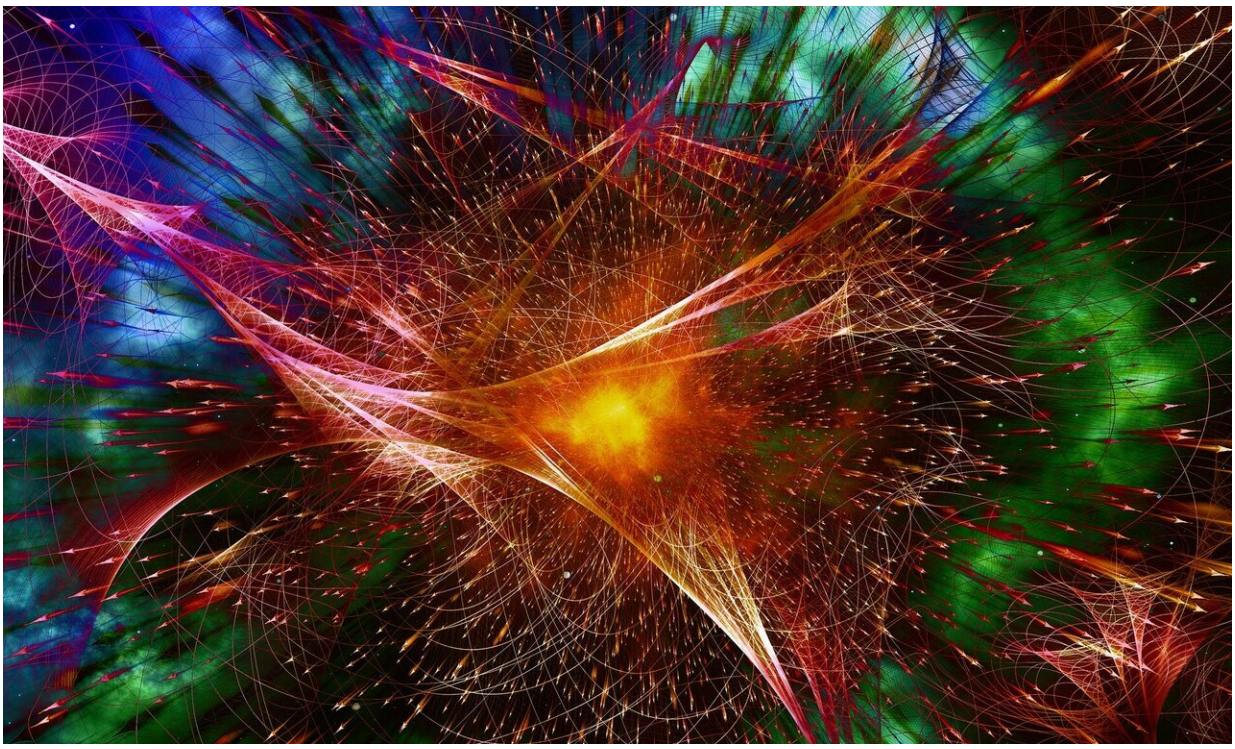
Researchers conduct security analysis and improve quantum random number generation

January 14 2021



Credit: Pixabay/CC0 Public Domain

Recently, the research team led by academician GUO Guangcan from the University of Science and Technology of China of the Chinese Academy of Sciences has made security analysis and improvement of

source independent quantum random number generators with imperfect devices.

By studying the actual characteristics of the measurement devices of the source-independent quantum random number generation, the researchers pointed out that the security issues were caused by afterpulse, detection efficiency mismatching, poor sensitivity to photon number distribution in measurement devices, etc., and gave the corresponding solutions. The study was published in *npj Quantum Information*.

The source-independent quantum random number generation protocol is a new quantum random number protocol proposed in 2016. This protocol can generate secure random numbers under the condition that the light source is completely untrusted by monitoring the error code of the mutual unbiased basis corresponding to the base of the random number generation. It can simultaneously meet the requirements of security and high rate of random number generator, and has a very high devices loss tolerance.

However, the protocol has some security problems, such as the failure to consider the afterpulse problem of the detector, the mismatch of detection efficiency, the poor sensitivity of the detector to the distribution of light source and other characteristics, which impedes the application of this protocol.

In this study, the researchers presented a detector model containing these actual parameters, and then evaluated the impact of these problems on actual security. At the same time, aiming at the afterpulse problem, they gave the security random number information upper bound with the existence of eavesdropping.

To solve the problem of detection efficiency mismatch and poor detector sensitivity to the distribution of light source, the researchers

proposed a method for monitoring the distribution of light source, and gave a bit rate formula based on the composable security with full consideration to the finite length effect.

This study has quantitatively analyzed the security problem caused by imperfect measurement devices in source-independent quantum random number systems and given the corresponding solutions, which provides an important theoretical support for the realization of ultra-fast commercial source-independent quantum random number generator.

More information: Xing Lin et al. Security analysis and improvement of source independent quantum random number generators with imperfect devices, *npj Quantum Information* (2020). DOI: 10.1038/s41534-020-00331-9

Provided by University of Science and Technology of China