BB84 Analysis of Operation and Practical Considerations and Implementations of Quantum Key Distribution Systems

Patryk Winiarczyk, Wojciech Zabierowski

***Abstract* — Nowadays cryptography is applied in more and more applications. Most often asymmetric or hybrid systems are used, which are based on mathematical concepts. However, a promising family of quantum solutions tries to take over control. This article describes a technique of quantum key distribution called BB84. It gives an insight into quantum physics governing the proper operation of any system in quantum cryptography and then presents the detailed analysis of BB48 system. Its operation and security it provides are discussed. Next aspect that is covered is dedicated to practical considerations of quantum cryptography. All basic problems encountered while implementing BB84 or any other quantum system are explained.**

***Index Terms*—QKD, quantum cryptography, quantum physics, photon, BB84**

I. Introduction

Any quantum system in cryptography is based on Heisenberg's uncertainty principle, which causes its disturbance when it is measured and hence any form of eavesdropping can be quickly detected. This particular feature makes quantum cryptography superior to conventional cryptography. In literature, it can be often encountered that the name quantum key distribution, abbreviated as QKD is used instead of quantum cryptography. QKD is a more accurate name as such a quantum system is used for key distribution and not for data encryption itself. The first quantum key distribution technique was presented by Bennett and Brassard in 1984 and was named BB84 protocol. Its first experimental demonstration was performed in 1991. The protocol takes use of photon polarization states. In such a system quantum communication channel can be free space or an optical fibre and it can be open to public so that any form of an external interference is accepted. The data sent in the channel is encoded by means of non-orthogonal states. These states cannot be measured without disturbing the original state and such quantum characteristic ensures the security of the whole system. This characteristic is often referred to as quantum indeterminacy.

Manuscript received November 8, 2011.

Patryk Winiarczyk, Wojciech Zabierowski, Ph.D. TUL, Department of Microelectronics and Computer Science, ul. Wólczańska 221/223 90-924 Łódź, POLAND, e-mail: wojtekz@dmcs.pl.

II. BB84 System Characteristics

Next point is dedicated to the description of the system. To simplify the whole procedure it is assumed that a photon might be polarized in one of four possible directions, i.e. 0, 45, 90 or 135 as depicted below (Fig. 1)

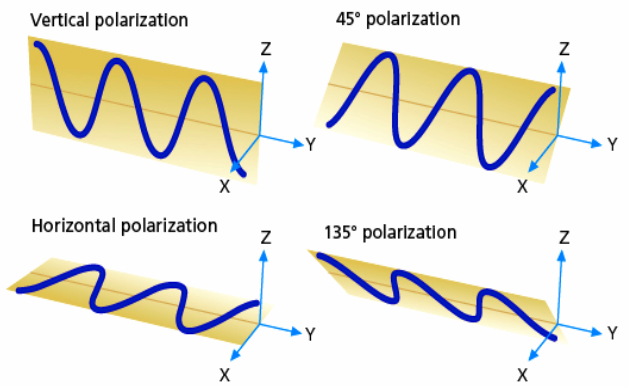

Fig. 1 Possible polarizations of light wave. [9]

Furthermore some convention of bit representation for photon orientations is essential. From the table below it can be observed that if a photon is vertical or 45-tilted then its corresponding binary representation will be 0. Simultaneously all horizontal or 135-tilted photons will be represented by 1.

TABLE 1
Symbolic and bit representations of differently polarized photon in BB84 protocol [1]

Polarization	0^0	45^0	90^0	135^0
Symbolic representation	I	/	-	\
Bit representation	0	0	1	1

The whole system must be equipped with two polarization filters. Two pairs of states are used in BB84 protocol and they are always conjugate to each other. States within a single pair are orthogonal to each other and known

as a basis. The commonly used orientations of bases are: rectilinear basis (vertical - 0 and horizontal - 90) and diagonal basis (tilt of 45 and 135).. For clarity, the rectilinear filter is denoted by + and diagonal one by X. A rectilinear filter detects correctly rectilinearly-oriented photons, whereas a diagonal filter diagonally-oriented photons. In other words, whatever the orientation of the photon hitting the filter it will always be detected but in statistically half cases the result will be wrong.

TABLE 2
PHOTON OUTPUTS FOR DIFFERENT INPUT AND FILTER SCENARIOS IN BB84 PROTOCOL [1]

Input	Filter	Output
\ or /	+	I or -
I or -	X	\ or /

Next step is the thorough description of the algorithm of key exchange itself. Sender, which is proverbial Alice creates a random sequence of bits switching between rectilinear and diagonal bases and sends it to recipient Bob taking notes of state, basis and time of each photon sent. As Bob does not know to which basis the photons coming are polarized he must switch randomly between two types of detectors. For each single photon he takes notes which detector he used and the binary value he obtained for the given detector. After the transmission process is completed Bob needs to inform Alice which detector was used for each single photon. Alice must simply provide him the feedback whether the detector used for a given photon was appropriate to correctly detect the corresponding bit. All bits for which the randomly chosen detector was inappropriate are discarded whereas the remaining bits constitute the key.

To visualize the whole concept we assume that Alice sends only 15 random bits to Bob. Bob has on average 50% chance of choosing the proper detector. For example, if the rectilinear detector is used by Bob and the photon sent is also rectilinearly-oriented the bit will be recorded properly, but if photon was polarized diagonally, its polarization will change and the bit measurement will be incorrect. Bob does not know which particular bits obtained from a choice of wrong detector match Alice's bits and he cannot ask about it as any eavesdropper could very easily intercept the key. Therefore all bits resulted from different choice of detectors must be discarded, despite the fact that approximately half of them would match Alice's bits.

III. BB84 OPERATION AND ITS ANALYSIS IN PRESENCE OF EAVESDROPPER

As it is already known the act of measuring the polarization of a photon may alter the polarization itself. Eavesdropper, proverbial Eve, takes notes of polarization of photons but simultaneously changes polarization of some of them. Therefore the string of photons that Bob receives may be considerably different from the one sent by Alice. Eve is in the exactly same position as Bob, which means that she is forced to choose detectors randomly. That in turn must result in statistically 50% wrong choice of detector. Still, even having the improper detector chosen, she has got a 50% chance of sending a photon polarized in the way that will yield Bob the bit representation equal to one sent by Alice. Therefore the final error rate on Bob's side after discarding all bits resulted from choice of different detectors by Alice and Bob will be 25%. In this manner both communicating parties will become certain that the channel has been eavesdropped when they will try to use the established key. To understand the idea thoroughly the table below should be investigated:

TABLE 3
ESTABLISHING THE FINAL KEY BETWEEN ALICE AND BOB IN PRESENCE OF EAVESDROPPER EVE IN BB84 PROTOCOL [1]

Alice's bits	0		1	1	1		0	1			0			
Alice's photons	\	/	\	\	\	\	I	I	\	\	/	I	\	\	/
Good detector	x	x	x	x	x	x	+	+	x	x	x	+	x	x	x
Eve's detector	+	+	x	+	x	x	+	+	x	x	+	x	+	x	x
Eve's photons	I	-	\	I	\	\	I	I	\	\	-	/	-	\	/
Bob's detector	+	x	+	x	x	x	x	+	x	+	+	+	+	+	+
Bob's bits		1		1	1	1		0	1			1			

In this example all wrong detectors chosen by Bob and Eve as well as the final bits that became changed because of the act of eavesdropping are denoted in red. As it can be observed, in this sequence of 15 bits 8 of them for which Bob used a wrong detector have been thrown away at once. From the remaining 7 bits a quantum distribution key should be created. However, it turns out that Alice's key differs from Bob's key due to action of eavesdropper, who changed 2 of 7 bits. Alice sends first bit equal to 0 using a diagonal filter, which according to the convention assumed becomes 45-oriented photon. Now, Eve sets the randomly chosen detector for that particular photon, which in this case is a rectilinear one. As quantum indeterminacy implies no possible measurement can distinguish four different polarization states that are not all orthogonal. The only possible measurement is between any two orthogonal states- a basis. That means that when Eve measures in the rectilinear basis it will give her a rectilinearly oriented photon. If this photon had been horizontally or vertically polarized before going through the polarizer the

measurement would have been absolutely correct. Eve is unfortunate as the photon is 45-tilted and thus the rectilinear measurement yields either horizontally or vertically polarized photon with the same probability. Furthermore, all information about the initial polarization of the photon is lost after Eve's measurement. In the case considered the photon becomes horizontally oriented and as such sent to Bob, which uses the detector oriented in the exactly same manner as Alice- diagonally. The horizontally oriented photon passes this detector and must turn into a diagonal orientation, either 45 or 135. In this case Bob receives bit 1, which means that the photon turned into 135 orientation. Summing up Eve by the act of eavesdropping changed the final bit on Bob's side. For the seventh bit in the Alice's final sequence the situation is similar. Eve uses an incorrect detector and it results in incorrect bit received by Bob. For the second bit of Alice's final key the detector used by Eve is again wrongly oriented but the photon passing the Bob's detector become polarized in the way that results in the correct bit representation being 1. For the bits from third to sixth one of Alice's key Eve luckily uses correctly oriented detectors so the polarization of photons will not be altered and Bob will receive correct bits. The final conclusion follows that sender and recipient unable to communicate will have the invaluable information about the potential eavesdropper on the line. Therefore the whole process of key exchange will have to be initialized once again preferably using a different quantum channel.

Next aspect to discuss is the eavesdropping act from Eve's perspective. The only result eavesdropper might obtain is to delay the key exchange and to force both parties to restart the whole procedure. If Eve's sequence of received bits is investigated it results, similarly as in the case of Bob's key when being eavesdropped, in statistically 25% error (a half of all her detectors are wrongly chosen and half of those will change the polarization of a given photon into the one that will be represented by the opposite bit to the original one). Therefore Eve, even knowing which detectors were discarded by Alice and Bob (she may simply eavesdrop their conversation on an open channel), still remains unable to intercept the whole key without any errors and to simultaneously keep her presence hidden. She might also decide to eavesdrop the subsequent conversation related to the establishing the correct detectors. Then her presence will be hidden but will gain no knowledge about the bits from the quantum key as it will be infeasible to calculate fast enough- for a key of n bits she will need to check 2possibilities, which is out of scope in case of real-life communication with long number of bits expressed in thousands.

IV. Practical Considerations and Problems Concerning Quantum Cryptography

Contrary to asymmetric methods of cryptography quantum cryptography is heavily dependent on hardware used. This seems to be the most crucial factor that limits its practical application.

The proper transmission and detection of photons must be satisfied so a precise method of emitting and detecting single photons is indispensable. Photons as very small particles of energy are difficult to be sent separately. By supplying the photon generator with only slightly too much energy several photons might be emitted at once, which is undesirable. Among the techniques proposed for generating single photon states the following are: faint laser pulses, parametric down conversion, single electrons in mesoscopic p-n junctions, photon emission of electron-hole pairs in a semiconductor quantum dot. Except precise emission equipment a detection one is of no less significance. A few possible solutions enabling photon detection exist and those are: photomultipliers, avalanche photo-diodes, multi-channels plates and superconducting Josepheson junctions. Detectors should have a high efficiency over a large spectral range and a short recovery time. Based on those criteria avalanche photo diodes are most advantageous. They operate beyond breakdown voltage of the diode, in a state called Geiger mode. In this mode the energy from a single absorbed photon is enough to cause an electron avalanche, which manifests itself in detectable flood of current. To detect another photon, the diode needs to be reset, which is a time-consuming process and results in detection rate that remains unsatisfactory. Depending on the wavelengths at which detection takes place different semiconductors (silicon, germanium and indium gallium arsenide) may be used.. Unfortunately, silicon has too large band gap so its sensitivity is not sufficient. Best detection wavelength of silicon is 800 nm, whereas at 1100 nm it becomes insensitive, which is still less than standards for telecommunications applications (1300 and 1550 nm). Therefore germanium or indium-gallium-arsenide detectors must be used at telecommunications wavelengths, even though they are far less efficient and must be cooled considerably below room temperature.

Among other factors influencing wider use of quantum cryptography distance of transmission, and dedicated network of fibre lines can be listed. As a medium of transmission fibre optic cables are used most often. Unfortunately their distance of transmission is limited whereas amplifiers cannot be used to send data on the longer distances as they may change the polarization of photons and facilitate the process of eavesdropping. Next trouble encountered concerning fibre lines is their integration with existing optical networks. The cost of building additional optical infrastructure still remains

relatively too high to use quantum cryptography more widely. Furthermore the maintenance of fibre lines is also expensive and if they are not properly protected then a cutting or blocking some part of the network may lead to denial of service, which is unacceptable.

To avoid a use of fibre network an alternative technology might be proposed that is so far still in the stage of preliminary tests and has not been demonstrated yet in practice. Quantum keys are exchanged in this method by means of free space with the aid of satellites. Such transmission is very fluctuating and has got high impedance in comparison with less noisy optical fibre transmission. The communication takes place between a terrestrial station and a low orbit satellite. The absorption of photons in the atmosphere can be minimized using an adequate wavelength. The atmosphere has a high transmission window at a wavelength of about 770 nm, where photons can be easily detected using efficient photon counting modules. At these wavelengths the atmosphere would not change the polarization of photons, which is a great advantage. The type of weather obviously influences the transmission as well. Phase shifts and polarization dependent losses would also have to be taken care of. A satellite obtains the key from the station on the ground, moves with respect to the earth surface and detecting a receiving station sends the key to it.

V. Practical Implementations of Quantum Systems

BB84 has been experimentally demonstrated to act correctly with bit rate of 1Mbit/s over 20 km and 10 kbit/s over 100 km of fiber optic cable. The most difficult obstacle for transmission of photons in fibre lines over longer distances is the signal strength. Theoretically devices similar to phone repeaters could be used to solve it but their drawback is that they introduce the act of measurement, which is undesirable as potential eavesdropper could take advantage of it. Hopefully, it has been proved by scientists that repeaters that do not perform any detectable measurements are feasible in principle but so far remain a far future prospect. It has been also shown in practice that quantum cryptography system might work over free space for a distance of over one hundred kilometers. Such demonstration was performed twice, first using EC91 protocol and later on with BB84 protocol enhanced with decoy states. In Massachusetts a 10-node quantum cryptography network, called DARPA was implemented in 2004. The first bank transfer with the aid of quantum cryptography was performed in 2004 in Vienna, where 4 years later at a scientific conference a quantum cryptography protected computer network was implemented consisting of 200 km of standard fibre optic cable. Quantum encryption technology was also used in Geneva to transmit ballot results in the national election in 2007.

VI. Summary

To introduce quantum cryptography into wide use a dedicated hardware network must be first precisely built. All the problems related to creating and running such a quantum network trigger off many doubts concerning its profitability. These obstacles also prevent a faster development of quantum protocols and their practical applications. As long as properly implemented asymmetric and hybrid algorithms ensure security, quantum cryptography will remain in the shade. Even though quantum cryptography provides the perfect security guaranteed by the laws of quantum physics, it must first find the effective solutions to all the problems discussed.

References

[1] http://zon8.physd.amu.edu.pl/~miran/lectures/optics/wstep.pdf
[2] http://en.wikipedia.org/wiki/BB84
[3] http://en.wikipedia.org/wiki/Quantum_cryptography
[4] http://arxiv.org/ftp/quant-ph/papers/9905/9905009.pdf
[5] V.K., Stanatuis. “Identifying Vulnerabilities of Quantum Cryptography in Secure Optical Data Transport”, IEEE Security & Privacy, 2007
[6] R. Tanaś, Wykład z podstaw klasycznej kryptografii z elementami kryptografii kwantowej (http://zon8.physd.amu.edu.pl/~tanas/kryptografia.pdf), Zakład Optyki Nieliniwej, Instytut Fizyki UAM.
[7] Elliott, Chip. “Quantum Cryptography”, IEEE Security & Privacy, 2004
[8] http://www.authorstream.com/Presentation/Malden-36580-Introduction-Quantum-Cryptography-List-frequently- asked-questions-Outline-CONVENTIONALCRY-to-as-Entertainment-ppt-powerpoint
[9] http://www.nikon.com/about/feelnikon/light/chap04/sec01.htm

Wojciech Zabierowski (Assistant Professor at Department of Microelectronic and Computer Science Technical University of Lodz) was born in Lodz, Poland, on April 9, 1975. He received the M.Sc. and Ph.D. degrees from the Technical University of Lodz in 1999 and 2008, respectively. He is an author or co-author of more than 70 publications: journals and most of them - papers in international conference proceedings. He was reviewer in six international conferences. He supervised more than 90 Msc theses. He is focused on internet technologies and automatic generation of music. He is working in linguistic analysis of musical structure.