Quantum Cryptography using Quantum Key Distribution and its Applications

N.Sasirekha, M.Hemalatha

Abstract-Secure transmission of message between the sender and receiver is carried out through a tool called as cryptography. Traditional cryptographical methods use either public key which is known to everyone or on the private key. In either case the eavesdroppers are able to detect the key and hence find the message transmitted without the knowledge of the sender and receiver. Quantum cryptography is a special form of cryptography which uses the Quantum mechanics to ensure unconditional security towards the transmitted message. Quantum cryptography uses the distribution of random binary key known as the Quantum Key Distribution (QKD) and hence enables the communicating parties to detect the presence of potential eavesdropper. This paper also analyses few application areas of quantum cryptography and its limitations.

Keywords- Classical Cryptography, Photon polarization, Qubit, Quantum Cryptography, Quantum entanglement, Quantum Key Distribution, Sifting key.

I. INTRODUCTION

Cryptography is the practice and study of encoding and decoding secret messages to ensure secure communications. There are two main branches of cryptography: secret-(symmetric-) key cryptography and public-(asymmetric) key cryptography. A key is a piece of information (a parameter) that controls the operation of a cryptographic algorithm. In encryption, a key specifies the particular transformation of plaintext into cipher text, or vice versa during decryption. Keys are also used in other cryptographic algorithms, such as digital signature schemes and message authentication codes. In practice, due to significant difficulties of distributing keys in secret key cryptography, public-key cryptographic algorithms are widely used in conventional cryptosystems.

Cryptographers make efforts to build more and more sophisticated means to obscure the sensitive information which is to be transmitted. But the hackers, code breakers, eavesdroppers work furiously to crack the systems. If either cryptographers achieve security or the code breakers decipher the security the success will be temporary. This process of securing the message using ciphering and breaking the system using deciphering is an endless process. Once, this scenario is a chase in the race.

Manuscript published on 30 April 2014.
***** Correspondence Author (s)

N. Sasirekha*, Department of Information Technology and Computer Technology, Rathinam College of Arts and Science, Coimbatore, Tamilnadu, India.
M.Hemalatha, Department of Computer Science, Karpagam University, Coimbatore, Tamilnadu, India.

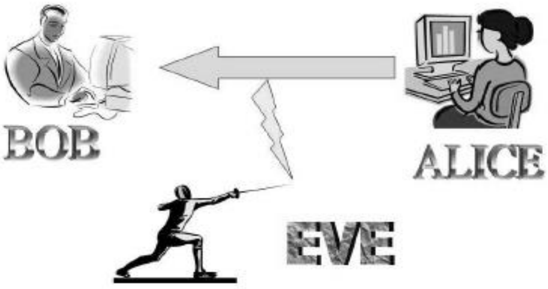


Fig 1: Communication in the presence of an Eavesdropper

Today, a technology known as Quantum key distribution (QKD) uses individual photons for the exchange of cryptographic key between the sender and the receiver. Each photon represents a single bit of data. The value of the bit, a 1 or a 0, is determined by states of the photon such as polarization or spin. With this method, one party can send a cryptographic key encoded with photons to another party. The unique properties of photons as quantum objects are such that any attempt to measure or to decipher the message will change the photons' state. This uncertainty ensures that the message will be destroyed or altered, making it easy for both the sender and receiver to detect that the message has been compromised. Thus, QKD doesn't rely on preventing interception or decryption, but rather on detecting eavesdropping and self-destructing the message as a result.

II. LITERATURE SURVEY

Smart cards, PINs, password authentication, etc., use current cryptographic techniques and they are performing well in keeping data secure. However, the overall security of an encryption system relies in the ability to keep cipher keys secret, but a typical human behavior is to write down passwords either in their inbox of mobile phone or e-mail id, this behavior makes security very vulnerable to attack. The concept of biometric-based keys seems to be one possible solution to this insecurity.[13] Security must be the primary consideration from a mission-critical or safety-related product’s conception, through design and development, production, deployment, and the end of its lifecycle.[18][19]

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)
© Copyright: All rights reserved.

Embedded systems that are installed in devices forms an integral part of the manufacturing, health, transportation, and finance sectors, as well as the military, without having near-flawless strong cryptographic security built into them might also be vulnerable to well organized crime, terrorists, or enemy governments. [14][18]-[20]

Data hiding methodologies aim is to solve modern network security, quality of services control, and secure communications, is also a cost-effective alternative to other means of data security, which does not require protocol modifications. This technology is compatible with existing standards of multimedia compression and communications.[15]

Security is an important aspect of any network, but in particular to mobile adhoc networks. The wireless networks are potential for hacking using mobile devices. There is no clear line of defense for protecting the mobile neworks. The development of the Mobile Application Security System which uses a layered security approach and strong cryptographic techniques is seen as a feasible and low-cost solution to protect these application-based wireless networks.[16] Finally, a new concept in cryptographic security known as Quantum Encryption, which uses quantum fluctuations of laser light at the physical layer introduced into existing networks. It enables ultra-secure communications and near perfect security. [17] Quantum cryptography was first proposed by Stephen Weisner in his work "Conjugate Coding" in the early 1970s. Conjugate coding is an extension of Random number generator. [1] In Sigact News, a proposal was published in the year 1983, and at that time two scientists Bennet and Brassard, who were familiar with Weisner's ideas, were ready to publish their own ideas. In 1984, they produced the "BB84" which is the first quantum cryptography protocol. [7] In 1991, the first experimental prototype based on this protocol was produced which operated over a distance of 32 centimeters. During that period, the technology has been refined and the distance may be increased to kilometers. [3], [6] In June 2003, a team at the University of Vienna transmitted entangled photons across the river Danube, through free space. In April 2004, the first money transfer encrypted by quantum keys was experimented between the two Austrian banks. These two buildings were 500 meters apart, and fibre optics was fed through 1.5 kilometers of sewage system to link them together. [5]

III. QUANTUM CRYPTOGRAPHY

Quantum cryptography [10],[11]solves the problems of secret-key cryptography by providing a way for two users who are in different locations to securely establish a secret key and to detect if eavesdropping has occurred[9]. Quantum cryptography does not depend on difficult mathematical problems for its security. Quantum cryptography accomplishes these remarkable feats by exploiting the properties of microscopic objects such as photons. The photons have three chosen bases of polarization and the probable results of a measurement according to the bases are:

- Rectilinear (horizontal or vertical)
- Circular (left-circular or right-circular)
- Diagonal (45° or 135°) [2].

Although there are three bases, only two bases are used in any given protocol for quantum cryptography. Photons can be measured to determine their orientation relative to one of these bases of polarization at a time. Classically, one would expect the photon to have a certain polarization, which can be measured but which is not changed by the measurement. Photons, however, are quantum objects, which are considered to have a property only after it is measured. The type of measurement impacts the property of the object. This implies that a photon can only be considered to have a particular polarization after it is measure, and that the basis chosen for the measurement will have an impact on the polarization.

A. *Process of Quantum Coding*

Many algorithms of encoding and decoding information using a given key have been created already, many years before quantum cryptography came into existence. Quantum cryptography is not replacing traditional cryptography but it allows for a more secure transfer of the keys used in encoding and decoding. The maximum speed, scale and security of the transfer is achieved by sending the secret key using quantum coding, but encoding and sending the data itself using traditional methods and algorithms.

Quantum Information Processing and Quantum Bit

Quantum information processing or quantum information science is an interdisciplinary field. It is an amalgamation of quantum physics, information science engineering, computer science, mathematics and chemistry.

A bit; a binary digit, is the base of classical information theory. Regardless of its physical representation, it is always read as either a 0 or 1. For instance, a 1 (true value) is represented by a high voltage, while a 0 (false value) is represented by a low voltage. A quantum bit, or qubit (sometimes qbit) is a unit of quantum information. In quantum cryptography, two process are carried out. They are conversion and polarization. That means the data is converted to bits of 0s and 1s, which are then transferred using polarized photons. Photons are placed into a particular quantum state by the sender which will be observed by the receiver.

A photon can be in one of four polarizations:

90, 0, 45 and -45 degrees

A photon is measured using three different bases: rectilinear (horizontal or vertical), circular (left-circular or right-circular), and diagonal. The receiver can distinguish the polarization of the photons between a 0 and 90 degrees polarizations, or -45 and 45 degrees polarizations.

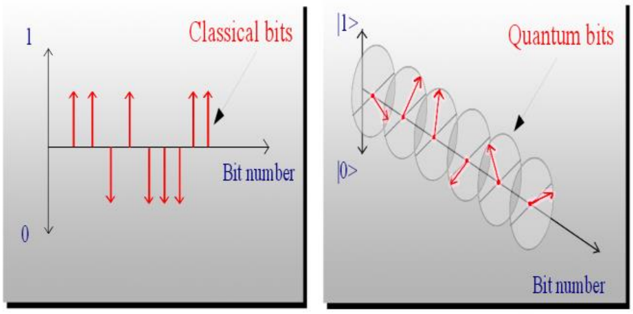


Fig 2: Classical bit Vs Quantum bit

B. Quantum Cryptography Model

In Quantum Key Distribution model, Alice is used to refer to as the sender, Bob as the receiver, and Eve as the eavesdropper. Figure 3 shows the QKD Model.

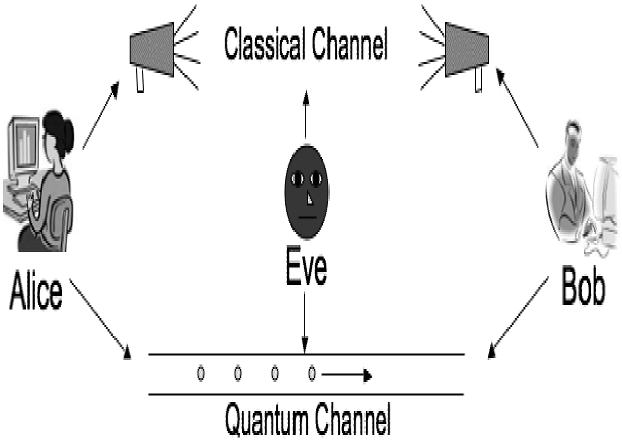


Fig3: Quantum Key Distribution Model

The most fundamental of the Heisenberg Uncertainty Principle (HUP) is that in a quantum system only one property of a pair of conjugate is known with certainty. As Heisenberg Uncertainty Principle states that who was initially referring to the position and momentum of a particle, described how any conceivable measurement of a particle's position would disturb its conjugate property. Therefore it is impossible to simultaneously know both the properties with certainty. Quantum cryptography can influence this principle but generally uses the polarization of photons on different bases as the conjugate property. The reason is that the photons can be exchanged over fiber optic links and are perhaps is the most practical quantum systems for transmission between sender and receiver.

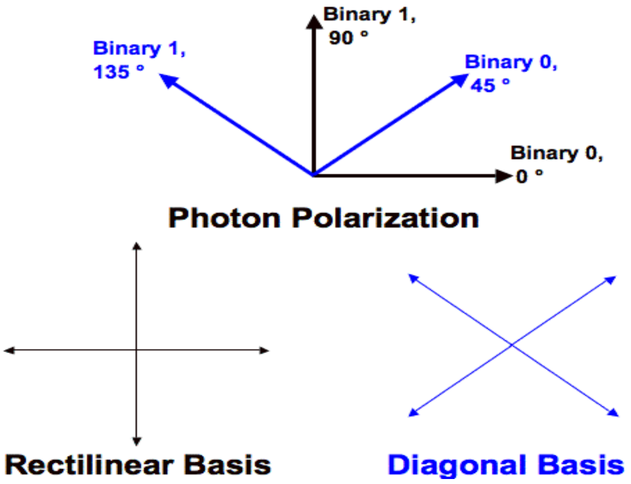


Fig 4: Photon Polarization

Figure 4 shows how a bit can be encoded in the polarization state of a photon. A binary 0 as a polarization of 0 degrees in the rectilinear bases or 45 degrees in the diagonal bases [7] [8]. Similarly a binary 1 can be 90 degrees in the rectilinear bases or 135 in diagonal bases. Thus a bit can be represented by polarizing the photon in either one of two bases.

C. Quantum key distribution- Key exchange methods

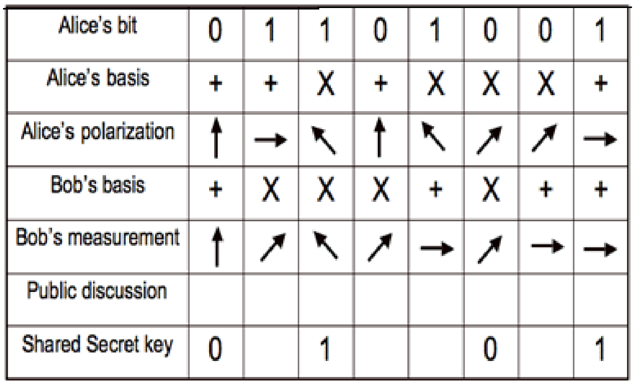
Consider a scenario in which the Alice and Bob communicates to agree on a key called a sifting key. This process is explained in two phases. Figure 5: illustrates on the bits Alice chose, the bases she encoded them in, the bases Bob used for measurement, and the resulting sifted key after Bob and Alice discarded their unmatched bits.

Phase I: Sending

1. Alice determines the polarization (horizontal, vertical, left-circular or right-circular) of each burst of photons which she's going to send to Bob. A common key is agreed between the sender and the receiver and the aim is not to transfer a specific key.
2. Polarized photons are produced using a light source from a light-emitting diode (LED) or from a laser.

Phase II: Receiving and converting

1. Bob randomly generates a sequence of bases (rectilinear or circular), and measures the polarization of each photon.
2. Bob tells Alice which sequence of bases he used, without worrying about other people hearing this information in the classical channel.
3. Alice publicly responds in the classical channel, which bases were chosen correctly.
4. Alice and Bob discard all observations except the correctly-chosen bases.
5. The remaining observations are converted on to binary code (left-circular or horizontal is 0, and right-circular or vertical is 1).



Alice's bit	0	1	1	0	1	0	0	1
Alice's basis	+	+	X	+	X	X	X	+
Alice's polarization	↑	→	↖	↑	↖	↗	↗	→
Bob's basis	+	X	X	X	+	X	+	+
Bob's measurement	↑	↗	↖	↗	→	↗	→	→
Public discussion								
Shared Secret key	0		1			0		1

Fig5: Sifted key

Correcting errors - Step 1

1. To randomize the positions of errors, Alice and Bob agree on random permutations of bits in the resulting string. Two errors adjacent to each other are very hard to detect, but it is likely that an error with the instruments or because of random noise may modify a sequence of bits one after the other. Randomization helps in this case.
2. The strings are partitioned into blocks of size k, with k ideally chosen to make the probability of multiple errors per block very small. For example consider the following situation

Alice's string contains 101100 and Bob's string contains 101111

Here the parity is the same, 1, even though there are two mistakes in the block. Making k small is one of the steps taken to minimize the chance of this happening, since the chances of having two errors in a block of size 50 is much less than in a block of 500, especially after the errors are randomized.

3. Alice and Bob compute and exchange parities for each block. The computed parity is made public, to ensure security and the last bit of each block is then discarded. This is to make the information useless for Eve.
4. Any block with different reported is broken down further. Binary search is used to locate and correct the error. Alternatively, if the length of the key is already sufficiently large, those blocks could be discarded.
5. In order to discover multiple errors, steps 2-5 are then repeated with increasing block size, k.

Correcting errors - Step 2

1. In order to determine if additional errors exist, Alice and Bob do another randomized check. They publicly agree on a random assortment of half the bit positions in their string, and compare parities, followed discarding the last digit, as mentioned earlier.
2. If the strings are different, then there is ½ probability of a disagreement of parities. Then a binary search is used to find and eliminate error, as described above.
3. After r repetitions of step 1 without disagreements, Alice and Bob can conclude that their strings disagree with probability (1/2)r, which can obviously be made arbitrarily small by increasing r.

D. Alternative methods for Key Exchange

The information can be exchanged in a number of ways. The other methods used are described as follows. [6]

One-time pad method

1. Alice generates two random bits, B1 and B2.

   B1 is used to select the basis and B2 is used to select the polarization of the photon.

   Bob generates a random bit B3 and sets his detector to that basis. Bob reads Alice's signal using that basis, and records B4.
2. Both Alice and Bob compares B1 and B3, the bases they used, over a public channel. These bases will be the same 1/2 of the time. The four possibilities are

   $(B1, B3) = (0, 0), (0, 1), (1, 0), (1, 1)$

   Here two bases may matches half of the time.
3. If B1 and B3 don't match, the bit should be resent until they match. To ensure privacy, every time the bases should be chosen randomly when they are resent.
4. If B1 and B3 match, Alice and Bob record B2 and B4, knowing that they are the same unless Eve is listening, in which case she would be changing the states of the photons. Comparing the strings using binary search as described earlier allows Alice and Bob to detect any interventions by Eve.

E. Quantum entanglement

This process can be generated by firing a laser through a crystal and splitting a single photon into two. By disturbing the state of one will instantly disturb the other, no matter how far apart they are. If one of the particles is measured according to the rectilinear basis and is in vertical polarization, then the other particle will be in a vertical polarization if it is measured according to the rectilinear basis. If however, the second particle is measured using circular basis, it may be found to have either left-circular or right-circular polarization. This is extremely useful in detecting eavesdroppers.

The procedures for a transfer are similar to the original process described earlier, where Alice sends polarized photons to Bob, who in turn measures the photons using randomly selected states. A photon generator is placed between Alice and Bob so that pairs of entangled photons with the same polarization go to Alice and Bob at the same time. Then both sender and receiver measure the signals with randomly varying bases, and record the result and the time received. After comparing the bases, they keep those that are the same and discard the bits measured with different bases. They can then test for errors using the algorithms described in the previous section.

F. Detecting eavesdropping

To detect the eavesdrop; polarization of the photon is to be measured. The key concept is that it is impossible to measure the polarization of the photon without destroying it. So if Eve intercepts the signal, she will have to send new photons to the receiver so that she may not be detected about her presence. However, she will inevitably introduce errors, since she doesn't know the state and polarization. So Alice and Bob can check for errors by revealing a random subset of their generated sequence and comparing it publicly. If they are not satisfied with the error rate, they can set up a different channel. This ensures that while Alice and Bob cannot stop Eve from listening in, they would always know that she is there.

In entangled photon transfer method can also be used for this purpose. According to physics law, a change in the polarization of one photon in a pair will affect the other one, no matter how far apart they are. In order to eavesdrop, Eve would have to detect one of the photons and measure it, thus destroying half of the pair. This act will end the quantum relationship of the two members of the pair, which is very easy to detect by Alice and Bob, and impossible to reverse for Eve. Without revealing the specific results of their measurements, the sender and the receiver can talk publicly and see where intervention has occurred. [4]

IV. APPLICATIONS OF QUANTUM CRYPTOGRAPHY

Quantum encryption already protects both sensitive national security information in the public sector and financial information in the private sector. Its security is tested and proven. Here are some current and near-future applications of quantum cryptography.

A. Ultra-Secure Voting

With political upheaval and accusations of voter fraud rampant in developed and developing countries alike, it's clear that making the voting process more secure is a necessity. Since 2007, Switzerland has been using quantum cryptography to conduct secure online voting in federal and regional elections. In Geneva, votes are encrypted at a central vote-counting station. Then the results are transmitted over a dedicated optical fiber line to a remote data storage facility. The voting results are secured via quantum cryptography, and the most vulnerable part of the data transaction when the vote moves from counting station to central repository is uninterruptible. This technology will soon spread worldwide, as many other countries face the specter of fraudulent elections.

B. Secure Communications with Space

Secure communications with satellites and astronauts is an increasing concern, and a company called Quintessence Labs is working on a project for NASA that will ensure secure communications from Earth with satellites and astronauts. The goal of the project is to achieve a protocol which guarantees the security of communications regardless of the technology or intelligence to which an adversary has access. It also includes a mandate to secure both information "at rest" and in transit. This would ultimately increase the safety of astronauts in space and ideally preclude the needs upgrade in the future beyond minor speed increases.

C. A Smarter Power Grid

It has been speculated that the American power grid is one of the most vulnerable targets for a cyber attack. In fact, some major U.S. utilities are under "constant" attack by cyber enemies. A small encryption device helps the workers to send totally secure signals using public data networks to control smart electricity grids. Smart grids are essential for balancing supply and demand for efficiency. Additionally, with proper precautions in place, they are significantly more secure than traditional grids.

D. Quantum Internet

Today's internet is relatively fast, but its security is paltry compared to quantum-encrypted transmissions. Quantum encryption would greatly slow down the internet. In the future, however, it's possible that we could switch effortlessly between "regular" and "quantum encrypted" internet, so that our most sensitive transmissions would be passed along in an ultra-secure manner. This would achieve the ideal of a simultaneously fast and secure internet.

V. LIMITATIONS

In case of entangled photons, which seems to be safe, there is also a practical problem not only with the cost, but also with keeping them entangled long enough to meet the needs of the real world.

Another problem is that for distances beyond 50 kilometers or so, the noise becomes so great that error rates also increases drastically. This leaves the channel very vulnerable for eavesdroppers, and makes the channel virtually impossible to send information. However, in future, it is possible for quantum keys to be exchanged through the air. Small telescopes may be aligned to detect the signal. Some calculations even suggest that photons could be detected by a satellite, which allows communication between any part of the world.

QKD is the first practical application of the foundations of quantum mechanics, and as such it indicates to the value of basic science research. If Quantum Key Distribution is to ever be used in practice its security must be certified, and hence the thorough examination is necessary with the aspects of quantum mechanics on which its security is based. To validate these security concepts new experiments should be performed based on the foundations of quantum mechanics.[12]

VI. CONCLUSION

It is concluded that to transmit sensitive information between two or more points, some stronger technique is needed. It's sure that Quantum key distribution and other quantum encryption methods will allow us to secure sensitive information more effectively in the future. Quantum encryption is a powerful and positive step in the right direction, toward a future in which we can feel more secure about how and what we share. Thus, we can also expect a considerable feedback from QKD into basic physics, which leads to a new perspective on the foundations of quantum mechanics. The perspective can be more "practical" than "philosophical."

REFERENCES

[1]. Wiesner, Stephen., 1983. "Conjugate coding." *ACM Sigact News* 15.1: 78-88.

[2]. Henle, F., 2002. BB84 Demo. http://www.cs.dartmouth.edu/~henle/Quantum/cgi-bin/Q2.cgi

[3]. Ford, James., 1996. "Quantum cryptography tutorial." http://www.cs.dartmouth.edu/~jford/crypto.html.

[4]. Harrison, David M., 2001. "Quantum Teleportation, Information and Cryptography." http://www.upscale.utoronto.ca/GeneralInterest/Harrison/QuantTeleport/ QuantTeleport.html.

[5]. Knight, Will., 2004. "Entangled photons secure money transfer." Newscientist.com. http://www.newscientist.com/news/news.jsp?id=ns99994914.

[6]. "Quantum cryptography." Wikipedia, the free encyclopedia. http://en.wikipedia.org/wiki/Quantum_cryptography. Modified 17 September 2004.

[7]. "The BB84 Quantum Coding Scheme", June 2001. http://www.cki.au.dk/experiment/qrypto/doc/QuCrypt/bb84coding.html

[8]. Gisin, N., Ribordy, G., Tittel, W., Zbinden, H., "Quantum Cryptography", Reviews of
Modern Physics, vol. 74, January 2002, pp. 146 - 195.
http://www.gap-optique.unige.ch/Publications/Pdf/QC.pdf

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

[9]. Martinez-Mateo, Jesus, David Elkouss, and Vicente Martin. "Key reconciliation for high
performance quantum key distribution." *Scientific reports* 3 (2013).

[10]. C. H. Bennett and G. Brassard. 1984.Quantum Cryptography: Public Key Distribution and Coin Tossing. In Proc. IEEE Int. Conf. on Comp.,Sys. and Signal Process., pages 175–179, Bangalore.

[11]. A. K. Ekert. Quantum Cryptography Based on Bell's Theorem. Phys. Rev. Lett. 67(6):661–663, 1991.

[12]. Hughes, Richard J., et al. 1995. "Quantum cryptography." *Contemporary Physics* 36.3: 149-163.

[13]. Hoque, S., Fairhurst, M., Howells, G., & Deravi, F. (2005, March 17). Feasibility of
generating biometric encryption keys. Electronics Letters, 41(6), 1-2.

[14]. Webb, W. (2006, July 20). Hack-proof design. (Cover story). EDN, 51(15), 46-54.

[15]. Lovoshynovskiy, S., Deguillaume, F., Koval, O., & Pun, T. (2005, January). Information-theoretic data-hiding:: recent achievements and openproblems. International Journal of Image & Graphics, 5(1), 5-35.

[16]. Floyd, D. (2006, Fall2006). Mobile application security system (MASS). Bell Labs Technical Journal, 11(3), 191-198.

[17]. Hughes, D. (2007, May). Cyberspace Security via Quantum Encryption. Military Technology,31(5), 84-87.

[18]. Sasirekha, N., And M. Hemalatha. "A Hybrid Indexed Table And Quasigroup Encryption Approach For Code Security Against Various Software Threats." Journal of Theoretical & Applied Information Technology 60.2 (2014).

[19]. Sasirekha, N., and M. Hemalatha. "Novel Secure Code Encryption Techniques Using Crypto Based Indexed Table for Highly Secured Software." International Review on Computers & Software 8.8 (2013).

[20]. Sasirekha, N., and M. Hemalatha. "A Quasigroup Encryption Based Cryptographic Scheme for Software Protection." International Journal of Advances in Engineering and Emerging Technology 3.1(2013).

Dr. N.Sasirekha, completed MCA., M.Phil., Ph.D in Computer Science. She is currently working as a Assistant Professor & Head, Department of Computer Technology & Information Technology, Rathinam College of Arts abd Science, Coimbatore, Tamilnadu, India. She has eleven years of teaching experience and presented fifteen papers in various National Conferences/ Seminars and Five papers in International Conferences. She has published sixteen research articles in various International Journals. Her area of research is Software Engineering, Data Mining, and Image Processing. She is also a Reviewer in several International Conferences and Journals.

Dr. M. Hemaltha completed MCA., MPhil., PhD in Computer Science and Currently working as a Asst Professor, Dept of Computer Science in Karpagam University. She has Eleven years of experience in teaching and published more than seventy papers in International Journals and also presented Seventy papers in various National Conferences and Twenty papers in International Conference. Her areas of research are Data mining, Software Engineering, Bioinformatics and Neural Networks. She is also a reviewer in several National and International Journals.