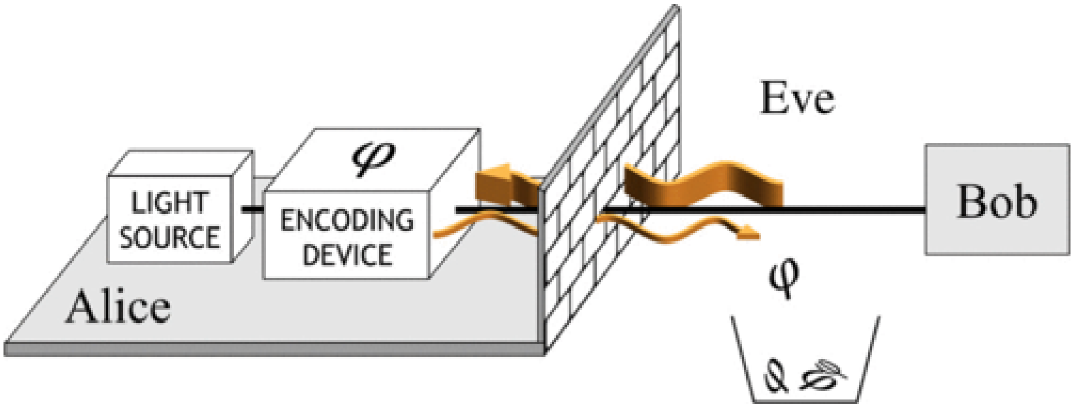
Researchers develop simple way to ward off Trojan attacks on quantum cryptographic systems

September 17 2015, by Bob Yirka



Representation of the Trojan-horse attack against an optical QKD setup. Eve sends a large amount of Trojan photons (thick arrow) against Alice's defensive structure. Some of the photons reach the encoding device, are encoded with the private information φ, and are reflected back to Eve (thin arrow), who retrieves the information by measuring the photons. Credit: *Phys. Rev. X* 5, 031030 – Published 9 September 2015.

(Phys.org)—A team of researchers working for Toshiba in Japan and the U.K. has found a way to prevent Trojan horse attacks on quantum key distribution (QKD) systems. They describe their ideas in a paper they have had published in *Physical Review X*.

One of the hot areas of study in creating secure computer messaging systems is QKD—encrypted keys can be sent securely across public domain fiber networks safe from prying snoopers—if a key is intercepted, quantum physics ensures that it will be made known to the party on the receiving end, who will then call for a new key. Such systems are not as perfect as they seem however, as there is always a weak point in any system. In those based on QKD, that weak point typically resides at the sending site—in one scenario, an interloper, in computer circles known as Eve, can simply shine a bright light on the sender's encoder and then measure the reflection of the light that comes back, revealing the information that was used to make the key. This is a form of Trojan attack. Some have suggested that one way to thwart such an attack is to install devices that detect the physical presence of a person or device near an encoder, but that leaves open the possibly of the attacker foiling the new devices as well. In this new research, the team at Toshiba proposes a new approach, modifying the transmitter so that reflected light will be too weak to reveal any useful information.

The modifications to the transmitter would include adding an attenuator which would reduce the pulse to just one photon, an isolator which would only allow out-going light to pass through, and of course, a filter which would prevent the transfer of any wavelengths not initially specified to be in the channel.

The team has already built and tested a partial system with the new passive Trojan battler and report that it does indeed protect against Trojan attacks. They note also that it is a relatively cheap way to get the job done and the devices can be installed rather easily. Next up is a prototype that will serve as the basis for a product for delivery to customers.

More information: Practical Security Bounds Against the Trojan-Horse Attack in Quantum Key Distribution, *Phys. Rev. X* 5, 031030 – Published 9 September 2015. journals.aps.org/prx/abstract/ …

03/PhysRevX.5.031030 . On *Arxiv*: arxiv.org/abs/1506.01989

ABSTRACT
In the quantum version of a Trojan-horse attack, photons are injected into the optical modules of a quantum key distribution system in an attempt to read information direct from the encoding devices. To stop the Trojan photons, the use of passive optical components has been suggested. However, to date, there is no quantitative bound that specifies such components in relation to the security of the system. Here, we turn the Trojan-horse attack into an information leakage problem. This allows us to quantify the system security and relate it to the specification of the optical elements. The analysis is supported by the experimental characterization, within the operation regime, of reflectivity and transmission of the optical components most relevant to security.

Citation: Researchers develop simple way to ward off Trojan attacks on quantum cryptographic systems (2015, September 17) retrieved 25 April 2024 from https://phys.org/news/2015-09-simple-ward-trojan-quantum-cryptographic.html