Secure Gaussian quantum state sharing for a network of five players

Dan Travers

Quantum state sharing (QSS) is the process by which a quantum state can be securely distributed among multiple recipients such that no individual can access it on their own but a large enough subset of the group can fully recreate it. In this report, the protocols for sharing a coherent secret state among five parties are proposed, such that any three of them can reconstruct the state, while the other two cannot. The level of entanglement that this (3,5)-threshold scheme requires to guarantee security is analysed, and an example physical set-up for one of the reconstruction protocols is presented.

I. INTRODUCTION

Quantum state sharing (QSS) is the process by which a quantum state can be securely distributed among multiple recipients such that no individual can access it on their own but a large enough subset of the group can fully recreate it [1]. A (k,n)-threshold scheme involves combining the secret state and resource states to form n different shares, such that a minimum of k of them must be recombined to reconstruct the state to some agreed-upon level of accuracy.

Previously, it has been shown that a (2,3)-threshold scheme can securely share an arbitrary coherent state by using a resource state which exhibits EPR steering [2]. In this report, it will be outlined how this scheme can be extended to securely share a coherent state in a (3,5)-threshold scheme by using two, two-mode, squeezed vacuum resource states. In the interest of keeping the analysis simple, transmission loss or quantum noise will not be considered.

Demonstrating that the next largest QSS scheme has a secure and feasible set of protocols provides a strong indication that much larger quantum state sharing schemes are achievable. These would enable larger computational networks and quantum communication systems to develop.

Secure QSS protocols have the potential to be extremely useful in the future in conjunction with quantum computers. For instance, QSS could allow quantum computers to carry out 'blind computing' [3]. Once a QSS protocol has split a secret quantum state into separate encrypted shares, these shares could be processed by different quantum computers separately. This guarantees that no single computer could access the encoded information. Then, once the computers had processed the shares, the outcome of the computation could be only accessed when the shares were recombined. Blind computing would thus allow users to have their confidential data processed by unverified quantum computers with full confidence. Another significant use case is secure communication, even in a situation where the security of any individual communication channel cannot be guaranteed. For instance, in a (3,5)-scheme, the principles of quantum mechanics guarantee that even if two communication channels (and thus two shares of the quantum state) were somehow compromised, the state would still be completely inaccessible to an eavesdropper.

In section II, it is outlined how the dealer protocol takes a secret state and the two resource states and mixes them into five different shares. Then, in section III, the optimal way of reconstructing the secret state given any three of the five shares is explored. After that, in section IV, the level of squeezing needed to entangle the resource states to reach the threshold of security is analysed. Finally, the findings are summarised and potential areas for future research related to this topic are considered.

II. THE DEALER PROTOCOL

The dealer protocol for the proposed (3,5)-threshold scheme is shown in Figure 1.

Before the dealer protocol, the scheme begins with an arbitrary coherent Gaussian secret state and two Gaussian resource states. A Gaussian state has a Gaussian Wigner function and is characterised by its mean vector and covariance matrix [4]. The covariance matrix for the secret state is simply the identity matrix since it is an unsqueezed, Gaussian state.

Each resource state is a two-mode, squeezed, vacuum state. The modes of each resource state are positively correlated in their X quadratures, and negatively correlated in their P quadratures. The mean vector of each resource state is taken to be zero without loss of generality, as their mean vectors have no impact on entanglement. The covariance matrix of a two-mode resource state with squeezing parameter r is given by

$$V_{\mathrm{EPR}} = \begin{pmatrix} \cosh 2r & 0 & \sinh 2r & 0 \\ 0 & \cosh 2r & 0 & -\sinh 2r \\ \sinh 2r & 0 & \cosh 2r & 0 \\ 0 & -\sinh 2r & 0 & \cosh 2r \end{pmatrix}. \tag{1}$$

The dealer protocol consists of running these shares through a set of beamsplitters to produce five different shares. These five shares are not pure states, but they can be written in shorthand notation (where the ket notation represents both the X and P quadratures) as

$$|1\rangle = \frac{1}{\sqrt{3}}|\psi\rangle + \sqrt{\frac{2}{3}}|a_1\rangle, \tag{2}$$

$$|2\rangle = \frac{1}{\sqrt{3}}|\psi\rangle - \frac{1}{\sqrt{6}}|a_1\rangle + \frac{1}{\sqrt{2}}|b_1\rangle, \tag{3}$$

$$|3\rangle = \frac{1}{\sqrt{3}}|\psi\rangle - \frac{1}{\sqrt{6}}|a_1\rangle - \frac{1}{\sqrt{2}}|b_1\rangle, \tag{4}$$

$$|4\rangle = \frac{1}{\sqrt{2}}|a_2\rangle + \frac{1}{\sqrt{2}}|b_2\rangle, \tag{5}$$

$$|5\rangle = \frac{1}{\sqrt{2}}|a_2\rangle - \frac{1}{\sqrt{2}}|b_2\rangle. \tag{6}$$

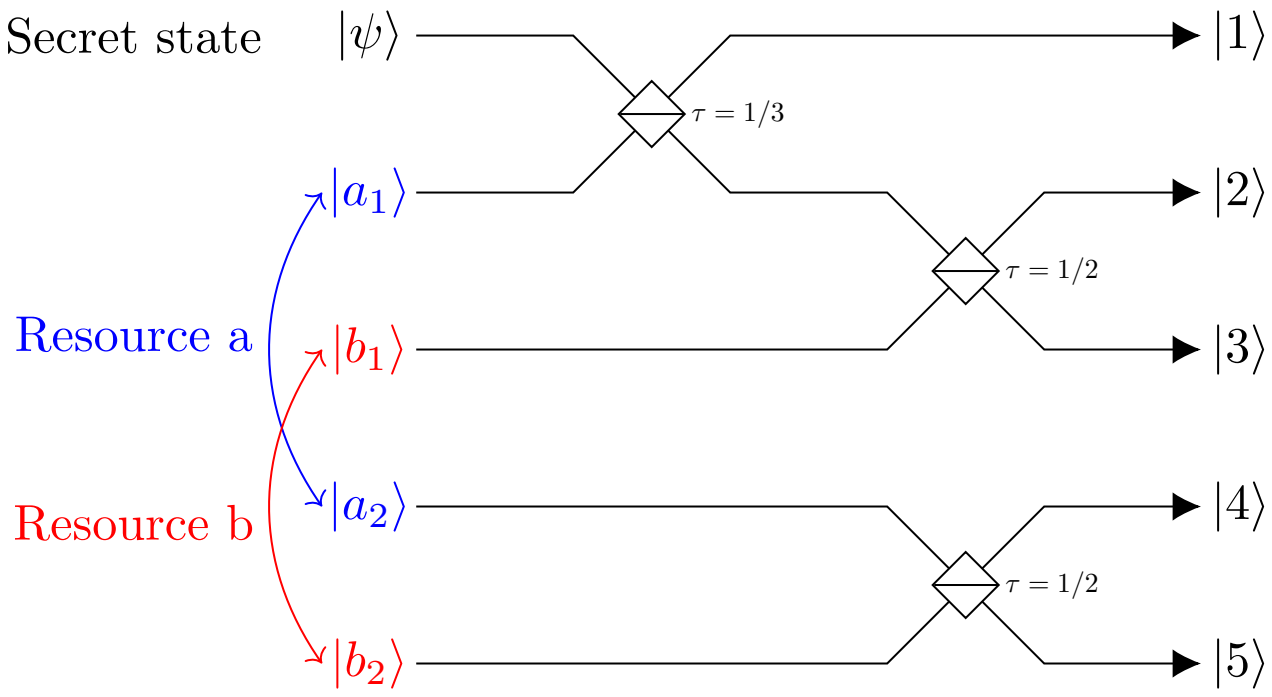

FIG. 1. The dealer protocol for the proposed (3,5)-threshold scheme. The secret state and four modes of two resource states are combined into five shares using beamsplitters.

The matrix which describes the action of the dealer protocol on the quadratures of the 5 initial states is

$$\begin{pmatrix} \hat{X}_1 \\ \hat{P}_1 \\ \hat{X}_2 \\ \hat{P}_2 \\ \hat{X}_3 \\ \hat{P}_3 \\ \hat{X}_4 \\ \hat{P}_4 \\ \hat{X}_5 \\ \hat{P}_5 \end{pmatrix} = \begin{pmatrix} \frac{1}{\sqrt{3}} & 0 & \sqrt{\frac{2}{3}} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & \frac{1}{\sqrt{3}} & 0 & \sqrt{\frac{2}{3}} & 0 & 0 & 0 & 0 & 0 & 0 \\ \frac{1}{\sqrt{3}} & 0 & -\frac{1}{\sqrt{6}} & 0 & 0 & 0 & \frac{1}{\sqrt{2}} & 0 & 0 & 0 \\ 0 & \frac{1}{\sqrt{3}} & 0 & -\frac{1}{\sqrt{6}} & 0 & 0 & 0 & \frac{1}{\sqrt{2}} & 0 & 0 \\ \frac{1}{\sqrt{3}} & 0 & -\frac{1}{\sqrt{6}} & 0 & 0 & 0 & -\frac{1}{\sqrt{2}} & 0 & 0 & 0 \\ 0 & \frac{1}{\sqrt{3}} & 0 & -\frac{1}{\sqrt{6}} & 0 & 0 & 0 & -\frac{1}{\sqrt{2}} & 0 & 0 \\ 0 & 0 & 0 & 0 & \frac{1}{\sqrt{2}} & 0 & 0 & 0 & \frac{1}{\sqrt{2}} & 0 \\ 0 & 0 & 0 & 0 & 0 & \frac{1}{\sqrt{2}} & 0 & 0 & 0 & \frac{1}{\sqrt{2}} \\ 0 & 0 & 0 & 0 & \frac{1}{\sqrt{2}} & 0 & 0 & 0 & -\frac{1}{\sqrt{2}} & 0 \\ 0 & 0 & 0 & 0 & 0 & \frac{1}{\sqrt{2}} & 0 & 0 & 0 & -\frac{1}{\sqrt{2}} \end{pmatrix} \begin{pmatrix} \hat{X}_\psi \\ \hat{P}_\psi \\ \hat{X}_{a_1} \\ \hat{P}_{a_1} \\ \hat{X}_{a_2} \\ \hat{P}_{a_2} \\ \hat{X}_{b_1} \\ \hat{P}_{b_1} \\ \hat{X}_{b_2} \\ \hat{P}_{b_2} \end{pmatrix}.$$

This dealer protocol is appropriate for two reasons. First, ψ is present in three shares, so whichever three shares are chosen, there is always some contribution from the secret state. Secondly, whichever three shares are chosen, there is always at least two components from the a resource state and two components from the b resource state, meaning it is possible to combine the quadratures of the shares in proportions which will cancel out the resource mode contributions as much as possible.

III. THE RECONSTRUCTION PROTOCOLS

For a QSS scheme to be secure, it must be ensured that the secret state can be reconstructed to a sufficient level of fidelity. Setting aside the trivial reconstruction of the {1,2,3} case, perfectly reconstructing the secret state is only possible in the limit of infinite squeezing and entanglement within the resource states. Therefore, we must consider how well reconstructed we would like the secret state to be. How well a state is reconstructed is measured in terms of fidelity. If fidelity equals 1, then the output state exactly resembles the initial state. A fidelity of 0 means the output state does not resemble the initial state at all. The level of fidelity we are considering as the benchmark of security is 2/3. If three shares are combined and a fidelity of 2/3 is reached, it is guaranteed that the collaborating parties have more information about the secret state than anyone else - even if the other two parties collaborate [5]. This is supported by the no-cloning theorem. Therefore, it is a suitable value of fidelity to require.

A reconstruction protocol describes the proportions in which the quadratures of the three shares should be combined to maximally cancel out the resource modes and accurately reconstruct the secret state. The reconstruction protocol will be different for each different combination of three shares since all of the shares are different.

Given that there are five shares, and we want to reconstruct the secret state with any three of them, the number of possible three-share combinations is $\binom{5}{3} = 10$. However, many of the three-share combinations are extremely similar. This is because shares two and three, and shares four and five differ only by a single phase difference in one of the resource mode contributions. The three-share combinations which have either shares two and three swapped, or shares four and five swapped will have very similar reconstruction protocols and the same entanglement requirements. Therefore, we group similar three-share combinations together in our analysis as follows:

A	**B**	**C**	**D**	**E**
1,2,3	1,2,4	1,4,5	2,3,4	2,4,5
	1,2,5		2,3,5	3,4,5
	1,3,4			
	1,3,5			

Rather than examining all 10 combinations, it is only necessary to analyse the first combination from each of these groupings. This is because it is expected that all share combinations within the same group yield the same fidelity as each other.

Because the X quadratures are positively correlated within modes from the same resource state and the P quadratures are negatively correlated, the proportions in which the quadratures are combined during a reconstruction protocol will be different. Therefore, a protocol which acts separately on each quadrature is required.

There are three constraints which determine the proportions that the quadratures should be mixed in. Firstly, it is desirable for the secret state not to be amplified or attenuated in the output; if the output state needed to be attenuated or amplified afterwards to obtain the original state, this would add noise and affect our final fidelity[4]. Secondly, it is desirable that the quadratures of resource state a cancel maximally and thirdly it is desirable that the quadratures of resource state b cancel maximally.

A. The {1,2,3} Protocol

The {1,2,3} reconstruction protocol is the trivial case. It is the only case where the X and P quadratures are combined in are the same proportions, and in which entanglement between different modes is not leveraged. Shares 1, 2 and 3 are formed by running ψ and the a_1 and the b_1 resource modes through two beamsplitters. For the reconstruction protocol, the shares can simply be run through the same apparatus backwards and the mixing can be undone to perfectly reconstruct the secret state.

The shares are

$$|1\rangle = \frac{1}{\sqrt{3}}|\psi\rangle + \sqrt{\frac{2}{3}}|a_1\rangle, \tag{7}$$

$$|2\rangle = \frac{1}{\sqrt{3}}|\psi\rangle - \frac{1}{\sqrt{6}}|a_1\rangle + \frac{1}{\sqrt{2}}|b_1\rangle, \tag{8}$$

$$|3\rangle = \frac{1}{\sqrt{3}}|\psi\rangle - \frac{1}{\sqrt{6}}|a_1\rangle - \frac{1}{\sqrt{2}}|b_1\rangle. \tag{9}$$

Throughout this report, shares or quadratures will be mixed with proportions of α, β and γ, with α corresponding to the lowest number share and γ corresponding to the highest one. To fulfil the constraints outlined previously, it is required that $\alpha = \beta = \gamma = \frac{1}{\sqrt{3}}$. Plugging this in confirms that the the secret state is fully recreated with no contributions from the resource modes:

$$\frac{1}{\sqrt{3}}|1\rangle + \frac{1}{\sqrt{3}}|2\rangle + \frac{1}{\sqrt{3}}|3\rangle = |\psi\rangle. \tag{10}$$

In matrix form, the reconstruction channel acting on the shares is

$$\begin{pmatrix} \frac{1}{\sqrt{3}} & \frac{1}{\sqrt{3}} & \frac{1}{\sqrt{3}} \\ & & \end{pmatrix} \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix} = \begin{pmatrix} \text{Output} \\ \end{pmatrix} = \begin{pmatrix} \psi \\ \end{pmatrix}. \tag{11}$$

The blank spaces represent the other two output beams of the reconstruction channel. Since we only are interested in one primary output beam, the other entries can be arbitrary. The only constraint is that the reconstruction matrix satisfies the relevant uncertainty relations. A quantum channel matrix, T, satisfies the canonical commutation relations when it satisfies the following positive semi-definite condition [4]:

$$i\Omega - iT\Omega T^T \geq 0, \tag{12}$$

where T^T is the transpose of T and Ω is the simplectic matrix of the form

$$\Omega = \bigoplus_n \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}. \tag{13}$$

The positive semi-definite condition $M \geq 0$ is satisfied when the real number $z^* M z$ is positive or zero for every non-zero complex column vector z, where z^* is the complex conjugate transpose of z.

B. The {1,2,4} Protocol

The quadratures that need to be combined in this protocol are

$$\hat{X}_1 = \frac{1}{\sqrt{3}}\hat{X}_\psi + \sqrt{\frac{2}{3}}\hat{X}_{a1}, \tag{14}$$

$$\hat{X}_2 = \frac{1}{\sqrt{3}}\hat{X}_\psi - \frac{1}{\sqrt{6}}\hat{X}_{a1} + \frac{1}{\sqrt{2}}\hat{X}_{b1}, \tag{15}$$

$$\hat{X}_4 = \frac{1}{\sqrt{2}}\hat{X}_{a2} + \frac{1}{\sqrt{2}}\hat{X}_{b2}, \tag{16}$$

$$\hat{P}_1 = \frac{1}{\sqrt{3}}\hat{P}_\psi + \sqrt{\frac{2}{3}}\hat{P}_{a1}, \tag{17}$$

$$\hat{P}_2 = \frac{1}{\sqrt{3}}\hat{P}_\psi - \frac{1}{\sqrt{6}}\hat{P}_{a1} + \frac{1}{\sqrt{2}}\hat{P}_{b1}, \tag{18}$$

$$\hat{P}_4 = \frac{1}{\sqrt{2}}\hat{P}_{a2} + \frac{1}{\sqrt{2}}\hat{P}_{b2}. \tag{19}$$

By fulfilling the constraints outlined at the beginning of section III, it is found that the X and P quadratures must be mixed in the following proportions:

$$X_1 + (\sqrt{3}-1)X_2 + (1-\sqrt{3})X_4 = \hat{X}_\psi + \frac{\sqrt{6}-\sqrt{2}}{2}(\hat{X}_{a1} - \hat{X}_{a2}) + \frac{\sqrt{6}-\sqrt{2}}{2}(\hat{X}_{b1} - \hat{X}_{b2}), \tag{20}$$

$$P_1 + (\sqrt{3}-1)P_2 + (\sqrt{3}-1)P_4 = \hat{P}_\psi + \frac{\sqrt{6}-\sqrt{2}}{2}(\hat{P}_{a1} + \hat{P}_{a2}) + \frac{\sqrt{6}-\sqrt{2}}{2}(\hat{P}_{b1} + \hat{P}_{b2}). \tag{21}$$

The modes within a resource state in the X quadratures are added in opposite proportions, and since they are positively correlated, they maximally cancel. Similarly, the modes within a resource state in the P quadratures are added in the same proportions, and since they are negatively correlated, they maximally cancel too. However, they do not cancel out perfectly. The degree to which the resource mode contributions cancel depends on the strength of entanglement between them. The stronger the entanglement between the modes in a resource state, the more correlated their quadratures, the more completely they cancel and the better the fidelity of the output state.

In matrix form, the reconstruction channel acting on the share quadratures is

$$\begin{pmatrix} 1 & 0 & \sqrt{3}-1 & 0 & 1-\sqrt{3} & 0 \\ 0 & 1 & 0 & \sqrt{3}-1 & 0 & \sqrt{3}-1 \\ & & & & & \\ & & & & & \\ & & & & & \\ & & & & & \end{pmatrix} \begin{pmatrix} \hat{X}_1 \\ \hat{P}_1 \\ \hat{X}_2 \\ \hat{P}_2 \\ \hat{X}_4 \\ \hat{P}_4 \end{pmatrix} = \begin{pmatrix} \hat{X}_{Out} \\ \hat{P}_{Out} \\ \\ \\ \\ \\ \end{pmatrix}. \tag{22}$$

C. The {1,4,5} Protocol

The quadratures that need to be combined in this protocol are

$$\hat{X}_1 = \frac{1}{\sqrt{3}}\hat{X}_\psi + \sqrt{\frac{2}{3}}\hat{X}_{a1}, \tag{23}$$

$$\hat{X}_4 = \frac{1}{\sqrt{2}}\hat{X}_{a2} + \frac{1}{\sqrt{2}}\hat{X}_{b2}, \tag{24}$$

$$\hat{X}_5 = \frac{1}{\sqrt{2}}\hat{X}_{a2} - \frac{1}{\sqrt{2}}\hat{X}_{b2}, \tag{25}$$

$$\hat{P}_1 = \frac{1}{\sqrt{3}}\hat{P}_\psi + \sqrt{\frac{2}{3}}\hat{P}_{a1}, \tag{26}$$

$$\hat{P}_4 = \frac{1}{\sqrt{2}}\hat{P}_{a2} + \frac{1}{\sqrt{2}}\hat{P}_{b2}, \tag{27}$$

$$\hat{P}_5 = \frac{1}{\sqrt{2}}\hat{P}_{a2} - \frac{1}{\sqrt{2}}\hat{P}_{b2}. \tag{28}$$

It is found that the X and P quadratures must be mixed in the following proportions:

$$\sqrt{3}X_1 - X_4 - X_5 = \hat{X}_\psi + \sqrt{2}(\hat{X}_{a1} - \hat{X}_{a2}), \tag{29}$$

$$\sqrt{3}P_1 + P_4 + P_5 = \hat{P}_\psi + \sqrt{2}(\hat{P}_{a1} + \hat{P}_{a2}). \tag{30}$$

In matrix form, the reconstruction channel acting on the share quadratures is =

$$\begin{pmatrix} \sqrt{3} & 0 & -1 & 0 & -1 & 0 \\ 0 & \sqrt{3} & 0 & 1 & 0 & 1 \\ & & & & & \end{pmatrix} \begin{pmatrix} \hat{X}_1 \\ \hat{P}_1 \\ \hat{X}_4 \\ \hat{P}_4 \\ \hat{X}_5 \\ \hat{P}_5 \end{pmatrix} = \begin{pmatrix} \hat{X}_{Out} \\ \hat{P}_{Out} \\ \\ \\ \\ \end{pmatrix}. \tag{31}$$

D. The {2,3,4} Protocol

The quadratures that need to be combined in this protocol are

$$\hat{X}_2 = \frac{1}{\sqrt{3}}\hat{X}_\psi - \frac{1}{\sqrt{6}}\hat{X}_{a1} + \frac{1}{\sqrt{2}}\hat{X}_{b1}, \tag{32}$$

$$\hat{X}_3 = \frac{1}{\sqrt{3}}\hat{X}_\psi - \frac{1}{\sqrt{6}}\hat{X}_{a1} - \frac{1}{\sqrt{2}}\hat{X}_{b1}, \tag{33}$$

$$\hat{X}_4 = \frac{1}{\sqrt{2}}\hat{X}_{a2} + \frac{1}{\sqrt{2}}\hat{X}_{b2}, \tag{34}$$

$$\hat{P}_2 = \frac{1}{\sqrt{3}}\hat{P}_\psi - \frac{1}{\sqrt{6}}\hat{P}_{a1} + \frac{1}{\sqrt{2}}\hat{P}_{b1}, \tag{35}$$

$$\hat{P}_3 = \frac{1}{\sqrt{3}}\hat{P}_\psi - \frac{1}{\sqrt{6}}\hat{P}_{a1} - \frac{1}{\sqrt{2}}\hat{P}_{b1}, \tag{36}$$

$$\hat{P}_4 = \frac{1}{\sqrt{2}}\hat{P}_{a2} + \frac{1}{\sqrt{2}}\hat{P}_{b2}. \tag{37}$$

It is found that the X and P quadratures must be mixed in the following proportions:

$$\frac{\sqrt{3}-1}{2}X_2 + \frac{\sqrt{3}+1}{2}X_3 + X_4 = \hat{X}_\psi + \frac{1}{\sqrt{2}}(\hat{X}_{a2} - \hat{X}_{a1}) + \frac{1}{\sqrt{2}}(\hat{X}_{b2} - \hat{X}_{b1}), \tag{38}$$

$$\frac{\sqrt{3}-1}{2}P_2 + \frac{\sqrt{3}+1}{2}P_3 - P_4 = \hat{P}_\psi - \frac{1}{\sqrt{2}}(\hat{P}_{a1} + \hat{P}_{a2}) - \frac{1}{\sqrt{2}}(\hat{P}_{b1} + \hat{P}_{b2}). \tag{39}$$

In matrix form, the reconstruction channel acting on the share quadratures is:

$$\begin{pmatrix} \frac{\sqrt{3}-1}{2} & 0 & \frac{\sqrt{3}+1}{2} & 0 & 1 & 0 \\ 0 & \frac{\sqrt{3}-1}{2} & 0 & \frac{\sqrt{3}+1}{2} & 0 & -1 \\ & & & & & \\ & & & & & \\ & & & & & \\ & & & & & \end{pmatrix} \begin{pmatrix} \hat{X}_2 \\ \hat{P}_2 \\ \hat{X}_3 \\ \hat{P}_3 \\ \hat{X}_4 \\ \hat{P}_4 \end{pmatrix} = \begin{pmatrix} \hat{X}_{Out} \\ \hat{P}_{Out} \\ \\ \\ \\ \\ \end{pmatrix}. \tag{40}$$

E. The {2,4,5} Protocol

The quadratures that need to be combined in this protocol are

$$\hat{X}_2 = \frac{1}{\sqrt{3}}\hat{X}_\psi - \frac{1}{\sqrt{6}}\hat{X}_{a1} + \frac{1}{\sqrt{2}}\hat{X}_{b1}, \tag{41}$$

$$\hat{X}_4 = \frac{1}{\sqrt{2}}\hat{X}_{a2} + \frac{1}{\sqrt{2}}\hat{X}_{b2}, \tag{42}$$

$$\hat{X}_5 = \frac{1}{\sqrt{2}}\hat{X}_{a2} - \frac{1}{\sqrt{2}}\hat{X}_{b2}, \tag{43}$$

$$\hat{P}_2 = \frac{1}{\sqrt{3}}\hat{P}_\psi - \frac{1}{\sqrt{6}}\hat{P}_{a1} + \frac{1}{\sqrt{2}}\hat{P}_{b1}, \tag{44}$$

$$\hat{P}_4 = \frac{1}{\sqrt{2}}\hat{P}_{a2} + \frac{1}{\sqrt{2}}\hat{P}_{b2}, \tag{45}$$

$$\hat{P}_5 = \frac{1}{\sqrt{2}}\hat{P}_{a2} - \frac{1}{\sqrt{2}}\hat{P}_{b2}. \tag{46}$$

It is found that the X and P quadratures must be mixed in the following proportions:

$$\sqrt{3}X_2 + \frac{1-\sqrt{3}}{2}X_4 + \frac{1+\sqrt{3}}{2}X_5 = \hat{X}_\psi + \frac{1}{\sqrt{2}}(\hat{X}_{a2} - \hat{X}_{a1}) + \sqrt{\frac{3}{2}}(\hat{X}_{b2} - \hat{X}_{b1}), \tag{47}$$

$$\sqrt{3}P_2 + \frac{\sqrt{3}-1}{2}P_4 - \frac{\sqrt{3}+1}{2}P_5 = \hat{P}_\psi - \frac{1}{\sqrt{2}}(\hat{P}_{a1} + \hat{P}_{a2}) + \sqrt{\frac{3}{2}}(\hat{P}_{b1} + \hat{P}_{b2}). \tag{48}$$

In matrix form, the reconstruction channel acting on the share quadratures is:

$$\begin{pmatrix} \sqrt{3} & 0 & \frac{1-\sqrt{3}}{2} & 0 & \frac{1+\sqrt{3}}{2} & 0 \\ 0 & \sqrt{3} & 0 & \frac{\sqrt{3}-1}{2} & 0 & -\frac{\sqrt{3}+1}{2} \\ & & & & & \\ & & & & & \\ & & & & & \\ & & & & & \end{pmatrix} \begin{pmatrix} \hat{X}_2 \\ \hat{P}_2 \\ \hat{X}_4 \\ \hat{P}_4 \\ \hat{X}_5 \\ \hat{P}_5 \end{pmatrix} = \begin{pmatrix} \hat{X}_{Out} \\ \hat{P}_{Out} \\ \\ \\ \\ \\ \end{pmatrix}. \tag{49}$$

IV. SECURITY ANALYSIS: CALCULATING FIDELITY

The security of this scheme is discussed in terms of the fidelity achieved in our output state. Fidelity is a measure of how well the output state resembles the secret state. A fidelity of 1 corresponds to perfect reconstruction and a fidelity of 0 corresponds to orthogonality between our output and secret state i.e. no resemblance. A QSS protocol is considered to be secure when the secret state can be reconstructed with a fidelity of 2/3, as this ensures that the collaborating majority has more information about the state than any other group could. The key to reaching this fidelity is to entangle the resource states strongly enough. As demonstrated in section III, the output state is always in the form of the secret state and then some contributions from the resource states. The resource state contributions are always in such a manner as to maximally cancel, and the more entangled the modes within a resource state are, the better this cancellation is.

The strength of the entanglement between resource modes is a consequence of the strength of the squeezing employed in their creation prior to the dealer protocol. As a consequence, there is a minimum amount of squeezing needed in their creation to meet the 2/3 fidelity threshold. The amount of squeezing required to make the proposed scheme secure is now examined.

A key thing to note is some three-share combinations reconstruct the secret state with different fidelities, for a given level of squeezing. This is a consequence of every share being slightly different. For a fully robust QSS system, it must be ensured that even the three-share combination which reconstructs the secret state with the worst fidelity meets this 2/3 fidelity threshold. To ensure this, 5 example cases of three-share combinations are examined, and how much squeezing is needed for the worst-fidelity combination to hit that 2/3 threshold is investigated. That amount of squeezing is the minimum required for the system as a whole to be secure.

For two Gaussian states which have the same mean vector, the fidelity of the output state relative to the input state is

$$\mathcal{F} = \frac{2}{\sqrt{\det(\mathbf{V}_{\text{in}} + \mathbf{V}_{\text{out}})}}. \tag{50}$$

In the proposed system, the input state and output state have the same mean. This is because the output state is always the secret state combined with some resource state contributions, and the resource states have a mean of 0. $\mathbf{V}$ is the covariance matrix which (along with the mean vector) characterises the Wigner function of the state.

The method of how to calculate $\mathbf{V}$ is shown explicitly in IV B. All other calculations of $\mathbf{V}$ are done in the same way.

A. The {1,2,3} Protocol

This three-share combination is a special case as entanglement does not have to be leveraged at all to reconstruct the secret state perfectly. Since this three-share combination gives a fidelity of 1 no matter the level of squeezing, it can be ignored in the security analysis.

B. The {1,2,4} Protocol

To calculate $\mathbf{V}_{\text{out}}$, it is necessary to start with a 10x10 matrix representing the covariance of all the quadratures of all 5 initial modes, prior to dealing.

The covariance matrix for a coherent, Gaussian secret state is

$$V_{\text{coherent}} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}. \tag{51}$$

r_A and r_B are defined as the squeezing parameters used in the creation of resource states A and B. The covariance matrix for resource states A and B, which show the relationships between $\hat{X}_{a1}, \hat{P}_{a1}, \hat{X}_{a2}, \hat{P}_{a2}$ and $\hat{X}_{b1}, \hat{P}_{b1}, \hat{X}_{b2}, \hat{P}_{b2}$ respectively, are given by

$$V_{\text{squeezedA}} = \begin{pmatrix} \cosh(2r_A) & 0 & \sinh(2r_A) & 0 \\ 0 & \cosh(2r_A) & 0 & -\sinh(2r_A) \\ \sinh(2r_A) & 0 & \cosh(2r_A) & 0 \\ 0 & -\sinh(2r_A) & 0 & \cosh(2r_A) \end{pmatrix}, \tag{52}$$

$$V_{\text{squeezedB}} = \begin{pmatrix} \cosh(2r_B) & 0 & \sinh(2r_B) & 0 \\ 0 & \cosh(2r_B) & 0 & -\sinh(2r_B) \\ \sinh(2r_B) & 0 & \cosh(2r_B) & 0 \\ 0 & -\sinh(2r_B) & 0 & \cosh(2r_B) \end{pmatrix}. \tag{53}$$

If these matrices are combined into a 10x10 covariance matrix where entries correspond to $\hat{X}_\psi$, $\hat{P}_\psi$, $\hat{X}_{a1}$, $\hat{P}_{a1}$, $\hat{X}_{a2}$, $\hat{P}_{a2}$, $\hat{X}_{b1}$, $\hat{P}_{b1}$, $\hat{X}_{b2}$, $\hat{P}_{b2}$, the initial covariance matrix can be written as

$$V_{\text{Initial}} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & \cosh(2r_A) & 0 & \sinh(2r_A) & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & \cosh(2r_A) & 0 & -\sinh(2r_A) & 0 & 0 & 0 & 0 \\ 0 & 0 & \sinh(2r_A) & 0 & \cosh(2r_A) & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -\sinh(2r_A) & 0 & \cosh(2r_A) & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & \cosh(2r_B) & 0 & \sinh(2r_B) & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & \cosh(2r_B) & 0 & -\sinh(2r_B) \\ 0 & 0 & 0 & 0 & 0 & 0 & \sinh(2r_B) & 0 & \cosh(2r_B) & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & -\sinh(2r_B) & 0 & \cosh(2r_B) \end{pmatrix}. \tag{54}$$

After applying the dealer protocol, the covariance matrix has the form

$$V_{\text{AfterDeal}} = T_{\text{Dealer}} \cdot V_{\text{Initial}} \cdot T_{\text{Dealer}}^T \tag{55}$$

where

$$T_{\text{Dealer}} = \begin{pmatrix} \frac{1}{\sqrt{3}} & 0 & \sqrt{\frac{2}{3}} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & \frac{1}{\sqrt{3}} & 0 & \sqrt{\frac{2}{3}} & 0 & 0 & 0 & 0 & 0 & 0 \\ \frac{1}{\sqrt{3}} & 0 & -\frac{1}{\sqrt{6}} & 0 & 0 & 0 & \frac{1}{\sqrt{2}} & 0 & 0 & 0 \\ 0 & \frac{1}{\sqrt{3}} & 0 & -\frac{1}{\sqrt{6}} & 0 & 0 & 0 & \frac{1}{\sqrt{2}} & 0 & 0 \\ \frac{1}{\sqrt{3}} & 0 & -\frac{1}{\sqrt{6}} & 0 & 0 & 0 & -\frac{1}{\sqrt{2}} & 0 & 0 & 0 \\ 0 & \frac{1}{\sqrt{3}} & 0 & -\frac{1}{\sqrt{6}} & 0 & 0 & 0 & -\frac{1}{\sqrt{2}} & 0 & 0 \\ 0 & 0 & 0 & 0 & \frac{1}{\sqrt{2}} & 0 & 0 & 0 & \frac{1}{\sqrt{2}} & 0 \\ 0 & 0 & 0 & 0 & 0 & \frac{1}{\sqrt{2}} & 0 & 0 & 0 & \frac{1}{\sqrt{2}} \\ 0 & 0 & 0 & 0 & \frac{1}{\sqrt{2}} & 0 & 0 & 0 & -\frac{1}{\sqrt{2}} & 0 \\ 0 & 0 & 0 & 0 & 0 & \frac{1}{\sqrt{2}} & 0 & 0 & 0 & -\frac{1}{\sqrt{2}} \end{pmatrix}. \tag{56}$$

The covariance matrix after applying the reconstruction channel is

$$V_{\text{AfterChannel}} = T_{\text{Channel}} \cdot V_{\text{AfterDeal}} \cdot T_{\text{Channel}}^T \tag{57}$$

where the channel matrix for 1,2,4 is

$$T_{\text{Channel}} = \begin{pmatrix} 1 & 0 & \sqrt{3}-1 & 0 & 0 & 0 & 1-\sqrt{3} & 0 & 0 & 0 \\ 0 & 1 & 0 & \sqrt{3}-1 & 0 & 0 & 0 & \sqrt{3}-1 & 0 & 0 \\ & & & & & & & & & \\ & & & & & & & & & \\ & & & & & & & & & \\ & & & & & & & & & \\ & & & & & & & & & \\ & & & & & & & & & \\ & & & & & & & & & \\ & & & & & & & & & \end{pmatrix}. \tag{58}$$

Because only a single output beam is important in the scheme, the fact that the bottom 8 rows of the channel are left empty actually doesn't affect the answer. Finally, to extract the 2x2 covariance matrix which describes the relationship between $\hat{X}_{Out}$ and $\hat{P}_{Out}$, the 2x2 block in the upper left corner of $V_{\text{AfterChannel}}$ is examined to find V_{Out}.

Figure 2 shows how the fidelity of the output state depends on the amount of squeezing employed in the creation of the resource states. The red line in the lower left corner shows the threshold for fidelity reaching 2/3. If it is assumed that resource states A and B are squeezed in the same magnitude, the minimum amount of squeezing needed to reach the 2/3 threshold is 0.301 dB (3 s.f).

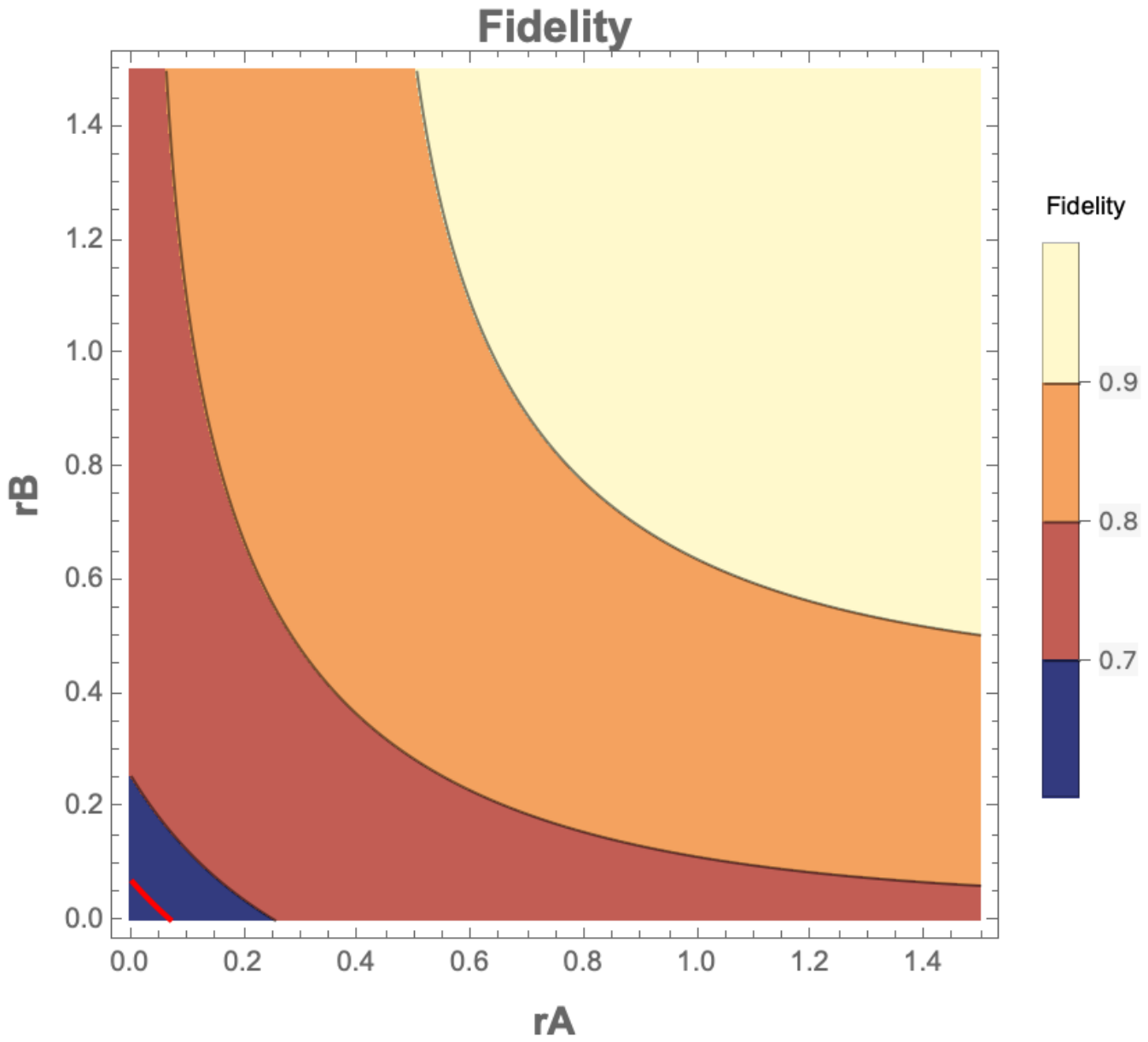

FIG. 2. Fidelity as a function of the squeezing parameters of resource states A and B, r_A and r_B, for the {1,2,4} set-up. The red line indicates the threshold where fidelity reaches 2/3. We arbitrarily choose $x_0 = p_0 = 3$ for the secret state mean for plotting purposes.

C. The {1,4,5} Protocol

If If it is assumed that resource states A and B are squeezed in the same magnitude, Figure 3 illustrates that the minimum amount of squeezing needed to reach the 2/3 threshold is 6.02 dB (3 s.f).

It should be noted that the squeezing value r_B is irrelevant to the fidelity. This is the case because the only contributions from resource state B to shares 1, 4 and 5 are in the b2 mode. Therefore, the entanglement between modes b1 and b2 is never leveraged, and hence the strength of the entanglement between them is irrelevant.

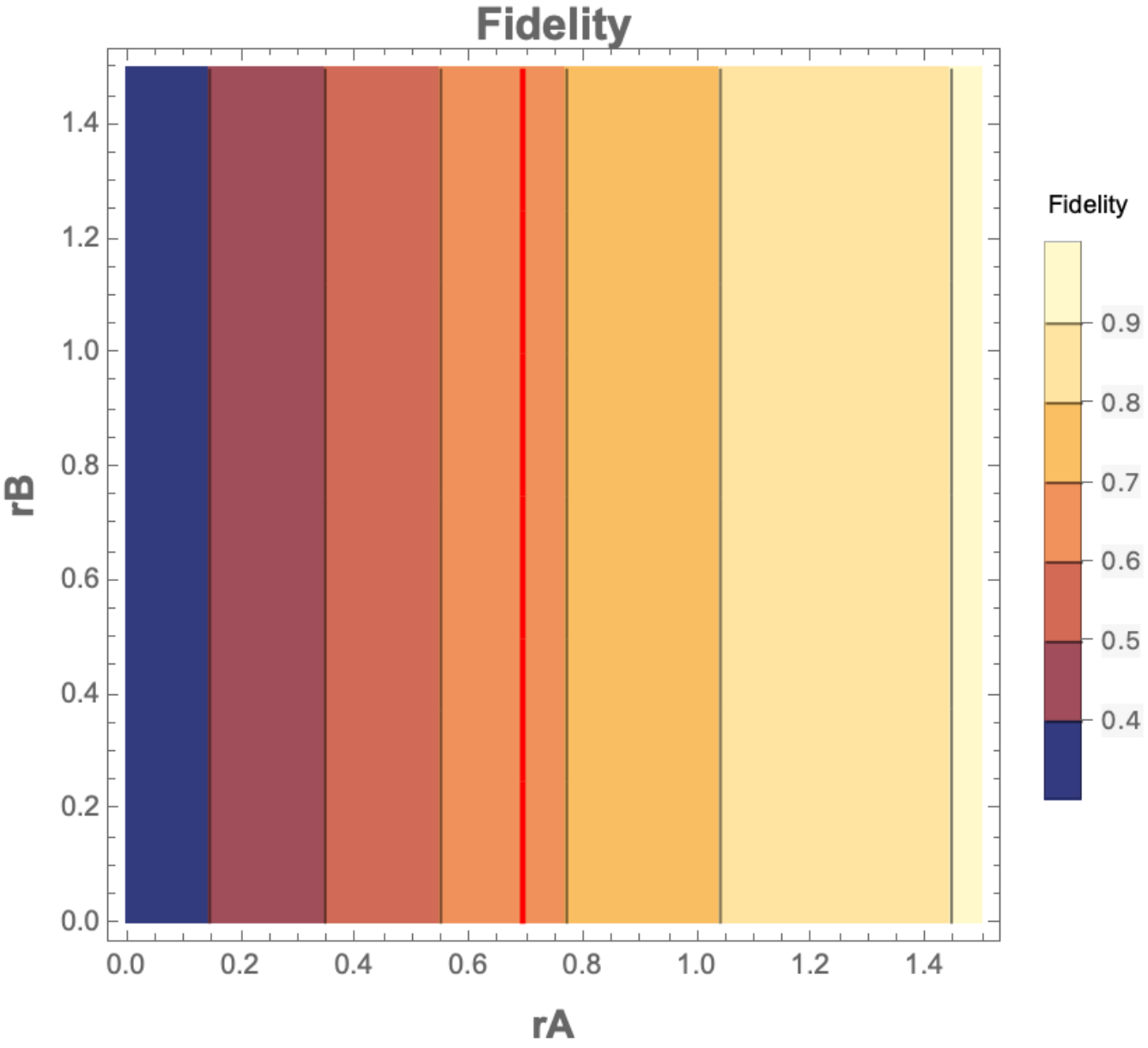

FIG. 3. Fidelity as a function of the squeezing parameters of resource states A and B, r_A and r_B, for the {1,4,5} set-up. The red line indicates the threshold where fidelity reaches 2/3. We arbitrarily choose $x_0 = p_0 = 3$ for the secret state mean for plotting purposes.

D. The {2,3,4} Protocol

The plot of the value of fidelity depends on r_A and r_B for this three-share combination is shown in Figure 4.

If it is assumed that resource states A and B are squeezed in the same magnitude, Figure 4 illustrates that the minimum amount of squeezing needed to reach the 2/3 threshold is 3.01 dB (3 s.f).

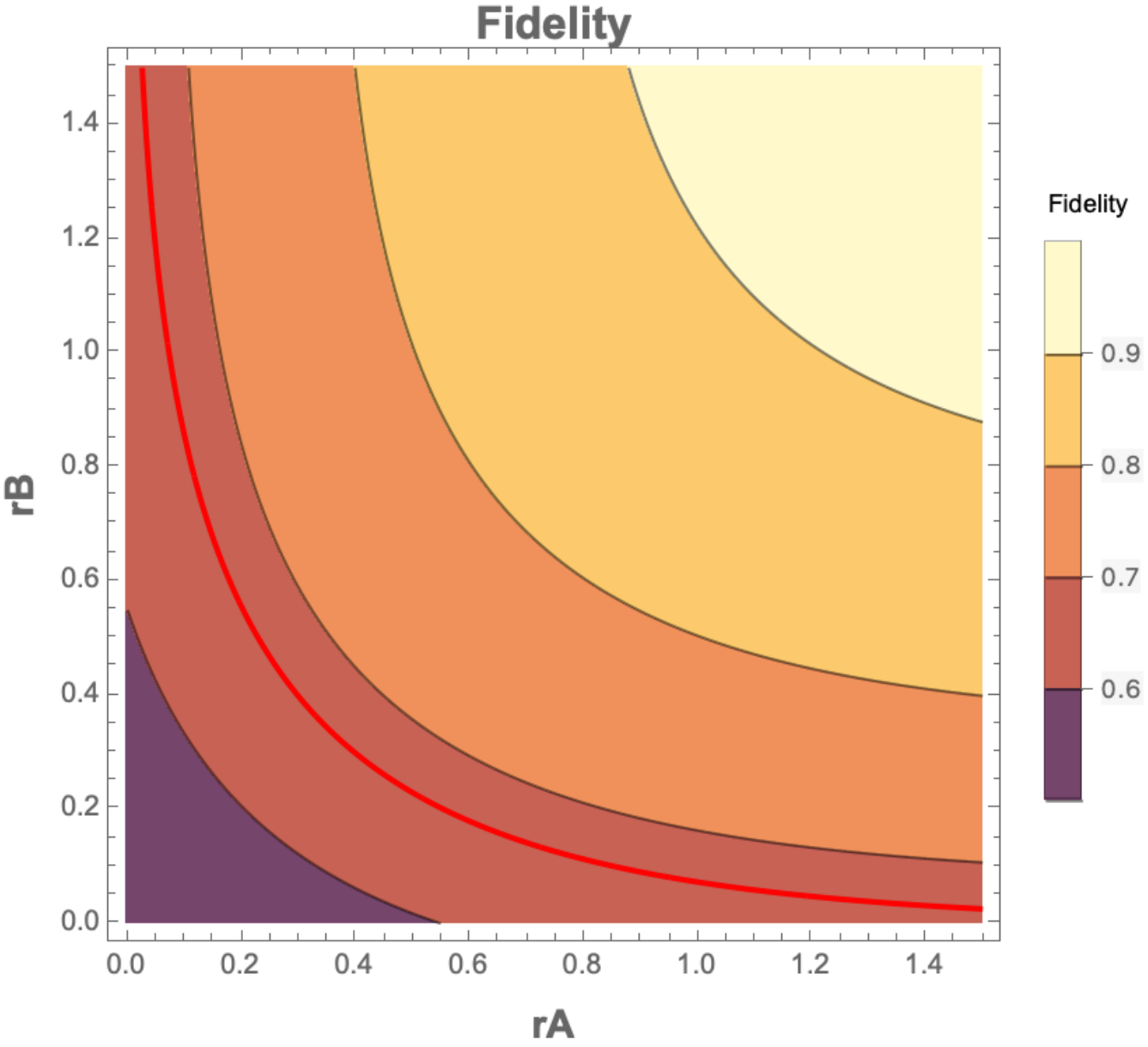

FIG. 4. Fidelity as a function of the squeezing parameters of resource states A and B, r_A and r_B, for the {2,3,4} set-up. The red line indicates the threshold where fidelity reaches 2/3. We arbitrarily choose $x_0 = p_0 = 3$ for the secret state mean for plotting purposes.

E. The {2,4,5} Protocol

The plot of the value of fidelity depends on r_A and r_B for this three-share combination is shown in Figure 5.

If it is assumed that resource states A and B are squeezed in the same magnitude, Figure 5 illustrates that the minimum amount of squeezing needed to reach the 2/3 threshold is 6.02 dB (3 s.f).

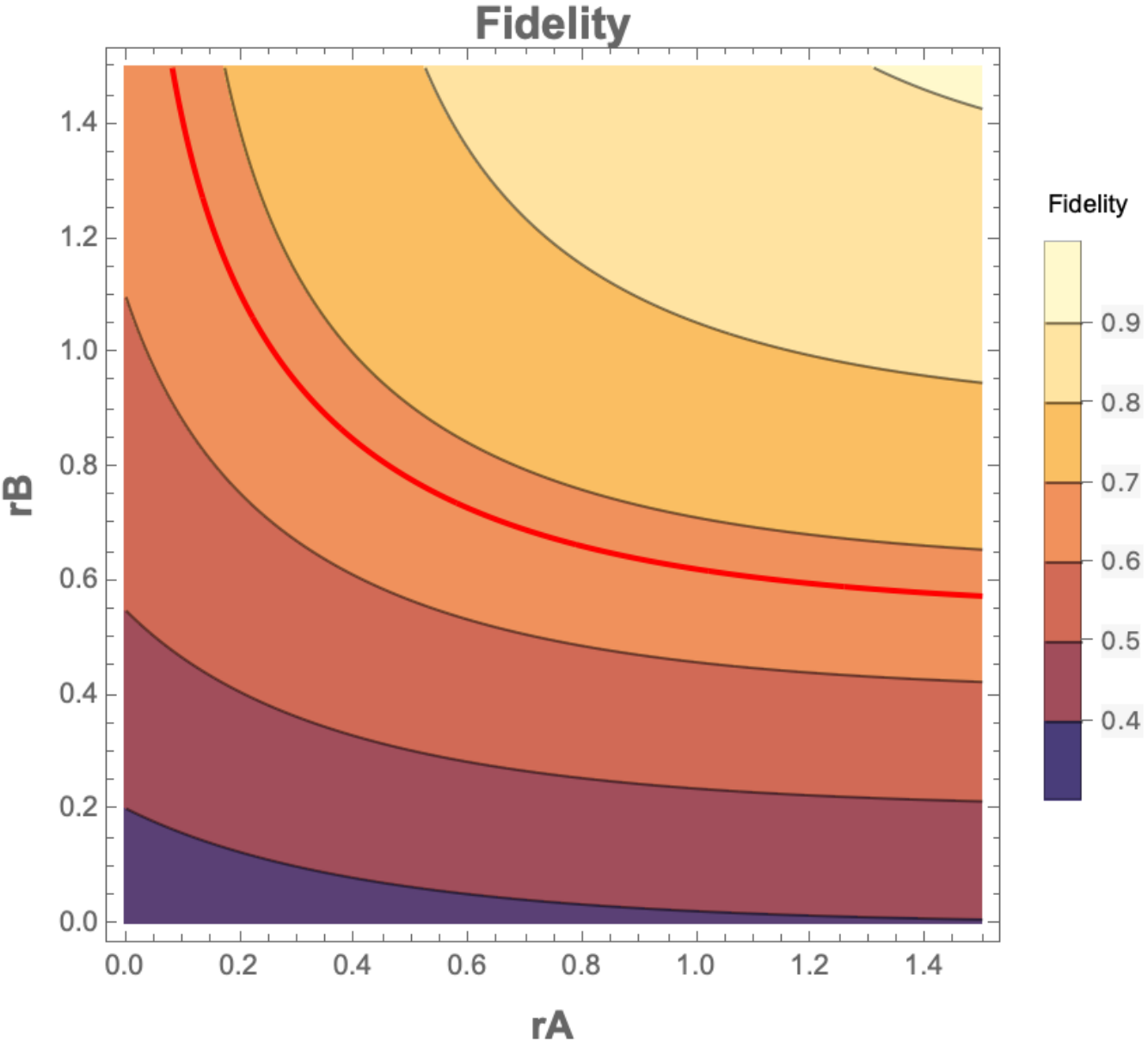

FIG. 5. Fidelity as a function of the squeezing parameters of resource states A and B, r_A and r_B, for the {2,4,5} set-up. The red line indicates the threshold where fidelity reaches 2/3. We arbitrarily choose $x_0 = p_0 = 3$ for the secret state mean for plotting purposes.

F. Summary of Security Analysis

In summary, if the same strength of squeezing is used in the preparation of resource state A and resource state B, the minimum amount of squeezing needed to reach a fidelity of 2/3 for each share combination is shown in Figure 6. For the proposal to be secure, it must be ensured that whichever three shares are chosen, the threshold of 2/3 fidelity is achievable. Consequently, the level of squeezing the proposed (3,5)-threshold scheme requires is the amount required in the worst cases (namely {1,4,5} and {2,4,5}). This is the squeezing level of ≈ 6.02 dB.

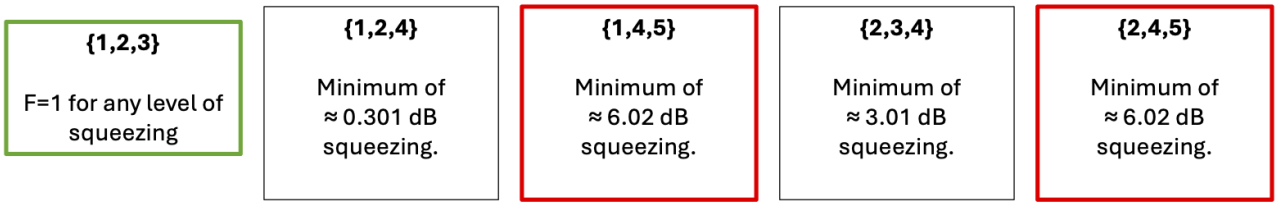

FIG. 6. A summary of the squeezing requirements in the resource states for five representative combinations of shares for secure QSS

V. EXAMPLE PHYSICAL SET-UP FOR {2,3,4} RECONSTRUCTION PROTOCOL

To bridge the gap between theory and practice, one considers how to physically carry out one of the reconstruction protocols with a physical set-up of optical components. Let us consider the {2,3,4} reconstruction protocol. The quadratures of the shares are

$$\hat{X}_2 = \frac{1}{\sqrt{3}}\hat{X}_\psi - \frac{1}{\sqrt{6}}\hat{X}_{a1} + \frac{1}{\sqrt{2}}\hat{X}_{b1}, \tag{59}$$

$$\hat{X}_3 = \frac{1}{\sqrt{3}}\hat{X}_\psi - \frac{1}{\sqrt{6}}\hat{X}_{a1} - \frac{1}{\sqrt{2}}\hat{X}_{b1}, \tag{60}$$

$$\hat{X}_4 = \frac{1}{\sqrt{2}}\hat{X}_{a2} + \frac{1}{\sqrt{2}}\hat{X}_{b2}, \tag{61}$$

$$\hat{P}_2 = \frac{1}{\sqrt{3}}\hat{P}_\psi - \frac{1}{\sqrt{6}}\hat{P}_{a1} + \frac{1}{\sqrt{2}}\hat{P}_{b1}, \tag{62}$$

$$\hat{P}_3 = \frac{1}{\sqrt{3}}\hat{P}_\psi - \frac{1}{\sqrt{6}}\hat{P}_{a1} - \frac{1}{\sqrt{2}}\hat{P}_{b1}, \tag{63}$$

$$\hat{P}_4 = \frac{1}{\sqrt{2}}\hat{P}_{a2} + \frac{1}{\sqrt{2}}\hat{P}_{b2}. \tag{64}$$

The reconstruction protocol found earlier is represented by the process:

$$\begin{pmatrix} \frac{\sqrt{3}-1}{2} & 0 & \frac{\sqrt{3}+1}{2} & 0 & 1 & 0 \\ 0 & \frac{\sqrt{3}-1}{2} & 0 & \frac{\sqrt{3}+1}{2} & 0 & -1 \\ & & & & & \end{pmatrix} \begin{pmatrix} \hat{X}_2 \\ \hat{P}_2 \\ \hat{X}_3 \\ \hat{P}_3 \\ \hat{X}_4 \\ \hat{P}_4 \end{pmatrix} = \begin{pmatrix} \hat{X}_{Out} \\ \hat{P}_{Out} \\ \\ \\ \\ \end{pmatrix}. \tag{65}$$

To implement this using optical components, the following strategy is proposed: first, use a pair of beamsplitters followed by a squeezer to combine the shares in the proportions which will mix the X quadratures as desired. Then, the two non-output beams and two feed-forward components are used to displace the P quadrature of the output beam by the correct amount.

A diagram of the experimental set-up is shown in Figure 7. The transmissivity of the beamsplitters are τ_1 and τ_2 respectively. The squeezing strength of the squeezer is β and the gain on the P quadratures in the feed-forward process is G_1 and G_2 respectively.

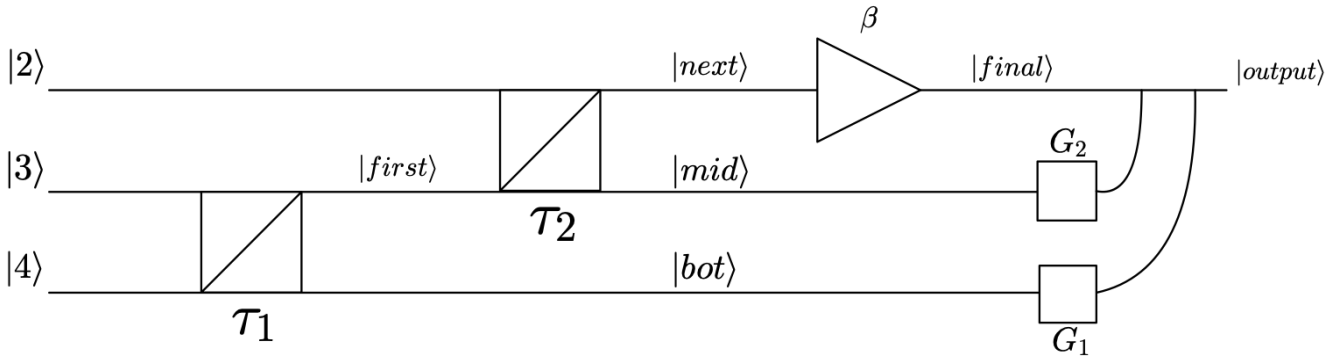

FIG. 7. A diagram of the experimental set-up proposed for the reconstruction protocol of {2,3,4}

An expression for $|output\rangle$ in terms of τ_1, τ_2, β, G_1 and G_2 is to be determined to calculate those constants and match $|output\rangle$ to the desired output. To do this, it is necessary to calculate $|first\rangle$, $|next\rangle$, $|mid\rangle$, $|bot\rangle$and $|final\rangle$ as well.

Firstly, let us determine $|first\rangle$, $|next\rangle$, $|mid\rangle$ and $|bot\rangle$. Since they only have gone through beamsplitters, their X and P quadratures are the same and they can be expressed in shorthand notation. They are found to be

$$|\text{first}\rangle = \sqrt{1-\tau_1}|3\rangle + \sqrt{\tau_1}|4\rangle, \tag{66}$$

$$|\text{bot}\rangle = \sqrt{\tau_1}|3\rangle - \sqrt{1-\tau_1}|4\rangle, \tag{67}$$

$$|\text{next}\rangle = \sqrt{1-\tau_2}|2\rangle + \sqrt{\tau_2}|\text{first}\rangle, \tag{68}$$

$$|\text{mid}\rangle = \sqrt{\tau_2}|2\rangle - \sqrt{1-\tau_2}|\text{first}\rangle. \tag{69}$$

Now, |final⟩ is calculated. The squeezer with squeezing parameter β will multiply the X quadrature by e^{β} and multiply the P quadrature by $e^{-\beta}$. Recall that the set-up aims to achieve the ideal proportions in the X quadrature after the squeezer. Thus, the following expression for the X quadrature of |final⟩ is obtained:

$$\hat{X}_{\text{final}} = e^{\beta}\hat{X}_{\text{next}} = e^{\beta}\left(\sqrt{1-\tau_2}\hat{X}_2 + \sqrt{\tau_2}\hat{X}_{\text{first}}\right) = e^{\beta}\left(\sqrt{1-\tau_2}\hat{X}_2 + \sqrt{(1-\tau_1)\tau_2}\hat{X}_3 + \sqrt{\tau_1\tau_2}\hat{X}_4\right). \tag{70}$$

The X quadratures need to be mixed in the following proportions: $\frac{\sqrt{3}-1}{2}$, $\frac{\sqrt{3}+1}{2}$ and 1.

Therefore, three equations must be satisfied:

$$e^{\beta}\sqrt{1-\tau_2} = \frac{\sqrt{3}-1}{2}, \tag{71}$$

$$e^{\beta}\sqrt{(1-\tau_1)\tau_2} = \frac{\sqrt{3}+1}{2}, \tag{72}$$

$$e^{\beta}\sqrt{\tau_1\tau_2} = 1. \tag{73}$$

Solving these gives:

$$\tau_1 = \frac{8 - 2\sqrt{3}}{13} \approx 0.349, \tag{74}$$

$$\tau_2 = \frac{4 + \sqrt{3}}{6} \approx 0.955, \tag{75}$$

$$\beta = \frac{\ln(3)}{2} \approx 0.549. \tag{76}$$

Now that τ_1, τ_2 and β have been determined and the X quadratures have been combined in the correct proportions, the feed-forward process is examined and G_1 and G_2 are determined. First, let us calculate $\hat{P}_{\text{final}}$. Then, an expression for $\hat{P}_{\text{output}}$ can be found in terms of $\hat{P}_{\text{final}}$, $\hat{P}_{\text{mid}}$, $\hat{P}_{\text{bot}}$, G_1 and G_2 and the unknowns can be calculated.

$$\hat{P}_{\text{final}} = e^{-\beta}\hat{P}_{\text{next}} = e^{-\beta}\left(\sqrt{1-\tau_2}\hat{P}_2 + \sqrt{\tau_2}\hat{P}_{\text{first}}\right) = e^{-\beta}\left(\sqrt{1-\tau_2}\hat{P}_2 + \sqrt{(1-\tau_1)\tau_2}\hat{P}_3 + \sqrt{\tau_1\tau_2}\hat{P}_4\right). \tag{77}$$

From this, it follows that

$$\hat{P}_{\text{output}} = \hat{P}_{\text{final}} + G_2\hat{P}_{\text{mid}} + G_1\hat{P}_{\text{bot}} = \hat{P}_{\text{final}} + G_2(\sqrt{\tau_2}\hat{P}_2 - \sqrt{1-\tau_2}\hat{P}_{\text{first}}) + G_1(\sqrt{\tau_1}\hat{P}_3 - \sqrt{1-\tau_1}\hat{P}_4). \tag{78}$$

Substituting the expressions for $\hat{P}_{\text{first}}$ and $\hat{P}_{\text{final}}$ gives

$$\begin{aligned}\hat{P}_{\text{output}} = {} & e^{-\beta}\left(\sqrt{1-\tau_2}\hat{P}_2 + \sqrt{(1-\tau_1)\tau_2}\hat{P}_3 + \sqrt{\tau_1\tau_2}\hat{P}_4\right) + G_2\sqrt{\tau_2}\hat{P}_2 \\ & - G_2\sqrt{1-\tau_2}(\sqrt{1-\tau_1}\hat{P}_3 + \sqrt{\tau_1}\hat{P}_4) + G_1\sqrt{\tau_1}\hat{P}_3 - G_1\sqrt{1-\tau_1}\hat{P}_4.\end{aligned} \tag{79}$$

Collecting terms into shares:

$$\begin{aligned}\hat{P}_{\text{output}} = {} & \hat{P}_2(e^{-\beta}\sqrt{1-\tau_2} + G_2\sqrt{\tau_2}) \\ & + \hat{P}_3(e^{-\beta}\sqrt{(1-\tau_1)\tau_2} - G_2\sqrt{(1-\tau_1)(1-\tau_2)} + G_1\sqrt{\tau_1}) \\ & + \hat{P}_4(e^{-\beta}\sqrt{\tau_1\tau_2} - G_2\sqrt{\tau_1(1-\tau_2)} - G_1\sqrt{1-\tau_1}).\end{aligned} \tag{80}$$

The P quadratures must be combined in the following proportions: $\frac{\sqrt{3}-1}{2}$, $\frac{\sqrt{3}+1}{2}$ and -1.
Therefore, two more equations must be satisfied:

$$e^{-\beta}\sqrt{(1-\tau_1)\tau_2} - G_2\sqrt{(1-\tau_1)(1-\tau_2)} + G_1\sqrt{\tau_1} = \frac{\sqrt{3}+1}{2}, \tag{81}$$

$$e^{-\beta}\sqrt{\tau_1\tau_2} - G_2\sqrt{\tau_1(1-\tau_2)} - G_1\sqrt{1-\tau_1} = -1. \tag{82}$$

Solving for G_1 and G_2 using the values for τ_1, τ_2 and β, it is determined that

$$G_1 = \sqrt{\frac{20 + 8\sqrt{3}}{13}} \approx 1.61, \tag{83}$$

$$G_2 = \sqrt{\frac{44 - 24\sqrt{3}}{39}} \approx 0.250. \tag{84}$$

In summary, the above workings show that the proposed physical system would carry out the reconstruction protocol for the {2,3,4} system, provided the calculated values are used for τ_1, τ_2, β, G_1 and G_2 are used.

VI. CONCLUSION

In this report, a (3,5)-threshold scheme for sharing Gaussian states was proposed. Starting with a simple dealer protocol, reconstruction protocols were formulated for five different three-share combinations. Those five combinations are representative of all 10 possible combinations, providing confidence that the conclusions are accurate in all cases. The reconstruction protocols for these five cases were examined and the amount of squeezing required to guarantee security was determined. It was established that a minimum of ≈ 6.02 dB of squeezing is required in the creation of the two resource states that the scheme uses. 6.02 dB is an achievable amount with current technology, demonstrating the practical feasibility of this protocol. This amount of squeezing ensures that the fidelity of the output state is a minimum of 2/3, ensuring that the collaborating majority has more information about the original state than anyone else.

In addition to this, an example physical set-up for the reconstruction protocol of shares {2,3,4} was found using beamsplitters, a squeezer and feed-forward components. The specific values of transmissivity, squeezing and gain for this set-up were also determined. Devising a relatively simple set-up which can carry out the protocol further supports the feasibility of this scheme.

There are several ways in which research in this area could be developed. The first is to consider how channel noise and transmission loss affect the effectiveness of this scheme. Another way is to model examples of physical set-ups for the other reconstruction protocols that have been proposed, to ensure that there are practical ways to realise them too. Lastly, research in this area could be developed by investigating how to securely share a non-Gaussian state. This would make the proposed scheme more versatile and allow QSS to be used in greater number of situations.

[1] Andrew M. Lance, Thomas Symul, Warwick P. Bowen, Barry C. Sanders, Tomáš Tyc, and T. C. Ralph, "Continuous-variable quantum-state sharing via quantum disentanglement," Phys. Rev. A 71, 033814 (2005). DOI: 10.1103/PhysRevA.71.033814.

[2] Cailean Wilkinson, Matthew Thornton, and Natalia Korolkova, "Quantum steering as a resource for secure tripartite quantum state sharing," Phys. Rev. A 107, 062401 (2023). DOI: 10.1103/PhysRevA.107.062401.

[3] Y. Ouyang, S. Tan, L. Zhao, and J.F. Fitzsimons, "Computing on quantum shared secrets," Phys. Rev. A 97, 052333 (2017). DOI: 10.1103/PhysRevA.97.052333.

[4] Christian Weedbrook, Stefano Pirandola, Raúl García-Patrón, Nicolas J. Cerf, Timothy C. Ralph, Jeffrey H. Shapiro, and Seth Lloyd, "Gaussian quantum information," Rev. Mod. Phys. 84, 621–669 (2012). DOI: 10.1103/RevModPhys.84.621.

[5] Frédéric Grosshans and Philippe Grangier, "Quantum cloning and teleportation criteria for continuous quantum variables," Phys. Rev. A 64, 010301 (2001). DOI: 10.1103/PhysRevA.64.010301.