Parabola Volume 42, Issue 3 (2006)

Quantum Cryptography

Nuno Crato

It sounds like science fiction, but it is a reality: the most bizarre properties of subatomic particles allow us to create unbreakable ciphers.

The security of bank transactions, electronic commerce, and email communication is based on the safest cryptography systems created by men. But "safest" does not mean "impossible to break". The safety of one of the most reliable modern cryptography systems, the so-called RSA, which we described in the earlier article in this series, is based on the difficulty of finding the prime factors of very large numbers. There are no algorithms known to date that enable their factorization in a reasonable amount of time, even if we use the most powerful computers available. However, if a mathematician discovers a process that enables a speedy factorization, or if a new generation of computers such as quantum computers are commercialized, the world of communication as we know it can be easily jeopardized. In the event that one of these revolutionary technologic advances becomes widespread, electronic commerce would cease to be secured, the military would have to reinvent its communication systems, and bank institutions would have to take a step back and make transactions at a very slow pace. It would be the collapse of informational technology in our present day society.

Not surprisingly, people are looking for a new cryptography system that will be absolutely secure. Before RSA can fail us, mathematicians, physicists, and computer scientists hope to develop a new procedure that will be virtually unbreakable. This might be possible because the new system scientists envision to create is based on the most profound laws of matter, those that govern the uncertainty of the quantum world. The impossibility of getting to know a priori the behavior of elementary particles is what will guarantee communication security.

The idea has been brewing in the minds of scientists for some time now. Charles Bennet, a computer scientist at the IBM Watson Research Center has been one of those looking for a solution to this problem. Finally, in the 80's he and his colleague Gilles Brassard managed to conceptualize a quantum cryptography system. For a long time their ideas were only dreams. During the last two years, however, technological and science advances have made it possible to build prototypes of quantum systems that seem to be absolutely unbreakable.

To discuss issues related to ciphered messages, experts usually refer to three different fictitious characters: Alice, Bob, and Eve. The first represents the sender, the second the receiver, and the third the intruder who attempts to break the secret communication. At the core of the process proposed by Charles Bennett and his collaborators, there is a random code key as long as the message itself. This key is simply a binary number, i.e. a sequence of zeros and ones led by a one. Alice begins by transforming the text she wants to send Bob by translating it into another binary number. Then, she

A new book explaining how quantum mechanics can be used to conceive an innovative computing system.

adds the key number to her message number. She sends the result to Bob, who has the key that Alice used. By subtracting the key to the message received, he gets the original message. To read it, he only has to transform the sequence of zeros and ones into a sequence of letters, but this is a routine procedure any computer is capable of doing.

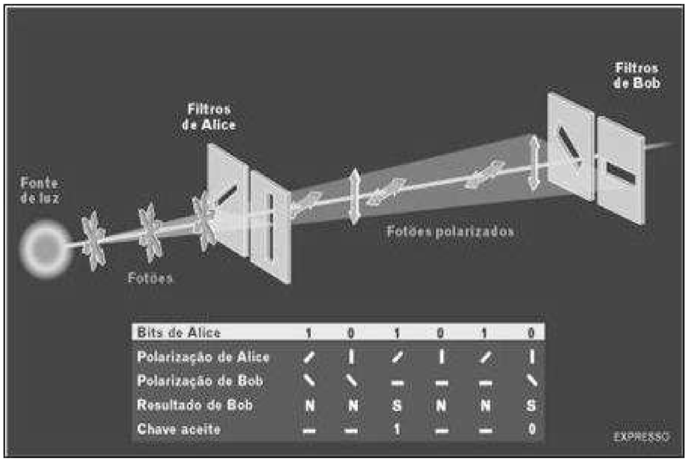
For this system to be unbreakable, it is important that the key is a random sequence of zeros and ones and that it is used only once. This usually means that those numbers have to be generated in advance and that Alice has to send them to Bob. This is where problems usually arise. If Alice and Bob never meet face to face, as it happens in e-commerce, they have to exchange the key through some communication channel. How can they do that? Well, they could agree on another key, but this again does not solve the problem, as to do this Alice and Bob would have to meet or trust a messenger . . .. Since Eve is always peering over them, absolute security seems impossible.

This is when the quantum world comes into play by the hands of Charles Bennett and other computer scientists. It is a strange world, with rules difficult to understand on the basis of our everyday experiences. One of those rules is uncertainty. And this uncertainty is not based on our insufficient knowledge; rather it is intrinsic to the very life of particles. How could this be used for safe communication?

In order to create the random code key, Alice begins by sending Bob a sequence of light particles, that is, a sequence of photons. She has two polarizers in her system, one vertically oriented and another tilted at 45°, as we can see in the figure. To set up the key, she randomly alternates the polarizers and, for example, makes zero correspond to a vertically polarized photon and makes one correspond to a $45°$ polarized photon. Bob has two other polarizers: one of them vertically oriented and another one at $-45°$. When he receives Alice's photons, he makes them pass through one of his polarizers, alternating the two in a completely random fashion.

The photons that Alice sends and Bob receives may or may not pass through his device, depending on how the polarizers are oriented. If Alice sends a photon polarized vertically and Bob makes it pass through his horizontal polarizer, the particle is stopped and does not pass. If Alice sends Bob a photon polarized at $45°$ and Bob receives it with the polarizer at $-45°$, the particle is also stopped and does not go through. Polarizers perpendicular to the photon polarization do not let the particles go through.

Surprises arise when Alice sends a vertically polarized photon and Bob receives it with the diagonal polarizer or when Alice sends a diagonally polarized photon and Bob receives it with the horizontal polarizer, that is, when Alice and Bob's polarizers make a $45°$ angle. In this case, the uncertainty principle of quantum mechanics is set in motion: half of the particles go through Bob's polarizer and the other half is stopped. And this happens without any prior knowledge of which particles are going to go through and which particles are going to be stopped.



Bits de Alice	1	0	1	0	1	0
Polarização de Alice	/	│	/	│	/	│
Polarização de Bob	\	\	—	—	—	\
Resultado de Bob	N	N	S	N	N	S
Chave aceite	—	—	1	—	—	0

At this stage, only Alice knows the polarization of the photons she sent. And only Bob knows which ones finished their trip. This way, Bob discovers the polarization established by Alice for the photons that passed through. Because if a photon passed through a diagonal filter, Alice must have polarized it vertically and it can be assigned the value zero. If, however, a photon passed through a horizontal filter, Alice must have polarized it diagonally and it can be assigned the value one. Those photons that were retained remain a mystery to Bob.

But now Alice needs to know which photons went through Bob's filters. To know this, Alice and Bob can communicate through a less secure system and they can even be heard by Eve. Even if Eve finds out which particles reached Bob, she still cannot figure out which filter they passed through. Thus, the key is established solely on the basis of the photons that completed the voyage. Now, Alice and Bob can communicate with complete security. The uncertainty of the quantum world gives them the certainty that their code cannot be broken.

Maybe we are close to implementing this cryptography system. Only a few years ago it all sounded like science fiction, but recent technological breakthroughs made it possible to create prototype computation models with viable applications of these ideas. As we can anticipate, technological challenges are huge. How do we transmit light a photon at a time? How do we make sure these particles reach their destination? Nonetheless, these problems are being solved little by little. We are already able to use quantum cryptography through fiber cables and through air for a few kilometers. Thus, we may not be far from being able to protect our secrets by making them travel a particle at a time—at the speed of light.