nature india

SCIENCE NEWS

India employs home-grown cryptographic scheme for secure communication

K. S. Jayaraman

doi:10.1038/nindia.2020.117 Published online 27 July 2020

Researchers at the Raman Research Institute (RRI) in Bangalore have implemented India's first quantum cryptographic scheme to enable secure communication of sensitive data[1] — an acute need during the COVID-19 pandemic with most government, defence and academic communication going online.

The widely used information transfer protocols employ a secret "key" known only to the communicating parties, who can encrypt and decrypt the messages. The mathematical toolbox used in such protocols is vulnerable to access by eavesdroppers.

"The answer to this lies in using the Quantum Key Distribution or QKD," says Urbasi Sinha, who heads the RRI team.

QKD is a cryptographic method that enhances the security of the communication link by exploiting the principles of quantum mechanics such as the uncertainty principle and no-cloning theorem, Sinha says.

The process enables two remote users to generate and share a secret key – composed of a string of ‘0’ and ‘1’ bits – which they can use to encrypt and decrypt secret messages. A unique property of QKD is that any unauthorized break-in is immediately detected. It also protects the encrypted information from threats that might arise from future advances in computational power.

The team developed QKD protocol indigenously as part of an ongoing project on secure quantum communication between two Indian ground stations using a satellite of the Indian Space Research Organisation (ISRO). "This is India’s first and only project on satellite based QKD," says Sinha. The protocol operated with a high key rate of 50Kbits/second and low quantum bit error rate (QBER) of~3.5% -- features that guarantee high security.

"QKD is one of the crucial components of the high-powered National Mission on Quantum Technologies just launched by the Indian government," Dipankar Home, a quantum physicist at the Bose Institute in Kolkata, told *Nature India.*

References

1. R. Chatterjee, *et al.* "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)