Improve security of quantum cryptography

Andreas Poppe

Quantum key distribution systems based on entangled photons are robust against recently published methods of attack.

Quantum key distribution (QKD) is a method to establish a secret key between two communicating parties, often referred to as Alice and Bob. Should an eavesdropper, Eve, spy on their communication, the laws of quantum physics stipulate that leakage of information will affect the quantum bit error rate (QBER). This alerts Alice and Bob that their communication has been compromised. In theory, QKD can be 'unconditionally secure,' meaning that Eve can use all present and future technologies to devise her measurement apparatus (including quantum computers, digital computers, and perfect software algorithms) and still not be able to break QKD. On the other hand, many practical implementations of QKD include non-optimized software or hardware and may therefore be vulnerable against two new types of attacks specially designed for QKD.1–4 Carefully optimized setups, like our entanglement-based quantum key distribution scheme, are immune to both classes of attacks.

In the original QKD scheme developed by Charles H. Bennett and Gilles Brassard, known as BB84, Alice sends Bob photons that have vertical and horizontal or +45° and −45° polarizations. The possible states in each basis are given the values 0 and 1: these are known as qubits, or quantum bits. When Alice sends a photon, she chooses both a basis and an orientation within that basis. Bob must choose which basis in which to measure each photon he receives. If he measures in a basis different from the one in which Alice sent the photon, he may obtain an incorrect orientation. After sending all the photons, Alice lets Bob know the basis she used for each one. They throw out the values he measured in the wrong basis, and the resulting values become the key.

One class of attacks on QKD uses entanglement to gain information about the communication.1 Experimental demonstrations of these attacks have been described.5 With this strategy the eavesdropper extracts information about the polarization state of the qubit by entangling it with another photon. However, this introduces a small but unavoidable polarization change. This attack comes close to the theoretical limit possible for individual attacks,5 as quantum mechanics does not permit the extraction of information without disturbing the qubits. We (and other groups) use this restriction to calculate how much information was leaked and shorten the key accordingly to restore security and thereby eliminate the threat of this entanglement-based attack.1
Figure 1. The polarization entangled source emits pairs of photons that Alice and Bob measure. Photons are analyzed by modules in different polarizations: H, V, +, −. Quantum effects cause correlations that can be transferred to a secure key by the field programmable gate array (FPGA). QKD: quantum key distribution, Pol.Cont.: polarization controller, H: horizontal, V: vertical, +: +45°, −: −45°.

Furthermore, entangled photon pairs can be used not only for the attack, but for QKD itself. Whereas the BB84-scheme includes one sender and one receiver, our entanglement-based scheme consists of two receivers powered by a source of polarization entangled photon pairs. Alice and Bob each receive one photon from the entangled pair. Because the polarizations of entangled photons are correlated, Alice and Bob can use this information to create a secret key. The observed correlations are stronger than classical physics allows, as both photons will always yield the same polarization results if measured in the same basis.

In our experimental setup, 810nm photons are detected by free-running silicon avalanche photodiodes (Si-APDs) waiting for the spontaneously generated photons (see Figure 1). The corresponding paired photon at 1550nm is sent to Bob via standard fibers and detected by InGaAs-APDs, which need to be gated. This is accomplished by classical pulses propagating to Bob and opening his detectors right on time to detect the corresponding 1550nm photons.

The second class of attack is based on technological imperfections in single-photon detectors or electronics. These imperfections allow possible timing attacks, which produce no observable increase in the QBER. Typical distribution of the arrival times (timing jitter) at the Si-APDs and the variation of the transit times between them is more than 100 times the coherence length of the generated photons. Eve may thus obtain unambiguous information about the fired APD by comparing the relative time delay between the classical gate pulse and the 1550nm photon. To close this loop hole, additional electronics carefully match delays in 20ps steps between all four Si-APDs on Alice's side to eliminate spurious timing information. In our current setup (see 'Individual delay modules' in Figure 1) we increased the overlap between different detectors to 99%.

Second, if the possible detection windows of the four gated InGaAs-APDs at Bob's side are only slightly shifted in time, Eve can hide her errors. After an intercept-resend attack, Eve wants Bob only to observe a signal in the basis corresponding to her measurement, as the other basis would disclose her attempts. Exploiting the different detector efficiencies, Eve can appropriately delay the photon and make sure that only the intended detector is ready to 'see' it. Again, a careful adjustment of the timing (see 'Individual timing modules' in Figure 1) of each individual bias pulse removes this threat.

Theory groups have analyzed quantum attacks on QKD for many years. The normal privacy amplification procedure can easily overcome such attacks, as we have shown in previous work. Thus, it is now important to consider all potential security loopholes that may result from real-world technological implementations of systems. While most experimental groups are aware of
security issues and take appropriate countermeasures, pointing out potential loopholes as well as finding practical means to close them will ultimately make all real-world quantum key distribution systems more secure.

Andreas Poppe  
Faculty of Physics  
University of Vienna  
Vienna, Austria  

References:
5. Quantum cryptography is hacked, news@nature. 23 April 2007  

DOI: 10.1117/2.1200708.0809  

http://spie.org/x15600.xml  
SPIE © 2007