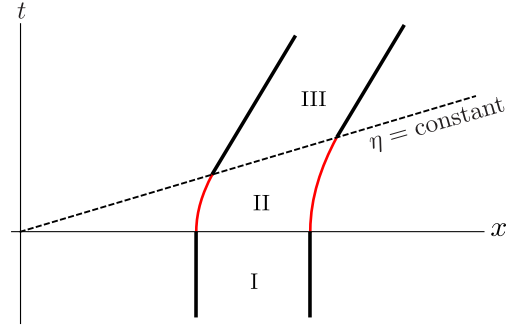

FIG. 1. Basic Building block for an arbitrary trajectory. The world lines of the left and right walls of the cavity are depicted. In region I, the cavity is inertial. In region II, the two walls of the cavity are accelerating with two different proper accelerations until the Rindler coordinate time $\eta = \frac{\tau}{a}$, where τ and a are proper time and acceleration respectively. In region III, the cavities have stopped accelerating and are back in the inertial frame again. The hyperbolas (red curves) represent the trajectories of the cavity walls moving with constant proper acceleration, and the (black) straight lines correspond to the trajectories of the walls while they move inertially.

by the symplectic transformation, $S_{\mathrm{I,II}}$. A symplectic transformation is a transformation that preserves the symplectic form; i.e.,

$$S \Gamma S^T = \Gamma; \qquad \Gamma := \bigoplus_i \Gamma_i, \qquad \Gamma_i := \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}. \quad (1)$$

Such a transformation preserves the bosonic canonical commutation relations of canonical variables [21]; i.e.,

$$[X_i, X_j] = i \Gamma_{ij}, \qquad (2)$$

where $X := (\hat{q}_1, \hat{p}_1, \hat{q}_2, \hat{p}_2, \ldots, \hat{q}_n, \hat{p}_n)$ and the quadrature operators are $\hat{q}_i := (\hat{a}_i + \hat{a}_i^\dagger)/\sqrt{2}$ and $\hat{p}_i := (\hat{a}_i - \hat{a}_i^\dagger)/i\sqrt{2}$.

Consider a massless scalar field in a cavity with Dirichlet boundary conditions; i.e., the field vanishes at the two cavity walls.[2] Two complete orthonormal sets of mode functions $\{\phi_n\}$ and $\{\psi_n\}$ can be used to expand the quantum field in regions I and II, respectively. These two sets of mode functions and their corresponding ladder operators are related via a Bogoliubov transformation as

$$\psi_j = \sum_i \tilde{\alpha}_{ij} \phi_i + \tilde{\beta}_{ij} \phi_i^*,$$

$$\hat{b}_j = \sum_i \tilde{\alpha}_{ij}^* \hat{a}_i - \tilde{\beta}_{ij}^* \hat{a}_i^\dagger, \qquad (3)$$

where $\tilde{\alpha}_{ij} := (\psi_i, \phi_j)$ and $\tilde{\beta}_{ij} := -(\psi_i, \phi_j^*)$ are the (Minkowski-to-Rindler) Bogoliubov coefficients and $(\cdot, \cdot)$

---

[1]The cavity motion is constructed so that the cavity remains rigid. This is in the sense that a comoving observer sees the cavity walls at a constant proper distance at all times.

[2]Our analyses can also be performed with Dirac spinor and Maxwell fields and with other boundary conditions such as Neumann boundary conditions [22].

represents the Klein-Gordon inner product [23]. The transformation $S_{\text{I,II}}$ in the quadrature basis is

$$S_{\text{I,II}} = \begin{bmatrix} \tilde{M}_{11} & \tilde{M}_{12} & \tilde{M}_{13} & \cdots \\ \tilde{M}_{21} & \tilde{M}_{22} & \tilde{M}_{23} & \cdots \\ \tilde{M}_{31} & \tilde{M}_{32} & \tilde{M}_{33} & \cdots \\ \vdots & \vdots & \vdots & \ddots \end{bmatrix}, \qquad (4)$$

where

$$\tilde{M}_{ij} = \begin{bmatrix} \text{Re}(\tilde{\alpha}_{ij} - \tilde{\beta}_{ij}) & \text{Im}(\tilde{\alpha}_{ij} + \tilde{\beta}_{ij}) \\ -\text{Im}(\tilde{\alpha}_{ij} - \tilde{\beta}_{ij}) & \text{Re}(\tilde{\alpha}_{ij} + \tilde{\beta}_{ij}) \end{bmatrix}. \qquad (5)$$

We denote the free evolution of the field in region II by S_{II} which reads as $S_{\text{II}} = \bigoplus_j G_j$, where G_j is a rotation in phase space. The transformation from the accelerating frame back to the inertial frame is the inverse of $S_{\text{I,II}}$; $S_{\text{II,III}} = S_{\text{I,II}}^{-1}$. Hence, the full symplectic transformation representing the evolution of the field from region I to region III is

$$S = S_{\text{I,II}}^{-1} S_{\text{II}} S_{\text{I,II}} = \begin{bmatrix} M_{11} & M_{12} & M_{13} & \cdots \\ M_{21} & M_{22} & M_{23} & \cdots \\ M_{31} & M_{32} & M_{33} & \cdots \\ \vdots & \vdots & \vdots & \ddots \end{bmatrix}, \qquad (6)$$

where

$$M_{ij} = \begin{bmatrix} \text{Re}(\alpha_{ij} - \beta_{ij}) & \text{Im}(\alpha_{ij} + \beta_{ij}) \\ -\text{Im}(\alpha_{ij} - \beta_{ij}) & \text{Re}(\alpha_{ij} + \beta_{ij}) \end{bmatrix}. \qquad (7)$$

The Bogoliubov coefficients are calculated perturbatively in $h = aL$, where a is the proper acceleration at the center of the cavity and L is the cavity length, such that

$$\alpha_{ij} = \alpha_{ij}^{(0)} + \alpha_{ij}^{(1)} h + \alpha_{ij}^{(2)} h^2 + O(h^3),$$
$$\beta_{ij} = \beta_{ij}^{(0)} + \beta_{ij}^{(1)} h + \beta_{ij}^{(2)} h^2 + O(h^3). \qquad (8)$$

Also, from (1), one observes that the Bogoliubov identity holds; i.e.,

$$\sum_i |\alpha_{ij}|^2 - |\beta_{ij}|^2 = 1. \qquad (9)$$

These perturbative Bogoliubov coefficients were computed [9] and, in particular, if $(i + j)$ is even then $\alpha_{ij}^{(1)} = \beta_{ij}^{(1)} = 0$. Using the perturbative expansions of the Bogoliubov coefficients (8), for the zero- and second-order terms of (9) we get

$$|\alpha_{ij}^{(0)}|^2 = 1, \qquad (10a)$$

$$\text{Re}(\alpha_{jj}^{(0)*} \alpha_{jj}^{(2)}) + f_{\alpha,k} - f_{\beta,k} = 0, \qquad (10b)$$

where

$$f_{\alpha,k} := \frac{1}{2} \sum_{n \neq k} |\alpha_{nk}^{(1)}|^2, \qquad f_{\beta,k} := \frac{1}{2} \sum_{n \neq k} |\beta_{nk}^{(1)}|^2, \qquad (11)$$

and first-order terms are zero.[3] From (10a) we conclude that $\alpha_{ij}^{(0)} = \delta_{ij} e^{i\phi_j}$, where

$$\phi_j := 2\pi j u, \qquad u := \frac{h\tau}{4L \, \text{arc} \tan h(h/2)}. \qquad (12)$$

Here, ϕ_j is a phase that mode j picks up during the accelerating motion of the cavity for the proper time τ with respect to the center of the cavity [10], i.e., region II.

In this section, we reviewed the BBB for a cavity of size L which accelerates for some time with a fixed proper acceleration a with respect to the center of the cavity. We employed the symplectic nature of the transformation from the inertial frame to the accelerating frame to write the Bogoliubov identities up to second order. We derived relations (10) for the perturbative Bogoliubov coefficients which helps us simplify the expressions for the fidelity of quantum secret sharing in different scenarios.

III. METHODS

In this section, we employ the framework of Gaussian quantum information [20,24] to write the evolution of the quantum field inside the cavity in a BBB, as depicted in Fig. 1, as a Gaussian quantum channel. We use this channel, in Sec. IV, to study the effect of noninertial motion of the shares on the fidelity of the quantum secret sharing. Moreover, we characterize the canonical form of the channel and show that it is a thermal lossy channel. To this aim, we summarize the framework of Gaussian quantum channels.

Gaussian states are completely characterized by their first and second moments and, for an n-mode Gaussian state, these are

$$\boldsymbol{d} = (\langle X_1 \rangle, \langle X_2 \rangle, ..., \langle X_n \rangle), \qquad (13a)$$

$$\sigma_{ij} = \langle X_i X_j + X_j X_i \rangle - 2\langle X_i \rangle \langle X_j \rangle. \qquad (13b)$$

By definition, Gaussian channels are the subset of quantum channels that transform Gaussian states to Gaussian states. The most general form of a Gaussian channel $\mathcal{E}$ is

---

[3]The Bogoliubov identities in the perturbative regime are also obtained using the fact that the change of basis from region I to region III is a unitary operation on cavity modes [10].

expressed in terms of its action on the first and second moments of the input states as

$$d \overset{\mathcal{E}}{\mapsto} Md + \alpha, \tag{14a}$$

$$\sigma \overset{\mathcal{E}}{\mapsto} M\sigma M^T + N, \tag{14b}$$

where, for n-mode Gaussian channels, M and N are real $2n \times 2n$ matrices, $\alpha \in \mathbb{R}^{2n}$ is a displacement vector, and N is a symmetric matrix; i.e., $N = N^T$.

In Fig. 2, we have depicted the scenario wherein all the modes of the cavity are prepared in the vacuum state except mode k, which is prepared in a Gaussian state with first and second moments d_I and σ_I, respectively. First, the initial state of the cavity evolves through the symplectic transformation S and subsequently all the modes except mode k are traced out. As both the symplectic operation and the tracing operation preserve the Gaussianity of a quantum state, the BBB can be written as a Gaussian channel, which transforms the initial Gaussian state to another one as given in Eq. (13). Hence, using (4), the matrices M and N for mode k read as

$$M_{kk} = \begin{bmatrix} \mathrm{Re}(\alpha_{kk} - \beta_{kk}) & \mathrm{Im}(\alpha_{kk} + \beta_{kk}) \\ -\mathrm{Im}(\alpha_{kk} - \beta_{kk}) & \mathrm{Re}(\alpha_{kk} + \beta_{kk}) \end{bmatrix}, \tag{15a}$$

$$N_k = \sum_{n \neq k} M_{nk} M_{nk}^T. \tag{15b}$$

We are interested in the final quantum state up to third order in $h = aL$, which means that we only need the
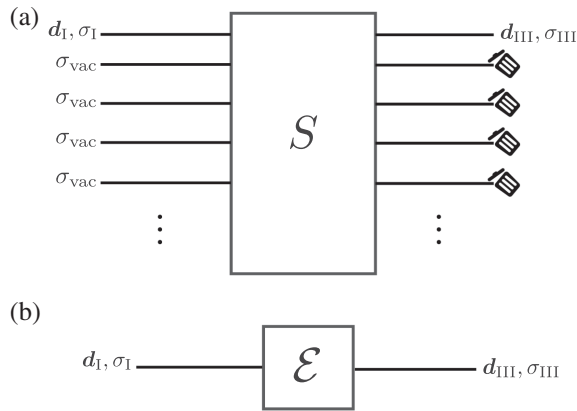

(a)

(b)

FIG. 2. (a) The BBB is depicted for the case wherein the first mode of the cavity is used to encode and decode quantum information. We assume all the other modes are initially prepared in vacuum and after the BBB (which is represented by the symplectic transformation S) the rest of the modes are ignored. (b) The operations performed in part (a) are all Gaussian operations which enables us to express the BBB as a Gaussian channel $\mathcal{E}$ acting on the first and second moments as given in Eq. (13).

matrices in Eq. (15) up to (but not including) third order in h; i.e.,

$$M_{kk} = M_{\phi_a}^{(0)} + M_{kk}^{(2)} h^2 + O(h^3),$$

$$N_k = N_k^{(2)} h^2 + O(h^3),$$

$$N_k^{(2)} = \sum_{n \neq k} M_{nk}^{(1)} M_{nk}^{(1)T},$$

$$M_{\phi_a}^{(0)} = \begin{bmatrix} \cos\phi_a & \sin\phi_a \\ -\sin\phi_a & \cos\phi_a \end{bmatrix},$$

$$M_{nk}^{(0)} = M_{kk}^{(1)} = 0 (n \neq k),$$

$$M_{nk}^{(i)} = \begin{bmatrix} \mathrm{Re}(\alpha_{nk}^{(i)} - \beta_{nk}^{(i)}) & \mathrm{Im}(\alpha_{nk}^{(i)} + \beta_{nk}^{(i)}) \\ -\mathrm{Im}(\alpha_{nk}^{(i)} - \beta_{nk}^{(i)}) & \mathrm{Re}(\alpha_{nk}^{(i)} + \beta_{nk}^{(i)}) \end{bmatrix}, \tag{16}$$

where in the last matrix $i = 1, 2$. We emphasize that as we are estimating the effect of the Gaussian channel up to third order in h, the term $M^{(2)} \sigma_I M^{(2)T}$ is to be ignored.

As was pointed out by Holevo [25], any Gaussian quantum channel can be decomposed into its canonical form and two Gaussian unitary operators; one on the input and one on the output. This means that we can decompose the Gaussian channel for the BBB as shown in Fig. 3. Here, S_I and S_{III} are two symplectic transformations in the regions I and III, which correspond to the two Gaussian unitary operators. We use M_c and N_c for the canonical form of the channel, $\mathcal{E}_c$, as opposed to the channel $\mathcal{E}$ for which we have used M and N.

In transforming a Gaussian quantum channel $\mathcal{E}$ to its canonical form $\mathcal{E}_c$, some properties of the channel remain invariant (up to symplectic transformations S_I and S_{III}). The first invariant is $r := \min[\mathrm{rank}(M), \mathrm{rank}(N)]$ which, for a single-mode channel, can take the possible values $r = 0$, 1,–2 and in our case we have $r = 2$. The second invariant is the *transmissivity* of the channel,

$$T = \det M = 1 - T^{(2)} h^2 + O(h^3), \tag{17}$$

where

$$T^{(2)} := 2(f_{\alpha,k} - f_{\beta,k}).$$

Note that, as $T^{(2)}$ increases, the transmissivity decreases. In Fig. 4, we plot $T^{(2)}$ as a function of u, where we observe
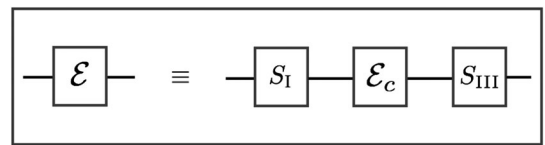

FIG. 3. The canonical form of the BBB Gaussian channel, $\mathcal{E}$, which is decomposed into its canonical form, $\mathcal{E}_c$, up to two symplectic transformations in regions I and III, i.e., S_I and S_{III}.
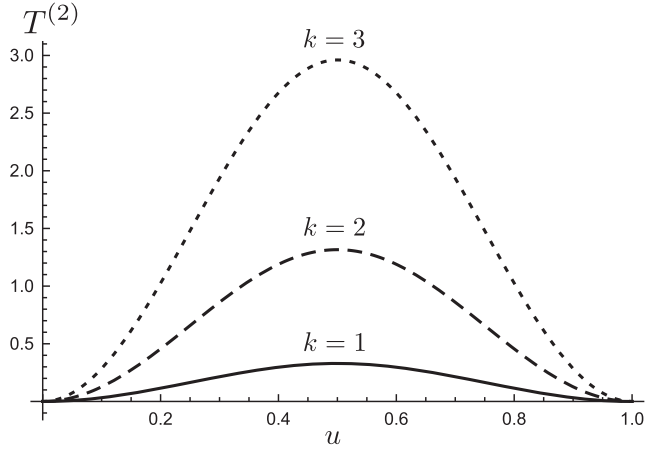
FIG. 4. The second-order coefficient of the transmissivity of the BBB channel, $T^{(2)}$, as a function of u for modes $k = 1, 2, 3$.

that by increasing the mode number k the transmissivity of the channel decreases. Here we choose to plot all the quantities in terms of u, as the Bogoliubov coefficients for a BBB are periodic in u with the period of 1.

The final invariant is thermal number $\bar{n}$ associated to the canonical form of the quantum channel E. We calculate the leading order term of $\bar{n}$, which is

$$\bar{n} := \frac{\sqrt{\det N}}{2|1-T|} - \frac{1}{2} = \frac{\sqrt{(f_{\alpha,k} + f_{\beta,k})^2 - 4|g_{\alpha\beta,k}|^2}}{2(f_{\alpha,k} - f_{\beta,k})} - \frac{1}{2}, \quad (18)$$

where $g_{\alpha\beta,k} := \sum_{n \neq k} \alpha_{nk}^{(1)} \beta_{nk}^{(1)}$. In Fig. 5, we plot this quantity as a function of u.

The main advantage in working with the canonical form of the BBB channel is that we can completely characterize it. For the symplectic invariants we find $T \in (0,1)$ and $r = 2$, from which we can conclude that the canonical form of the BBB channel is a thermal lossy Gaussian channel. The channel is lossy due to the fact that its transmissivity is
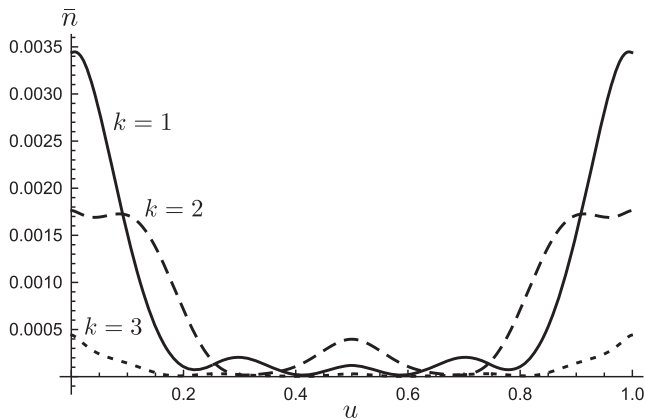

FIG. 5. The average number of thermal particles as a function of u for modes $k = 1, 2, 3$.

smaller than one; i.e., $T < 1$. Furthermore, from this analysis, we conclude that the quantum channel $\mathcal{E}_c$ can be simulated by interacting mode k of the cavity and a thermal state with mean photon number $\bar{n}$ via a beam splitter of transmittance T.

In this section, we employed the framework of Gaussian channels to find matrices M and N in (14) for a BBB. From this point on, we use them to include the effect of relativity on the quantum field inside a cavity while the cavity moves noninertially. Moreover, we computed the channel invariants, transmissivity, and the average number of thermal particles, which enabled us to identify the BBB as a thermal lossy channel.

IV. THE RELATIVISTIC PROTOCOL

In this section, we present the relativistic variant of (2,3)-threshold continuous-variable quantum secret sharing. We first include the effect of acceleration on the distribution of quantum shares and then we consider different possible collaboration scenarios between the players. In each case, we show that the fidelity of quantum secret sharing is reduced, except for a thermal state, when compared to the nonrelativistic scenarios.

A. Distribution of quantum shares

In our case, modes 1, 2, and 3 are three quantum Gaussian shares and each mode corresponds to a mode in a cavity. The Gaussian state of each quantum share occupies one mode inside each cavity, and the other modes inside each cavity are all in vacuum states. Figure 6 shows the encoding protocol of a (2,3)-threshold quantum secret sharing scheme as proposed by Tyc and Sanders [3]. The dealer encodes the quantum secret into a three-mode Gaussian state, i.e., modes 1, 2, and 3. He prepares modes 2 and 3 in a two-mode squeezed-vacuum state, with the squeezing parameter, s. Then, he combines modes 1 (the quantum secret) and 2 on a balanced beam splitter. The two output beams of the beam splitter, together with the third beam encoding the other half of the two-mode squeezed
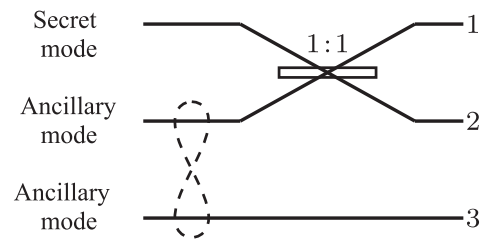

FIG. 6. The encoding circuit for continuous-variable (2,3)-threshold quantum secret sharing. The "8" shaped symbol represents a two-mode squeezed-vacuum state. The upper two modes are combined on a balanced beam splitter. The three outputs are three quantum shares, denoted by mode 1, mode 2, and mode 3.
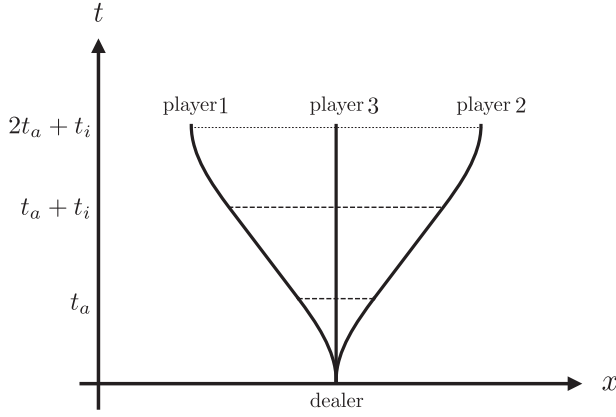
FIG. 7.   The worldlines of the quantum shares during distribution. From $t = 0$ to $t = t_a$, the two cavities, represented by the furthest left and the furthest right worldlines, accelerate with the proper acceleration a in two opposite directions. From $t = t_a$ to $t = t_a + t_i$, they move with constant velocities. From $t = t_a + t_i$ to $t = 2t_a + t_i$, the two cavities decelerate with the proper acceleration a and become stationary. The cavity represented by the middle world line remains static.

state, are the three quantum shares, which are distributed to the three players.

After encoding, the dealer distributes the three cavities to the three players. Figure 7 shows the distribution of the quantum shares. The three players are located at different spacetime points. One player (player 3) is at the same spatial position as the dealer and the other two players (players 1 and 2) have the same distance to the dealer.[4] The dealer and three players are all static, so they share an inertial frame. As depicted in Fig. 7, cavities 1 and 3 inevitably need to be accelerated and then decelerated to reach the spacetime regions of players 1 and 3, respectively. Using the quantum channel derived in Sec. III, we consider the effect of such a nonuniform motion of the cavities on the quantum share, which is encoded in a single mode of each cavity. In this scenario, cavity 3 remains static during the whole distribution.

B. Players' collaboration

After the quantum shares are distributed between the three players, two of them need to collaborate to decode the quantum secret. Three different scenarios are possible; players 1 and 3, 2 and 3, or 1 and 2 can constitute the subset of collaborating players. The effect of acceleration on the fidelity of quantum secret sharing in the latter two cases is the same (due to the present symmetry), and we only consider the scenario wherein players 2 and 3 collaborate.

---

[4]To simplify the calculations, we have chosen the symmetric configuration of the players and the dealer, Fig. 7, which suffices to study the relativistic effects in the distribution stage.
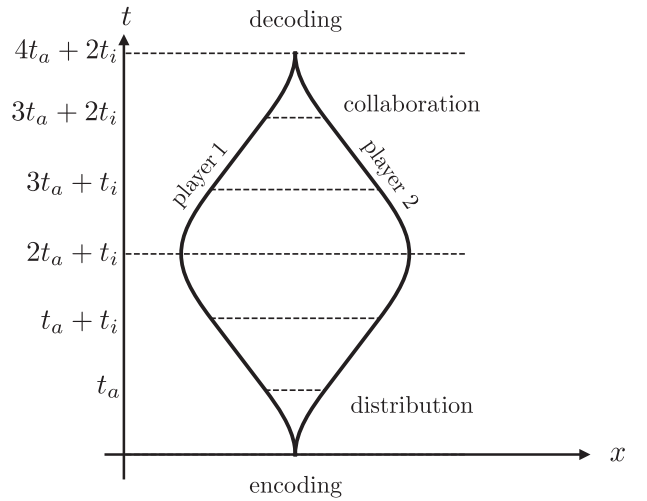

FIG. 8.   The two curves represent two worldlines in spacetime. Each worldline is the trajectory of one cavity carrying a quantum share. From $t = 2t_a + t_i$ to $t = 3t_a + t_i$, the two cavities accelerate with proper acceleration a towards each other. From $t = 3t_a + t_i$ to $t = 3t_a + 2t_i$, the two cavities are moving with constant velocity. From $t = 3t_a + 2t_i$ to $t = 4t_a + 2t_i$, the two cavities decelerate with proper acceleration a to arrive at the same spacetime point.

1. Collaboration between players 1 and 2

First, we consider the case wherein players 1 and 2 are collaborating. To decode the quantum secret, their cavities are transported to the same spacetime point as shown in Fig. 8. After the two cavities are at the same region, the quantum secret is decoded by beam splitting the two modes that were employed to encode the quantum secret. From $t = 2t_a + t_i$ to $t = 4t_a + 2t_i$, each mode of the two-mode Gaussian state goes through the same single-mode Gaussian channel $\mathcal{E}_1$ as shown in Fig. 9.

The Gaussian quantum channel $\mathcal{E}_1$ is composed of five Gaussian channels in series [See Fig. 9(b)]. The channel $\mathcal{E}(\tau_a)$ corresponds to uniformly accelerated motion of the cavity to the left (or to the right) during the proper time τ_a, while the channel $\mathcal{E}(2\tau_a)$ represents the cavity moving with constant proper acceleration to the right (or to the left) during the proper time $2\tau_a$. Also, the quantum channel $G(\tau_i)$ corresponds to the inertial movement of the cavity with constant velocity for the proper time τ_i. Using (16), the first and second moments of the kth mode of the cavity, up to third order in h, are transformed as

$$\boldsymbol{d} \overset{\mathcal{E}(\tau_a)}{\mapsto} (M_{\phi_a}^{(0)} + M_{kk}^{(2)}h^2)\boldsymbol{d}, \tag{19a}$$

$$\sigma \overset{\mathcal{E}(\tau_a)}{\mapsto} M_{\phi_a}^{(0)}\sigma M_{\phi_a}^{(0)T} + (M_{\phi_a}^{(0)}\sigma M_{kk}^{(2)T} + M_{kk}^{(2)}\sigma M_{\phi_a}^{(0)T})h^2$$
$$+ N_k^{(2)}h^2, \tag{19b}$$

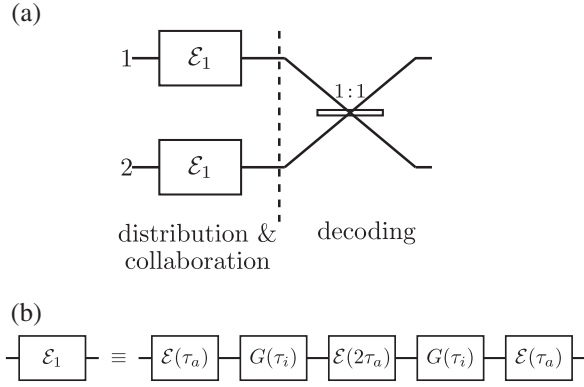where $M_{\phi_a}^{(0)}$, $M_{kk}^{(2)}$, and $N_k^{(2)}$ are given in (16).

(a)

(b)

FIG. 9. (a) The thermal lossy channel $\mathcal{E}_1$ is the Gaussian channel that represents the total evolution of the first and the second quantum shares during the distribution and the collaboration stage. Then the quantum secret is decoded using a balanced beam splitter. (b) $\mathcal{E}_1$ is a single-mode Gaussian channel composed of five Gaussian channels in series. $\mathcal{E}(\tau_a)$ is the Gaussian channel for a BBB during the proper time τ_a and $G(\tau_i)$ represents the Gaussian channel of the free evolution in an inertial frame with proper time τ_i.

The Gaussian channel $G(\tau_i)$ represents the free evolution of the Gaussian state during the inertial movement of the cavity in proper time τ_i,

$$d \overset{G(\tau_i)}{\mapsto} M^{(0)}_{\phi_i} d, \tag{20a}$$

$$\sigma \overset{G(\tau_i)}{\mapsto} M^{(0)}_{\phi_i} \sigma M^{(0)T}_{\phi_i}, \tag{20b}$$

where

$$M^{(0)}_{\phi_i} = \begin{bmatrix} \cos\phi_i & -\sin\phi_i \\ \sin\phi_i & \cos\phi_i \end{bmatrix},$$

and $\phi_i = \frac{k\pi\tau_i}{L}$ is the phase accumulated during the free evolution from $t = t_a$ to $t = t_a + t_i$, and from $t = 3t_a + t_i$ to $t = 3t_a + 2t_i$. To simplify the later calculations, we suppose the phase shift during the inertial movement is $\phi_i = \pi - 2\phi_a$.

Therefore, we can express the collaboration between players 1 and 3, shown in Fig. 8, as the Gaussian channel $\mathcal{E}_1$,

$$\mathcal{E}_1 := \mathcal{E}(\tau_a) \circ G(\tau_i) \circ \mathcal{E}(2\tau_a) \circ G(\tau_i) \circ \mathcal{E}(\tau_a). \tag{21}$$

If the secret Gaussian state is a coherent state and the free evolution is ignored; i.e., $M^{(0)} = \mathbb{I}$, the Gaussian transformation of the channel $\mathcal{E}_1$ for the mode k is

$$d \overset{\mathcal{E}_1}{\mapsto} d + (2M^{(2)}_{kk,\tau_a} + M^{(2)}_{kk,2\tau_a})h^2 d, \tag{22a}$$

$$\mathbb{I} \overset{\mathcal{E}_1}{\mapsto} \mathbb{I} + (2M^{(2)}_{kk,\tau_a} + 2M^{(2)T}_{kk,\tau_a} + M^{(2)}_{kk,2\tau_a} + M^{(2)T}_{kk,2\tau_a}$$
$$+ 2N^{(2)}_{k,\tau_a} + N^{(2)}_{k,2\tau_a})h^2, \tag{22b}$$

where $M^{(2)}_{kk,\tau_a}$ and $N^{(2)}_{k,\tau_a}$ are in terms of proper time τ_a.
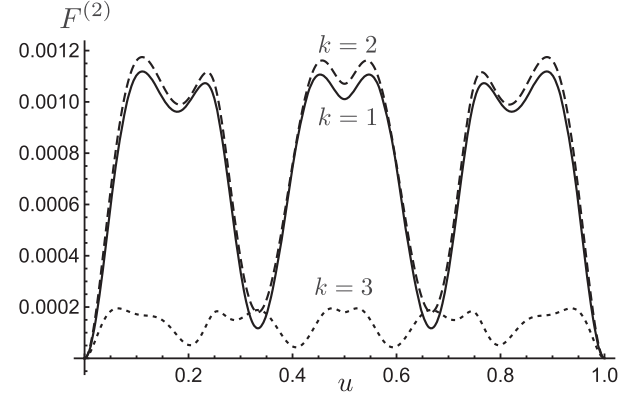

FIG. 10. $F^{(2)}$ as a function of u for modes $k = 1$ (solid), 2 (dashed), and 3 (dotted) when the secret Gaussian state is a coherent state.

After the two cavities arrive at the same spacetime region, the two Gaussian quantum shares are combined using a balanced beam splitter, as shown in Fig. 9. The decoded Gaussian quantum secret is not a pure state anymore due to the effect of acceleration during distribution and collaboration. For a coherent state as the encoded secret Gaussian state, we calculate the fidelity of the quantum secret sharing [1,4]

$$F = 1 - 2(2f_{\beta,k,2u} + f_{\beta,k,u})h^2 + O(h^3). \tag{23}$$

In Fig. 10, we plot the second-order coefficient of the fidelity for a coherent state as the quantum secret and we compare the decrease in the fidelity of quantum secret sharing for $k = 1$, 2, and 3. Interestingly, from (23), we conclude that the fidelity for a coherent state is independent of the initial mean photon number of the quantum secret. In other words, the fidelity of a coherent state is the same as the fidelity of the vacuum state.

In Fig. 11, we have plotted the second-order coefficient of the fidelity, $F^{(2)}$, for a squeezed-vacuum quantum secret; i.e., $F = 1 - F^{(2)}h^2$. The figure shows that the fidelity
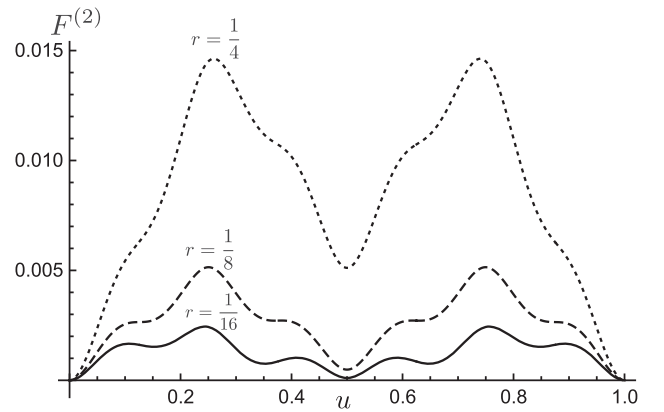

FIG. 11. $F^{(2)}$ as a function of u for the ground mode ($k = 1$), when the secret Gaussian state is a squeezed-vacuum state for squeezing parameters $r = \frac{1}{16}$ (solid), $\frac{1}{8}$ (dashed), and $\frac{1}{4}$ (dotted).
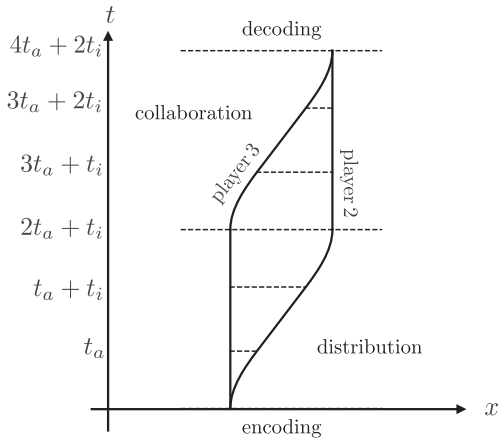
FIG. 12. The two curves represent two worldlines in spacetime. The left worldline is the trajectory of the cavity carrying the third quantum share and the right worldline is the trajectory of the cavity carrying the second quantum share. From $t = 2t_a + t_i$ to $t = 4t_a + 2t_i$, the third cavity remains static. From $t = 2t_a + t_i$ to $t = 3t_a + t_i$, the second cavity accelerates with proper acceleration a. From $t = 3t_a + t_i$ to $t = 3t_a + 2t_i$, it moves with constant velocity and from $t = 3t_a + 2t_i$ to $t = 4t_a + 2t_i$, decelerates with proper acceleration a.

decreases as the squeezing parameter r increases, i.e., as the mean photon number in the secret increases. This is in contrast to the case where the secret state is a coherent state.

2. Collaboration between players 2 and 3

The second collaboration scenario we consider is the case wherein players 2 and 3 collaborate to reconstruct the secret quantum state.[5] Similar to the previous case, the quantum shares of players 2 and 3 are first transported to the same spacetime region. Figure 12 shows the trajectories of the two corresponding cavities in this scenario. Note that the trajectory of the second cavity during the collaboration stage is the same as the trajectory of the third cavity during the distribution stage of the protocol. As Fig. 13 shows, the second quantum share goes through the channel $\mathcal{E}_2$ during distribution, while it goes through the channel $G(2t_a + t_i)$ during collaboration. The third quantum share first goes through the channel $G(2t_a + t_i)$ when the shares are being distributed and then is affected by the channel $\mathcal{E}_2$, which represents the effect of acceleration on this quantum share during collaboration.

As shown in Fig. 13, the quantum Gaussian channel $\mathcal{E}_2$ is a combination of three quantum Gaussian channels, one of which is merely a phase rotation, i.e., $G(\tau_i)$. Assuming the input state of the Gaussian channel $\mathcal{E}_2$ is a coherent state and the free evolution is ignored, then the transformation of

---

[5]We emphasize that the collaboration between players 1 and 2 results in the same results for the fidelity of the quantum secret sharing, which is simply due to the symmetry in the configuration of the players.
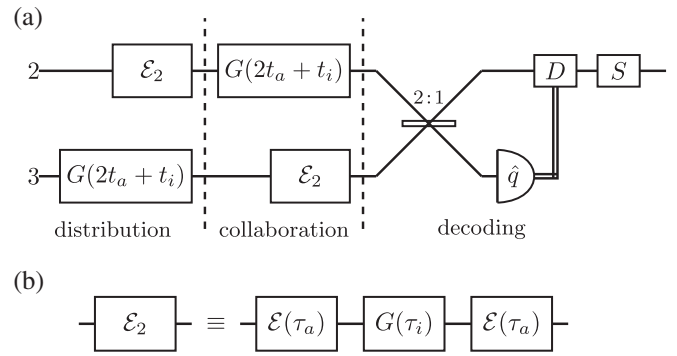

FIG. 13. (a) The decoding circuit for the case wherein players 2 and 3 collaborate. $\mathcal{E}_2$ is a Gaussian thermal lossy channel. $G(2t_a + t_i)$ is the free evolution in the inertial frame. First, the two modes are combined on a beam splitter with reflectivity 2/3. Then the quadrature $\hat{q}$ of the second output mode is measured and a displacement operation controlled by the measurement outcome and a squeezing operation are applied on the first output mode. (b) $\mathcal{E}_2$ is a single-mode Gaussian channel composed of three Gaussian channels in series.

the first and second moments due to the channel $\mathcal{E}_2$ can be written as

$$\boldsymbol{d} \overset{\mathcal{E}_2}{\mapsto} (\mathbb{1} + 2M^{(2)}_{kk}h^2)\boldsymbol{d}, \tag{24a}$$

$$\mathbb{1} \overset{\mathcal{E}_2}{\mapsto} \mathbb{1} + 2(M^{(2)}_{kk} + M^{(2)T}_{kk} + N^{(2)}_k)h^2. \tag{24b}$$

After the second and the third quantum shares reach the same spacetime region, the decoding of the quantum secret begins. For decoding, we employ the procedure introduced in [1,4]. The optical decoding circuit is shown in Fig. 13, which is applied to reconstruct the secret quantum Gaussian state. We calculate the fidelity of quantum secret sharing in this case up to third order; i.e.,

$$F = F^{(0)} - F^{(2)}h^2 + O(h^3), \tag{25}$$

where $F^{(0)}$ and $F^{(2)}$ are

$$F^{(0)} = \frac{1}{1 + e^{-s}},$$
$$F^{(2)} = \frac{4e^s}{(1 + e^s)^2}[f_{\beta,k} - f_{\alpha,k} + e^s(f_{\alpha,k} + 2f_{\beta,k})]. \tag{26}$$

In Fig. 14, we plotted the second-order coefficient of the fidelity $F^{(2)}$ as a function of u for $k = 1, 2, 3$. We observe from this figure that as the mode number k increases, the fidelity decreases, which suggests that the optimal mode for encoding the quantum secret is $k = 1$.

In the limit $s \to \infty$, the fidelity up to third order is

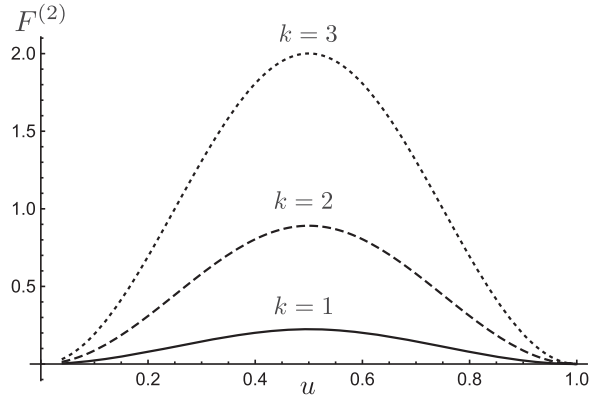$$F = 1 - 4(f_{\alpha,k} + 2f_{\beta,k})h^2 + O(h^3). \tag{27}$$

FIG. 14. $F^{(2)}$ as a function of u for modes $k = 1$ (solid), 2 (dashed), and 3 (dotted) when the two-mode squeezing parameter, $s = 1$.

Hence, in the limit of infinite squeezing and in the absence of acceleration ($h = 0$), fidelity is one. However, for nonzero acceleration, fidelity is always smaller than one, even if a maximally entangled state is employed to encode the quantum secret.

V. CONCLUSIONS AND DISCUSSIONS

Here we study the effect of relativistic motion on (2,3)-threshold quantum Gaussian secret sharing. In our scheme, the dealer employs a single mode of a cavity to encode each quantum share. We begin by fully characterizing the BBB as a quantum Gaussian channel. We find that the canonical form of this channel is a thermal lossy channel. This form of the channel is useful for studying relativistic effects in quantum-information-processing tasks.

We consider different possible collaboration scenarios between different subsets of players and analyze how each scenario can be written as a composition of quantum Gaussian channels. We find that the decoherence, due to the relativistic motion of the quantum shares during distribution and also collaboration, reduces the fidelity of quantum secret sharing.

Interestingly, we observe in the scenario wherein players 1 and 2 are collaborating, depicted in Fig. 8, the fidelity is independent of the initial mean photon number in the encoded secret. Hence, in this case, the fidelity for a coherent state is the same as that of a vacuum state. Moreover, in the second scenario, Fig. 12, we find that when the quantum secret is a coherent state (or a vacuum state), the best encoding strategy is to encode the quantum secret in the ground mode of the cavity. We observe that the fidelity of the protocol is smaller than one, even in the limit of infinite squeezing, i.e., when maximal entanglement is used as a resource [see Eq. (27)].

As a future line of research, we are interested in extending our results to the more general case of (k, n)-threshold quantum secret sharing. Furthermore, our hope is that the methods developed here can be employed to relax the conditions on the spacetime replication of quantum states [26,27], i.e., to consider the effect of nonuniform motion on this task.

[1] A. M. Lance, T. Symul, W. P. Bowen, B. C. Sanders, and P. K. Lam, Phys. Rev. Lett. **92**, 177903 (2004).

[2] J. Niset, J. Fiurášek, and N. J. Cerf, Phys. Rev. Lett. **102**, 120501 (2009).

[3] T. Tyc and B. C. Sanders, Phys. Rev. A **65**, 042310 (2002).

[4] A. M. Lance, T. Symul, W. P. Bowen, T. Tyc, B. C. Sanders, and P. K. Lam, New J. Phys. **5**, 4 (2003).

[5] T. Tyc, D. J. Rowe, and B. C. Sanders, J. Phys. A **36**, 7625 (2003).

[6] I. Kogias, Y. Xiang, Q. He, and G. Adesso, Phys. Rev. A **95**, 012315 (2017).

[7] D. Markham and B. C. Sanders, Phys. Rev. A **78**, 042309 (2008).

[8] R. Cleve, D. Gottesman, and H.-K. Lo, Phys. Rev. Lett. **83**, 648 (1999).

[9] D. E. Bruschi, I. Fuentes, and J. Louko, Phys. Rev. D **85**, 061701 (2012).

[10] N. Friis, Ph.D. thesis, University of Nottingham, 2013, arXiv:1311.3536.

[11] A. Dragan, J. Doukas, and E. Martín-Martínez, Phys. Rev. A **87**, 052326 (2013).

[12] A. Dragan, J. Doukas, E. Martín-Martínez, and D. E. Bruschi, Classical Quantum Gravity **30**, 235006 (2013).

[13] M. Ahmadi, K. Lorek, A. Chęcińska, A. R. H. Smith, R. B. Mann, and A. Dragan, Phys. Rev. D **93**, 124031 (2016).

[14] B. Richter, K. Lorek, A. Dragan, and Y. Omar, Phys. Rev. D **95**, 076004 (2017).

[15] T. G. Downes, T. C. Ralph, and N. Walk, Phys. Rev. A **87**, 012327 (2013).

[16] J. Lindkvist, C. Sabín, I. Fuentes, A. Dragan, I.-M. Svensson, P. Delsing, and G. Johansson, Phys. Rev. A **90**, 052113 (2014).

[17] N. Friis, A. R. Lee, K. Truong, C. Sabín, E. Solano, G. Johansson, and I. Fuentes, Phys. Rev. Lett. **110**, 113602 (2013).

[18] M. Ahmadi, D. E. Bruschi, C. Sabín, G. Adesso, and I. Fuentes, Sci. Rep. **4**, 4996 (2014).

[19] M. Ahmadi, D. E. Bruschi, and I. Fuentes, Phys. Rev. D **89**, 065028 (2014).

[20] G. Adesso, S. Ragy, and A. R. Lee, Open Syst. Inf. Dyn. **21**, 1440001 (2014).

[21] Arvind, B. Dutta, N. Mukunda, and R. Simon, Pramana J. Phys. **45**, 471 (1995).

[22] N. Friis, A. R. Lee, and J. Louko, Phys. Rev. D **88**, 064028 (2013).

[23] N. D. Birrell and P. C. W. Davies, *Quantum Fields in Curved Space*, Cambridge Monographs on Mathematical Physics (Cambridge University Press, Cambridge, 1982).

[24] C. Weedbrook, S. Pirandola, R. García-Patrón, N. J. Cerf, T. C. Ralph, J. H. Shapiro, and S. Lloyd, Rev. Mod. Phys. **84**, 621 (2012).

[25] A. S. Holevo, Probl. Inf. Transm. **43**, 1 (2007).

[26] P. Hayden, S. Nezami, G. Salton, and B. C. Sanders, New J. Phys. **18**, 083043 (2016).

[27] P. Hayden and A. May, J. Phys. A **49**, 175304 (2016).