Quantum Cryptography

Gilles Brassard
brassard@iro.umontreal.ca

Département IRO, Université de Montréal
C.P. 6128, succursale centre-ville, Montréal, Québec, Canada H3C 3J7

For ages, mathematicians have searched for a system that would allow two people to exchange messages in absolute secrecy. Around the middle of last century, Shannon proved that this dream is possible if and only if the legitimate participants share a random secret key as long as the message they wish to transmit. But Shannon's theorem did not take account of the quantum world in which we live. When information is appropriately encoded as quantum states, any attempt from an eavesdropper to access it yields partial information at best and entails a probability of spoiling it irreversibly. This unavoidable disturbance can be detected by the legitimate users. This phenomenon can be exploited to implement a cryptographic system that is unconditionally secure even against an eavesdropper with unlimited computing power and technology, with no need for a long shared secret key. This can be accomplished by the use of very faint pulses of polarized light that consist on the average of less than one photon. Alternatively, entanglement can be harnessed to the same cause. Sophisticated prototypes have been built in several countries, including England, Switzerland and the United States. In particular, the Swiss prototype works over 23 kilometres of ordinary optical fibre deployed beneath Lake Geneva. Another prototype, built at the Los Alamos National Laboratory, implements quantum cryptography on a free line-of-sight optical path, without any need for a waveguide. Sattelite based implementations are being contemplated.

I shall describe the basics of quantum cryptography and discuss the (in)security of some current prototypes. I shall discuss also issues that concern the use of quantum cryptography beyond the transmission of confidential information. Are there other tasks of a cryptographic nature that could benefit from quantum mechanics? For many years, the chief candidate was bit commitment, a primitive that would allow one person to commit to the value of a bit in a way that this value remains concealed until that person wishes to reveal it, at which time it is not possible to reveal a bit different from what had been sealed in the commitment. In particular, this primitive could be used to implement perfect zero-knowledge protocols and protect private information while it is being used to reach public decisions. It is obvious that unconditionally secure bit commitment cannot exist according to the laws of classical physics. Yet, hopes were high that a quantum version of this powerful primitive was possible, but they were struck down five years ago. Despite this setback, quantum mechanics does provide powerful tools for cryptography. For example, it allows for a coin tossing protocol in which neither party can make the coin fall on their chosen side with a probability better than 75 %. Also, it allows for the computationally-secure distributed computation of functions on secret inputs under the only assumption that (quantum) one-way functions exist. (This assumption is believed to be too weak in a classical setting.) I shall discuss these results as well as other more recent work on quantum authentication and the transmission of confidential quantum information.

We end with a speculation that the foundations of quantum mechanics can be laid on the understanding of which information processing tasks are possible (such as unconditionally secure confidential communication) and which are not (such as unconditionally secure bit commitment). Could it be that if God had wanted to provide Her creatures with confidential communication but not with the ability to compute on secret data, then She had no choice but to invent quantum mechanics? Wouldn't that be a nicer foundation for quantum mechanics than the current cumbersome axioms?

No prior knowledge of classical cryptography will be assumed.