Bell nonlocality is not sufficient for the security of standard device-independent quantum key distribution protocols

Maria Balanzó-Juandó
Máté Farkas, Karol Lukanowski, Jan Kolodynski, Antonio Acín

ICFO - Institut de Ciències Fotòniques, Av. Carl Friederich Gauss, 3, 08860-Castelldefels (Spain)

maria.balanzo@icfo.eu

One of the most profound features of Bell nonlocality is that it allows us to rule out a local realist explanation of an experiment—and thus to verify its quantum nature—without having to characterise the devices used. As such, Bell nonlocality is at the heart of various (device-independent) quantum information processing protocols, harnessing the strong correlations of nonlocal statistics. In this work, we investigate the foundational role of Bell nonlocality in the task of device-independent quantum key distribution, in particular, whether Bell nonlocality is sufficient for its security. Device-independent quantum key distribution allows two honest users to establish a secret key, while putting minimal trust in their devices. Most of the existing protocols have the following structure: first, a bipartite nonlocal quantum state is distributed between the honest users, who perform local measurements to establish nonlocal correlations. Then, they announce the implemented measurements and extract a secure key by post-processing their measurement outcomes. In this work, we show that no protocol of this form allows for establishing a secret key for a large class of nonlocal correlations. To prove this result, we introduce a technique for upper-bounding the asymptotic key rate of device-independent quantum key distribution protocols, based on a simple eavesdropping attack. Our results imply that either different reconciliation techniques are needed for device-independent quantum key distribution in the large-noise regime, or Bell nonlocality is not sufficient for this task. Going beyond the scope of the published work, I will also explain how the results extend to protocols in which only one party announces their measurement settings.

Figures

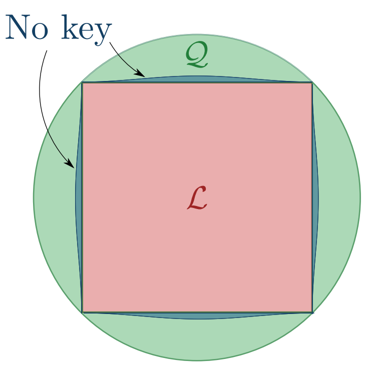

Figure 1: In this Figure, we depict the set of nonlocal correlations (green), the set of local correlations (red), and the nonlocal region which is not enough to ensure secure quantum key distribution using standard protocols, i.e., where Alice and Bob cannot extract a secure key (blue).

References

1. Máté Farkas, Maria Balanzó-Juandó, Karol Lukanowski, Jan Kolodynski, Antonio Acín, Physical Review Letters, 127, 050503 (2021).