Quantum Cryptography: Privacy Through Uncertainty

(Released October 2002)

by Salvatore Vittorio

Review Key Citations Web Sites Glossary Conferences Editor

Review Article

1. Cryptography - an Overview

I can't speak without an interception.
This is private; please get off my line.
Please tell me when I can have my privacy. - Ray and Dave Davies

The purpose of cryptography is to transmit information in such a way that access to it is restricted entirely to the intended recipient, even if the transmission itself is received by others. This science is of increasing importance with the advent of broadcast and network communication, such as electronic transactions, the Internet, e-mail, and cell phones, where sensitive monetary, business, political, and personal communications are transmitted over public channels.

Cryptography operates by a sender scrambling or encrypting the original message orplaintext in a systematic way that obscures its meaning. The encrypted message orcryptotext is transmitted, and the receiver recovers the message by unscrambling ordecrypting the transmission.

Originally, the security of a cryptogram depended on the secrecy of the entire encrypting and decrypting procedures. Today, however, we use ciphers in which thealgorithm for encrypting and decrypting could be revealed to anybody without compromising the security of a particular message. In such ciphers a set of specific parameters, called a key, is used together with the plaintext as an input to the encrypting algorithm, and together with the cryptotext as an input to the decrypting algorithm. The encrypting and decrypting algorithms are publicly announced; the security of the cryptogram depends entirely on the secrecy of the key. To prevent this being discovered by accident or systematic search, the key is chosen as a very large number.

Once the key is established, subsequent secure communication can take place by sending cryptotext, even over a public channel that is vulnerable to total passive eavesdropping, such as public announcements in mass media. However, to establish the key, two users, who may not be in contact or share any secret information initially, will have to discuss it, using some other reliable and secure channel. But since interception is a set of measurements performed by an eavesdropper on a channel, however difficult this might be from a technological point of view, any classical key distribution can in principle be passively monitored, without the legitimate users realizing that any eavesdropping has taken place.

Cryptographers have tried hard to solve this key distribution problem. The 1970s brought a clever mathematical discovery in the form of public key cryptography (PKC) [1, 2]. The idea of PKC is for each user to randomly choose a pair of mutually inverse transformations -- a scrambling transformation and an unscrambling transformation -- and to publish the directions for performing the former but not the latter. The transformation is designed so that the unscrambling operation cannot be deduced easily from the scrambling operation, enabling only the user to read scrambled messages. In these systems users do not need to agree on a secret key before they send a message. They work similarly to a drop mailbox with two locks. The owner of the mailbox provides everybody with a key for dropping mail into his box, but only he has the key to open it and read the messages inside. PKC was introduced in 1976 [1].

PKC systems exploit the fact that certain mathematical operations are easier to do in one direction than the other. The systems avoid the key distribution problem, but unfortunately their security depends on unproven mathematical assumptions about the intrinsic difficulty of certain operations. The most popular public key cryptosystem, RSA (Rivest-Shamin-Adleman), gets its security from the difficulty of factoring large numbers [2]. This means that if ever mathematicians or computer scientists come up with fast and clever procedures for factoring large numbers, then the whole privacy and discretion of widespread cryptosystems could vanish overnight. Indeed, recent work inquantum computation suggests that in principle quantum computers might factorize huge integers in practical times, which could jeopardize the secrecy of many modern cryptography techniques [3].

But quantum technology promises to revolutionize secure communication at an even more fundamental level. While classical cryptography relies on the limitations of various mathematical techniques or computing technology to restrict eavesdroppers from learning the contents of encrypted messages, in quantum cryptography the information is protected by the laws of physics. This Hot Topic will discuss some of the basics of how this can be achieved.

2. Classical Cryptography

Gentlemen do not read each other's mail - Henry Stimson, U.S. Secretary of State

Cryptography is the art of devising codes and ciphers, and cryptoanalysis is the art of breaking them. Cryptology is the combination of the two. In the literature of cryptology, information to be encrypted is known as plaintext, and the parameters of the encryption algorithm that transforms the plaintext are collectively called a key. The keys used to encrypt most messages, such as those used to exchange credit-card information over the Internet, are themselves encrypted before being sent [4]. The schemes used to disguise keys are thought to be secure, because discovering them would take too long for even the fastest computers.

Existing cryptographic techniques are usually identified as "traditional" or "modern." Traditional techniques date back for centuries, and use operations of coding (use of alternative words or phrases), transposition (reordering of plaintext), and substitution (alteration of plaintext characters). Traditional techniques were designed to be simple, for hand encoding and decoding. By contrast, modern techniques use computers, and rely on extremely long keys, convoluted algorithms, and intractable problems to achieve assurances of security.

There are two branches of modern cryptographic techniques: public key encryption and secret key encryption. In PKC, as mentioned above, messages are exchanged using an encryption method so convoluted that even full disclosure of the scrambling operation provides no useful information for how it can be undone. Each participant has a "public key" and a "private key"; the former is used by others to encrypt messages, and the latter is used by the participant to decrypt them.

The widely used RSA algorithm is one example of PKC. Anyone wanting to receive a message publishes a key, which contains two numbers. A sender converts a message into a series of digits, and performs a simple mathematical calculation on the series using the publicly available numbers. Messages are deciphered by the recipient by performing another operation, known only to him [5]. In principle, an eavesdropper could deduce the decryption method by factoring one of the published numbers, but this is chosen to typically exceed 100 digits and to be the product of only two largeprime numbers, so that there is no known way to accomplish this factorization in a practical time.

In secret key encryption, a *k*-bit "secret key" is shared by two users, who use it to transform plaintext inputs to cryptotext for transmission and back to plaintext upon receipt. To make unauthorized decipherment more difficult, the transformation algorithm can be carefully designed to make each bit of output depend on every bit of the input. With such an arrangement, a key of 128 bits used for encoding results in a choice of about 10^{38} numbers. The encrypted message should be secure; assuming that brute force and massive parallelism are employed, a billion computers doing a billion operations per second would require a trillion years to decrypt it. In practice, analysis of the encryption algorithm might make it more vulnerable, but increases in the size of the key can be used to offset this.

The main practical problem with secret key encryption is exchanging a secret key. In principle any two users who wished to communicate could first meet to agree on a key in advance, but in practice this could be inconvenient. Other methods for establishing a key, such as the use of secure courier or private knowledge, could be impractical for routine communication between many users. But any discussion of how the key is to be chosen that takes place on a public communication channel could in principle be intercepted and used by an eavesdropper.

One proposed method for solving this key distribution problem is the appointment of a central key distribution server. Every potential communicating party registers with the server and establishes a secret key. The server then relays secure communications between users, but the server itself is vulnerable to attack. Another method is a protocol for agreeing on a secret key based on publicly exchanged large prime numbers, as in the Diffie Hellman key exchange. Its security is based on the assumed difficulty of finding the power of a base that will generate a specified remainder when divided by a very large prime number, but this suffers from the uncertainty that such problems will remain intractable. Quantum encryption, which will be discussed later, provides a way of agreeing on a secret key without making this assumption.

Communication at the quantum level changes many of the conventions of both classical secret key and public key communication described above. For example, it is not necessarily possible for messages to be perfectly copied by anyone with access to them, nor for messages to be relayed without changing them in some respect, nor for an eavesdropper to passively monitor communications without being detected [6]. To understand these ideas, we must first discuss some underlying physics.

3. Quantum Cryptography Fundamentals

Nobody understands quantum theory. - Richard Feynman, Nobel prize-winning physicist

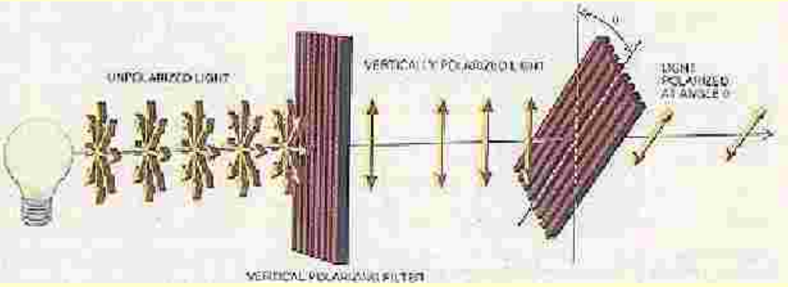
Electromagnetic waves such as light waves can exhibit the phenomenon of polarization, in which the direction of the electric field vibrations is constant or varies in some definite way. A polarization filter is a material that allows only light of a specified polarization direction to pass. If the light is randomly polarized, only half of it will pass a perfect filter.

According to quantum theory, light waves are propagated as discrete particles known as photons. A photon is a massless particle, the quantum of the electromagnetic field, carrying energy, momentum, and angular momentum. The polarization of the light is carried by the direction of the angular momentum or spin of the photons. A photon either will or will not pass through a polarization filter, but if it emerges it will be aligned with the filter regardless of its inital state; there are no partial photons. Information about the photon's polarization can be determined by using a photon detector to determine whether it passed through a filter.

"Entangled pairs" are pairs of photons generated by certain particle reactions. Each pair contains two photons of different but related polarization. Entanglement affects the randomness of measurements. If we measure a beam of photons E1 with a polarization filter, one-half of the incident photons will pass the filter, regardless of its orientation.

Whether a particular photon will pass the filter is random. However, if we measure a beam of photons E2 consisting of entangled companions of the E1 beam with a filter oriented at 90 degrees (deg) to the first filter, then if an E1 photon passes its filter, its E2 companion will also pass its filter. Similarly, if an E1 photon does not pass its filter then its E2 companion will not.

The foundation of quantum cryptography lies in the Heisenberg uncertainty principle, which states that certain pairs of physical properties are related in such a way that measuring one property prevents the observer from simultaneously knowing the value of the other. In particular, when measuring the polarization of a photon, the choice of what direction to measure affects all subsequent measurements. For instance, if one measures the polarization of a photon by noting that it passes through a vertically oriented filter, the photon emerges as vertically polarized regardless of its initial direction of polarization. If one places a second filter oriented at some angle q to the vertical, there is a certain probability that the photon will pass through the second filter as well, and this probability depends on the angle q. As q increases, the probability of the photon passing through the second filter decreases until it reaches 0 at q = 90 deg (i.e., the second filter is horizontal). When q = 45 deg, the chance of the photon passing through the second filter is precisely 1/2. This is the same result as a stream of randomly polarized photons impinging on the second filter, so the first filter is said to randomize the measurements of the second.


UNPOLARIZED LIGHT
VERTICALLY POLARIZED LIGHT
θ
LIGHT POLARIZED AT ANGLE θ
VERTICAL POLARIZING FILTER

Polarization by a filter: Unpolarized light enters a vertically aligned filter, which absorbs some of the light and polarizes the remainder in the vertical direction. A second filter tilted at some angle q absorbs some of the polarized light and transmits the rest, giving it a new polarization.
(From "Quantum Cryptography" by Charles H. Bennett, Gilles Brassard, and Artur K. Ekert, http://www.cyberbeach.net/~jdwyer/quantum_crypto/quantum2.htm.)

A pair of orthogonal (perpendicular) polarization states used to describe the polarization of photons, such as horizontal/vertical, is referred to as a basis. A pair of bases are said to be conjugate bases if the measurement of the polarization in the first basis completely randomizes the measurement in the second basis [7], as in the above example with q = 45 deg. It is a fundamental consequence of the Heisenberg uncerty principle that such conjugate pairs of states must exist for a quantum system.

If a sender, typically designated Alice in the literature, uses a filter in the 0-deg/90-deg basis to give the photon an initial polarization (either horizontal or vertical, but she doesn't reveal which), a receiver Bob can determine this by using a filter aligned to the same basis. However if Bob uses a filter in the 45-deg/135-deg basis to measure the photon, he cannot determine any information about the initial polarization of the photon [8].

These characteristics provide the principles behind quantum cryptography. If an eavesdropper Eve uses a filter aligned with Alice's filter, she can recover the original polarization of the photon. But if she uses a misaligned filter she will not only receive no information, but will have influenced the original photon so that she will be unable to reliably retransmit one with the original polarization. Bob will either receive no message or a garbled one, and in either case will be able to deduce Eve's presence.

4. Quantum Cryptography Application

And I would send a message
To find out if she's talked,
But the post office has been stolen,
And the mailbox is locked. - Bob Dylan

Sending a message using photons is straightforward in principle, since one of their quantum properties, namely polarization, can be used to represent a 0 or a 1. Each photon therefore carries one bit of quantum information, which physicists call a qubit. To receive such a qubit, the recipient must determine the photon's polarization, for example by passing it through a filter, a measurement that inevitably alters the photon's properties. This is bad news for eavesdroppers, since the sender and receiver can easily spot the alterations these measurements cause. Cryptographers cannot exploit this idea to send private messages, but they can determine whether its security was compromised in retrospect.

The genius of quantum cryptography is that it solves the problem of key distribution. A user can suggest a key by sending a series of photons with random polarizations. This sequence can then be used to generate a sequence of numbers. The process is known as quantum key distribution. If the key is intercepted by an eavesdropper, this can be detected and it is of no consequence, since it is only a set of random bits and can be discarded. The sender can then transmit another key. Once a key has been securely received, it can be used to encrypt a message that can be transmitted by conventional means: telephone, e-mail, or regular postal mail [9].

The first published paper to describe a cryptographic protocol using these ideas to solve the key distribution problem was written in 1984 by Charles Bennett and Gilles Brassard [10]. In it, Bennett and Brassard described an unconditionally secure quantum key distribution system. The system is called the BB84 system (after Bennett and Brassard, 1984), and its operation is as follows [11].

Alice and Bob are equipped with two polarizers each, one aligned with the rectilinear 0-deg/90-deg (or +) basis that will emit - or | polarized photons and one aligned with the diagonal 45-deg/135-deg (or X) basis that will emit \ or / polarized photons. Alice and Bob can communicate via a quantum channel over which Alice can send photons, and a public channel over which they can discuss results. An eavesdropper Eve is assumed to have unlimited computing power and access to both these channels, though she cannot alter messages on the public channel (see below for discussion of this).

Alice begins to send photons to Bob, each one polarized at random in one of the four directions: 0, 45, 90, or 135 deg. As Bob receives each photon, he measures it with one of his polarizers chosen at random. Since he does not know which direction Alice chose for her polarizer, his choice may not match hers. If it does match the basis, Bob will measure the same polarization as Alice sent, but if it doesn't match, Bob's measurement will be completely random. For instance, if Alice sends a photon | and Bob measures with his + polarizer oriented either - or |, he will correctly deduce Alice sent a | photon, but if he measures with his X polarizer, he will deduce (with equal probability) either \ or /, neither of which is what Alice actually sent. Furthermore, his measurement will have destroyed the original polarization.

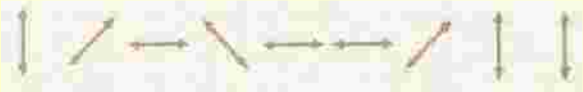
To eliminate the false measurements from the sequence, Alice and Bob begin a public discussion after the entire sequence of photons has been sent. Bob tells Alice which basis he used to measure each photon, and Alice tells him whether or not it was the correct one. Neither Alice nor

Bob announces the actual measurements, only the bases in which they were made. They discard all data for which their polarizers didn't match, leaving (in theory) two perfectly matching strings. They can then convert these into bit strings by agreeing on which photon directions should be 0 and which should be 1.

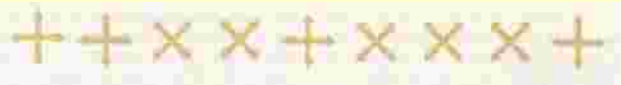
This provides a way for Alice and Bob to arrive at a shared key without publicly announcing any of the bits. If an eavesdropper Eve tries to gain information about the key by intercepting the photons as they are transmitted from Alice to Bob, measuring their polarization, and then resending them so Bob does receive a message, then since Eve, like Bob, has no idea which basis Alice uses to transmit each photon, she too must choose bases at random for her measurements. If she chooses the correct basis, and then sends Bob a photon matching the one she measures, all is well. However, if she chooses the wrong basis, she will then see a photon in one of the two directions she is measuring, and send it to Bob. If Bob's basis matches Alice's (and thus is different from Eve's), he is equally likely to measure either direction for the photon. However, if Eve had not interfered, he would have been guaranteed the same measurement as Alice. In fact, in this intercept/resend scenario, Eve will corrupt 25 percent of the bits [7]. So if Alice and Bob publicly compare some of the bits in their key that should have been correctly measured and find no discrepancies, they can conclude that Eve has learned nothing about the remaining bits, which can be used as the secret key. Alternatively, Alice and Bob can agree publicly on a random subset of their bits, and compare the parities. The parities will differ in 50 percent of the cases if the bits have been intercepted. By doing 20 parity checks, Alice and Bob can reduce the probability of an eavesdropper remaining undetected to less than one in a million [8]. It is of course crucial that they do not discuss the orientation of the polarization filters until after the message has been sent, or Eve could use this to intercept and resend the photons correctly.

An Illustration of Quantum Key Distribution:

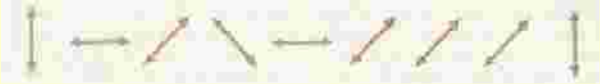
A quantum cryptography system allows two people, say Alice and Bob, to exchange a secret key. Alice uses a transmitter to send photons in one of four polarizations: 0, 45, 90 or 135 degrees. Bob uses a receiver to measure each polarization in either the rectilinear basis (0 and 90) or the diagonal basis (45 and 135); according to the laws of quantum mechanics he cannot simultaneously make both measurements. The key distribution requires several steps. Alice sends photons with one of the four polarizations, which she chooses at random.



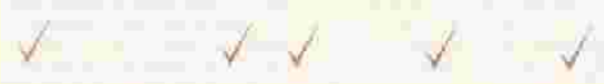
For each photon, Bob chooses at random the type of measurement: either the rectilinear type (+) or the diagonal type (X).



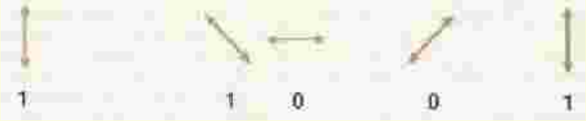
Bob records the result of his measurements but keeps it a secret.



After the transmission, Bob tells Alice the measurement types he used (but not his results) and Alice tells him which were correct for the photons she sent. This exchange may be overheard.



Alice and Bob keep all cases in which Bob should have measured the correct polarization. These cases are then translated into bits (1s and 0s) to define the key.



As a check, Alice and Bob choose some bits at random to reveal. If they agree, they can use the remaining bits with assurance that they have not been intercepted. But if they find a substantial number of discrepancies, it indicates unavoidable tampering due to eavesdropping, and they should start over to transmit another key.
(From "Quantum Cryptography" by Charles H. Bennett, Gilles Brassard, and Artur K. Ekert, http://www.cyberbeach.net/~jdwyer/quantum_crypto/quantum1.htm.)

The BB84 system is now one of several types of quantum cryptosystems for key distribution. Another one involves cryptosystems with encoding built upon quantum entanglement and Bell's Theorem, proposed by Artur K. Ekert (1990) [12, 13]. The basic idea of those cryptosystems is as follows. A sequence of correlated particle pairs is generated, with one member of each pair being detected by each party. An eavesdropper on this communication would have to detect a particle to read the signal, and retransmit it in order for his presence to remain unknown. However, the act of detection of one particle of a pair destroys its quantum correlation with the other, and the two parties can easily verify whether this has been done, without revealing the results of their own measurements, by communication over an open channel.

5 . Quantum Privacy Attacks

A sekret ceases tew be a sekret if it iz once confided ... - "Affurisms from Josh Billings: His Sayings," Henry Wheeler Shaw

Quantum cryptography obtains its fundamental security from the fact that each qubit of information is carried by a single photon, and that each photon will be altered as soon as it is read once. This foils attempts to intercept message bits without being detected.

Quantum cryptographic techniques provide no protection against the classic bucket brigade attack (also known as the "man-in-the-middle attack"). In this scheme, an eavesdropper Eve is assumed to have the capacity to monitor the communications channel and insert and remove messages without inaccuracy or delay. When Alice attempts to establish a secret key with Bob, Eve intercepts and responds to messages in both directions, fooling both Alice and Bob into believing she is the other. Once the keys are established, Eve receives, copies, and resends messages so as to allow Alice and Bob to communicate. Assuming that processing time and accuracy are not difficulties, Eve will be able to retrieve the entire secret key, and thus the entire plaintext of every message sent between Alice and Bob, without any detectable signs of eavesdropping.

Even if Eve does not practice interference of this kind, there are other methods she can still attempt to use. Because of the difficulty of using single photons for transmissions, most systems use small bursts of coherent light instead. In theory, Eve might be able to split single photons out of the burst, reducing its intensity but not affecting its content. By observing these photons (if necessary, holding them somehow until the correct basis for observation is announced) she might gain information about the information transmitted from Alice to Bob.

A confounding factor in detecting attacks is the presence of noise on the quantum communication channel. Eavesdropping and noise are indistinguishable to the communicating parties, and so either can cause a secure quantum exchange to fail. This leads to two potential problems: a malicious eavesdropper could prevent communication from occurring, and attempts to operate in the expectation of noise might make eavesdropping attempts more feasible.

6 . State of Quantum Cryptography Technologies

What hath God wrought. - first message sent by telegraph, by Samuel F. B. Morse

Experimental implementations of quantum cryptography have existed since 1990, and today quantum cryptography is performed over distances of 30-40 kilometers using optical fibers.

Essentially, two technologies make quantum key distribution possible: the equipment for creating single photons and that for detecting them. The ideal source is a so-called photon gun that fires a single photon on demand. As yet, nobody has succeeded in building a practical photon gun, but several research efforts are under way. Jungsang Kim at Stanford University, California, and colleagues, for example, are working on a light-emitting p-n junction that produces well-spaced single photons on demand. Others are working with a diamond-like material in which one carbon atom in the structure has been replaced with nitrogen. That substitution creates a vacancy similar to a hole in a p-type semiconductor, which emits single photons when excited by a laser. Many groups are also working on ways of making single ions emit single photons.

None of these technologies, however, is mature enough to be used in current quantum cryptography experiments. As a result, physicists have to rely on other techniques that are by no means perfect from a security viewpoint. Most common is the practice of reducing the intensity of a pulsed laser beam to such a level that, on average, each pulse contains only a single photon. The problem here is the small but significant probability that the pulse contains more than one photon. This extra photon is advantageous for Eve, who can exploit the information it contains without Alice and Bob being any the wiser.

Single-photon detection is tricky too. The most common method exploits avalanche photodiodes. These devices operate beyond the diode's breakdown voltage, in what is called Geiger mode. At that point, the energy from a single absorbed photon is enough to cause an electron avalanche, an easily detectable flood of current. But these devices are far from perfect. To detect another photon, the current through the diode must be quenched and the device reset, a time-consuming process.

Furthermore, silicon's best detection wavelength is 800 nanometers (nm, where 1 nm = one one-billionth of a meter), and it is not sensitive to wavelengths above 1100 nm, well short of the 1300- and 1550-nm standards for telecommunication. At telecommunications wavelengths, germanium (Ge) or indium-gallium-arsenide (InGaAs) detectors must be used, even though they are far less efficient and must be cooled well below room temperature. While commercial single-photon detectors at telecommunications wavelengths are beginning to appear on the market, they still lack the efficiencies useful for quantum cryptography [9].

The distance that the key can be transmitted is also an important technical limitation. Most experts agree that a 67-km transmission achieved by a group of physicists at the University of Geneva on October 2001 is close to the maximum that can be achieved with current technology. Beyond about 80 km of cable, too few photons make it from Alice to Bob. The range could be extended by devices that strengthen the signal as it passes by, like those used to send telephone conversations over long distances. However, unlike telephone repeaters, quantum versions would have to bolster the signal without measuring the photons. Scientists have shown that creating a repeater that doesn't measure is feasible in principle, but the technology to building one is a long way off [5].

Satellites could provide an alternative means of achieving long-distance transmission. A quantum cryptography team led by physicist Richard Hughes at the Los Alamos National Laboratory in New Mexico is developing a key-distribution system that sends single photons through open air. So that the photons can be distinguished from all the others bombarding the detector, the team uses various techniques to filter the incoming light. In a recent paper [14], Hughes and his colleagues have described how they sent keys over a distance of 10 km with rates similar to those achieved using optical fibers. Ten kilometers is a long way short of the hundreds of kilometers between the Earth's surface and satellites, but because air turbulence, the factor that most disrupts the photons, occurs predominately in the lower 2 km of the atmosphere, Hughes believes his system should be able to send signals to satellites. The team is now trying to make the receiver light and sturdy enough to fit in a satellite and survive a rocket launch. Combined with optical fibers, satellites could eventually form part of a long-distance transmission system.

In the shorter term, the technology might help to protect the security of satellite television broadcasts. In one such breach, a hacker known as Captain Midnight interrupted a 1986 broadcast by HBO (the Home Box Office company) and sent over half of the company's customers a five-minute broadcast of a message complaining about the firm's new subscription charges.

7 . Conclusion

Quantum cryptography promises to revolutionize secure communication by providing security based on the fundamental laws of physics, instead of the current state of mathematical algorithms or computing technology. The devices for implementing such methods exist and the performance of demonstration systems is being continuously improved. Within the next few years, if not months, such systems could start encrypting some of the most valuable secrets of government and industry [5].