Secure Continuous-Variable Gaussian Quantum State Sharing for a Network of Five Players

Daniel Travers | Supervised by Natalia Korolkova

School of Physics and Astronomy, University of St Andrews

1. What is Quantum State Sharing?

A quantum state is a description of a physical system at the smallest of scales. A quantum state might represent the state of a subatomic particle such as an electron, or, as in this project, the states of photons of light. Quantum state sharing (QSS) is the process by which a quantum state is split up into shares and distributed among multiple recipients. By leveraging quantum entanglement, it can be ensured that no individual can get information from the quantum state on their own, but a large enough subset of the group can fully recreate it [1]. In practical applications, quantum states can be used to store information, so QSS enables the encryption of quantum information and secures it from eavesdropping. As a result, QSS has the potential to be vital in maintaining the security of future quantum computing networks.

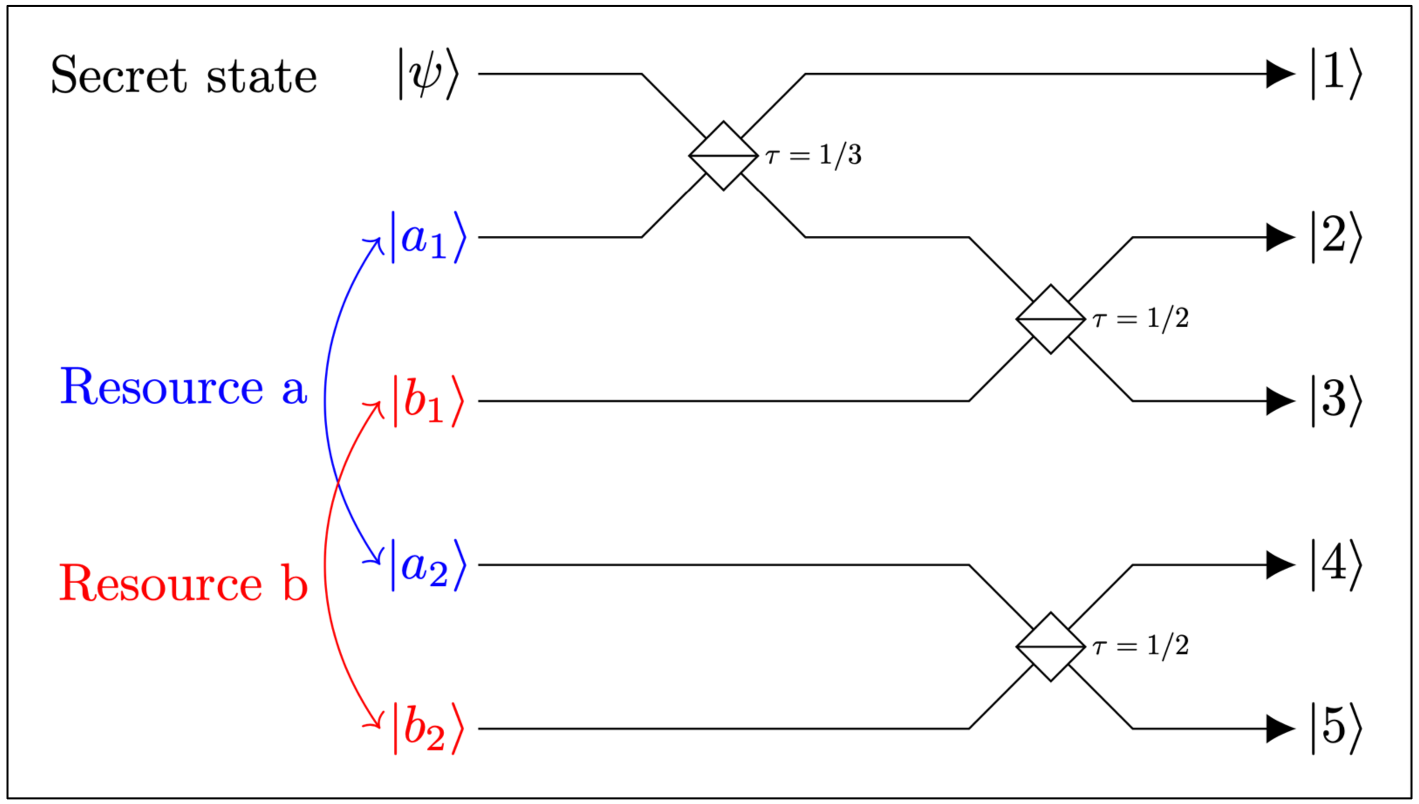


Figure 1 – The dealer protocol which mixes the secret state with the entangled resource states.

2. Project Aims

To date, only the simplest protocol (involving 3 players) for sharing a Gaussian quantum state of light has been shown to be secure. A quantum state of light is called Gaussian when its defining measurements (called quadratures) have a symmetric, Gaussian distribution. In this project, the aim was to extend QSS to the next largest network, where the quantum state is split into five shares and a minimum of three of them are needed to fully recreate it.

Extending QSS to this network size involves taking a dealer protocol (the way the shares are created) and determining the optimal way to recombine the shares to recreate the quantum state - the reconstruction protocol. In addition, the security of QSS relies on quantum entanglement, a phenomenon where physically separated systems (e.g. different photons of light) exhibit correlations in their measurements. To ensure the scheme's practicability, it is also necessary to find the level of entanglement that is required for a certain threshold of security.

3. The Dealer Protocol

The dealer protocol in this QSS scheme takes the initial secret state and mixes it with two resource states to produce five different shares. Each resource state has two parts (called modes) which are entangled with each other. This entanglement is key for the reconstruction process later. The mixing together in the dealer protocol is done with beamsplitters - optical devices that are partially reflective and allow incoming beams to overlap and interfere. The dealer protocol is shown in **Figure 1**.

The resource states are unrelated to the secret state, so it would seem that the mixing process would destroy the information contained within the secret state. However, the secret state can be reobtained by leveraging quantum entanglement. To understand how, consider the following analogy. The secret state is like a black and white photograph and the resource states are like random TV static. When the static is added to the photograph, the contents of the photograph are obscured. Quantum entanglement is a phenomenon where different, separated states exhibit correlations within their measurements. In this analogy, this is akin to the TV static of one resource mode being the exact same as the other mode but with their black and white switched. Therefore, if we mixed the secret state and state a_1, we could undo the muddying of the picture by adding the entangled a_2 state on. This is in essence how the shares obtained at the end of the dealer protocol can be combined in such a way as to obtain the secret state again.

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

Figure 2 – The reconstruction protocol for shares 2, 4 and 5.

4. The Reconstruction Protocol

To reconstruct the secret state optimally, I had to determine the proportions in which the different shares must be combined. One example of a reconstruction protocol is shown in **Figure 2**. It describes how shares 2, 4 and 5 can be optimally recombined. Having developed the reconstruction protocols for five three-share combinations, I developed an example physical set-up for reconstructing the secret state using shares 2, 3 and 4. This set-up bridges the gap between abstract proportions of share combinations and the optical components which could be used to achieve this process in practice. The optical devices used include beam splitters, squeezers and feed-forward components. The transmissivity, squeezing strength and gain were all determined too, yielding practical values for modern technology.

5. Security Analysis

Having found the reconstruction protocols, the next step was to determine the level of entanglement in the resource states needed for the scheme to be secure. The scheme is considered secure when the fidelity (how much the output state resembles the original state) exceeds 2/3. For five representative three-share combinations, I determined the level of squeezing (a proxy for entanglement) required. **Figure 3** shows an example plot where the axes measure the amount of squeezing needed in each resource state and the plotted value is the fidelity of the output state. Thus, it could then be determined the degree of squeezing required to guarantee security. The squeezing requirements are specified in **Figure 4**.

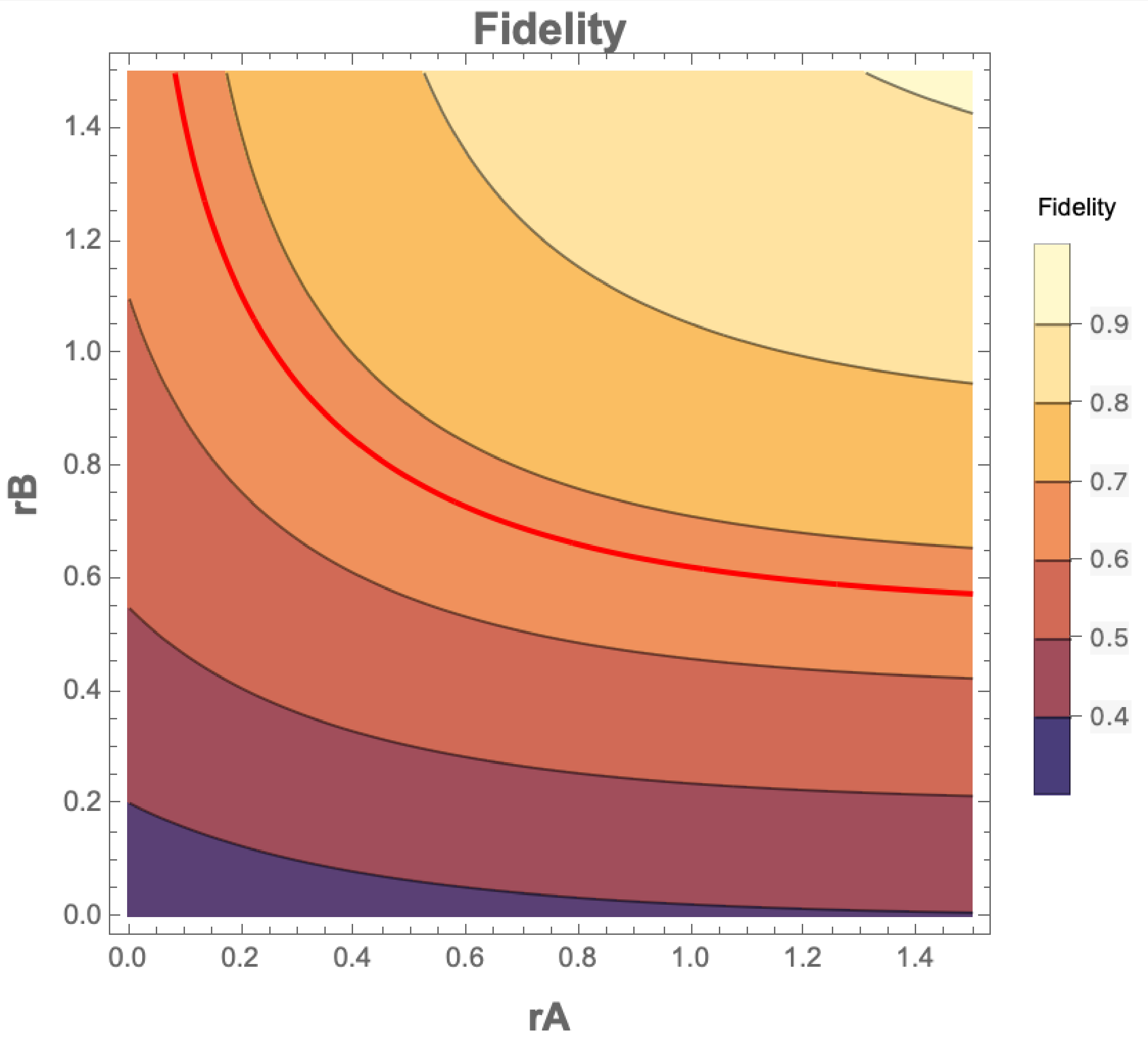
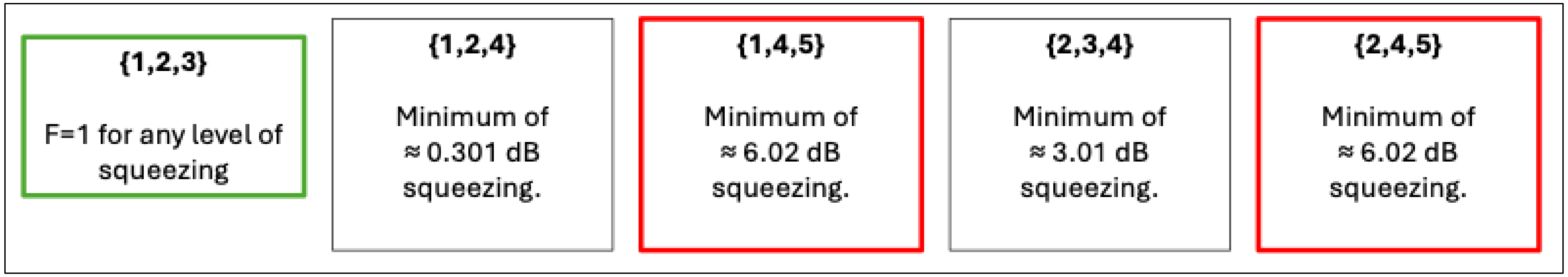


Figure 3 – Fidelity as a function of the squeezing parameters (a proxy of entanglement) of resource states A and B, rA and rB, for the {2,4,5} set-up. The red line indicates the threshold where fidelity reaches 2/3.

6. Conclusion

In summary, my project began with determining the reconstruction protocols for five different three-share combinations, given a specific dealer protocol. 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. 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 a greater number of situations.



{1,2,3}

F=1 for any level of squeezing

{1,2,4}

Minimum of ≈ 0.301 dB squeezing.

{1,4,5}

Minimum of ≈ 6.02 dB squeezing.

{2,3,4}

Minimum of ≈ 3.01 dB squeezing.

{2,4,5}

Minimum of ≈ 6.02 dB squeezing.

Figure 4 – The amount of squeezing needed to ensure security for each three-share combination.

[1] Andrew M. Lance, Thomas Symul, Warwick P. Bowen, Barry C. Sanders, Toma´˘s 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.