Multipartite measurement-device independent quantum cryptography: Conferencing and secret sharing [1]

Carlo Ottaviani, Cosmo Lupo, Riccardo Laurenza, Stefano Pirandola

Computer Science and York Centre for Quantum Technologies, University of York, York YO10 5GH, UK

Today, much of the effort in quantum key distribution (QKD) protocols is devoted in developing solutions to increase the key rate. At the same time, it is desirable to move towards a full end-to-end network scenario. Continuous variable (CV) systems can offer a solution to both these problems: Using bright coherent states and efficient homodyne detection, one can increase the key rate; then, adopting the configuration of measurement-device independent (MDI) QKD, one can make the first step towards the end-to-end principle. For this reason, CV-MDI-QKD protocols [2, 3] are appealing for quantum networks, especially at the metropolitan distances [4].

In this work we extend CV-MDI-QKD to a multipartite symmetric configuration (star network), where N Bobs send N modulated coherent states to an untrusted relay which performs a multipartite Bell detection. The outcomes γ's are broadcast to the parties. The resulting post-relay N-partite state can then be exploited for private communication, with the trusted parties extracting N keys, that are used to distill a single conference key.

In the fully symmetric configuration the parties are equidistant from the relay and the action of the eavesdropper (Eve) is described by a memory-less thermal channel. The performances of the scheme are quantified in terms of achievable key-rate and distances for fixed number of parties. We perform the security analysis in the entanglement-based representation. Using the Devetak-Winter security criterion, we bound Eve's information by the Holevo function

$$\chi = 2h(\nu) - h(\nu_N), \tag{1}$$

where $\nu = [\mu\,[\eta + \omega\mu(1-\eta)]\,/\,(\eta\mu + (1-\eta)\omega)]$,

$$h(x) = \frac{x+1}{2}\log_2\frac{x+1}{2} - \frac{x-1}{2}\log_2\frac{x-1}{2}, \tag{2}$$

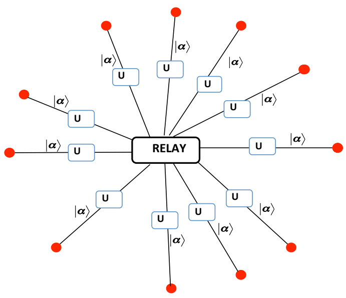
and ν_N is a symplectic eigenvalue depending on the number of users N.

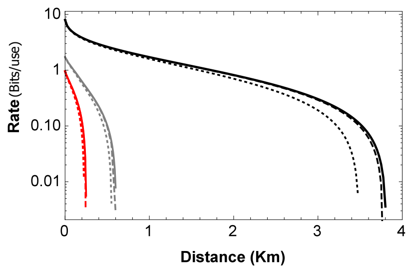
From the post-relay CM $\mathbf{V}_{i|\gamma}$, associated with the ith Bob, and from the conditional CM $\mathbf{V}_{i|\gamma\beta_j}$, after heterodyne detection by jth, we obtain the mutual information between two arbitrary Bobs $I_{B_iB_j} = \frac{1}{2}\log\Sigma$, where Σ depends on $\mathbf{V}_{i|\gamma}$ and $\mathbf{V}_{i|\gamma\beta_j}$. We finally get key conference key rate

$$R = \frac{1}{2}\log\Sigma - 2h(\nu) + h(\nu_N). \tag{3}$$

The figure shows the optimal rate for $N = 2$ (black), 10 (gray), 100 (red) users, assuming no thermal noise (solid lines), 0.01 thermal noise (dashed lines), and 0.1 thermal noise (dotted lines).

In summary we found that high-rate quantum conference-key-agreement is possible over distances between hundreds of meters and a few kilometers, with a large number of users.





[1] C. Ottaviani, C. Lupo, S. Pirandola, *in preparation.*
[2] S. Pirandola *et al.,* Nature Photon. **9**, 397 (2015).
[3] C. Ottaviani *et al.,* Phys. Rev. A **91**, 022320 (2015).
[4] Pirandola S. *et. al.*, Nature Photonics **9**, 773 (2015).