Quantum secret sharing and microwave quantum networks

N. Korolkova[1], **C. Wilkinson**[1], **W. K. Yam**[2,3], **K. G. Fedorov**[2,3]

[1]*School of Physics and Astronomy, University of St. Andrews, United Kingdom*
[2]*Walther-Meißner-Institut, Bayerische Akademie der Wissenschaften, 85748 Garching, Germany*
[3]*School of Natural Sciences, Technical University of Munich, 85748 Garching, Germany*

Quantum secret sharing (QSS) is one of the key protocols for multipartite quantum networks and can provide an unconditionally secure way to share (secret) quantum states among n players. We analyze the continuous variable (CV) QSS for sharing general single-mode Gaussian quantum states, Fock states and quantum superposition states and demonstrate that quantum steering is the required resource enabling the protocol to proceed securely [1].

We then report the first demonstration of this traditionally quantum optics protocol using continuous quantum variables in microwave regime. We implement the ((2, 3)) threshold CV QSS protocol with $n = 3$ parties in a superconducting microwave quantum network [2], where a subset of at least $k = 2$ players must collaborate to faithfully reconstruct the original secret, represented by a codebook of quantum coherent states (Figure 1). The Dealer superimposes an unknown secret coherent state with one mode of a two-mode squeezing (TMS) entanglement resource and distributes the outcome to the three players, P_i. The TMS entanglement resource is generated by two Josephson Parametric Amplifiers, JPAs, that produce orthogonally squeezed states with squeezing level S. The symmetric beam splitter operations are implemented using microwave hybrid rings. We demonstrate reconstructed-state fidelities that surpass the asymptotic no-cloning threshold of $F_{\rm nc} = 2/3$ and identify a parameter regime that allows for unconditionally secure communication in the presence of an omnipotent dishonest player.

The concept of multipartite quantum networks, a rapidly developing field holding a promise for hybrid architectures for quantum internet, is a central feature in our work. We not only demonstrate for the first time the CV QSS in a tripartite superconducting network. We also experimentally show how QSS enables other fundamental quantum information processing tasks, such as quantum dense coding and elementary quantum error correction of channel erasures [2] (all the protocols can be realised either in optical or in microwave regime). Ultimately, QSS has the potential to be extended towards different quantum protocols, from conference key agreement to the blind quantum computation.

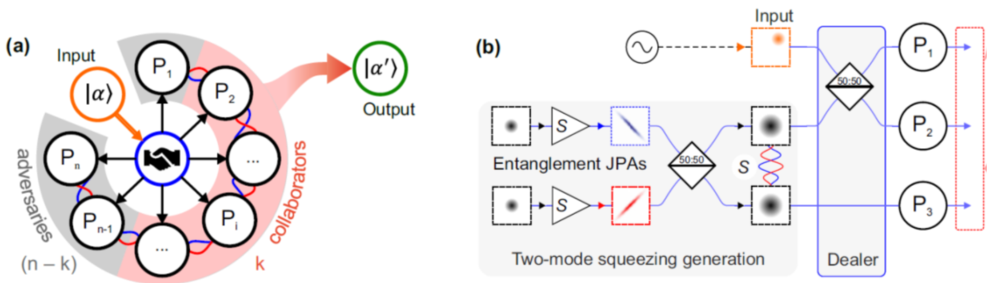

Figure 1: Schematic overview of the $((2, 3))$ threshold QSS protocol implemented in this work [2]. (a) Illustration of $((k, n))$ secret sharing among n players, where only a subset of $k > n/2$ players collaborate to securely reconstruct a secret input state $|\alpha\rangle$. (b) Experimental scheme of the Dealer part of the QSS protocol. The input and resource states are depicted by their phase-space diagrams, showing respective Gaussian-distributed quantum uncertainties.

References

[1] C. Wilkinson, M. Thornton, and N. Korolkova, *Quantum steering as a resource for secure tripartite quantum state sharing*, Phys. Rev. **A 107**, 062401 (2023).

[2] W. K. Yam, C. Wilkinson, S. Gandorfer, F. Fesquet, M. Handschuh, A. Marx, R. Gross, N. Korolkova, K. G. Fedorov, *Quantum secret sharing in tripartite superconducting network*, arXiv:2604.13643 [quant-ph] (2026).