

# RRI researchers' toolkit to aid secure communication

## Research Part Of India's First Quantum Experiments Using Sat Tech

**Chethan.Kumar**  
@timesgroup.com

**Bengaluru:** Researchers from the Raman Research Institute (RRI), as part of India's first Quantum Experiments using Satellite Technology (QuEST) project supported by the Indian Space Research Organisation (Isro), have come up with a unique simulation toolkit for end-to-end QKD (quantum key distribution), which will help secure digital communication.

The novel toolkit comes at a time advisories from the Ministry of Home Affairs (MHA) to ensure online communication via secure platforms have highlighted the increasing need for measures to ensure security in the virtual world as Covid-19 confines most day-to-day activities to the digital space.

The secure part of any information transfer protocol is in the distribution of the key used to encrypt and decrypt the messages, RRI, an autonomous institute under the department of science and technology (DST), said.

To tackle this challenge, RRI researchers have come up with a unique simulation



Picture for representation

The toolkit comes at a time MHA advisories have highlighted the increasing need for measures to ensure security in the virtual world

toolkit for end-to-end QKD named 'qkdSim', which is based on modular principles that allow it to be grown into different classes of protocols using various underpinning technologies.

The research led by Prof Urbasi Sinha's team was done in collaboration with Prof Barry Sanders from University of Calgary, Canada, and is a part of QuEST. Their work has been accepted by the journal Physical Review Applied.

"The novelty lies in its exhaustive inclusion of different experimental imperfections, both device-based and

process-based. Thus, results will match with actual experimental implementations to much better accuracy than existing toolkit, making it a QKD experimenter's best friend," DST said.

As QKD grows rapidly in academic, industrial, government, and defence laboratories, this toolkit, accompanied by an instructive application to the uniquely designed "B92 experiment" — a QKD protocol using single photons and associated laws of physics like the Uncertainty Principle and No-Cloning theorem to assure perfect security — will be influential,

according to the DST.

"Secure error free communication protocols are assuming extraordinary importance for which QKD is an attractive solution," said Prof Ashutosh Sharma, Secretary, DST.

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, they've performed implementation of what is called a prepare and measure QKD protocol (B92), which has higher key rates and lower quantum bit error rate.

"This is India's first end-to-end free space QKD experiment. It also has internationally competitive key rates and error rates. RRI plans to follow this up by expanding current scope of qkdSim to include entanglement based QKD protocols and experimental comparisons for the same. This can lead to a whole new software that will be highly beneficial to the experimental secure quantum communication community," DST added.