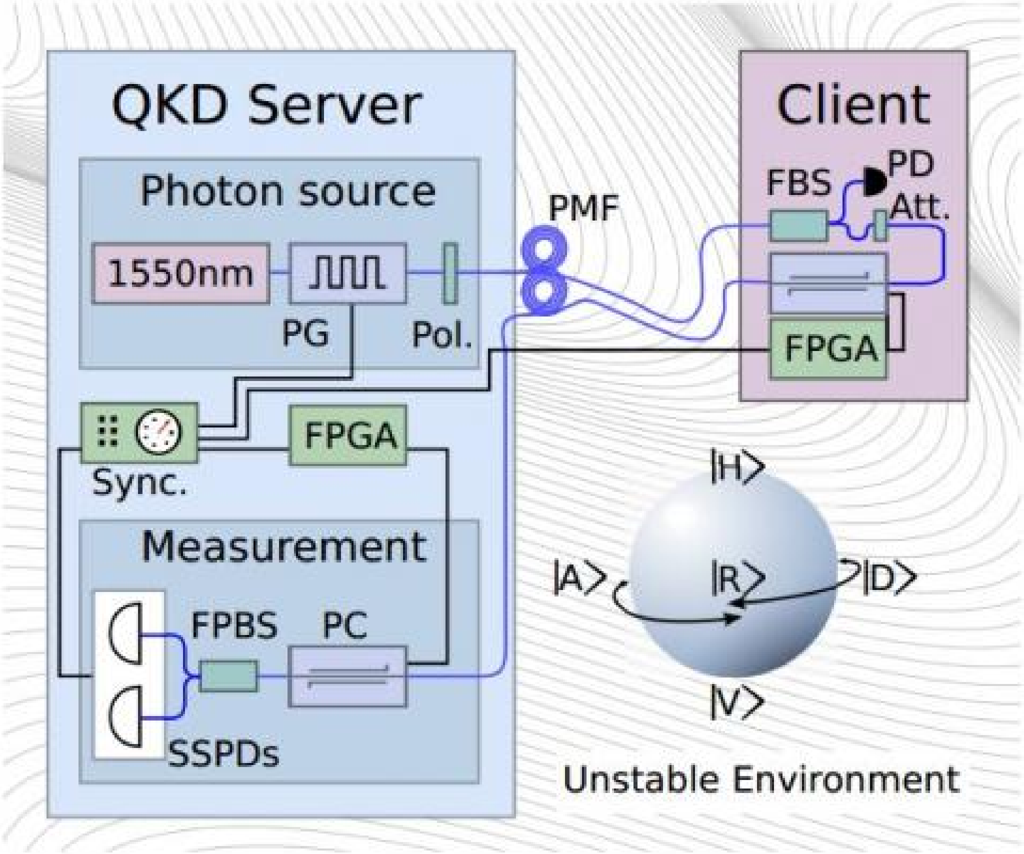
Physics team suggests possible way to make quantum cryptography available in handheld machines

August 30 2013, by Bob Yirka



Experimental set-up for client-server rfiQKD. The server side holds a telecom wavelength (1550 nm) laser with a 1 MHz pulse generator (PG) and fixed polariser, to send light pulses to the client through a polarisation maintaining fibre (PMF). At the client side, an integrated polarisation controller (PC) encodes qubits into the polarisation of the attenuated (Att.) light. A fibre beam splitter (FBS) and photodetector (PD) continuously monitor power for malicious attacks.

Qubits received back at the server side are measured with a similar PC, fibre polarising beamsplitter (FPBS), and superconducting single photon detectors (SSPDs), all controlled by an electronic board synchronisation (Sync.), function programmable gate array (FPGA), and processor. The Bloch sphere illustrates the effects of an unstable environment on polarisation. Credit: arXiv:1308.3436 [quant-ph]

(Phys.org) —A team of physicists at Bristol University in the U.K. has proposed a possible way to allow for quantum cryptography between a large station and a small hand held device. They describe such a technique in a paper they have uploaded to the preprint server *arXiv*.

Being able to encrypt data and the key that allows for unlocking it has become important in modern life. Companies spend millions attempting to protect sensitive information while hackers work non-stop trying to overcome such hurdles to access that information. The current system (RSA) is believed to be, at least for now, just ahead of the hackers. It relies on public key encryption of plain text and privately encrypted keys. This system has two weak points. The first is that it assumes that a hacker has not been able to gain access to a private key through nonconventional means and the second is that it's based on mathematical algorithms that can be cracked given fast enough computers. To gain the upper hand, cryptologists have turned to quantum key distribution (QKD), where quantum bits are used to represent private keys. The main advantage here is that according to the laws of physics, it should be impossible for a hacker to use the key without their interception being detected, which would prevent the sensitive data from being sent.

Up till now, the main hindrance to using QKD has been that it requires a lot of heavy duty equipment and a straight line mode of transport between the sender and receiver due to its sensitivity to noise. In their paper, the team from Bristol claim to have come up with a scheme that should allow a way to overcome such restrictions, at least on the receiver side. It's based on what they call a reference frame independent QKD protocol for polarization of qubits in polarization maintaining fiber—which in essence means they use math (based on measurements made in random directions) to describe a way for moving photons through fiber cables without disturbing their polarization

The team has not yet built such a device of course, that will need to be done by applied physicists, engineers and computer professionals—thus it's not yet a certainty that such a device will work as imagined. One sticking point in particular might be whether the real-world system is actually able to overcome the inherent noise sensitivity.

More information: Reference frame independent quantum key distribution server with telecom tether for on-chip client, arXiv:1308.3436 [quant-ph] arxiv.org/abs/1308.3436

Abstract
We demonstrate a client-server quantum key distribution (QKD) scheme, with large resources such as laser and detectors situated at the server-side, which is accessible via telecom-fibre, to a client requiring only an on-chip polarisation rotator, that may be integrated into a handheld device. The detrimental effects of unstable fibre birefringence are overcome by employing the reference frame independent QKD protocol for polarisation qubits in polarisation maintaining fibre, where standard QKD protocols fail, as we show for comparison. This opens the way for quantum enhanced secure communications between companies and members of the general public equipped with handheld mobile devices, via telecom-fibre tethering.

via Arxiv Blog

Citation: Physics team suggests possible way to make quantum cryptography available in handheld machines (2013, August 30) retrieved 27 April 2024 from https://phys.org/news/2013-08-physics-team-quantum-cryptography-handheld.html