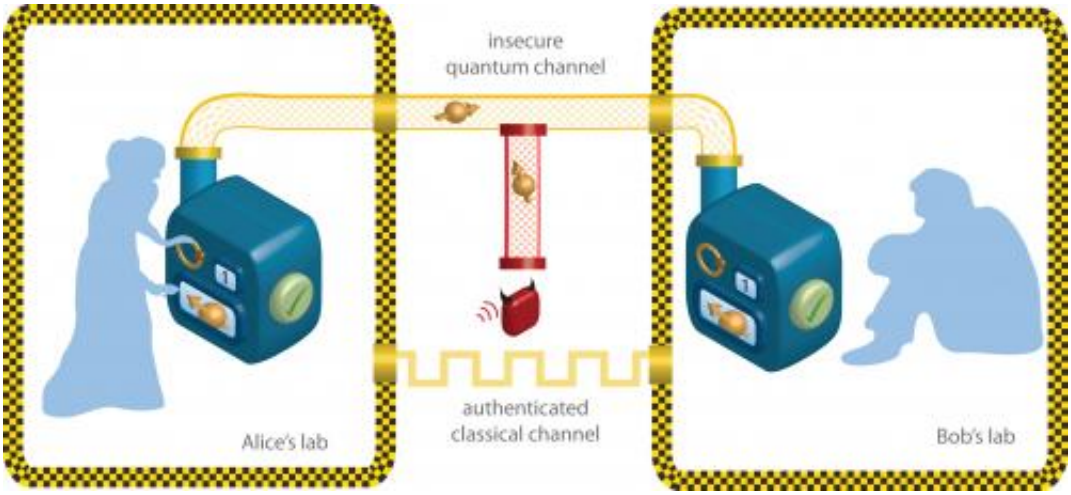
Researchers test quantum encryption hacking risk

May 28 2013



This image illustrates the standard assumption made in quantum cryptography, namely that the devices, such as photon sources and detectors, used by the honest parties, "Alice" and "Bob," are completely trusted (yellow boxes indicate the trusted region), whereas the channel connecting Alice and Bob may be controlled by an adversary. Credit: Renato Renner.

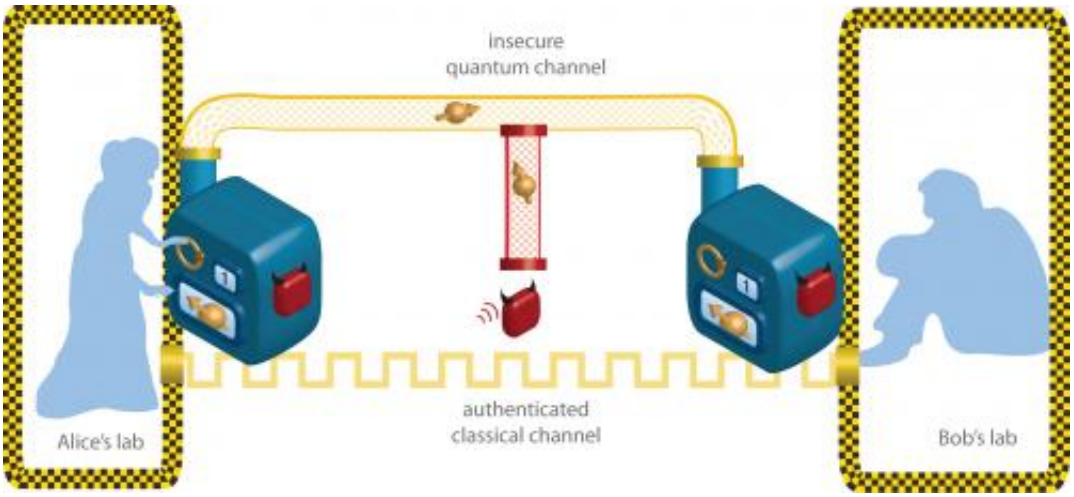
(Phys.org) —Quantum communication systems offer the promise of virtually unbreakable encryption. Unlike classical encryption, which is used to send secure data over networks today and whose security depends on the difficulty of solving mathematical problems like the factoring of large numbers, most quantum encryption schemes keep the encryption key separate from the data. This approach ensures that an eavesdropper with access only to the data could not decipher the key.

However, researchers have recently demonstrated that even quantum encryption may be susceptible to hacking.

In a presentation next month at the Conference on Lasers and Electro-Optics (CLEO: 2013) in San Jose, Calif., Renato Renner of the Institute for Theoretical Physics in Zurich will discuss how he and his team of theoretical physicists are working on new ways to calculate the failure probability of certain quantum encryption schemes. The numbers would allow users to estimate how likely it would be that an adversary could read their secret messages—information that is critical for ensuring the overall security of quantum communications.

Quantum key distribution (QKD) is a kind of quantum encryption in which a secret password is shared between two distant parties (usually named Alice and Bob in thought experiments). The secret password, or key, is distributed as bits of quantum data, so that if an eavesdropper (usually named Eve) tries to intercept the message, the bits will be disturbed and Alice and Bob will know the transmission has been compromised. If the key is not disturbed, it can be used to encode messages that are sent over an insecure channel.

"The security of Quantum Key Distribution systems is never absolute," says Renner. He notes that the security of QKD systems depends on three assumptions: the initial secrecy of the password, the correctness and completeness of quantum theory, and the reliability of the devices in the quantum communication system.



In device-independent cryptography, the required trust is much smaller (indicated by the smaller yellow boxes). Here, security is guaranteed even if Alice and Bob's devices do not work according to their specifications. Credit: Renato Renner.

Recent work by other research groups has illustrated how real-world devices that are not 100 percent reliable can leave weaknesses in quantum communication schemes that may be exploited by a clever hacker. For example, the photon detectors used in QKD should click with a certain probability whenever a photon is detected, but in practice the devices can be "blinded" by a strong light pulse and not click. "In fact, an adversary may use strong light pulses to 'remotely control' the detector," says Renner.

Since such bright light hacking techniques were first demonstrated in 2010, physicists have been keen to find ways to calculate the security of quantum encryption schemes without making assumptions about the reliability of the devices. The quest has generated a lot of interest in a field called device-independent cryptography.

"In device-independent cryptography, the proof of security is based

solely on directly observable correlations between sender and receiver, and it does not matter how these correlations have been established," says Renner. "Even if the detectors were blinded, for instance, as long as they produce the right correlations, a secret key can be extracted from them." This differs from the traditional approach to calculating quantum encryption security, which is only valid in the nearly impossible case of the devices working exactly according to theoretical specifications.

Renner and others are working on theory-based calculations that establish the device-independent security of certain QKD systems. "With modern proof techniques, it is now possible to quantify their security in terms of a 'failure probability,'" says Renner. "Specifically, it is possible to make claims such as 'the probability that this particular QKD system can be broken is at most 10-20,'" a vanishingly small number.

Renner notes that it is important to be able to reliably calculate the order of magnitude of the failure probability of an encryption system, whether it is tiny like 10-20 or significantly larger. "Compare it to an aircraft," he says. "Once we realize it is not 100 percent safe, we want to be sure that the failure probability is still small enough so that we are ready to carry the risk. If we have a system that may fail, but do not know how likely it is to fail, then we will probably not want to use it."

More information: CLEO: 2013 presentation QTu2C.1. "How secure is quantum cryptography?" by Renato Renner is at 2 p.m. on Tuesday, June 11 in the San Jose Convention Center. CLEO: 2013 www.cleoconference.org/

Provided by Optical Society of America

Citation: Researchers test quantum encryption hacking risk (2013, May 28) retrieved 27 April

2024 from https://phys.org/news/2013-05-quantum-encryption-hacking.html

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.