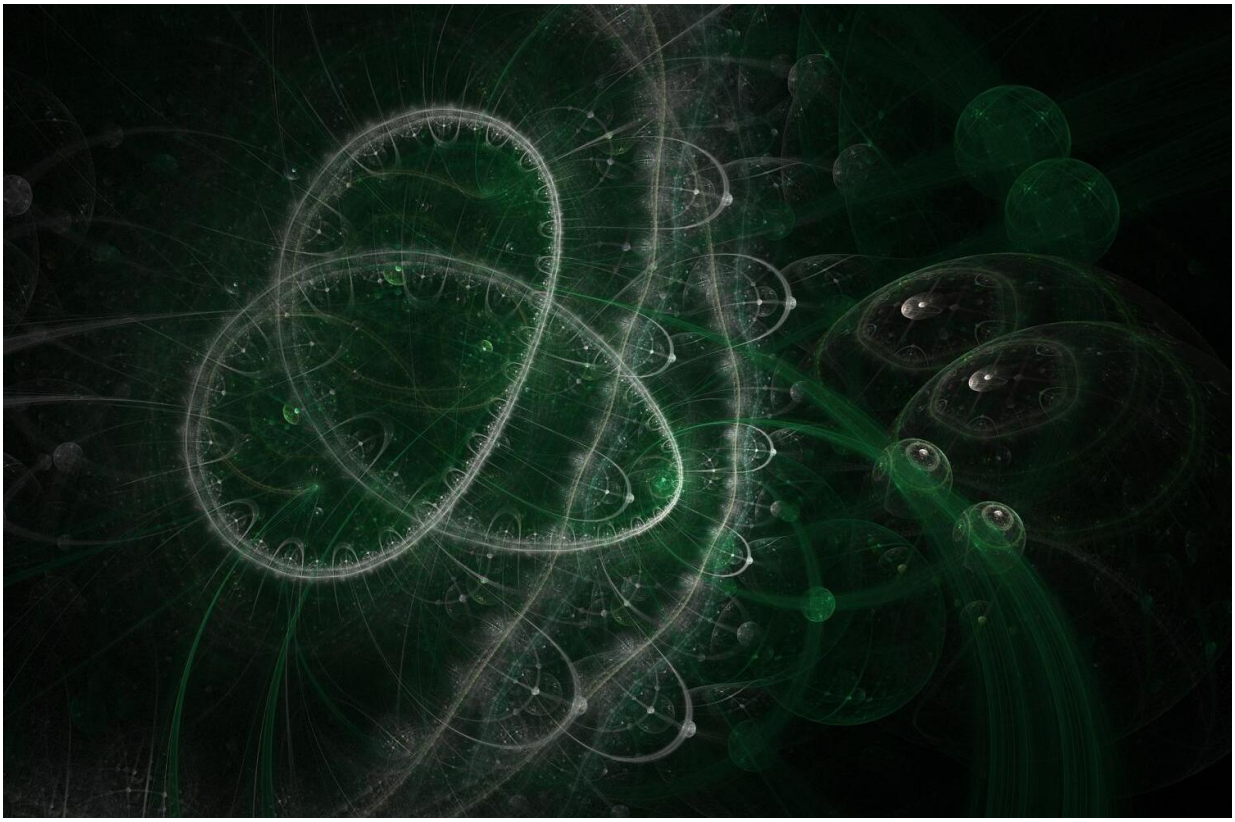
Cost effective quantum moves a step closer

September 19 2017



Credit: CC0 Public Domain

Canadian and US researchers have taken an important step towards enabling quantum networks to be cost-effective and truly secure from attack.

The experiments, by the team from the University of Calgary, the

California Institute of Technology and the National Institute of Standards and Technology, Colorado, prove the viability of a measurement-device-independent quantum key distribution (QKD) system, based on readily available hardware.

QKD provides a method of provably secure communication. Many QKD systems, including commercial systems, have been developed during the last 30 years, and important elements such as secret key rates and maximum transmission have continuously improved.

The team's results, published today in the journal *Quantum Science and Technology*, shows how they employed cost-effective and commercially available hardware such as distributed feedback (DFB) lasers and field-programmable gate arrays (FPGA) electronics, which enable time-bin qubit preparation and time-tagging, and active feedback systems that allow for compensation of time-varying properties of photons after transmission through deployed fibre.

The first author Raju Valivarthi said: "Quantum hacking over the past decade has also shown, however, that the specifications of components and devices used in actual QKD systems never perfectly agree with the theoretical description used in security proofs, which can compromise the security of real QKD systems. For instance, so-called 'blinding attacks' exploit vulnerabilities of single photon detectors (SPDs) to open a side-channel, via which an eavesdropper can gain full information about the (assumed-to-be) secure key. Making practical QKD systems secure against all such attacks is a challenging task."

Senior author Dr. Qiang Zhou said: "Our MDI-QKD system includes four parts: qubit preparation module, Bell state measurement (BSM) module, control module, and time-tagging module, which allows key generation from qubits in randomly prepared states. It is worth to note that our control module in the demonstration is further improved to

control the polarisation and arrival-time of photons travelling from Alice and Bob to Charlie, which ensures their indistinguishability at the moment of the BSM."

Group leader Professor Wolfgang Tittel said: "Our experimental demonstration paves the way for MDI-QKD-based star-type quantum networks with kbps secret key rates spanning geographical distances of more than 100km."

More information: Raju Valivarthi et al, A cost-effective measurement-device-independent quantum key distribution system for quantum networks, *Quantum Science and Technology* (2017). DOI: 10.1088/2058-9565/aa8790

Provided by Institute of Physics