RRI comes up with simulation toolkit to ensure safety in secure quantum communication platforms

The recent advisories by the Ministry of Home Affairs 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. Such standard key distribution schemes, usually based on mathematical resolution of problems, are vulnerable to algorithmic breakthroughs and 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 or QKD.

To tackle this challenge, researchers from Raman Research Institute (RRI), an autonomous institute of the Department of Science & Technology (DST), Government of India have come up with a unique simulation toolkit for end-to-end QKD simulation named as 'qkdSim', which is based on modular principles that allow it to be grown to different classes of protocols using various underpinning technologies. The research led by Prof. Urbasi Sinha and her team, in collaboration with Prof. Barry Sanders from the University of Calgary, Canada is a part of the Quantum Experiments using Satellite Technology (QuEST) project, India's first satellite-based secure quantum communication effort, supported by the Indian Space Research Organisation (ISRO). This work is going to appear in the journal *Physical Review Applied* (in press).

The novelty of their toolkit lies in its exhaustive inclusion of different experimental imperfections, both device-based as well as process-based. Thus their simulation results will match with actual experimental implementations to much better accuracy than any other existing toolkit, making it a QKD experimenter's best friend.

As QKD is growing rapidly in academic, industrial, government, and defence laboratories, this newly developed simulation toolkit, accompanied by an instructive application to the uniquely designed B92 experiment, will be extremely influential. The B92 is a QKD protocol, which uses single photons and associated laws of Physics like the Uncertainty Principle and the No-Cloning theorem to assure perfect security.

"Secure error free communication protocols are assuming extraordinary importance for which Quantum key distribution (QKD) is an attractive solution, which relies on a cryptographic protocol. A shared random secret key known only to the communicating parties is employed to encrypt and decrypt messages. A unique property of quantum key distribution is that any break in attempt by an unauthorized party is immediately detected. This is because any process of measuring a quantum system creates detectable anomalies," 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 hand, they have performed a novel implementation of what is called a prepare and measure QKD protocol (B92), which has higher key rates and lower quantum bit error rate than earlier reported works following similar source methodology. In fact, this is India's first end to end free space QKD experiment. It also has internationally competitive key rates and error rates. RRI team plans to follow this up by expanding the 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.

This first-of-its-kind practical tool will be indispensable to design, set up, optimize, and evaluate experiments for demonstrating QKD and will engender further development to broaden the simulation tool's applicability. 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.

Figure: Presenting qkdSim: a QKD experimentalist's best friend. Two QKD experimentalists figuring out the most cost-effective and efficient design for their experiment. They run qkdSim, include all the perceived device and process imperfections, and optimize their design for the best possible key rates and lowest possible error rates.

Publication details:

R. Chatterjee, K. Joarder, S. Chatterjee, B. C. Sanders, and U. Sinha, "qkdSim: An experimenter's simulation toolkit for QKD with imperfections, and its performance analysis with a demonstration of the B92 protocol using heralded photons", arXiv:1912.10061v1 (2019). (In Press: Physical Review Applied)

For more details, Prof. Urbasi Sinha (usinha@rri.res.in) can be contacted.