Quantum Cryptography using Thermal States

Anne Ghesquière, Elizabeth Newton, Freya L. Wilson,
Matthew C. J. Everitt, Benjamin T. H. Varcoe

We present a scheme which uses thermal states to distribute a quantum secure key. Whereas many of the currently operating quantum key distribution (QKD) schemes rely on optical communication set-ups, we propose to use naturally emerging correlations within thermal radiation to perform QKD. Indeed, thermal radiation is bunched; this means that its quanta are likely to be found in highly correlated pairs. These correlations have been found to produce quantum discord [1]; also, in [2], it was shown theoretically that discord is a necessary condition for QKD.

These correlations can be exploited through the Hanbury Brown and Twiss (HBT) interferometer, which can be described in its simplest terms as follows. A source shines onto a beamsplitter, creating two arms, each of which is detected independently. We propose a central broadcast scheme where a beamsplitter splits the thermal signal into two arms; one of these arms is detected by Alice, the other by Bob. Alice's and Bob's signals are then quantum correlated and they can proceed with the usual slicing and privacy amplification schemes. This protocol is called a central broadcast scheme, and in [2], it was shown that positive discord in a CBS means that a quantum secure key can be extracted even during high noise levels.

We construct a central broadcast protocol, where the eavesdropper Eve performs an antangling cloner attack on the message going to Bob. We model this attack as a beamsplitter that Eve controls, inserted on the path of the signal to Bob. The set-up was realised experimentally, using a superluminescent diode which can switch between thermal and coherent operational mode. We show that there is secrecy when the radiation is thermal using the lower bound on secrecy defined as $K(A:B \parallel E) = I(A:B) - I(B:E)$ [3]. Furthermore, we present a theoretical analysis of the protocol, for the case where Eve's input state is vacuum and for the case that it is not. We find that there is secrecy in both cases, and also confirm that there are quantum correlations, by calculating the quantum discord.

References

[1] Sammy Ragy and Gerardo Adesso. *Physica Scripta*, 2013(T153):014052, 2013.

[2] Stefano Pirandola. *Scientific Reports*, 4:6956, 2014.

[3] U. M. Maurer. *IEEE Transactions on Information Theory*, 39(3):733–742, 1993.