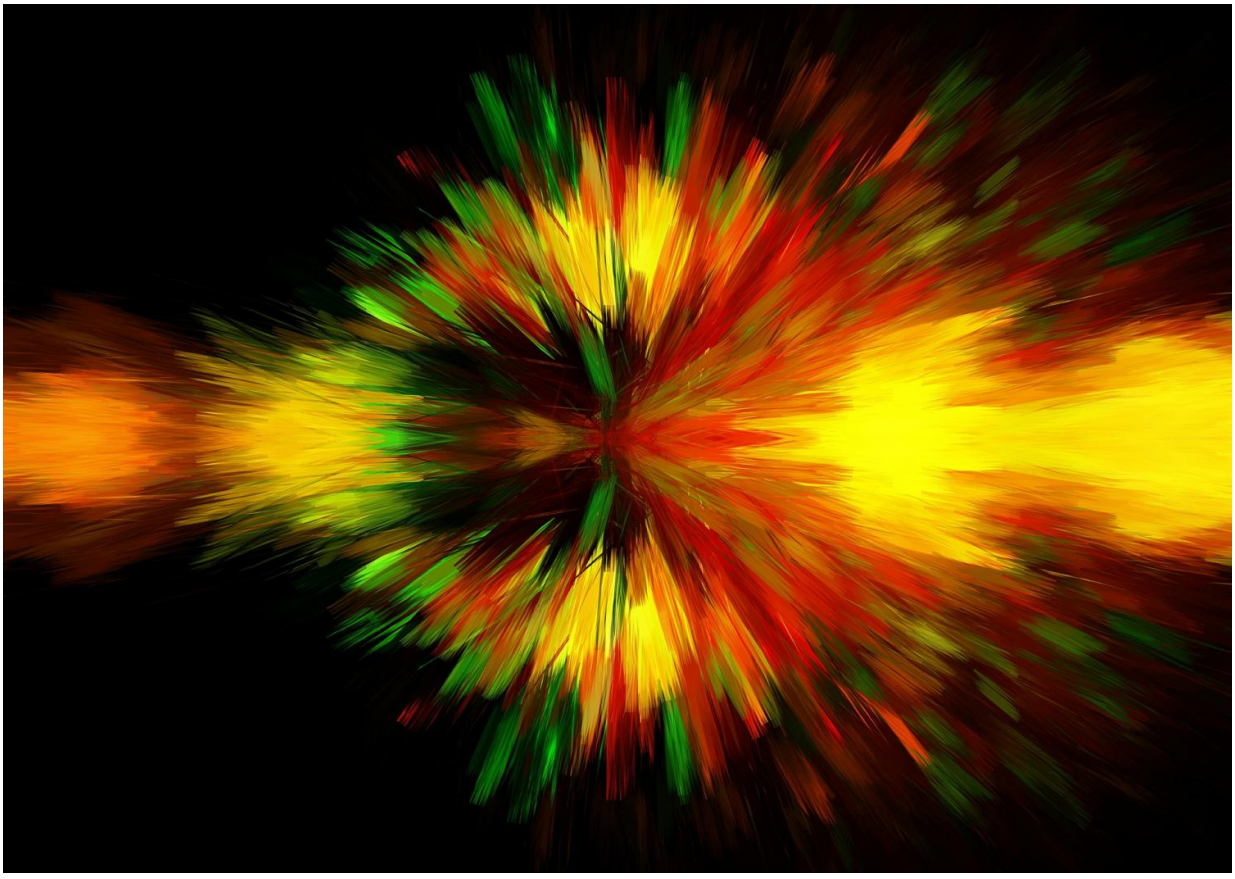
Better safeguards for sensitive information

January 28 2019



Credit: CC0 Public Domain

Despite being the most advanced quantum technology, secure encryption of information units based on a method called quantum key distribution (QKD) is currently limited by the channel's capacity to send or share secret bits. In a recent study published in *EPJ D*, Gan Wang, who is

affiliated with both Peking University, Bejing, China, and the University of York, UK, and colleagues show how to better approach the secret key capacity by improving the channel's lower boundary.

The secure encryption of information units based on a method called quantum key distribution (QKD) involves distributing secret keys between two parties—namely, Alice, the sender, and Bob, the receiver—by using quantum systems as information carriers. However, the most advanced quantum technology, QKD, is currently limited by the channel's capacity to send or share secret bits. In a recent study published in EPJ D, Gan Wang, who is affiliated with both Peking University, Bejing, China, and the University of York, UK, and colleagues show how to better approach the secret key capacity by improving the channel's lower boundary.

The first stage of a QKD transmission is monitored by an eavesdropper, named Eve, as Alice and Bob share a raw key. However, Eve does not have access to a perfect copy of the signals sent by Alice due to quantum rules. During the second stage, Alice and Bob follow classical protocols involving the correction of errors and enhancement of privacy levels. Thus, Alice and Bob share a complete secret key that can later be used to send confidential messages.

The authors focus on a particular type of channel, called the noisy thermal amplifier channel, where the input signals are amplified together with noise induced by the thermal environment. The authors calculate the highest-known amount of secret information units, or bits, that Alice and Bob can share via such a channel. This is done by injecting controlled noise—made up of well-defined thermal agitation—into the detection apparatuses. By optimizing over this noise, they improve the lower boundary of the capacity in the amplifier channel. The authors also confirm that the distribution of secret keys over this channel may occur at higher rates than the transmission of quantum information

itself.

More information: Gan Wang et al, Improving the lower bound to the secret-key capacity of the thermal amplifier channel, *The European Physical Journal D* (2019). DOI: 10.1140/epjd/e2018-90351-0

Provided by Springer