Hack Me If You Can

Quantum cryptography promises inherently secure communications… in theory! But what actually happens in practice? Recent studies show how weaknesses in a real system can be exploited to perform an "undetectable" quantum hack.

Pick a card, any card...: how do magicians always manage to guess the right one? Is it really magic? or do they trick us without our perceiving it? If we were to use a special, quantum card deck of cards, however, it would be that much harder for the magician in question to perform his tricks without our noticing it. And this is what lies at the heart of quantum cryptography. Be that as it may, researchers from the Norwegian University of Science and Technology (Trondheim, Norway) and the Max Planck Institute of the Science of Light (Erlangen, Germany) have nevertheless been able to successfully hack commercial quantum cryptography systems in ways that can go undetected.

How can a private conversation be truly guaranteed? Take Alice and Bob, the archetypal characters used in the common parlance of communication research: how can Alice securely send a private message to Bob? She could encrypt her message, making it decryptable only by the holder of the *right key*. Essentially, this would be like Alice sending Bob a letter in a box locked with a security padlock: Alice and Bob must agree on a security mechanism (e.g. a set of keys) with which to open and close this security padlock. Unfortunately, however, this, in its turn, would create the new problem of how Alice and Bob can agree on what type of key to use in order to guarantee the safety of their communication. Alice could send the keys separately in a different envelope, but she must always bear in mind the possibility that a third party, traditionally identified as *Eve*, may attempt to make a copy of the key while this is in transit — and succeed.

Every day, billions of electronic keys are exchanged over the Internet, in sending private emails, making online payments or carrying out online banking transactions. Current methods of cryptography and key distribution usually rely on the computational difficulty in *cracking* these keys. Early cryptographic methods that used to be secure in the past are deemed insecure today as a result of the ever more powerful computers available. In fact, the only absolutely secure way to communicate is to use a device commonly referred to as a *one-time pad*: a random key that is of the same length as the message and that is used once only. In essence, this is like Alice replacing each letter of her message with a random letter of the alphabet, and relying on Bob knowing how to decipher this. Secure, unarguably! But not at all practical — until quantum cryptography came along, that is!

Quantum cryptography enables secure communication between two partners because it relies on the laws of quantum physics to ensure that nobody can eavesdrop unnoticed in the time that it takes for a one-time pad to be established. One standard approach to Quantum Key Distribution (QKD) can be illustrated as follows. Alice sends a random series of 0s and 1s to Bob, each represented by the polarization of a photon: one half of the photons are either vertically polarized (0) or horizontally polarized (1); the other half are either diagonally polarized at +45° (0) or at -45° (1). Technically speaking, these two types of photons are encoded in two different bases. For each photon Bob has to guess the base in which this was encoded. If his guess is right, he retrieves the value sent by Alice; otherwise, he gets a random value, uncorrelated with Alice's value. If Eve tries to intercept the photons, she will alter their polarization state in a way that Alice and Bob can recognize. In this case, Alice and Bob can simply abort the establishment of the secret key and look for a different communication channel. Thus, Alice and Bob can be sure that Eve will never know the content of their message.

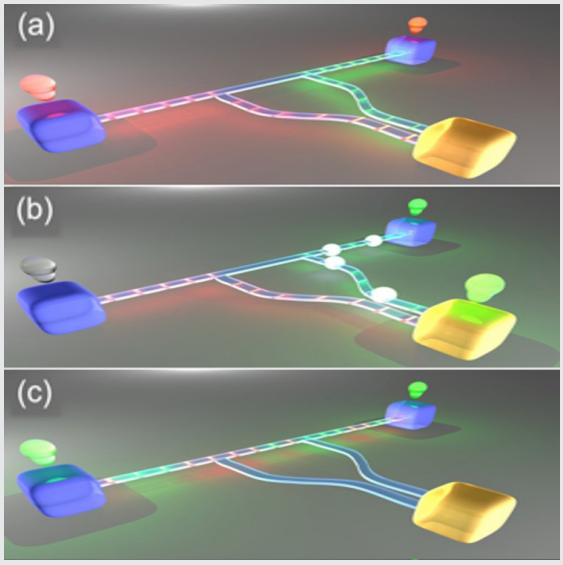

Figure 1: Quantum key distribution hack. *Unsuccessful hack*: (a) Alice sends the key to Bob; Eve interferes with the communication (here represented by a change in color). Alice and Bob detect the attack. *Successful hack*: (b) Eve blinds Bob with bright pulses; (c) Alice and Bob think that the communication channel is safe.

Despite the fact that this is a relatively new technology, QKD is already being implemented in commercial devices. Lars Lydersen, from the Norwegian University of Science and Technology of Trondheim, and colleagues have ma-

naged to show that such QKD implementations still leave some room for successful attacks. They exploited the fact that the avalanche photodiodes used as single-photon detectors are not ideal and can be tricked. In a nutshell, Eve can control the measurement of the photodetector from a distance, making sure that it does not detect a signal unless she guesses the right base; in this way, Alice and Bob can be deceived into thinking that their communication channel is secure.

Lydersen and colleagues' work moves the focus from implementing QKD to how QKD is actually implemented. "The impact of their work is significant," says Nicolas Gisin from the University of Geneva [1], "and it shows that QKD has entered an advance stage of maturity where even complex details are seriously analyzed by independent researchers. The users of QKD have thus been reassured that their system's practical security is thoroughly analyzed." "The fact that we find loopholes," agrees Lydersen, "merely serves to additionally strengthen the security rather than to prove that QKD is insecure." Despite Lydersen and colleagues' successful hack, both Gisin and Lydersen agree on the fact that Quantum Key Distribution is the cryptography scheme of the future, especially in the case of high security applications.

[1] N. Gisin *et al.*, *Quantum Cryptography*, Rev. Mod. Phys. **74**, 145–195 (2002).

Giorgio Adamo

© 2011 Optics & Photonics Focus

Lars Lydersen, Carlos Wiechers, Christoffer Wittmann, Dominique Elser, Johannes Skaar & Vadim Makarov, **Hacking commercial quantum cryptography systems by tailored bright illumination**, Nature Photonics (2010) **4**, 686-689.