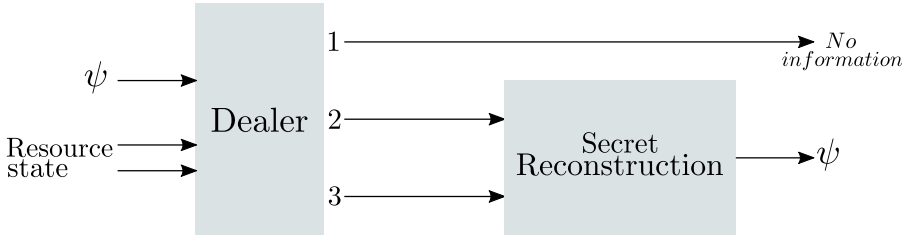
Secure tripartite quantum state sharing in the continuous-variable domain

C. Wilkinson[1], **M. Thornton**[1], **N. Korolkova**[1]

[1] *School of Physics and Astronomy, University of St Andrews*



Quantum state sharing (QSS) is a cryptographic technique which splits the information describing a single quantum state across a number of modes, each distributed to a single potentially-dishonest player as shown above. Importantly, the original state is then inaccessible to any individual player acting alone. Only by collaborating can a subset of the players reconstruct the original state. The information is then guarded against dishonest individuals without hindering access when not all players are available [1, 2].

We present a quantum state sharing (QSS) protocol suitable for the sharing of any Gaussian state between three players and certify its security for any *pure* Gaussian state. Our protocol is a generalisation of one previously discussed by Tyc & Sanders [3] and Lance *et al.* [4] which allows the use of a wider variety of resource states.

We show that the tripartite quantum state sharing of coherent states can be achieved securely with the use of any two-mode Gaussian resource exhibiting any degree of EPR-steering [5]. We also show that displaced squeezed states can also be shared securely with an increase in the entanglement requirement dependent on the degree of squeezing allowed in the input states.

References

[1] R. Cleve, D. Gottesman, and H.-K. Lo, Physical Review Letters **83**, 648 (1999).

[2] M. Hillery, V. Bužek, and A. Berthiaume, Physical Review A **59**, 1829 (1999).

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

[4] A. M. Lance, T. Symul, W. P. Bowen, B. C. Sanders, and P. K. Lam, Physical Review Letters **92**, 177903 (2004).

[5] H. M. Wiseman, S. J. Jones, and A. C. Doherty, Physical Review Letters **98**, 140402 (2007).