A method for secure transmission: Quantum Cryptography

P. Navez and G. Van Assche
English translation by J. Barrett

April 2002

Abstract— **At the cutting edge of technology, quantum cryptography guarantees absolute confidentiality for information exchanged via an optic fibre. The secret of this ability lies in the possibility of storing information in the elementary constituent of light: the photon.**

I. THE VULNERABILITY OF CONVENTIONALLY ENCRYPTED TRANSMISSIONS

How can we communicate secret messages and be sure that they are not read by an undesirable third person? Cryptography is the discipline that tries to answer this question.

In traditional cryptography, only the Vernam cipher permits the establishment of an unconditionally secure channel between a sender (Alice) and a receiver (Bob). This method requires Alice and Bob both to agree on a secret key, which is determined beforehand. Alice encodes the message using this key, and the encoded message cannot then be decoded, except by using the same key, i.e., by Bob. The rule for encoding is simple. Suppose that Alice wants to transmit one bit of information. For this she uses one bit of the key, performing an ”exclusive-or” operation with the bit to be transmitted. Bob, on his part, can redo the same operation, which cancels out the first ”exclusive-or”, to decode the transmitted bit.

Unfortunately, the Vernam cipher suffers from a major inconvenience. For the method to remain unbreakable, the key must consist of as many secret bits as the message to be transmitted, since the key can only be used once. Using a key more than once causes the Vernam cipher to lose its property of being unbreakable and allows a fairly easy cryptanalysis after successive transmissions.

Strictly speaking, the secret key must originally be exchanged from hand to hand by Alice and Bob. This means that if one wants to transmit a gigabit of secret information, Alice and Bob must meet to exchange, for example, a CD-ROM containing a billion random bits. This procedure is not practical because it imposes that Alice and Bob must meet, even if they then want to communicate at a distance of 10 000 km.

Mathematicians have therefore developed other cryptographic methods, looking to rectify these difficulties.

The first difference between the Vernam cipher and current methods of encoding consists in replacing the simple ”exclusive-or” operation by a much more complicated operation between the key and the plaintext message. Using these methods, it is practically infeasible to recover the plaintext from the encoded message, or even to recover the key from the plaintext together with corresponding encoded message, even if the key is much smaller than the message to be sent. This is the case, for example, with the DES block cipher [4], or the more recent Belgian Rijndael algorithm, chosen to be the new AES standard [5].

Thanks to these algorithms, Alice and Bob can now exchange a small key, which is useful for encoding big messages. The price to be paid for this advantage is that absolute security is lost, and an assumption must be adopted. In theory, it is now possible to recover the plaintext message from the encoded message, but doing this is sufficiently difficult that we can suppose that the enemy does not have the computational resources to do it.

In practice, this assumption is realistic. A hacker will find it much easier, in general, to exploit the weaknesses of an information processing system itself than to perform the necessary calculations to break the algorithm, even if in possession of today’s most powerful computers. Nevertheless, nothing says that in the long term, developments in mathematics or information theory will not make feasible the extraction of the plaintext message from the encoded message.

The second improvement of modern cryptography is

Authors are with the Service de Théorie de l’Information et des Communications (N. Cerf), Ecole Polytechnique, Université Libre de Bruxelles, Brussels, Belgium. (e-mail: patrick.navez@ulb.ac.be, gvanassc@ulb.ac.be, jbarrett@ulb.ac.be)

G. Van Assche is also with the Smart Card Security Center of Excellence (Y. Moulart), Proton World, member of ERG Group, Brussels, Belgium.

the introduction of public key cryptography, allowing Alice and Bob to exchange secret messages without meeting beforehand to exchange a key.

In public key cryptosystems, widely used these days, each correspondant possesses two keys. One key is public and known to all (for example, it may be published in a directory) and only permits the encoding of a message, not the decoding. The second key, on the other hand, is private, and only permits decoding. To send a message from Alice to Bob, the procedure is as follows. If she hasn't already done this, Alice procures Bob's public key (from a public database, or perhaps she simply asks Bob for it). Then, Alice uses Bob's public key to encode her confidential message and sends the encoded information to Bob. Bob is the only person in possession of the corresponding private key, and thus the only person able to decode the message which Alice has just sent him. In this scheme, the essential idea is that encoding is public, in the sense that anyone can send an encrypted message to Bob, but that decoding requires knowledge of the private key.

Again, the practical advantages of public key cryptography should be weighed against the loss of security that is introduced (compared with the Vernam cipher). A connection exists between the public key and the corresponding private key, and it is therefore possible in theory to recover the one from the other. Nevertheless, it is fortunately very difficult to carry out this operation within the limits of current mathematical knowledge and the power of contemporary computers.

In order to demonstrate these ideas, let us take the example of the Rivest-Shamir-Adleman (RSA) algorithm, which can be used as the basis of a public key cryptosystem [4]. In this system, the private key can be deduced from the public key if one is able to factorise numbers larger than a certain number of digits, which is currently very difficult. In fact, while it is easy to multiply two large prime numbers together, recovering them from the product is much more difficult. Unfortunately, advances in factorisation always raise the bar for cryptographers, who must use keys, and thus numbers to factorise, that are larger and larger. In addition, if a mathematician one day discovers an algorithm enabling the rapid factorisation of large numbers, he will be able to decode all messages encoded with RSA without anyone knowing it, since he has access to all the public keys.

This danger is all the greater since physicists have devised a new method of doing calculations, using a quantum computer. This new generation of computers, still at an essentially theoretical stage, has the property of being able to solve rapidly certain problems that are believed to be difficult with traditional information theoretic techniques. Thus Peter Shor [6] has discovered a quantum algorithm (that is an algorithm that runs on a quantum computer) allowing the factorisation of large numbers in a reasonable time.

It seems, therefore, that many dangers are present for the long term security of current cryptographic techniques. Classical cryptography, while popular and currently offering a level of security that is largely sufficient, gives no long term guarantee of the messages it is used to protect. This is why we want to present here an alternative manner of securing the confidentiality of a message, without relying on technological assumptions, or complexity assumptions (i.e., assumptions about the speed with which a certain mathematical operation can be carried out using the computers of today).

II. Solution: Quantum Cryptography

Are we then condemned to exchange, by hand and in advance, megabits of secret keys in order to guarantee absolute security? From the point of view of the most fundamental laws of physics known today, there is another possibility. Quantum physics, describing the individual dynamics of each elementary particle (photons, electrons,. . .) that makes up our universe can offset this difficulty and allows the construction of communication protocols with no security weaknesses. This is the aim of quantum cryptography.

Quantum cryptography was born around 20 years ago when two researchers, Charles Bennett and Gilles Brassard [1], had the idea of using quantum physics for transmitting confidential messages. The transmission is achieved using individual photons (”quanta” of light) sent from a sender (Alice) to a receiver (Bob) via an optic fibre.

A theorem known as the ”no-cloning theorem” prevents a third party (Eve) from being able to decode the information transmitted. Indeed it can be shown that if one does not have in advance a precise characterisation of the quantum state describing the light, and in particular of the state of the photon, then it is impossible to reproduce the state, that is to make a clone. In fact, the simple act of observing a photon, in order to determine its state, disturbs it in such a way that afterwards, one cannot return it to its initial state, or produce a clone. The no-cloning theorem is bad news for anyone wanting to determine completely the quantum state of a photon. On the other hand, it can be seen as positive from the point of view of cryptography. Eve, who wants to read the secret information without being detected, needs to copy the quantum state of the photon. Since this is impossible,

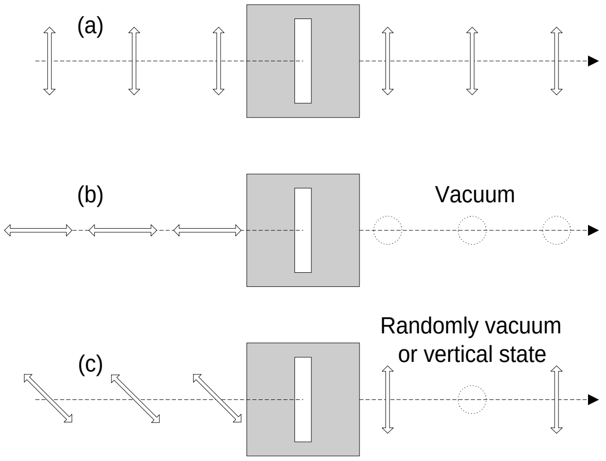

Fig. 1. A single photon impinging upon a filter that only allows vertically polarised light to pass. (a) Vertically polarised photons pass through the filter without being absorbed. (b) Horizontally polarised photons are all absorbed. (c) Diagonally polarised photons are absorbed or transmitted at random. An observer placed after the filter cannot, therefore, determine in a deterministic manner the state of the photon before the filter, in contrast with the vertical-horizontal case.

she must at least determine the quantum state of the photon. But by attempting to do this, she introduces disturbances, and can therefore be detected by Alice and Bob.

The essential goal, then, is for Alice and Bob to exchange a secret key with the assurance that any attempt at eavesdropping by a third party will be detected. If this secret key is correctly transmitted, then Alice and Bob can use it with the Vernam cipher method described above, thus obtaining a cryptosystem that is unconditionally secure even at a distance.

Beginning with the idea of no-cloning, researchers have described a communication protocol that uses the polarisation of photons to encode the bits that will be the secret key. Photons possess two states of polarisation that can be distinguished using a polarising filter (such as a calcite crystal, for example). Like this, vertically polarised light will pass through a filter oriented in the same sense, while horizontally polarised light will not pass, but will be abosorbed by the filter. If now the light is diagonally polarised at 45°, only half of the light intensity will pass. What happens if we only allow a single photon at a time, diagonally polarised, to impinge upon the filter? Clearly the photon cannot be divided into two, since it is the indivisible building block of light. Experiment shows that, as predicted by quantum theory, half of the time the photon will pass through the filter, and half of the time it will be absorbed.

III. An infallible protocol

If Alice limits herself to encoding secret bits in the two polarisation states, vertical and horizontal, then Bob is able to read these bits by distinguishing the polarisation of each photon using a filter. But then Eve is able to intercept the communication without being detected. It suffices for her to read the bits in the same manner as Bob, and then to encode once more the bits in the same manner as Alice, in the polarisation states of photons which she sends on to Bob. However, suppose that Alice uses a strategy in which she encodes bits half of the time in photons that are polarised either horizontally or vertically, and half of the time in photons polarised diagonally at 45° and 135°. In this case, Eve would need to distinguish between four distinct polarisation states. But a polarising filter can only distinguish between states of polarisation along two orthogonal axes, and according to the principles of quantum mechanics, no device can exist that could distinguish one out of the four polarisation states.

This impossibility is an illustration of the famous no-cloning theorem. If such a polariser existed, we could characterise the polarisation state of the photon in a non-ambiguous manner and create as many clones as necessary in the same state. Like this, Eve could keep a copy for herself and send another to Bob, all without being detected. Given the no-cloning theorem, however, the best she can do is to orient her polariser at random in the vertical or diagonal sense, which will inevitably introduce errors and disturb the communication.

What is true for Eve is also inevitably true for Bob, who must also choose the axis in which to measure the polarisation. In order to exchange secret bits in this scenario, Bob must therefore communicate publicly to Alice the axis of polarisation in which he performed his measurement. Then, Alice compares the axis in which she sent each bit with the axis chosen by Bob. If they correspond, Alice lets Bob know publicly, and a secret bit has thus been established; if not the bit must simply be rejected, as there is no correspondence.

Any intervention by Eve will always end up introducing errors in the bits shared by Alice and Bob. Suppose, for example, that Eve measures a photon in the diagonal basis, while Alice had sent the photon with vertical polarisation. Eve sends a photon on to Bob with the polarisation that she measured. If Bob measures horizontal polarisation, then although Alice's and Bob's measurement axes correspond, they will obtain different values for the secret bit. To detect the presence of Eve, it suffices therefore to sacrifice a small number of the large number of bits exchanged. This small fraction of the total number of bits is exchanged publicly between Alice and Bob in order to verify the rate of error of the communication. If this rate, which will also inevitably include errors due to technical imperfections, is abnormally high then this indicates that the communication has been intercepted.

IV. How good is security based on quantum mechanics?

In this protocol, the security is based, amongst other things, on the non-existence of a polarising filter that allows four polarisation states to be distinguished. How can we believe this? Should we trust physicists? Quantum theory allows us to understand, in the most precise manner to date, all known physical phenomena. It describes equally well microscopic phenomena, from elementary particles to atoms, and macroscopic phenomena, which follow from the collective dynamics of these same particles and atoms. And if this theory's century of existence, during which it has never been at fault, is not sufficient to convince the reader, can we not imagine that a ghostly, perhaps invisible, man can look inside the computers of others? Quantum theory does not predict these eventualities, nor can other malevolant demons exist. In other words to believe in the reality of the world that surrounds us is also to believe in the predictions of quantum physics.

V. Current technological developments

Based on the same fundamental principle, numerous laboratories have been able to realise experimentally quantum cryptographic protocols. An optic cable from an ordinary telephone network has been used to transport confidential quantum information over 20 km, under Lake L´eman. Without going into details, the system uses optical interferometry rather than the polarisation of light for transmitting information. However, the apparatus, while perfectly operational, still presents some problems. The first problem is that, due to signal losses in the optic fibre, the transmission can only take place over a relatively short distance, limiting the possible applications to communications within, say, a large town. This problem is the object of a theoretical investigation, and while some progress has been made by researchers, it has not been entirely resolved. The second problem is that experimental production of single photon pulses, as well as their detection, is still imperfect. Perfect control over the dynamics of a photon, from its creation until its detection, would allow a higher rate of transmission of secret bits. Obviously, research and development in these areas are proceeding constantly and the results will be commercially viable in a relatively short time.

Many other improvements to quantum cryptography are currently being studied, both at the Universit´e Libre de Bruxelles, in the Service Th´eorie de l'Information et des Communications, and elsewhere. Several ongoing research projects, in collaboration with the Service Optique et Acoustique and the Service Physique Th´eorique, aim to improve the rate at which secret bits are exchanged, or the range of cryptographic apparatus by using alphabets larger than the binary one. Other theoretical projects, involving collaboration with other European universities, concentrate on the possibility of using beams of light that are more intense (i.e., have more photons), but which keep the quantum characteristics allowing quantum cryptography, in order to bypass the problems associated with single photon techniques. These possibilities involve so-called ”coherent” and ”squeezed” states of light.

VI. Quantum cryptography: an interdisciplinary subject

As one can see, quantum cryptography gathers together a multitude of disciplines. One finds very abstract questions of mathematics and of fundamental physics that bear on quantum mechanics, questions of how to improve the performance of the necessary optical instruments (lasers, detectors, optical fibres), questions of how to adapt the results to industrial ends, not to mention the ethical questions posed by the issue of confidentiality in today's world. In short, it is a contemporary field that covers a very large range of disciplines, from fundamental physics to industrial applications. The results of this research should improve the security of our confidential transmissions, all the more important in the light of online commerce and financial transactions.

VII. To know more:

To know more, the reader may like to consult the popular articles [1] and [2] or the more technical review article [3].

References

[1] C. H. Bennett, G. Brassard and A. K. Ekert, *Quantum Cryptography*, Sc. Am. **267**, p. 50 (1992)

[2] N. J. Cerf and N. Gisin, *Les promesses de l'information quantique*, La Recherche **327**, p. 46 (2000)

[3] N. Gisin, G. Ribordy, W. Tittel and H. Zbinden, *Quantum Cryptography*, Rev. Mod. Phys. **74**, p. 145 (2002)

[4] A. J. Menezes, P. C. van Oorschot and S. A. Vanstone, *Handbook of Applied Cryptography*, CRC Press LLC (1997)

[5] J. Daemen and V. Rijmen, *The block cipher Rijndael*, `http://www.nist.gov/aes`

[6] P. W. Shor, *Algorithms for quantum computation: discrete logarithms and factoring*, in Proceedings of the 35th Symposium on Foundations of Computer Science (1994), p. 124