Multiuser quantum key distribution using quotient graph states derived from continuous-variable dual-rail cluster states

Akash nag Oruganti*
Department of Optics, Palacký University, Olomouc 77146, Czech Republic

(Received 19 December 2024; revised 6 August 2025; accepted 24 September 2025; published 17 November 2025)

Multipartite entangled states are essential for multiuser quantum cryptography. While large-scale continuous-variable (CV) cluster states, particularly the dual-rail cluster state, have been well studied in measurement-based quantum computation, their cryptographic potential remains underexplored. Here, we propose a three-user conference key protocol using a CV dual-rail cluster state. By applying a node-coloring scheme to the infinite dual-rail graph, we create a six-mode pure graph state ideal for cryptographic tasks. Our results demonstrate near-GHZ (Greenberger-Horne-Zeilinger) performance for quantum conference key agreement (QCKA). Crucially, our protocol uniquely enables bipartite keys post-QCKA, which GHZ states cannot provide. It also surpasses two-mode squeezed vacuum states in generating bipartite keys within downstream-access networks. Considering finite-size effects and impure squeezed states, our scheme remains robust despite experimental imperfections. We also introduce an enhanced method to more accurately estimate bipartite key generation capacity in quantum networks, paving the way for practical multiuser quantum cryptography.

DOI: 10.1103/vsqj-ndkn

I. INTRODUCTION

Multipartite entangled states are essential resources for various multiuser quantum cryptographic tasks, such as quantum voting [1–3], quantum secret sharing [4–6], multipartite quantum direct communication [7,8], and quantum conference key agreement (QCKA) [9,10], among others. These tasks leverage the unique properties of entanglement to enable secure and efficient communication protocols in quantum networks.

In the realm of continuous-variable (CV) quantum systems, the development and application of multipartite entangled states have predominantly focused on measurement-based quantum computation, particularly using cluster states [11–15]. Despite significant technological advances in the generation of large-scale CV cluster states, especially the dual-rail cluster state, these resources have not been thoroughly explored for quantum cryptographic applications. This gap is notable given the experimental maturity achieved in creating such states through techniques like time-domain [16–19] and frequency-domain multiplexing [20–23].

In discrete-variable (DV) systems, GHZ (Greenberger-Horne-Zeilinger) and W states have been identified as ideal resources for QCKA [9,24]. In CV systems, GHZ and W states are effectively equivalent, both represented by fully symmetric multimode squeezed states [25]. However, it remains uncertain whether these CV equivalents, produced with finite squeezing, are the most suitable multipartite states for QCKA. Unlike DV systems, CV systems offer unique advantages, such as the ability to utilize conditional data post-QCKA to derive additional bipartite keys. This multifaceted use of data enhances the efficiency and security of quantum communication protocols, a feature we explore extensively in this work.

In this paper, we address this gap by introducing a novel protocol for generating a three-user conference key using a CV dual-rail cluster state. To enable its application in QCKA, we introduce the concept of a quotient graph state, employing a node-coloring scheme on the infinite dual-rail graph. By forming the quotient graph through vertex identification based on this coloring, we obtain a six-vertex graph representing a pure six-mode graph state. This concept is new and provides a method for state engineering tailored for quantum communication applications, leveraging the properties of the dual-rail cluster state.

The underlying concept of a "quotient graph" is a well-established tool in graph theory [26] used to simplify complex graphs by partitioning vertices. This technique has found applications in quantum mechanics for studying symmetries in quantum graphs [27–29]. Our work extends this principle to a new domain: We apply the quotienting procedure not merely for analysis, but as a constructive method to engineer a target multipartite entangled state from a larger, periodic resource state. This approach retains

*Contact author: akash.nag.10@gmail.com

Published by the American Physical Society under the terms of the Creative Commons Attribution 4.0 International license. Further distribution of this work must maintain attribution to the author(s) and the published article's title, journal citation, and DOI.

the essential entanglement and connectivity properties required for cryptographic protocols.

We investigate three schemes for generating QCKA in a three-user network. (i) *Direct reconciliation:* The dealer (the one who generates the multipartite state) performs a measurement on one or more modes of the multipartite state, and the outcome is used as the reference to generate the conference key. (ii) *Reverse reconciliation:* One of the remote user's measurements is used as the reference to generate the conference key. (iii) *Entanglement in the middle:* All modes are sent to the remote users without the dealer retaining any part of the state. Any remote user's measurement can serve as the reference, analogous to protocols where entanglement is distributed without a central party. After generating the conference key, the conditional measurement data can still be used to establish bipartite keys post-QCKA between the remaining users. Additionally, we consider generating bipartite keys directly between the dealer and the users without involving QCKA.

Our results demonstrate that the proposed protocol using the dual-rail cluster state and quotient graph state not only outperforms the GHZ/W states generated with the same level of squeezing for QCKA using direct reconciliation, achieving positive key generation under a wider range of channel conditions, but also significantly outperforms them for generating bipartite keys post-QCKA across all methods (direct reconciliation, reverse reconciliation, and entanglement in the middle). Moreover, when compared to a downstream access network utilizing two-mode squeezed vacuum states with equivalent squeezing, our protocol achieves superior performance in generating bipartite keys without involving QCKA.

Recognizing the importance of practical implementations, we extend our analysis to consider real-world conditions. We examine the performance of our protocol in the finite-size regime, which is crucial when the number of signals exchanged is limited. Our finite-size analysis provides insights into the key rates achievable under realistic conditions, accounting for statistical fluctuations due to finite sample sizes.

Additionally, we consider the impact of using impure squeezed states for generating the multipartite entangled states. In practical scenarios, experimental imperfections lead to squeezed states that are not perfectly pure [30], affecting the overall performance of quantum protocols. By incorporating impure squeezed states into our analysis, we provide a more realistic assessment of our protocol's robustness against imperfections in state preparation.

This study highlights the importance of quotient graph states in CV quantum systems for state engineering in quantum networks, offering improved key rates and robustness against losses, noise, and experimental imperfections. We also introduce a more accurate method for estimating bipartite key rates in a downstream-access network (DAN), enhancing the evaluation of CV system's key generation capabilities.

This paper is structured as follows. In Sec. II, we delve into the complexities of classical information processing for multiple users. In Sec. III, we present the security analysis of a general multipartite state distributed among trusted users and provide their key rate expressions. In Sec. IV, we discuss the generation of various tripartite states from squeezed states, including the impact of impurity. In Sec. V, we introduce techniques for utilizing dual-rail cluster states in various cryptographic protocols. In Sec. VI, we introduce and analyze various multiuser cryptographic protocols. In Sec. VII, we summarize the major results of our analysis. Finally, in Sec. VIII, we review the outcomes of our research and discuss potential avenues for future work.

II. MULTIVARIATE GAUSSIAN CORRELATIONS AND MULTIUSER QUANTUM KEY DISTRIBUTION

This section simplifies the discussion of multivariate Gaussian correlations by focusing on three users, A, B, and C, although the principles discussed can be extended to larger networks. To analyze the interuser relationships and their implications for quantum key distribution (QKD), it is useful to classify the types of correlations that may occur. In the context of error correction and key generation, the structure of these correlations profoundly influences the strategies we must employ.

In what follows, we delineate three primary correlation scenarios that capture the essence of these interactions. These correlation scenarios are as follows.

Symmetric correlations:

All users share equal correlations. Any user can disclose error-correction information (syndrome) to enable the others to derive the same raw key, facilitating a shared conference key after privacy amplification.

Centralized correlations:

User A is more strongly correlated with users B and C than they are with each other, allowing for the following.

(1) *Conference key agreement (CKA).* User A shares the syndrome, enabling users B and C to establish a conference key.

(2) *Independent key generation.* Users B and C transmit their syndromes to A, allowing A to establish separate keys with each of them.

Induced correlations:

Initially uncorrelated users become correlated if a user or dealer, already correlated with them, shares the necessary syndrome for error correction.

Elaborating on the second and third scenarios, consider three users, specifically A, B, and C. A aims to generate

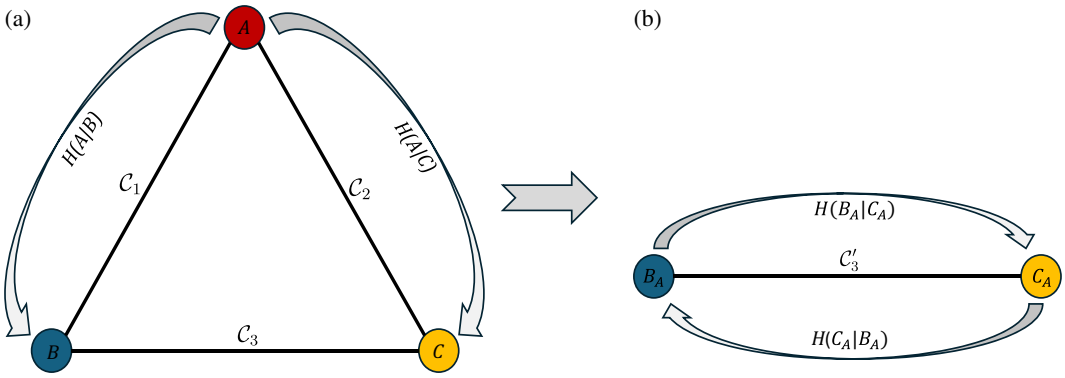


FIG. 1. (a) Information reconciliation for conference key agreement with user A as the reference. (b) Bipartite information reconciliation post-CKA.

a key with B and C, which can be accomplished through two separate techniques. The first technique requires A to convey the essential information for error correction to B and C. Conversely, B and C could forward the necessary information for error correction to A. In the initial scenario, the keys generated will be perfectly correlated as both B and C use the data possessed by A to generate a key. However, in the second scenario, the situation gets more complicated if B and C are correlated, resulting in a potential partial correlation of the keys. In the event of correlations, B and C cannot be treated separately, as the mutual information $I(A:B,C) \neq I(A:B)+I(A:C)$, but rather $I(A:B,C) = I(A:B)+I(A:C|B) = I(A:C)+I(A:B|C)$. The mutual information is defined as $I(i:j) = H(i) - H(i|j) = H(j) - H(j|i)$, and the conditional mutual information $I(i:j|k) = H(i|k) - H(i|j,k)$. Here, $H(\cdot)$ represents the Shannon entropy. When dealing with multiple correlated users, it becomes essential to ascertain the optimal syndrome length that needs to be transferred for successful error correction. In the given example, B and C must jointly transmit an amount of information quantified as $H(BC|A)$ to A. The restriction lies in the collective syndrome delivered by B and C. The individual syndromes of B, say S_B, and C, say S_C, can exceed in length, provided that $H(S_B,S_C) = H(BC|A)$.

When B and C exhibit no correlation, i.e., $I(B:C) = 0$, this does not necessarily mean that the conditional mutual information $I(B:C|A) = 0$. If both B and C are correlated with A, then disclosing A, or ideally, having A communicate the syndromes to B and C for error correction and to establish a conference key among A, B, and C, will induce a correlation in the conditional data between B and C. This, in turn, enables them to generate a key among themselves. It should be noted that the sequence in which keys are generated influences the nature of the keys that can be produced. In the discussed case, a one-dimensional graph facilitated the creation of a conference key among A, B, and C. Subsequently, B and C are able to establish a key between themselves. Alternatively, if B or C instead of A transmits the syndrome to A, they are capable of creating separate keys with A. In a more general setting, the conditional covariance between B and C, represented as $\langle B_A C_A\rangle = \mathcal{C}_3 - \mathcal{C}_1\mathcal{C}_2/V$, where B_A and C_A denote the conditional data held by B and C, disclosing A diminishes the correlation between B and C if $\mathrm{Sgn}(\mathcal{C}_1\mathcal{C}_2)/V = \mathrm{Sgn}(\mathcal{C}_3)$, eliminates it when $\mathcal{C}_1\mathcal{C}_2/V = \mathcal{C}_3$, and enhances it under other circumstances. Here, $\mathcal{C}_1 = \langle AB\rangle$, $\mathcal{C}_2 = \langle AC\rangle$, $\mathcal{C}_3 = \langle BC\rangle$, and $V = \langle A^2\rangle = \langle B^2\rangle = \langle C^2\rangle$.

Figure 1 illustrates the information reconciliation process for CKA with A as the reference. In this scenario, after reconciliation, B and C can also extract a bipartite key [see Figs. 1(a) and 1(b)]. Figure 2 depicts the information reconciliation process for independent bipartite key generation, where user A establishes separate keys with B and C.

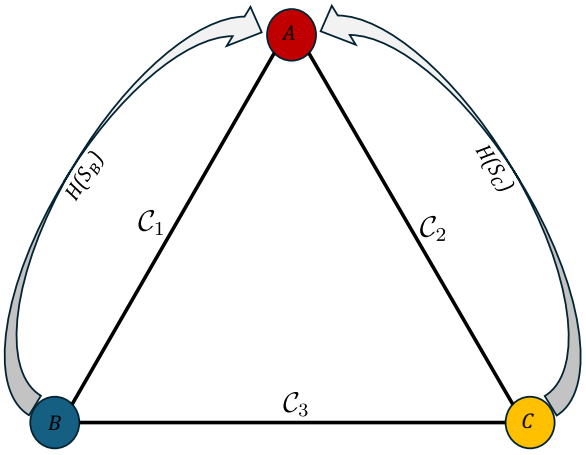


FIG. 2. Information reconciliation for independent bipartite key generation between user A and users B and C. User A establishes separate keys with B and with C, each sending a syndrome S_B or S_C to A. The quantities $H(S_B)$ and $H(S_C)$ denote the entropies of the communicated syndromes, and their optimal joint entropy satisfies $H(S_B,S_C) = H(BC|A)$.

III. SECURITY ANALYSIS

A. Holevo bound

In the context of CV-QKD, the Holevo bound represents the upper limit on the information accessible to an eavesdropper about the measurement outcomes of the parties whose data are used to generate a secure key. To determine this bound, we assume that the eavesdropper, E, purifies the state of the legitimate parties, denoted as A, B, and C (we consider three parties for simplicity, but the underlying principles can be extended to more parties and modes) [31,32]. This entanglement leads us to posit that the entire system $ABCE$ is in a pure state. Consequently, the von Neumann entropy of the combined system, $S(ABCE)$, is zero.

Before proceeding, we must clarify our notation. Throughout this work, the term $S(I|J)$ denotes the entropy of subsystem I evaluated in the state, $\rho_{I|J}$, which results *after* a measurement on subsystem J. The entropy is calculated as $S(I|J) := S(\rho_{I|J}) = -\mathrm{Tr}[\rho_{I|J} \log_2 \rho_{I|J}]$.

This definition should not be confused with the standard conditional von Neumann entropy, which is an algebraic property of the initial (premeasurement) state ρ_{IJ}. The standard definition, which we denote as $S(I|J)_{\mathrm{std}}$, is given by $S(I|J)_{\mathrm{std}} = S(IJ) - S(J)$, or explicitly

$$S(I|J)_{\mathrm{std}} = -\mathrm{Tr}[\rho_{IJ} \log_2 \rho_{IJ}] + \mathrm{Tr}[\rho_J \log_2 \rho_J]. \tag{1}$$

Crucially, our notation $S(I|J)$ refers to the entropy of a state produced by a physical measurement process, while the standard definition does not.

With this notational framework, we can establish the relationships needed to bound Eve's information. Since the overall state of $ABCE$ is pure, the entropy of any subsystem is equal to that of its complement; thus, $S(ABC) = S(E)$. Furthermore, a measurement on subsystem A collapses the remaining system BCE into a new pure state. For any tripartite pure state, the entropy of a subsystem is equal to that of its complement. This physical principle directly leads to the equality $S(BC|A) = S(E|A)$, where both quantities are entropies of the respective subsystems in the postmeasurement state conditioned on the outcome at A.

Eve's knowledge of the measurement outcome of A is upper-bounded by the Holevo quantity χ_A, which is the initial entropy of Eve's system reduced by the entropy remaining after A's measurement. This can be written as $\chi_A = S(E) - S(E|A)$. Using the relations established above, this bound becomes

$$\chi_A = S(ABC) - S(BC|A). \tag{2}$$

This framework can be extended to sequential key generation. Here, the analysis of a subsequent key between B and C is performed on the conditional state $\rho_{BC|A}$. This approach, where the protocol conditions on A's data and the security proof assumes this data is known to all parties, including Eve, is a deliberate choice made for two critical security reasons. First, the assumption that Eve has access to A's data allows us to establish the most conservative (worst-case) upper bound on her information for the subsequent key. Second, by generating the key only from the data corresponding to the conditional state $\rho_{BC|A}$, we ensure the new key is statistically independent (uncorrelated) of A's original data. This prevents vulnerabilities that could arise from cross-key correlations.

It is important to note that this conditioning does not require a sequential quantum measurement process. The protocol imposes no specific temporal order on the measurements; each party simply measures their respective quantum state upon receipt, and the "conditioning" is performed entirely during classical postprocessing. As will be detailed in the key rates analysis (Sec. III B), this classical step requires at least one of the parties (B or C) to have knowledge of A's data. Therefore, the analysis of this stage is not an examination of a hypothetical scenario, but a direct assessment of the cryptographic resource available to the remaining parties under this robust security model. For a key generated between B and another party using this state, the information leaked to Eve is bounded by quantities that depend on the entropy of the full remaining system, $S(BC|A)$, reduced by the entropy of the system left after B's measurement. The bounds are thus given by

$$\chi_{B|A} = S(BC|A) - S(C|AB) \tag{3}$$

and similarly, for a key generated by C,

$$\chi_{C|A} = S(BC|A) - S(B|AC). \tag{4}$$

We consider Gaussian states that are fully described by their first moments (mean quadrature values) and second moments, captured in the covariance matrix Σ. This matrix is defined as

$$\Sigma_{ij} = \tfrac{1}{2}\langle \hat{x}_i\hat{x}_j + \hat{x}_j\hat{x}_i\rangle - \langle \hat{x}_i\rangle\langle \hat{x}_j\rangle, \tag{5}$$

where $\langle\cdot\rangle$ denotes expectation values. Diagonal elements of the matrix indicate the variance of each quadrature, representing their uncertainties, while off-diagonal elements represent correlations between different quadratures.

The von Neumann entropy of these states is derived from the symplectic eigenvalues ν_i of the covariance matrix [31] and is given by

$$S = \sum_i [(\nu_i + \tfrac{1}{2})\log(\nu_i + \tfrac{1}{2}) - (\nu_i - \tfrac{1}{2})\log(\nu_i - \tfrac{1}{2})]. \tag{6}$$

Similarly, conditional entropies $S(p|q)$ can be derived from the corresponding conditional covariance matrices.

The conditional covariance matrix $\Sigma_{p|q}$ is expressed as

$$\Sigma_{p|q} = \Sigma_p - \Sigma_{pq}(X\Sigma_q X)^{\mathrm{MP}}\Sigma_{pq}^T, \tag{7}$$

where Σ_p denotes the covariance matrix of the unmeasured modes of the multipartite state, Σ_q represents the covariance matrix of the measured modes, Σ_{pq} is the covariance matrix between the measured and unmeasured modes, and X is defined as $\mathrm{Diag}(1,0)$ for measurements in the x quadrature and in the Moore-Penrose (MP) inverse.

The overall covariance matrix Σ of the system, incorporating both measured and unmeasured modes, is structured as follows:

$$\Sigma = \begin{pmatrix} \Sigma_p & \Sigma_{pq} \\ \Sigma_{pq}^T & \Sigma_q \end{pmatrix}. \tag{8}$$

Throughout this work, we assume homodyne detection of the x quadrature unless stated otherwise. For all graph states studied here, except the GHZ/W state, the quadratures are symmetric in phase space, meaning the variances of the x and p quadratures are equal. As a result, the choice of measurement quadrature does not affect the key rate or security analysis. In the case of the GHZ/W state, our construction yields lower variance in the x quadrature, making it the favorable choice for measurement. We also considered heterodyne detection as an alternative, but it was consistently found to be suboptimal compared to homodyne detection across all scenarios analyzed. To maintain clarity and avoid redundancy, all references to measurement in this paper should be understood as x-quadrature homodyne detection.

B. Key rates

Having addressed the complexities of multiuser QKD in the context of information reconciliation and the estimation of the Holevo bound, we are now positioned to establish expressions for various key rates [31,33,34]. For a three-user system, three distinct types of keys can be generated:

(1) conference key agreement;
(2) bipartite key generation post-CKA; and
(3) independent bipartite key generation.

1. Conference key agreement

Conference key agreement can be realized among the users if there exists at least one user who is correlated with the remaining users. The amount of information (syndrome) that needs to be communicated to the rest of the users is determined by the lowest mutual information between this central user and the other users. The conference key rate can be expressed as

$$K^i(i:j:k) = \beta \min[I(i:j), I(i:k)] - \chi_i, \tag{9}$$

where β is the reconciliation efficiency [35], and the superscript i signifies the reference data of the user i used to generate the key. The efficiency β is a crucial practical parameter that accounts for the fact that real-world error-correction protocols, used by the parties to reconcile their correlated data into an identical string, are not perfectly efficient and have a communication overhead.

2. Bipartite keys post-CKA

Once a CKA with user i as the reference is complete, the conditional data possessed by the remaining two users, j and k, can be utilized to generate a new, independent key. Following a successful CKA, both users j and k now possess the measurement outcomes of user i. This allows either party to act as the reference for the subsequent key generation. A secure key can be generated from this conditional resource provided that the conditional mutual information between j and k, $I(j:k|i)$, is greater than the information Eve can obtain about the raw key.

To determine the Holevo bound for this subsequent stage, we apply the same security principles as before. We pessimistically assume that Eve also knows the measurement outcomes of i. The security analysis is then performed on the conditional state $\rho_{jk|i}$, where we posit that Eve holds a purification of this state. Following the arguments presented in Sec. III A, we can then calculate the bound on Eve's information for this specific conditional resource. The key rate for this scenario depends on which user acts as the reference for error correction. If user j is the reference, the key rate is given by

$$K^j(j:k|i) = \beta I(j:k|i) - \chi_{j|i}. \tag{10}$$

If, instead, k is used as the reference, the key rate is

$$K^k(j:k|i) = \beta I(j:k|i) - \chi_{k|i}. \tag{11}$$

3. Independent bipartite keys

A user can generate independent bipartite keys with the users with whom it is correlated, provided the mutual information of this user (say i) with the rest of the users is higher than the mutual information between the other users (ideally zero). The key rates are

$$K^j(i:j) = \beta I(i:j) - \chi_j \tag{12}$$

and $K^k(i:k|j)$. In the scenario where the mutual information between the other users is zero, the equation simplifies to $K^k(i:k)$. Notice that, even when j and k are identical, the order of key generation influences the key rates. This

sequential dependence is critical. After user i establishes a key with user j [corresponding to the rate $K^j(i:j)$], user i now possesses the measurement outcomes of user j after successful error correction. This knowledge enables the subsequent step. For the key rate $K^k(i:k|j)$, where user k provides the reference data, key generation is possible because user i has the necessary conditional information (its own data and j's data) to perform error correction and privacy amplification. However, alternative reconciliation with key rate $K^i(i:k|j)$ would not be described by this framework, as it would require user k to perform error correction and privacy amplification, for which it would need access to j's measurement outcomes—information they do not have. It is more useful to consider the sum of independent keys that i can generate with other users. The actual key rates with each user depend on the information disclosed for error correction, specifically the syndrome length. The sum of independent keys is given by

$$\begin{aligned} K^{j,k}(i:jk) &= H(j,k) - \zeta H(j,k|i) - \chi_{jk} \\ &= K^j(i:j) + K^k(i:k|j). \end{aligned} \tag{13}$$

As discussed in Sec. II, $H(j,k|i)$ represents the optimal amount of information that j and k need to communicate to i to facilitate error correction, and $\zeta \geq 1$ accounts for inefficient information reconciliation. For the symmetric case, the independent key rates can be computed as follows:

$$\begin{aligned} K(i:j) &= K(i:k) \\ &= \tfrac{1}{2}[H(j,k) - \zeta H(\boldsymbol{S}_j, \boldsymbol{S}_k) \\ &\quad - S(ijk) + S(i \mid jk)]. \end{aligned} \tag{14}$$

Here, $\boldsymbol{S}_j$ and $\boldsymbol{S}_k$ are the syndromes with entropies $H(\boldsymbol{S}_j) = H(\boldsymbol{S}_k)$. In this paper, we focus on the conditions under which a positive key rate can be achieved, and therefore, we emphasize the sum of independent keys rather than individual key rates.

C. Finite-size analysis

In practical implementations, the number of exchanged quantum signals is inherently finite. This finite data sample introduces statistical fluctuations that can significantly impact the security and performance of the QKD protocol. This is unlike in the asymptotic regime, discussed in the previous section, where it is assumed that an infinite number of signals are exchanged, allowing statistical uncertainties to vanish. In the finite-size regime, the key rate is affected by the statistical estimation of channel parameters.

The order in which error correction and parameter estimation are performed affects the finite-size key rate expression [36]. When error correction is performed *after* parameter estimation, some transmitted signals are disclosed to estimate the channel parameters. Let N be the total number of signals exchanged, and n be the number of signals used for key generation after discarding $N-n$ signals for parameter estimation. The finite-size key rate K is given by

$$K = \frac{n}{N}[K_\infty(t^{\text{low}}, V_\epsilon^{\text{up}}) - \Delta(n)]. \tag{15}$$

Alternatively, when error correction is performed *before* parameter estimation, all measurements can be used for both parameter estimation and key generation, allowing for better estimates of the channel parameters since no data are discarded [36,37]. In this case, the finite-size key rate K is

$$K = K_\infty(t^{\text{low}}, V_\epsilon^{\text{up}}) - \Delta(n). \tag{16}$$

In both expressions, $K_\infty(t^{\text{low}}, V_\epsilon^{\text{up}})$ is the asymptotic key rate calculated using conservative estimates of the channel transmission t and excess noise $V_\epsilon = t\epsilon$ to account for statistical fluctuations due to the finite sample size. These adjusted parameters are

$$t^{\text{low}} = t - 6.5\sigma_t \tag{17}$$

$$V_\epsilon^{\text{up}} = V_\epsilon + 6.5\sigma_\epsilon, \tag{18}$$

where σ_t and σ_ϵ are the standard deviations of the estimators of t and V_ϵ, respectively (see Appendix D). The factor 6.5 corresponds to a confidence level ensuring an error probability of 10^{-10}. The finite-size correction term $\Delta(n)$ [38] accounts for the statistical fluctuations in the mutual information,

$$\Delta(n) = 7\sqrt{\frac{\log_2(2\times 10^{10})}{n}}, \tag{19}$$

with n being the number of signals used for key generation.

IV. GENERATION OF TRIPARTITE STATES

The generation of multipartite states in CV systems can be efficiently realized by manipulating squeezed light states through beam splitters [25,39]. This method allows us to explore different configurations of squeezed states and beam splitters that result in distinct tripartite states. We define a general structure of the covariance matrix as follows:

$$\begin{pmatrix} V_A & C_{AB} & C_{AC} \\ C_{AB} & V_B & C_{BC} \\ C_{AC} & C_{BC} & V_C \end{pmatrix}. \tag{20}$$

Here, V_i represents the variance of mode $i = A, B, C$, and C_{ij} denotes the covariance between the quadratures of modes i and j.

A. GHZ-like state and downstream-access network

We consider two configurations: the symmetric GHZ-like state and the downstream-access network. The GHZ-like state is of interest because it has maximum correlation equally distributed among all modes. The DAN configuration is appealing because it can be easily implemented by substituting the two-mode squeezed vacuum with either modulated squeezed or coherent states, and it offers an advantage in producing bipartite keys.

In the first configuration, referred to as the *symmetric GHZ-like state*, three squeezed states with x-quadrature variances $V_1 = V$, $V_2 = 1/V$, and $V_3 = 1/V$ are directed into two beam splitters with transmissions $t_1 = \frac{2}{3}$ and $t_2 = \frac{1}{2}$ (see Fig. 3). This setup yields a symmetric covariance matrix where

$$V_A = V_B = V_C = \mathrm{Diag}\left[\frac{1+2V^2}{3V}, \frac{2+V^2}{3V}\right], \tag{21}$$

and the covariances between modes are given by

$$C_{AB} = -C_{AC} = C_{BC} = \mathrm{Diag}\left[\frac{V^2-1}{3V}, \frac{1-V^2}{3V}\right]. \tag{22}$$

This state exhibits maximum correlation equally among all modes, analogous to the GHZ state in discrete-variable systems.

The second configuration is based on the *downstream access network* approach, which is a cost-effective setup for generating tripartite states. In this scheme, two squeezed states with x-quadrature variances $V_1 = V$ and $V_2 = 1/V$, along with a vacuum mode $V_3 = 1$, are combined using two beam splitters, with transmissions $t_1 = t_2 = \frac{1}{2}$. This results in a covariance matrix where

$$\begin{aligned} V_A &= \mathrm{Diag}\left[\frac{1+V^2}{2V}, \frac{1+V^2}{2V}\right], \\ V_B &= V_C = \mathrm{Diag}\left[\frac{(1+V)^2}{4V}, \frac{(1+V)^2}{4V}\right], \\ C_{AB} &= -C_{AC} = \mathrm{Diag}\left[\frac{V^2-1}{2\sqrt{2}\,V}, \frac{1-V^2}{2\sqrt{2}\,V}\right], \\ C_{BC} &= \mathrm{Diag}\left[-\frac{(V-1)^2}{4V}, -\frac{(1-V)^2}{4V}\right]. \end{aligned} \tag{23}$$

This configuration simplifies implementation and reduces costs compared to other schemes, as the two-mode squeezed vacuum can be replaced with a modulated squeezed state.

B. Effect of impurity in squeezed states

In practical implementations, squeezed states are often not pure due to technical imperfections and decoherence, which introduce additional noise in the antisqueezed quadrature (AS noise), which usually is proportional to the degree of squeezing [30]. We characterize this impurity by an additional noise parameter V_N, such that, if the variance of the squeezed quadrature is V, the variance of the antisqueezed quadrature becomes $V_N + 1/V$.

To account for the impurity, we modify the covariance matrices of the input squeezed states. For the GHZ-like state configuration, the covariance matrices of the input squeezed states become

$$\begin{aligned} V_1 &= \mathrm{Diag}\left[V, V_N + \frac{1}{V}\right], \\ V_2 &= V_3 = \mathrm{Diag}\left[V_N + \frac{1}{V}, V\right]. \end{aligned} \tag{24}$$

Similarly, for the DAN configuration, the covariance matrices are

$$\begin{aligned} V_1 &= \mathrm{Diag}\left[V, V_N + \frac{1}{V}\right], \\ V_2 &= \mathrm{Diag}\left[V_N + \frac{1}{V}, V\right], \\ V_3 &= \mathrm{Diag}\left[1, 1\right]. \end{aligned} \tag{25}$$

Using these modified input variances, we can compute the resulting covariance matrices after the beam splitter transformations, taking into account the impurity.

For the *GHZ-like state* with impure squeezed states, the variances and covariances become

$$\begin{aligned} V_A &= V_B = V_C \\ &= \mathrm{Diag}\left[\frac{1+2V^2+VV_N}{3V}, \frac{2+V^2+2VV_N}{3V}\right], \end{aligned} \tag{26}$$

and the covariances between modes are given by

$$\begin{aligned} C_{AB} &= -C_{AC} = C_{BC} \\ &= \mathrm{Diag}\left[\frac{V^2-1-VV_N}{3V}, \frac{1-V^2+VV_N}{3V}\right]. \end{aligned} \tag{27}$$

For the *DAN configuration*, the variances and covariances are

$$\begin{aligned} V_A &= \mathrm{Diag}\left[\frac{1+V^2+VV_N}{2V}, \frac{1+V^2+VV_N}{2V}\right], \\ V_B &= V_C = \mathrm{Diag}\left[\frac{(1+V)^2+VV_N}{4V}, \frac{(1+V)^2+VV_N}{4V}\right], \\ C_{AB} &= -C_{AC} = \mathrm{Diag}\left[\frac{V^2-1-VV_N}{2\sqrt{2}V}, \frac{1-V^2+VV_N}{2\sqrt{2}V}\right], \\ C_{BC} &= \mathrm{Diag}\left[-\frac{(V-1)^2+VV_N}{4V}, -\frac{(1-V)^2+VV_N}{4V}\right]. \end{aligned} \tag{28}$$

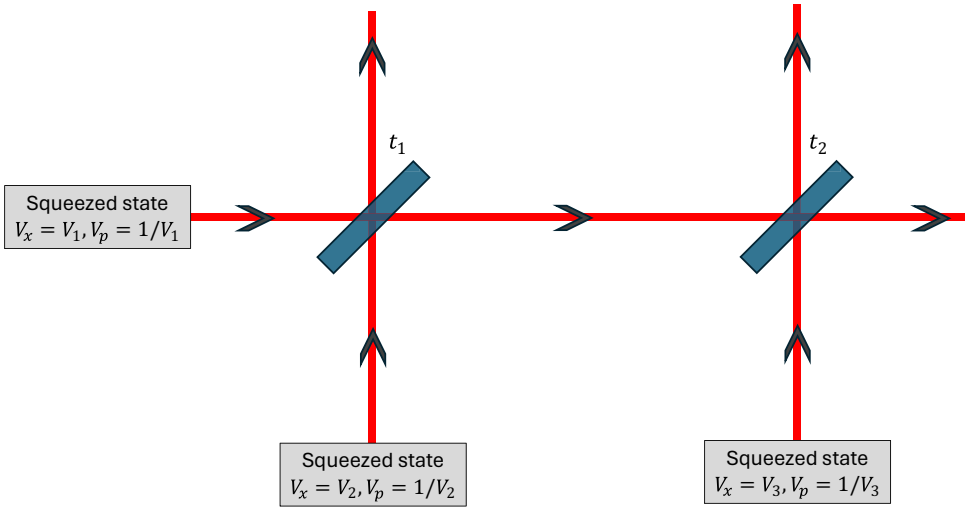


FIG. 3. Schematic diagram for generating tripartite states.

By incorporating the impurity parameter V_N, we can examine the effect of nonideal squeezing on the generated tripartite states. The presence of additional noise increases the variances of the antisqueezed quadratures, thereby impacting the correlations among the modes. This noise must be carefully accounted for to ensure the viability of cryptographic tasks. We assume that this preparation noise is trusted and does not provide information to eavesdroppers.

To address this, we introduce an additional mode for each squeezed state to account for the noise, ensuring that the two modes together form a pure bipartite state. Specifically, we consider the impure squeezed state as one of the outputs of a beam splitter fed by two pure squeezed states with x-quadrature variances Γ_1 and Γ_2 at the input. The impure squeezed state is then related to the variances of the input pure squeezed states as follows:

$$\begin{aligned}\Gamma_1 &= V - \frac{V^3 V_N}{\sqrt{V^3 V_N \left(1 + V^3 V_N\right)}},\\ \Gamma_2 &= V + \frac{V^3 V_N}{\sqrt{V^3 V_N \left(1 + V^3 V_N\right)}}.\end{aligned} \tag{29}$$

V. DUAL-RAIL CLUSTER STATE FOR QKD

In this analysis, we propose a distribution strategy for the modes of a dual-rail cluster state in a multinode QKD network. Unlike a finite graph defined by a discrete set of nodes, the dual-rail cluster state represents an open-ended repeating lattice of interconnected modes. Each mode is typically linked to four others, creating an extensive and complex structure that is difficult to handle as it is.

A. Coloring scheme

To make this infinitely repeating configuration more tractable, we introduce a coloring scheme inspired by graph theory terminology. By assigning colors to modes and then grouping all modes of the same color together, we form what we call a quotient graph state. This quotient graph serves as a finite, homomorphic image of the original dual-rail lattice, preserving key connectivity patterns while reducing its complexity. Although we draw on terms like "coloring" and "quotient graph" from graph theory, our approach focuses on using these concepts to describe and manage the grouping process, rather than relying on advanced graph-theoretic techniques.

The resulting quotient graph state provides a simplified framework that retains the essential structural features of the dual-rail cluster state. In doing so, it creates a more manageable platform for implementing robust and scalable continuous-variable QKD protocols, ensuring that the underlying entanglement resources can be effectively harnessed in practical quantum communication networks.

The optimal homomorphic graph corresponds to a six-mode graph state, achievable through a coloring strategy detailed in Fig. 4. The covariance matrix of this six-mode graph state is (refer to Appendix A for derivation)

$$\begin{pmatrix} \boldsymbol{V} & \boldsymbol{0} & \boldsymbol{C} & -\boldsymbol{C} & \boldsymbol{C} & \boldsymbol{C} \\ \boldsymbol{0} & \boldsymbol{V} & \boldsymbol{C} & -\boldsymbol{C} & -\boldsymbol{C} & -\boldsymbol{C} \\ \boldsymbol{C} & \boldsymbol{C} & \boldsymbol{V} & \boldsymbol{0} & \boldsymbol{C} & -\boldsymbol{C} \\ -\boldsymbol{C} & -\boldsymbol{C} & \boldsymbol{0} & \boldsymbol{V} & \boldsymbol{C} & -\boldsymbol{C} \\ \boldsymbol{C} & -\boldsymbol{C} & \boldsymbol{C} & \boldsymbol{C} & \boldsymbol{V} & \boldsymbol{0} \\ \boldsymbol{C} & -\boldsymbol{C} & -\boldsymbol{C} & -\boldsymbol{C} & \boldsymbol{0} & \boldsymbol{V} \end{pmatrix}, \tag{30}$$

where the diagonal covariance matrix $\boldsymbol{V}$ and the off-diagonal covariance matrix $\boldsymbol{C}$ are defined as follows for

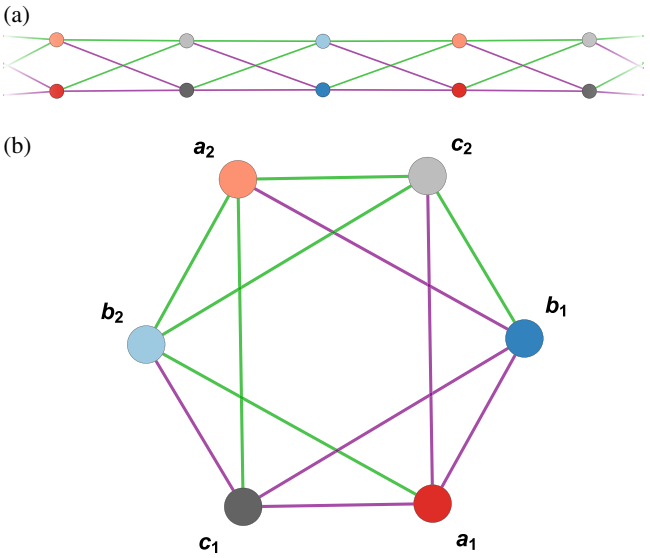


FIG. 4. The coloring scheme of the dual-rail cluster state (a) used to obtain the six-mode graph state (b). The edges in the graph illustrate the correlations between modes, with edges in two colors indicating the sign of the correlation. Edges of one color represent positive correlations, while edges of the other color represent negative correlations.

pure squeezed states:

$$\boldsymbol{V} = \begin{pmatrix} \frac{1+V^2}{2V} & 0 \\ 0 & \frac{1+V^2}{2V} \end{pmatrix} \quad \text{and}$$
$$\boldsymbol{C} = \begin{pmatrix} \frac{1-V^2}{4V} & 0 \\ 0 & \frac{V^2-1}{4V} \end{pmatrix}. \tag{31}$$

Here V is the variance of the squeezed quadrature of the squeezed state. For impure squeezed states, as described in the previous section, the impurity parameter V_N modifies these matrices to

$$\boldsymbol{V} = \begin{pmatrix} \frac{1+V^2+V_N}{2V} & 0 \\ 0 & \frac{1+V^2+V_N}{2V} \end{pmatrix},$$
$$\boldsymbol{C} = \begin{pmatrix} \frac{1-V^2+VV_N}{4V} & 0 \\ 0 & \frac{V^2-1-VV_N}{4V} \end{pmatrix}. \tag{32}$$

This six-mode graph state provides a versatile platform for various QKD strategies. We present optimal methods for generating a three-user conference key and independent bipartite keys, which we compare to the three-mode tripartite states discussed in the previous section.

B. Distribution strategies for six-mode graph state

In our investigation of six-mode graph states for QKD, we explored a wide array of strategies for distributing the quantum states among users. However, due to space constraints and to focus on the most impactful designs, here we present only the strategies that proved to be the most noteworthy in terms of operational performance and security. We categorize the strategies based on whether the dealer also participates as a user or acts solely as a distributor.

Dealer as a participant:

(1) *Distribution 1* [Fig. 5(a)]. The dealer sends modes b_1 and c_1 to two distant users through a channel characterized by channel transmission t and channel excess noise ϵ, transforming the modes to $\tilde{b}_1$ and $\tilde{c}_1$, with covariance matrix $\tilde{\boldsymbol{V}} = t(\boldsymbol{V} + \epsilon\mathbb{I} - \mathbb{I}) + \mathbb{I}$, with $\mathbb{I}$ being the 2×2 identity matrix. The dealer retains the rest of the modes, a_1, a_2, b_2, and c_2.

(2) *Distribution 2* [Fig. 5(b)]. The dealer sends modes b_1 and b_2 to one user and modes c_1 and c_2 to the other user. The dealer retains modes a_1 and a_2.

Dealer as a distributor:

(1) *Distribution 3* [Fig. 5(c)]. Modes a_1, b_1, and c_1 are distributed to three separate users; the rest are retained by the dealer.

(2) *Distribution 4* [Fig. 5(d)]. All the modes are sent through the channel to three remote users; one user gets a_1 and a_2, another receives b_1 and b_2, and the third c_1 and c_2.

Each of these strategies offers distinct advantages, and the choice of strategy should consider the operational context and security requirements of the QKD system. Table I summarises the recommended distribution strategies, their operational context, and the corresponding information-reconciliation choices.

VI. QUANTUM CONFERENCE KEY DISTRIBUTION PROTOCOLS

Quantum conference key distribution protocols like standard two-user QKD protocols can be broadly categorized into three categories, based on the role of the dealer and the method of key reconciliation. Understanding these protocols is essential for evaluating the security and efficiency of multiuser quantum communication systems. In our analysis, we assume that the channel parameters are symmetric, meaning that all users have identical channel conditions.

A. Direct reconciliation (DR)

In the direct reconciliation protocol, the dealer retains one or more modes of the multipartite state they prepare and uses their measurement outcomes as references for

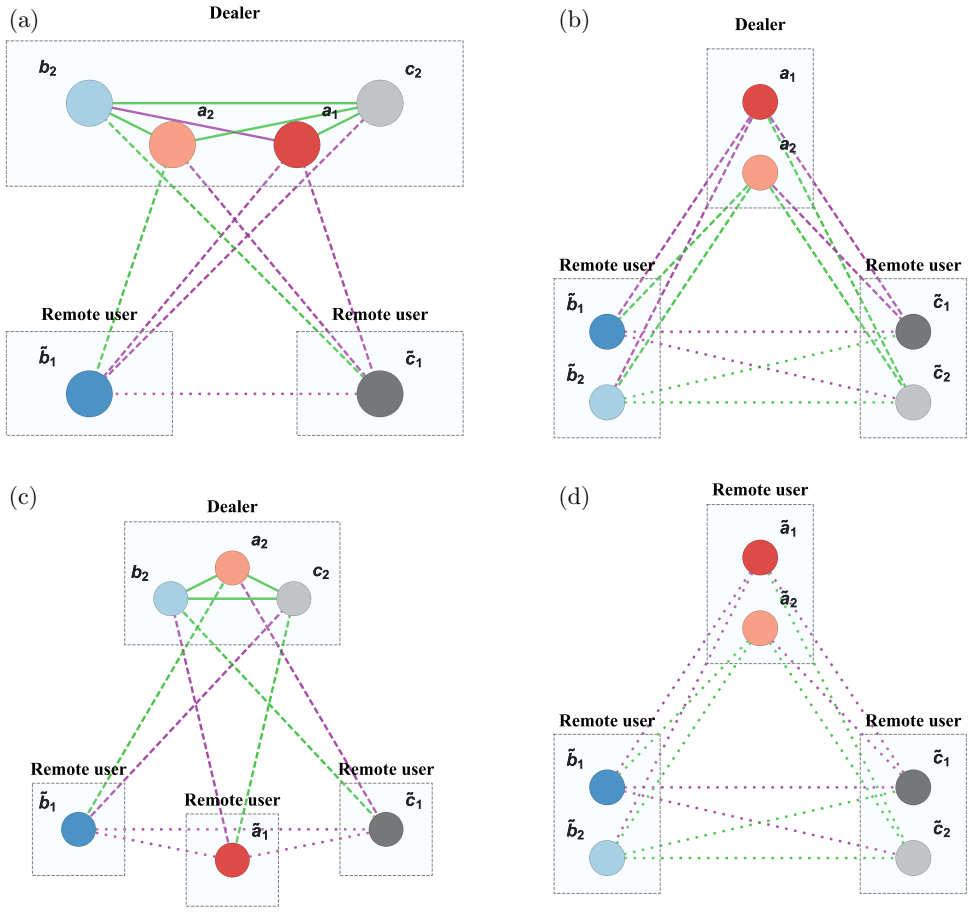


FIG. 5. Graphs depicting various methods for distributing a six-mode graph state among three users. Dashed lines indicate that the correlations (i.e., covariance between the modes $\boldsymbol{C}$) have been reduced by a factor of $\sqrt{t}$, while dotted lines indicate a reduction by a factor of t.

key generation. The remote parties receive the necessary information and perform the required error correction.

For the GHZ state described in Sec. IV, the covariance matrix given in Eq. (20) transforms to

$$\begin{pmatrix} V_A & \sqrt{t}\,C_{AB} & \sqrt{t}\,C_{AC} \\ \sqrt{t}\,C_{AB} & t(V_B+\epsilon-1)+1 & t\,C_{BC} \\ \sqrt{t}\,C_{AC} & t\,C_{BC} & t(V_C+\epsilon-1)+1 \end{pmatrix}. \tag{33}$$

The key rate for this approach is given by $k^A(A:\tilde{B}:\tilde{C})$ [refer to Eq. (9)], where the notation $\tilde{M}$ indicates that mode M has been transmitted through a quantum channel.

We explore two distribution strategies for a six-mode graph state intended for three-user conference key generation via direct reconciliation, as illustrated in Figs. 5(a) and 5(b).

There are multiple methods for conference key generation based on distribution 1 [Fig. 5(a)]. Among these, the key $k^{a_1}(a_1:\tilde{b}_1:\tilde{c}_1|a_2)$ proves most robust against channel losses and noise in the asymptotic regime when reconciliation efficiency is perfect ($\beta=1$); see Fig. 6(a). Note that a_1 and a_2 are not interchangeable due to the correlation type (sign) with the remote user's modes. Depending on the channel parameters, leveraging measurements from multiple modes as references can further enhance the conference key rate.

From Fig. 6(a), we observe that, under finite squeezing, the GHZ state is not the optimal multipartite resource for maximizing distance in conference key generation with direct reconciliation under ideal conditions. Among the configurations tested, distribution 1 achieves the greatest distances, particularly under high excess channel noise $0.08<\epsilon<0.5$ SNU (signal noise units). Although trusted noise does not hinder the performance of distribution 1 or GHZ-based protocols in the asymptotic regime (and may even assist them), it offers no similar advantage to distribution 2, yet it does not significantly degrade its performance either.

In the finite-size regime, for $n=10^7$ measurements and imperfect reconciliation ($\beta=0.95$), distribution 2 [Fig. 5(b)] with key rate $k^{a_1}(a_1:\tilde{b}_1\tilde{b}_2:\tilde{c}_1\tilde{c}_2|a_2)$ enables key generation over greater distances for channel noise $0<\epsilon<0.27$ SNU; see Fig. 7(a). This is in contrast to what

TABLE I. Recommended distribution strategies and corresponding information reconciliation methods for multiuser QKD.

Strategy	Operational context	Information reconciliation	Advantages
Distribution 1	Dealer is also a user	Direct reconciliation, Reverse reconciliation	Optimal for maximal distance; robust against trusted noise
Distribution 2	Dealer is also a user	Direct reconciliation, Reverse reconciliation	Better performance in finite-size regime; enhanced channel parameter estimation via multiple correlations
Distribution 3	The dealer distributes three modes; measures and publicly discloses the remaining three	Entanglement in the middle	Suitable for decentralized conference key agreement
Distribution 4	Fully distributed; no dealer involvement after state distribution	Entanglement in the middle	Enables fully peer-to-peer operation
Distribution 5	Dealer sends two uncorrelated modes to remote users	Direct reconciliation (CKA), Reverse reconciliation	Best suited for generating separate keys between dealer and users

we observe in the asymptotic regime, where distribution 1 enables key generation for the largest distances. This is due to the fact that distribution 2 enables the users and the dealer to use four correlations as opposed to three for distribution 1 to enable better estimation of the channel parameters (see Appendix D).

B. Reverse reconciliation (RR)

Contrary to direct reconciliation, reverse reconciliation involves a remote user serving as the reference. This user sends error-correction information to the dealer and other participants, facilitating key alignment based on their reference measurements.

The conference key rate for tripartite states under reverse reconciliation is given by $k^{\tilde{B}}(A:\tilde{B}:\tilde{C})$. For the six-mode graph state with distribution 1 [Fig. 5(a)], we find that the optimal key rate for achieving higher tolerance to channel parameters under reverse reconciliation is

$$k^{\tilde{b}_1}(a_1:\tilde{b}_1:\tilde{c}_1|b_2a_2c_2).$$

For distribution 2 [Fig. 5(b)], the optimal conference key is

$$k^{\tilde{b}_1}(a_1a_2:\tilde{b}_1\tilde{b}_2:\tilde{c}_1\tilde{c}_2|\tilde{b}_2).$$

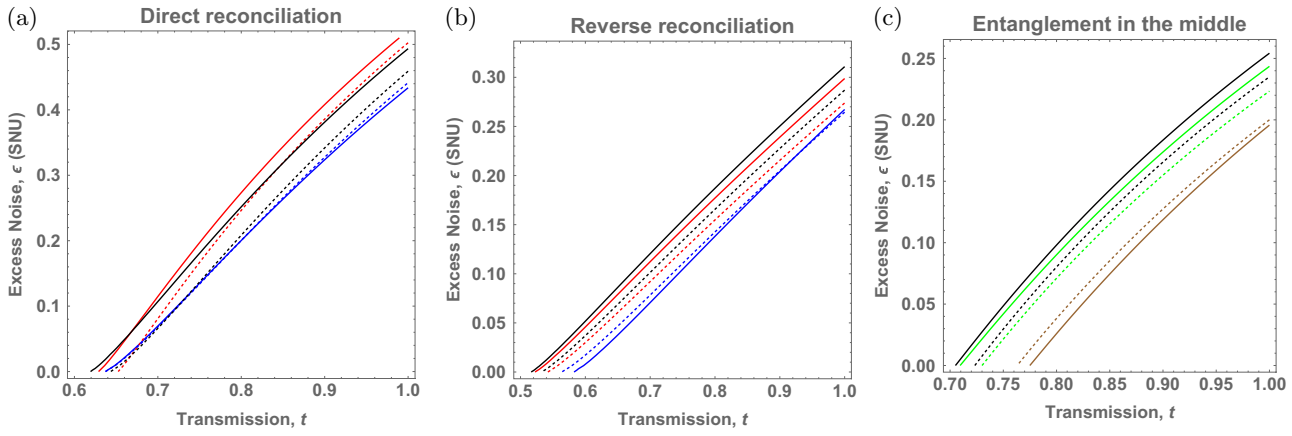


FIG. 6. Plots illustrating the maximum tolerable channel losses and noise in the asymptotic regime. Key generation is possible only for channel parameters lying below the plotted curves. The red curve corresponds to distribution 1, the blue to distribution 2, the green to distribution 3, the brown to distribution 4, and the black to the GHZ state. Dashed lines represent pure squeezed states, while solid lines indicate impure but trusted squeezed states with $V_N = 10$. The reconciliation efficiency is $\beta = 1$, and the variance of the squeezed quadrature is $V = 0.1$ SNU.

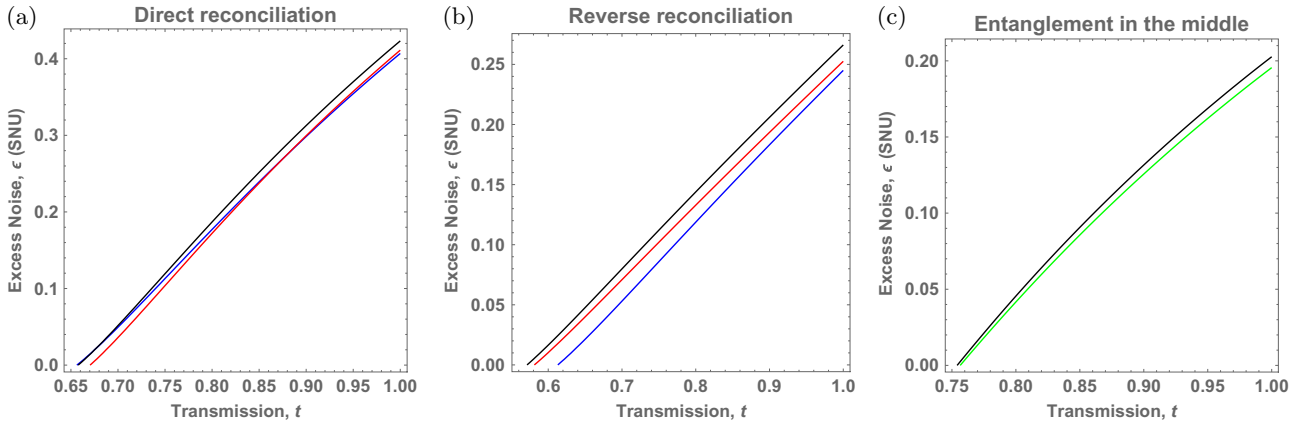


FIG. 7. Plots illustrating the maximum tolerable channel losses and noise in the finite-size regime with $n = 10^7$ measurements. Key generation is possible only for channel parameters lying below the plotted curves. The red curve corresponds to distribution 1, the blue to distribution 2, the green to distribution 3, and the black to the GHZ state. Here trusted AS noise $V_N = 10$ SNU. The reconciliation efficiency is $\beta = 0.95$, and the variance of the squeezed quadrature is $V = 0.1$ SNU.

From Fig. 6(b), it is apparent that the GHZ state generates positive keys under a broader range of channel conditions. Comparable performance is achieved with distribution 1. The influence of trusted noise for reverse reconciliation is the same as for direct reconciliation; it shows little to no effects on protocols with distribution 2 but benefits protocols with distribution 1 and the GHZ state.

In the finite-size regime [see Fig. 7(b)], the trend remains the same, with the GHZ state enabling the largest distances followed by distribution 1 and distribution 2, though the difference is not significant.

C. Entanglement in the middle (Mid)

In this protocol, the dealer prepares entangled states and distributes them among the users but does not have access to the conference key being generated.

The conference key rate for tripartite states in the entanglement-in-the-middle protocol is given by $k^{\tilde{A}}(\tilde{A} : \tilde{B} : \tilde{C})$. For the six-mode graph state with distribution 3 [Fig. 5(c)], the dealer discloses the measurement outcomes of all of their modes, effectively disconnecting themselves from the conditional data held by the other users. This leads to the conference key rate between the users being

$$k^{\tilde{a}_1}(\tilde{a}_1 : \tilde{b}_1 : \tilde{c}_1 | a_2 b_2 c_2).$$

It should be noted that, instead of disclosing the measurement outcomes, the dealer can generate three sets of conference keys with any two remote users, with conference key rates $k^{a_2}(a_2 : \tilde{b}_1 : \tilde{c}_1)$, $k^{b_2}(b_2 : \tilde{a}_1 : \tilde{c}_1 | a_2)$, and $k^{c_2}(c_2 : \tilde{a}_1 : \tilde{b}_1 | a_2 b_2)$. However, the tolerance to channel noise and loss for the conference key $k^{b_2}(b_2 : \tilde{a}_1 : \tilde{c}_1 | a_2)$ was found to be very low.

For distribution 4 [Fig. 5(b)], the optimal conference key is

$$k^{\tilde{a}_1 \tilde{a}_2}(\tilde{a}_1 \tilde{a}_2 : \tilde{b}_1 \tilde{b}_2 : \tilde{c}_1 \tilde{c}_2).$$

From Fig. 6(c), we observe that, similar to the case in reverse reconciliation, the protocol with the GHZ state outperforms other protocols. Distribution 3 closely matches the GHZ state's performance. The adverse influence of trusted noise for distribution 4 is noticeable here, though its presence proves beneficial for protocols with distribution 3 and the GHZ state.

In contrast to distribution 3, neither the GHZ state nor distribution 4 can directly estimate the channel transmission between the dealer and the users. To enable channel parameter estimation, the dealer must occasionally retain, measure, and disclose a subset of the modes. In Fig. 7(c), we allocate half of the 10^7 measurements for channel estimation and use the remaining half for key generation. Under these conditions, while the GHZ state still maintains a slight advantage, the performance gap narrows considerably.

D. Bipartite key post-CKA

Following the generation of a conference key using any of the schemes mentioned in the previous section, bipartite keys can be generated using the conditional data of the remaining users. This data, conditioned on the reference data used for conference key generation, allows for the creation of additional bipartite keys. Table II summarizes various scenarios and their corresponding key rate expressions.

When comparing the overall multiuser QKD capabilities (CKA and subsequent bipartite key generation) of multipartite states, the six-mode graph state derived from

TABLE II. Summary of bipartite key rates post-QCKA for different scenarios and distributions.

Scenario	Tripartite-states key rate	Distrib.	Key rate expression
Bipartite key rate post-CKA with DR	$k^{\tilde{B}}(\tilde{B}:\tilde{C}\|A)$	1	$k^{\tilde{b}_1}(\tilde{b}_1:\tilde{c}_1\|a_1a_2)$
			$k^{\tilde{b}_1\tilde{b}_2}(\tilde{b}_1\tilde{b}_2:\tilde{c}_1\tilde{c}_2\|a_1a_2)$
Bipartite key rate with DR post-CKA with RR	$k^{A}(A:\tilde{C}\|\tilde{B})$	1	$k^{a_1}(a_1:\tilde{c}_1\|b_2a_2c_2\tilde{b}_1)$
			$k^{a_1a_2}(a_1a_2:\tilde{c}_1\tilde{c}_2\|\tilde{b}_1\tilde{b}_2)$
Bipartite key rate with RR post-CKA with RR	$k^{\tilde{C}}(A:\tilde{C}\|\tilde{B})$	1	$k^{\tilde{c}_1}(a_1:\tilde{c}_1\|b_2a_2c_2\tilde{b}_1)$
			$k^{\tilde{c}_1\tilde{c}_2}(a_1a_2:\tilde{c}_1\tilde{c}_2\|\tilde{b}_1\tilde{b}_2)$
Bipartite key rate post-CKA with Mid	$k^{\tilde{B}}(\tilde{B}:\tilde{C}\|\tilde{A})$	3	$k^{\tilde{b}_1}(\tilde{b}_1:\tilde{c}_1\|a_2b_2c_2\tilde{a}_1)$
			$k^{\tilde{b}_1\tilde{b}_2}(\tilde{b}_1\tilde{b}_2:\tilde{c}_1\tilde{c}_2\|\tilde{a}_1\tilde{a}_2)$

a dual-rail cluster state significantly outshines the GHZ state; see Fig. 8. For CKA via DR, distribution 1 supports CKA and bipartite key generation under a broader range of channel conditions than any other considered multipartite state or strategy. For CKA via RR, distribution 2 excels beyond all others. For CKA via Mid, distribution 4 facilitates CKA and bipartite keys under more extensive channel conditions. In the finite-size regime, bipartite keys generated using the GHZ state become infeasible for measurements with fewer than $n = 10^8$ samples. In contrast, protocols employing dual-rail cluster states enable the generation of bipartite keys after the conference key is established, making them applicable to all the protocols introduced. However, the distribution strategy must be carefully tailored to the specific requirements of the quantum network.

E. Independent bipartite keys

In Sec. III, we discussed the utility of analyzing the sum of independent bipartite keys that can be generated by a central user who has higher correlations with other users. This approach is particularly informative in symmetric cases, where the collective key rate helps establish bounds on the symmetric channel parameters required for independent key generation by all the users with the central user. As outlined in Sec. II, generating independent keys necessitates one user having a stronger correlation with the rest of the users than between the users themselves.

It is more advantageous in terms of classical information processing for these remote users to be uncorrelated. We introduce a distribution 5, depicted in Fig. 9(a), specifically because the remote users are not correlated. It is evident from Fig. 9(b) that this approach offers a significant enhancement compared to DAN.

VII. RESULTS

In this work, we have introduced a novel protocol for three-user conference key generation using dual-rail cluster states, employing the concept of a *quotient graph state* to create a finite six-mode pure graph state suitable for cryptographic applications. Our comparative analysis with GHZ/W states generated under similar squeezing conditions yielded the following key findings.

(1) *Asymptotic regime (CKA):* In the limit of infinite signals, our protocol outperforms GHZ/W states in the direct reconciliation scheme but does not surpass them in reverse reconciliation or entanglement-in-the-middle schemes.

(2) *Finite-size regime (CKA):* GHZ states maintain a slight performance advantage for generation of conference key in all schemes explored, direct reconciliation,

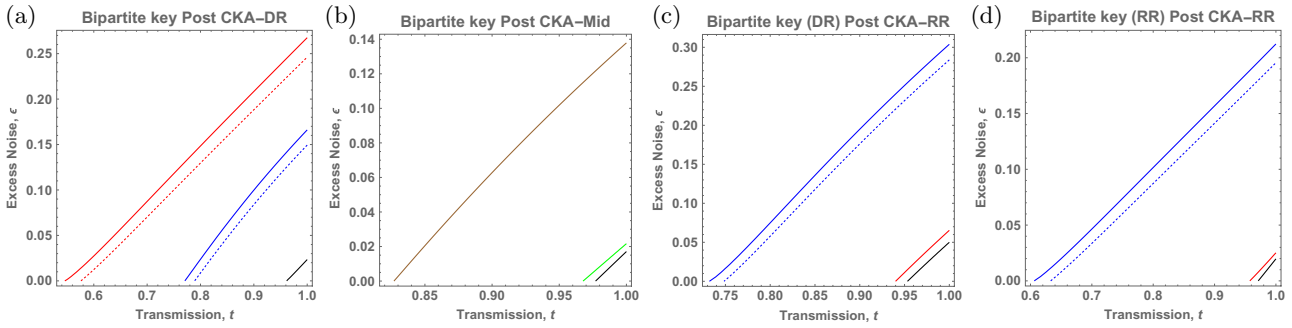


FIG. 8. Maximum tolerable excess noise ϵ (in SNU) versus transmission t for bipartite keys post-CKA generation: red, distribution 1; blue, distribution 2; green, distribution 3; brown, distribution 4; black, GHZ state; dashed, finite-size keys; and solid, asymptotic. Parameters: $V_N = 10$, $\beta = 0.95$, and squeezed variance $V = 0.1$ SNU.

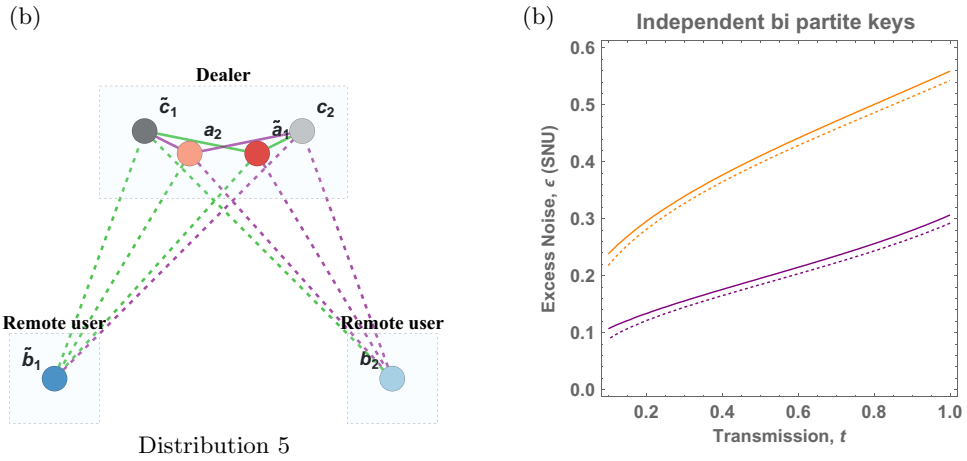


FIG. 9. (a) Distribution 5. (b) The maximum tolerable excess noise ϵ for varying transmission of the channel t for generating independent bipartite keys between the dealer and the remote users. Orange plots correspond to distribution 5 and the purple plot corresponds to DAN. Dashed lines correspond to finite-size keys ($n = 10^7$) and solid lines correspond to asymptotic keys. For AS noise of $V_N = 10$, the reconciliation efficiency is $\beta = 0.95$, and the variance of the squeezed quadrature is $V = 0.1$ SNU.

reverse reconciliation, and entanglement in the middle. However, the performance gap narrows significantly as our protocol leverages multiple modes per user, enhancing channel parameter estimation and mitigating finite-size effects. This improvement brings the key rates closer to those achieved with GHZ states, reducing the impact of statistical fluctuations inherent in finite-size scenarios.

(3) *Bipartite key generation post-QCKA:* Our protocol significantly outperforms GHZ states in generating bipartite keys after the conference key agreement across all methods (direct reconciliation, reverse reconciliation, and entanglement in the middle). The ability to derive additional bipartite keys post-QCKA enhances the overall efficiency and security of the quantum network.

(4) *Bipartite key generation without QCKA:* When compared to downstream-access networks utilizing two-mode squeezed vacuum states with equivalent squeezing, our protocol achieves superior performance in generating bipartite keys without involving QCKA. This demonstrates the versatility of our protocol in supporting both conference and individual key generation within the network.

(5) *Robustness to imperfections:* The protocol maintains its advantages even when using impure squeezed states (provided the impurity is trusted), demonstrating robustness against experimental imperfections. This robustness is critical for practical implementations where perfect state preparation is challenging.

VIII. CONCLUSION

In this work, we have introduced a novel protocol for three-user conference key generation using dual-rail cluster states, employing the concept of a *quotient graph state* to create a six-mode pure graph state suitable for cryptographic applications. Our comparative analysis with GHZ/W states generated under similar squeezing conditions has yielded significant insights.

In the asymptotic regime, where the number of signals approaches infinity, our protocol outperforms GHZ/W states in the direct reconciliation scheme but does not surpass them in reverse reconciliation or entanglement-in-the-middle schemes. In the finite-size regime, GHZ states still perform marginally better in each scheme. However, the performance gap narrows significantly as our protocol benefits from each user accessing multiple modes, which enhances channel parameter estimation and mitigates finite-size effects. This improved estimation reduces the impact of statistical fluctuations, bringing the maximum achievable distances closer to those achieved with GHZ states.

Additionally, our protocol significantly outperforms GHZ/W states in generating bipartite keys after the conference key agreement across all methods. It also surpasses downstream-access networks utilizing two-mode squeezed vacuum states in generating bipartite keys without involving QCKA. This versatility demonstrates the adaptability of our protocol in supporting both conference and individual secure communications within the network.

Our protocol maintains its advantages even when using impure squeezed states, showcasing robustness against experimental imperfections. This robustness is critical for practical implementations where perfect state preparation is challenging.

These results underscore the importance of tailoring quantum cryptographic solutions to the specific demands of quantum networks. The use of dual-rail cluster states and quotient graph states provides a pathway to more robust, flexible, and efficient quantum cryptographic protocols with continuous-variable systems.

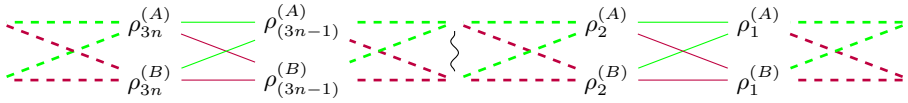


FIG. 10. Dual-rail cluster state ρ_{dual} comprising two parallel rails (A and B). Each node is labeled by its rail and position i.

Looking ahead, the insights gained from this work highlight several promising directions for future research. Exploring alternative multipartite states with configurations that allow users to access multiple modes could further enhance key rates and robustness in quantum communication protocols. Extending the protocol to networks with more than three users and examining the performance benefits in larger, more complex quantum networks is a natural progression. Developing advanced methods for channel parameter estimation that leverage access to multiple modes per user could further mitigate finite-size effects and improve the security and efficiency of the protocols. A crucial next step for this protocol is its experimental implementation, which presents a set of engineering challenges. For scalable, time-multiplexed resources, a central challenge is the engineering of high-speed optical switches to demultiplex and distribute modes to multiple users. While minimizing loss is ideal, the security framework can accommodate these losses if the device is trusted and well characterized, shifting the problem toward precise calibration. Additionally, extending the security analysis to consider more sophisticated eavesdropping strategies would verify the protocol's robustness against a wider range of attacks.

ACKNOWLEDGMENTS

I would like to acknowledge Vladyslav Usenko, Ivan Derkach, Tobias Gehring, Christoph Pacher, Florian Kanitschar, and Ulrik Lund Andersen for valuable discussions. I acknowledge the project 8C22002 (CVStar) of the Czech Ministry of Education, Youth and Sports, which has received funding from the European Union's Horizon 2020 Research and Innovation Framework Programme under Grant Agreements No. 731473 and No. 101017733, and the Project No. 21-44815L of the Czech Science Foundation. I also acknowledge the project IGA-PrF-2025-010 of Palacký University Olomouc. This work has also received funding from the European Union's Horizon Europe research and innovation programme under the project "Quantum Security Networks Partnership" (QSNP, Grant Agreement No. 101114043).

DATA AVAILABILITY

The data that support the findings of this article are not publicly available. The data are available from the author upon reasonable request.

APPENDIX A: DUAL-RAIL CLUSTER STATE TO SIX-MODE GRAPH STATE

In Sec. V, we introduced a method to generate a pure six-mode graph state from a dual-rail cluster state. Here, we provide a justification for this method. Since we are working with Gaussian states, it suffices to show that, after appropriately grouping the nodes as suggested by the coloring scheme in Fig. 4(a), the covariance matrix of the resulting state corresponds to that of a pure six-mode graph state.

The dual-rail cluster state, denoted here by ρ_{dual}, consists of two parallel chains (rails) of quantum states: rail A and rail B. Each node (quantum state) in these rails is uniquely identified by its rail (A or B) and its position i along that rail, as illustrated in Fig. 10.

To construct the six-mode graph state, we group the nodes from each rail into three groups by selecting every third node. For each node at position i in rail R, we define the constituent state $\rho_i^{(R)}$ as the reduced density operator obtained by tracing out all other nodes from the dual-rail cluster state ρ_{dual}:

$$\rho_i^{(R)} = \text{Tr}_i^{(R)}(\rho_{\text{dual}}).$$

Here $\text{Tr}_i^{(R)}$ denotes the partial trace over all modes except the one at position i in rail R. We then form statistical mixtures by averaging the constituent states within each group. For each group $j \in \{1,2,3\}$ in rail R, the mixed state $\boldsymbol{\rho}_j^{(R)}$ is defined as

$$\boldsymbol{\rho}_j^{(R)} = \frac{1}{n}\sum_{m=1}^{n} \rho_{3m-(3-j)}^{(R)}, \tag{A1}$$

where n is the total number of grouping repetitions along each rail. Specifically, the positions i of the nodes included in each group are as follows:

(1) for $j = 1$, positions $i = 3m - 2$,
(2) for $j = 2$, positions $i = 3m - 1$, and
(3) for $j = 3$, positions $i = 3m$,

with $m \in \{1, 2, \ldots, n\}$.

By forming these statistical mixtures, we create six mixed states in total (three groups in each of the two rails). The quadrature operators associated with these mixed states are denoted $\boldsymbol{x}_j^{(R)}$ and $\boldsymbol{p}_j^{(R)}$, where $j \in \{1,2,3\}$ and $R \in \{A, B\}$.

Since the constituent states $\rho_i^{(R)}$ are uncorrelated in the statistical mixture, the variances and covariances of the quadratures of these mixed states are given by

$$\left\langle \left(\boldsymbol{X}_j^{(R)}\right)^2 \right\rangle = \frac{1}{n}\sum_{m=1}^{n} \left\langle \left(X_{3m-(3-j)}^{(R)}\right)^2 \right\rangle, \tag{A2}$$

$$\frac{1}{2}\left\langle \left[\boldsymbol{X}_p^{(R)}, \boldsymbol{X}_q^{(S)}\right]_+ \right\rangle = \frac{1}{2n}\sum_{m=1}^{n} \left\langle \left[X_{3m-(3-p)}^{(R)}, X_{3m-(3-q)}^{(S)}\right]_+ \right\rangle, \tag{A3}$$

where $R, S \in \{A, B\}$, $p = 2$, $q \in \{1, 3\}$, $X_i^{(R)} \in \{x_i^{(R)}, p_i^{(R)}\}$, with $[\,\cdot\,]_+$ denoting the anticommutator, and

$$\frac{1}{2}\left\langle \left[\boldsymbol{X}_1^{(k)}, \boldsymbol{X}_3^{(l)}\right]_+ \right\rangle = \frac{1}{2n}\sum_{m=2}^{n} \left\langle \left[X_{3m-3}^{(k)}, X_{3m-2}^{(l)}\right]_+ \right\rangle. \tag{A4}$$

The covariance matrix of the six-mode graph state is then constructed from these variances and covariances. We arrange the quadrature operators in the following order:

$$\boldsymbol{X} = \left(\boldsymbol{x}_1^{(A)}, \boldsymbol{p}_1^{(A)}, \boldsymbol{x}_1^{(B)}, \boldsymbol{p}_1^{(B)}, \boldsymbol{x}_2^{(A)}, \boldsymbol{p}_2^{(A)}, \boldsymbol{x}_2^{(B)}, \boldsymbol{p}_2^{(B)}, \boldsymbol{x}_3^{(A)}, \boldsymbol{p}_3^{(A)}, \boldsymbol{x}_3^{(B)}, \boldsymbol{p}_3^{(B)}\right)^T. \tag{A5}$$

With this ordering, the covariance matrix $\boldsymbol{\sigma}$ of the six-mode graph state is given by

$$\boldsymbol{\sigma} = \begin{pmatrix} \boldsymbol{V} & \boldsymbol{0} & \boldsymbol{C} & -\boldsymbol{C} & \frac{n-1}{n}\boldsymbol{C} & \frac{n-1}{n}\boldsymbol{C} \\ \boldsymbol{0} & \boldsymbol{V} & \boldsymbol{C} & -\boldsymbol{C} & -\frac{n-1}{n}\boldsymbol{C} & -\frac{n-1}{n}\boldsymbol{C} \\ \boldsymbol{C} & \boldsymbol{C} & \boldsymbol{V} & \boldsymbol{0} & \boldsymbol{C} & -\boldsymbol{C} \\ -\boldsymbol{C} & -\boldsymbol{C} & \boldsymbol{0} & \boldsymbol{V} & \boldsymbol{C} & -\boldsymbol{C} \\ \frac{n-1}{n}\boldsymbol{C} & -\frac{n-1}{n}\boldsymbol{C} & \boldsymbol{C} & \boldsymbol{C} & \boldsymbol{V} & \boldsymbol{0} \\ \frac{n-1}{n}\boldsymbol{C} & -\frac{n-1}{n}\boldsymbol{C} & -\boldsymbol{C} & -\boldsymbol{C} & \boldsymbol{0} & \boldsymbol{V} \end{pmatrix}. \tag{A6}$$

Here, $\boldsymbol{V}$ and $\boldsymbol{C}$ are 2×2 matrices representing the variances and covariances of the quadrature operators, respectively. These can be expressed as a function related to the squeezed quadrature variance v and excess AS noise of the squeezed state employed in generating the dual-rail cluster state, Eq. (32). Specifically, $\boldsymbol{V}$ is the covariance matrix of a single mixed state, and $\boldsymbol{C}$ captures the correlations between different mixed states.

The factor $(n-1)/n$ within the covariance matrix is due to the fact that the count of vertices in a group that includes the extreme vertices cannot match the number of edges linking them. This factor makes the multipartite Gaussian state impure. One can purify this impurity, introduced due to finite states, by introducing additional modes. Alternatively, one can consider a pure six-mode covariance matrix by removing the factor $(n-1)/n$. Introducing additional modes to purify the covariance matrix in Eq. (A6) would give us a tighter bound than considering the covariance matrix in Eq. (30). That is, considering the pure six-mode covariance matrix to estimate the Holevo bound is more pessimistic than considering a purified state corresponding to the covariance matrix in Eq. (A6) to estimate the Holevo bound. For sufficiently large n, the covariance matrix $\boldsymbol{\sigma}$ can be approximated to Eq. (30), a pure six-mode state, and hence the improvement achieved through purification is insignificant.

APPENDIX B: CONGRUENCE TRANSFORMATION FOR COVARIANCE MATRICES

Given an original covariance matrix $\boldsymbol{\Sigma}$ of dimension $12n \times 12n$, of the modes of the dual-rail cluster state under consideration for grouping, we can derive the covariance matrix $\boldsymbol{\sigma}$ of dimension 12×12 corresponding to the six-mode graph state. This is achieved by applying a congruence transformation using a matrix $\boldsymbol{A}$ of size $12 \times 12n$, such that

$$\boldsymbol{\sigma} = \frac{1}{n}\boldsymbol{A}\boldsymbol{\Sigma}\boldsymbol{A}^T. \tag{B1}$$

The ordering of quadratures in the covariance matrix of the modes of the dual-rail cluster states considered for grouping is

$$(x_1^{(a)}, p_1^{(a)}, x_1^{(b)}, p_1^{(b)}, x_2^{(a)}, p_2^{(a)}, x_2^{(b)}, p_2^{(b)} \ldots). \tag{B2}$$

Here, $\boldsymbol{A}^T$ denotes the transpose of $\boldsymbol{A}$. This operation effectively projects the original covariance matrix onto a lower-dimensional subspace defined by $\boldsymbol{A}$, capturing the relevant quadrature correlations between the groups (color classes) of modes.

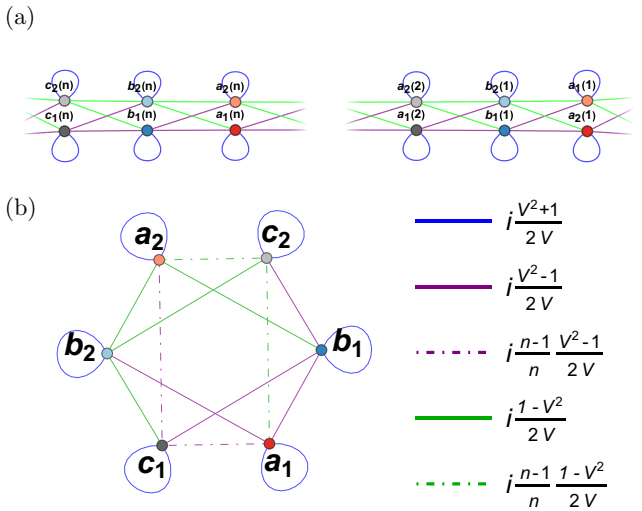


FIG. 11. (a) Complex weighted graph of dual-rail cluster state. (b) Complex weighted graph of quotient graph derived from dual-rail cluster state.

The matrix $\boldsymbol{A}$ consists of vectors that indicate the modes present within a color class:

$$\boldsymbol{A}_{ij} = \begin{cases} 1 & \text{if } j \equiv i \pmod{11}, \\ 0 & \text{otherwise.} \end{cases} \tag{B3}$$

A congruence transformation for the covariance matrix is possible provided the modes within each color class remain uncorrelated. However, if correlations exist among modes within a color class, the congruence transformation outlined above does not yield the covariance matrix of the statistical mixture defined by such a coloring scheme. Note that

$$\boldsymbol{X}_{\text{six-mode}} \neq \frac{1}{\sqrt{n}}\boldsymbol{A}\boldsymbol{X}_{\text{dual}}.$$

Based on the above congruence transformation, one might be inclined to define the quadrature operation of the six-mode graph state as a linear combination of the quadrature operators from the constituent states in the dual-rail cluster state. However, it is essential to recognize that statistical mixtures cannot be represented by linear transformations of quadrature operators because the modes are not coherently combined. Instead, the covariance matrix of the mixture is the average of the covariance matrices of the constituent states.

1. Congruence transformation for adjacency matrices

A complex-weighted adjacency matrix is used in continuous-variable quantum computing to represent Gaussian pure states, extending the real-weighted graphs of ideal cluster states to more realistic, physical states [40]. This formalism simplifies the analysis of entanglement structures, Gaussian operations, and deviations from ideal behaviors, which are essential for applications in CV quantum computing. Thus, we define a similar transformation to the one used in the previous section, enabling us to derive the adjacency matrix for a six-mode graph state $\boldsymbol{Z}_{\text{six-mode}}$ from the adjacency matrix of a dual-rail cluster state $\boldsymbol{Z}_{\text{dual}}$:

$$\boldsymbol{Z}_{\text{six-mode}} = \frac{1}{n}\boldsymbol{B}\boldsymbol{Z}_{\text{dual}}\boldsymbol{B}^T \tag{B4}$$

$$\boldsymbol{B}_{ij} = \begin{cases} 1 & \text{if } j \equiv i \pmod{5}, \\ 0 & \text{otherwise.} \end{cases} \tag{B5}$$

The corresponding complex-weighted graph of the dual-rail lattice and the resulting six-mode quotient graph are shown in Fig. 11.

APPENDIX C: RATIONALE FOR THE COLORING STRATEGY

To convert the infinitely repeating dual-rail cluster lattice into a finite resource that is easy to manipulate in security proofs, we map groups of physical modes onto *color classes* and then merge every class into a single vertex; the resulting state is called a *quotient graph state*.

1. Operational procedure

The coloring we adopt is engineered to satisfy the following two operational requirements.

(1) *Neighborhood preservation:* The quotient must retain all edges that enter the closed neighborhood $N[v]$ of at least one vertex v in the original lattice, so that any pair of modes that were immediate neighbors remain directly correlated after the homomorphism.

(2) *Purity:* The quotient state should be a *pure* Gaussian graph state; purity simplifies both covariance-matrix algebra and the security analysis in Sec. III.

The procedure is generic and can be reused for other cluster topologies; we describe it once here and apply it to the dual-rail lattice below.

Step 1: Identify a unit cell that encloses a full closed neighborhood. Let $G = (V, E)$ be the graph of the open-ended lattice. We search for the smallest *induced* subgraph $G_{\text{cell}} \subset G$ that contains a vertex v together with all vertices in $N[v]$. For the dual-rail lattice, this unit cell contains six vertices: two from each rail at positions $3m-2$, $3m-1$, and $3m$ ($m \in \mathbb{Z}$).

Step 2: Assign one color per vertex inside the cell. Each vertex of G_{cell} receives a distinct color $c \in 1, \ldots, |V(G_{\text{cell}})|$. Translational tiling of the cell propagates this coloring across the infinite lattice, producing exactly six global color classes in the dual-rail case.

Step 3: Form the quotient graph. Vertices that share the same color are identified (fused) into a single vertex. If

colors c_i and c_j appeared on adjacent physical vertices, the corresponding quotient vertices are connected by an edge. Algebraically, if Z_{dual} is the complex-weighted adjacency matrix of the dual-rail lattice, the quotient adjacency matrix is obtained via the congruence transformation

$$Z_{\text{quot}} = \frac{1}{n} B Z_{\text{dual}} B^T, \tag{C1}$$

where the selector matrix B is defined in Appendix B and n is the number of cell repetitions.

Step 4: Verify purity and neighborhood fidelity. The same transformation applied to the lattice covariance matrix Σ yields

$$\sigma = \frac{1}{n} A \Sigma A^T, \tag{C2}$$

with A given in Eq. (B3). Taking the limit $n \to \infty$ removes boundary terms proportional to $(n-1)/n$, leaving the six-mode covariance matrix of Eq. (30) which is pure ($\text{Det}[\sigma] = 1$). Moreover, every edge that linked a vertex to its first neighbors inside G_{cell} survives in Z_{quot}, so immediate-neighbor correlations are identical to those of the parent lattice.

2. Result for the dual-rail lattice

Applying the above steps to the dual-rail cluster yields the coloring shown in Fig. 4(a). The six color classes correspond to the vertices a_1, a_2, b_1, b_2, c_1, and c_2 of Fig. 4(b). This six-mode pure quotient graph state is the smallest resource that simultaneously preserves all closed-neighborhood correlations and admits a compact security proof.

3. Reuse for other lattices

For any future cluster geometry, one simply (i) locates a cell containing a full neighborhood, (ii) assigns unique colors to its vertices, and (iii) repeats the tiling. The size of the quotient graph is bounded below by the cardinality of that neighborhood and above by the chromatic number of the lattice.

APPENDIX D: PARAMETER ESTIMATION

To estimate the channel transmission t, we use the fact that the correlation between the measurements of the dealer and the remote user scales as $\sqrt{t}$. Specifically, we can estimate the channel transmission from the following relation:

$$\sqrt{t}\mathcal{C} = \frac{1}{n}\sum_{i=1}^{n} d_i u_i := C_{du}, \tag{D1}$$

where $\mathcal{C} = (1/2)\langle [X^d, X^u]_+ \rangle$ is the expectation value of the anticommutator of the quadrature operators X^d and X^u, measured by the dealer and the user before the state is sent through the channel. Here, d_i and u_i are the measurement outcomes corresponding to these quadratures for the dealer and the remote user, respectively.

We define C_{du} as

$$C_{du} := \frac{1}{n}\sum_{i=1}^{n} d_i u_i, \tag{D2}$$

which serves as an estimator for $\sqrt{t}\mathcal{C}$.

Rearranging the equation, we express the transmission t as

$$t = \left(\frac{C_{du}}{\mathcal{C}}\right)^2. \tag{D3}$$

Since C_{du} is a random variable due to measurement fluctuations, we are interested in the variance of our estimator for t:

$$\text{Var}[t] = \frac{\text{Var}[C_{du}^2]}{\mathcal{C}^4}. \tag{D4}$$

Assuming that C_{du} is approximately normally distributed (by the central limit theorem, since it is the average of n independent measurements), C_{du}^2 follows a noncentral chi-squared distribution with one degree of freedom. The variance of C_{du}^2 is given by

$$\text{Var}[C_{du}^2] = 2(\text{Var}[C_{du}])^2 + 4(\mathbb{E}[C_{du}])^2 \,\text{Var}[C_{du}]. \tag{D5}$$

Since C_{du} is an average over n terms, its variance is

$$\text{Var}[C_{du}] = \frac{1}{n}\,\text{Var}[X^d \tilde{X}^u], \tag{D6}$$

where $\tilde{X}^u$ is the quadrature operator of the state that the user possesses after transmission through the channel, and X^u is the quadrature operator of the state before it is sent through the channel.

Substituting back, we have

$$\text{Var}[t] = \frac{2(\text{Var}[C_{du}])^2 + 4(\mathbb{E}[C_{du}])^2 \,\text{Var}[C_{du}]}{\mathcal{C}^4}. \tag{D7}$$

For large n, the term $2(\text{Var}[C_{du}])^2$ is of order $1/n^2$ and can be neglected compared to $4(\mathbb{E}[C_{du}])^2\,\text{Var}[C_{du}]$, which is of

order $1/n$. Therefore, we approximate

$$\mathrm{Var}[t] \approx \frac{4(\mathbb{E}[C_{du}])^2\,\mathrm{Var}[C_{du}]}{\mathcal{C}^4}. \tag{D8}$$

Substituting $\mathrm{Var}[C_{du}] = (1/n)\,\mathrm{Var}[X^d\tilde{X}^u]$ and $\mathbb{E}[C_{du}] = \mathbb{E}[X^d\tilde{X}^u]$, we obtain

$$\mathrm{Var}[t] \approx \frac{4(\mathbb{E}[X^d\tilde{X}^u])^2\,\mathrm{Var}[X^d\tilde{X}^u]}{n\mathcal{C}^4} = \frac{4t\,\mathrm{Var}[X^d\tilde{X}^u]}{n\mathcal{C}^2}. \tag{D9}$$

In Ref. [41], we have shown that combining the measurement outcomes of both quadratures can increase the precision of our estimation of the channel transmission. Here, we apply the same principle by leveraging multiple correlations to decrease the variance of our estimators. For example, when the dealer has two modes that are correlated with the user's measurements, we can define the estimator

$$\sqrt{t}\left(\frac{\mathcal{C}^a + \mathcal{C}^b}{2}\right) = \frac{1}{2n}\left(\sum_{i=1}^{n} d_i^a u_i + \sum_{i=1}^{n} d_i^b u_i\right) := C_{du}, \tag{D10}$$

where $\mathcal{C}^i = \langle [X_i^d, X^u]_+ \rangle$ for $i = a, b$, and X_i^d are the quadratures of the modes possessed by the dealer.

For a symmetric case where $\mathcal{C}^a = \mathcal{C}^b$ and $\mathrm{Var}[X_a^d\tilde{X}^u] = \mathrm{Var}[X_b^d\tilde{X}^u]$, the new variance of the estimator for t becomes

$$\mathrm{Var}[t] \approx \frac{4t\,\mathrm{Var}[X^d\tilde{X}^u]}{2n\,\mathcal{C}^2}. \tag{D11}$$

We can generalize this result for any number k of symmetric correlations used to estimate the channel transmission:

$$\mathrm{Var}[t] \approx \frac{4t\,\mathrm{Var}[X^d\tilde{X}^u]}{kn\,\mathcal{C}^2}. \tag{D12}$$

Thus, by leveraging multiple correlated modes, we reduce the variance of the estimator for the transmission t by a factor of k, enhancing the precision of our estimation.

We estimate the excess noise as follows:

$$V_\epsilon = \frac{1}{n}\sum_{i}^{n} u_i^2 + t(1 - \mathrm{Var}[X^u]) - 1. \tag{D13}$$

The variance of the excess noise estimator can be approximated to

$$\mathrm{Var}[V_\epsilon] \approx \frac{2}{n}(\mathrm{Var}[\tilde{X}^u])^2 + \mathrm{Var}[t](1 - \mathrm{Var}[X^u])^2. \tag{D14}$$

We now define the quadrature operators x_d and x_u for the three multipartite states under consideration. Recall that the tilde notation $\tilde{x}_u$ has been introduced earlier to represent sending a mode with quadrature x_u through a channel with transmission t, specifically $\tilde{x}_u = \sqrt{t}\,x_u + \sqrt{1-t}\,x_0$, where x_0 is the quadrature operator of a vacuum state.

In protocols involving a six-mode graph state, the quadrature of each mode is a linear function composed of quadratures from four squeezed states. Any two modes have two of these squeezed states quadrature in common. Consequently, any two correlated modes of a six-mode graph state can be expressed in terms of the quadrature operators of six squeezed states, all characterized by the same quadrature variance. For example, consider the following two quadratures corresponding to dealer's mode x_d and mode meant for a remote user x_u:

$$x_d = \tfrac{1}{2}(p^{(2)} + p^{(4)} - x^{(1)} + x^{(3)}), \tag{D15}$$

$$x_u = \tfrac{1}{2}(\mp p^{(4)} + p^{(6)} \pm x^{(3)} + x^{(5)}). \tag{D16}$$

Here, $x^{(i)}$ denotes a squeezed quadrature with variance V, while $p^{(i)}$ denotes the corresponding antisqueezed quadrature with variance $V_N + 1/V$.

Since we are dealing with Gaussian states, straightforward algebraic manipulations yield the following expression for the variance $\mathrm{Var}[x_d\tilde{x}_u]$:

$$\mathrm{Var}[x_d\tilde{x}_u] = \frac{t}{16}\left(5\left(V_N + \frac{1}{V}\right)^2 + 5V^2 + 6\left(V_N + \frac{1}{V}\right)V\right) + (1-t)\left(\frac{1 + V(V_N + V)}{2V}\right). \tag{D17}$$

Turning to the three-mode GHZ state, the relevant quadratures are given by

$$x_1 = \frac{\sqrt{2}\,p^{(1)} + x^{(2)} + \sqrt{3}\,x^{(3)}}{\sqrt{6}},$$
$$x_2 = \frac{\sqrt{2}\,x^{(2)} - p^{(1)}}{\sqrt{3}}, \tag{D18}$$
$$x_3 = \frac{-\sqrt{2}\,p^{(1)} - x^{(2)} + \sqrt{3}\,x^{(3)}}{\sqrt{6}}.$$

Although two of these modes incorporate quadrature components from three squeezed states each, and one mode has components from only two squeezed states, this difference does not influence the choice of which mode is sent through the transmission channel. The variance $\mathrm{Var}[x_d\tilde{x}_u]$ remains the same, given by

$$\mathrm{Var}[x_d\tilde{x}_u] = \frac{t}{9}\left(2\left(V_N + \frac{1}{V}\right)^2 + 5V^2 + 2\left(V_N + \frac{1}{V}\right)V\right) + (1-t)\left(\frac{1 + V(V_N + 2V)}{3V}\right). \tag{D19}$$

For a DAN with a two-mode squeezed vacuum, the relevant quadratures for the dealer and the remote user modes are

$$x_d = \frac{x^{(1)} + p^{(2)}}{\sqrt{2}} \quad \text{and} \quad x_u = \frac{1}{2}(\sqrt{2}p^{(0)} - x^{(1)} + p^{(2)}). \tag{D20}$$

Similarly, we obtain

$$\mathrm{Var}[x_d \tilde{x}_u] = \frac{t}{8}\left(V_N + \frac{1}{V}\right)\left(V_N + \frac{1}{V} + 1\right) + V(1+V) + (1-t)\left(\frac{1 + V(V_N + V)}{2V}\right). \tag{D21}$$

[1] J. Wang, G.-B. Xu, and D.-H. Jiang, Quantum voting scheme with Greenberger–Horne–Zeilinger states, Int. J. Theor. Phys. **59**, 2599 (2020).

[2] Y. Guo, Y. Feng, and G. Zeng, Quantum anonymous voting with unweighted continuous-variable graph states, Quantum Inf. Process. **15**, 3327 (2016).

[3] Q. Wang, C. Yu, F. Gao, H. Qi, and Q. Wen, Self-tallying quantum anonymous voting, Phys. Rev. A **94**, 022333 (2016).

[4] H.-K. Lau and C. Weedbrook, Quantum secret sharing with continuous-variable cluster states, Phys. Rev. A **88**, 042313 (2013).

[5] Y. Wu, R. Cai, G. He, and J. Zhang, Quantum secret sharing with continuous variable graph state, Quantum Inf. Process. **13**, 1085 (2014).

[6] A. Karlsson, M. Koashi, and N. Imoto, Quantum entanglement for secret sharing and secret splitting, Phys. Rev. A **59**, 162 (1999).

[7] D. Pan, G.-L. Long, L. Yin, Y.-B. Sheng, D. Ruan, S. X. Ng, J. Lu, and L. Hanzo, The evolution of quantum secure direct communication: On the road to the Qinternet, IEEE Commun. Surv. Tutorials **26**, 1898 (2024).

[8] C. Wang, F. G. Deng, and G. L. Long, Multi-step quantum secure direct communication using multi-particle Greenberger–Horne–Zeilinger state, Opt. Commun. **253**, 15 (2005).

[9] G. Murta, F. Grasselli, H. Kampermann, and D. Bruß, Quantum conference key agreement: A review, Adv. Quantum Technol. **3**, 2000025 (2020).

[10] W. Zhao, R. Shi, Y. Feng, and X. Ruan, Conference key agreement based on continuous-variable quantum key distribution, Laser Phys. Lett. **18**, 075205 (2021).

[11] N. C. Menicucci, P. van Loock, M. Gu, C. Weedbrook, T. C. Ralph, and M. A. Nielsen, Universal quantum computation with continuous-variable cluster states, Phys. Rev. Lett. **97**, 110501 (2006).

[12] N. C. Menicucci, Fault-tolerant measurement-based quantum computing with continuous-variable cluster states, Phys. Rev. Lett. **112**, 120504 (2014).

[13] M. V. Larsen, C. Chamberland, K. Noh, J. S. Neergaard-Nielsen, and U. L. Andersen, Fault-tolerant continuous-variable measurement-based quantum computation architecture, PRX Quantum **2**, 030325 (2021).

[14] R. Raussendorf and H. J. Briegel, A one-way quantum computer, Phys. Rev. Lett. **86**, 5188 (2001).

[15] R. Raussendorf, D. E. Browne, and H. J. Briegel, Measurement-based quantum computation on cluster states, Phys. Rev. A **68**, 022312 (2003).

[16] N. C. Menicucci, X. Ma, and T. C. Ralph, Arbitrarily large continuous-variable cluster states from a single quantum nondemolition gate, Phys. Rev. Lett. **104**, 250503 (2010).

[17] N. C. Menicucci, Temporal-mode continuous-variable cluster states using linear optics, Phys. Rev. A **83**, 062314 (2011).

[18] S. Yokoyama, R. Ukai, S. C. Armstrong, C. Sornphiphatphong, T. Kaji, S. Suzuki, J.-i. Yoshikawa, H. Yonezawa, N. C. Menicucci, and A. Furusawa, Ultra-large-scale continuous-variable cluster states multiplexed in the time domain, Nat. Photonics **7**, 982 (2013).

[19] M. V. Larsen, X. Guo, C. R. Breum, J. S. Neergaard-Nielsen, and U. L. Andersen, Deterministic generation of a two-dimensional cluster state, Science **366**, 369 (2019).

[20] N. C. Menicucci, S. T. Flammia, H. Zaidi, and O. Pfister, Ultracompact generation of continuous-variable cluster states, Phys. Rev. A **76**, 010302(R) (2007).

[21] N. C. Menicucci, S. T. Flammia, and O. Pfister, One-way quantum computing in the optical frequency comb, Phys. Rev. Lett. **101**, 130501 (2008).

[22] M. Chen, N. C. Menicucci, and O. Pfister, Experimental realization of multipartite entanglement of 60 modes of a quantum optical frequency comb, Phys. Rev. Lett. **112**, 120505 (2014).

[23] J. Roslund, R. Medeiros de Araújo, S. Jiang, C. Fabre, and N. Treps, Wavelength-multiplexed quantum networks with ultrafast frequency combs, Nat. Photonics **8**, 109 (2014).

[24] A. Pickston, J. Ho, A. Ulibarrena, F. Grasselli, M. Proietti, C. L. Morrison, P. Barrow, F. Graffitti, and A. Fedrizzi, Conference key agreement in a quantum network, npj Quantum Inf. **9**, 82 (2023).

[25] G. Adesso, A. Serafini, and F. Illuminati, Multipartite entanglement in three-mode Gaussian states of continuous-variable systems: Quantification, sharing structure, and decoherence, Phys. Rev. A **73**, 032345 (2006).

[26] C. Godsil and G. Royle, *Algebraic Graph Theory*, Graduate Texts in Mathematics, Vol. 207 (Springer, New York, 2001).

[27] R. Band, O. Parzanchevski, and G. Ben-Shach, The isospectral fruits of representation theory: Quantum graphs and drums, J. Phys. A: Math. Theor. **42**, 175202 (2009).

[28] G. Mutlu, On the quotient quantum graph with respect to the regular representation, Commun. Pure Appl. Anal. **20**, 885 (2021).

[29] H. Krovi and T. A. Brun, Quantum walks on quotient graphs, Phys. Rev. A **75**, 062332 (2007).

[30] H.-Y. Hsieh, Y.-R. Chen, H.-C. Wu, H. L. Chen, J. Ning, Y.-C. Huang, C.-M. Wu, and R.-K. Lee, Extract the

degradation information in squeezed states with machine learning, Phys. Rev. Lett. **128**, 073604 (2022).
[31] C. Weedbrook, S. Pirandola, R. García-Patrón, N. J. Cerf, T. C. Ralph, J. H. Shapiro, and S. Lloyd, Gaussian quantum information, Rev. Mod. Phys. **84**, 621 (2012).
[32] R. García-Patrón and N. J. Cerf, Unconditional optimality of Gaussian attacks against continuous-variable quantum key distribution, Phys. Rev. Lett. **97**, 190503 (2006).
[33] I. Devetak and A. Winter, Relating quantum privacy and quantum coherence: An operational approach, Phys. Rev. Lett. **93**, 080501 (2004).
[34] I. Devetak and A. Winter, Distillation of secret key and entanglement from quantum states, Proc. R. Soc. A **461**, 207 (2005).
[35] S. Yang, Z. Yan, H. Yang, Q. Lu, Z. Lu, L. Cheng, X. Miao, and Y. Li, Information reconciliation of continuous-variables quantum key distribution: Principles, implementations and applications, EPJ Quantum Technol. **10**, 40 (2023).
[36] A. Leverrier, Composable security proof for continuous-variable quantum key distribution with coherent states, Phys. Rev. Lett. **114**, 070501 (2015).
[37] N. Walenta, A. Burg, D. Caselunghe, P. Trinkler, A. Poppe, T. Lunghi, C. Barreiro, M. Perrenoud, R. J. Hughes, and H. Zbinden, A fast and versatile quantum key distribution system with hardware key distillation and wavelength multiplexing, New J. Phys. **16**, 013047 (2014).
[38] A. Leverrier, F. Grosshans, and P. Grangier, Finite-size analysis of a continuous-variable quantum key distribution, Phys. Rev. A **81**, 062343 (2010).
[39] P. van Loock and S. L. Braunstein, Multipartite entanglement for continuous variables: A quantum teleportation network, Phys. Rev. Lett. **84**, 3482 (2000).
[40] N. C. Menicucci, S. T. Flammia, and P. van Loock, Graphical calculus for Gaussian pure states, Phys. Rev. A **83**, 042335 (2011).
[41] A. N. Oruganti, I. Derkach, R. Filip, and V. C. Usenko, Continuous-variable quantum key distribution with noisy squeezed states, Quantum Sci. Technol. **10**, 025023 (2025).