

# Safety in secure quantum communication platforms

July 1, 2020

Researchers from **Raman Research Institute (RRI), an autonomous institute of the Department of Science & Technology (DST)** have come up with a unique simulation toolkit for end-to-end **Quantum Key Distribution simulation** named as 'qkdSim'. It ensures online communications (via platforms) are secure, and has gained significance as Covid-19 confines most day to day activities to the digital space.

## Quantum Key Distribution

The secure part of any information transfer protocol is in the distribution of the key used to encrypt and decrypt the messages. Such **standard key distribution schemes**, usually based on mathematical resolution of problems, are **vulnerable to algorithmic breakthroughs and the possibility to run new codes on the up and coming quantum computers**. The solution to ensuring the security of the key transfer process lies in using the laws of quantum physics, wherein any eavesdropping activity will leave tell-tale signs and hence will be easily detected. This is achieved by using Quantum Key Distribution.

Quantum key distribution (QKD) is a secure communication method which implements a **cryptographic protocol involving components of quantum mechanics**. It enables two parties to produce a shared random secret key known only to them, which can then be used to encrypt and decrypt messages. A fundamental aspect of quantum mechanics: the process of measuring a quantum system in general disturbs the system. A third party trying to eavesdrop on the key must in some way measure it, thus introducing **detectable anomalies**.

qkdSim

The research is a part of the Quantum Experiments using Satellite Technology (QuEST) project, India's first **satellite-based secure quantum communication effort**, supported by the ISRO.

The research work is two-fold in its novelty as well as process development. On the one hand, they have developed a simulation toolkit, which bridges a significant gap in the QKD community. On the other hand, they have performed a novel implementation of what is called a prepare and measure QKD protocol, which has higher key rates and lower quantum bit error rate than earlier reported works. In fact, this is **India's first end to end free space QKD experiment**.

With the advent of the upcoming **National Mission on Quantum Technologies and Applications**, this work provides the bedrock for such developments in the country and hence will be of great interest.