Volume 3, Issue 7, July 2013 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Cryptography and its Prominent Branches

Pratibha, Shivi Goel

UIET, Kurukshetra University
Haryana, India

Abstract: Cryptography is the art and science of achieving security by encoding messages to make them non readable. Cryptography has a long and fascinating history. Now a day, there are many branches of cryptography like lattice cryptography, quantum cryptography, and visual cryptography and so on. Each method has its own advantages and limitations. This paper critically reviews such branches of cryptography.

Keywords: cryptography, lattice, quantum, visual cryptography, Threshold cryptography

I. **Introduction**

Cryptography is a fundamental building block for building information systems, and as we enter the so-called "information age" of global networks, ubiquitous computing devices, and electronic commerce, we can expect that the cryptography will become more and more important with time. In cryptographic terminology, the message is called *plaintext* or clear text. Encoding the contents of the message in such a way that hides its contents from outsiders is called *encryption*. The encrypted message is called *cipher text*. The process of retrieving the plaintext from the cipher text is called *decryption*. Encryption and decryption usually make use of a key, and the coding method is such that decryption can be performed only by knowing the proper key. There are two classes of key-based encryption algorithms, *symmetric* (or secret-key) and *asymmetric* (or public-key) algorithms. The difference is that symmetric algorithms use the same key for encryption and decryption (or the decryption key is easily derived from the encryption key), whereas asymmetric algorithms use a different key for encryption and decryption, and the decryption key cannot be derived from the encryption key. Symmetric algorithms can be divided into *stream ciphers* and *block ciphers*. Stream ciphers encrypt a single bit of plaintext at a time, whereas block ciphers take a number of bits (typically 64 bits in modern ciphers), and encrypt them as a single unit. Asymmetric ciphers (also called public-key algorithms) permit the encryption key to be public (it can even be published to a web site), allowing anyone to encrypt with the key, whereas only the proper recipient (who knows the decryption key) can decrypt the message. The encryption key is also called the *public key* and the decryption key the *private key*. The security provided by these ciphers is based on keeping the private key secret.
Rest of the paper describes the major branches of cryptography.

II. **Lattice-Based Cryptography**

Lattice is a mathematical representation where lattice 'L' is a set of points in the n-dimensional Euclidian space R^n with a strong periodicity property. Basis for 'L' is a set of vectors such that every element of 'L' is uniquely represented on those vectors linear combination with integer coefficients. Talking about cryptography, mathematical problems are used to construct a cryptography system, these problems are usually hard to solve unless we have some extra information. Mathematical problems based on lattices are: *Shortest Vector Problem (SVP):* From the given basis of a lattice, find the shortest vector in the lattice. *Closest Vector Problem (CVP):* From the given basis of a lattice and a vector that is not in the lattice, find a vector with a least distance to the 1st vector. Solution to such problems can be achieved through lattice basis reduction which is actually a transformation of an integer lattice basis in order to find a basis which has short, nearly orthogonal vectors .Once, such a transformation is achieved CVP and SVP can be solved easily.

A. *Security concerns of LBC:*

The cryptographic constructs made through implementing LBC [1] promise a dignified security for post-quantum cryptography. They are really efficient and simple to implement, the cryptographic constructs like cipher texts and confidential messages are all believed to be secure against attacks made by conventional or quantum computers. Lattice based cryptographic constructs can be classified under two types: Practical proposals that is efficient enough in cryptography but lack a supporting proof of security. Other type is those constructs which are not that sufficiently efficient to be applied practically but provide strong provable security which is based on a worst-case hardness of lattice problems.

B. *Worst-case hardness:*

Worst-case hardness implements the breaking of any lattice based cryptographic construction into numerous small instances and then solving those instances and checking for the worst-case hardness. This study has two importances:

i.) It assures us that attacks on the cryptographic constructs are usually proven to work effectively on small choices of parameters and not asymptotically. Thus, the hardness detection helps make design decisions regarding the algorithms, constructs etc.

ii.) It can also help in selecting the concrete parameters for the cryptosystem, since it formulates the instances of the entire cryptosystem problem.

Hence, studying and working on these instances will eventually help choose those specific concrete parameters that need to be very efficient in order to create secure and reliable cryptographic constructs. Lattice based problems are quite hard to solve, even the best known algorithms provide running times in exponential notations and sometimes provide bad approximation ratios. No specific quantum algorithms have since been suggested to solve these problems over the classical (non-quantum) algorithms. But still these are considered as natural problems because these are not considered as NP-hard problems, which are actually hard to be solved. The basic signature scheme using LBC in implementation is a combination scheme.

III. **Elliptic Curve Cryptography**

ECC [2] is an approach to public-key cryptography which is based upon the algebraic structure of the elliptic curves over finite fields. Elliptic Curve Cryptography was discovered by Victor Miller (IBM) and Neil Koblitz (University of Washington) as an alternative mechanism for implementing public-key cryptosystems.

ECE works as follows:

Key Generation: For encryption the sender will be using the receiver's public key and the receiver would eventually decrypt it while using its private key. So, for key generation select a number'd' within the range of 'n'. Use the simple equation and generate the public key.

Q = d*P Here'd 'is a random number within the range 1 to n-1 and 'P' is a point on the curve. 'Q' is generated as the public key'd' is the private key.

Encryption in ECC: 'm' will be the message to be sent. Using ECC we have to represent it on the curve. Mainly two algorithms are used here for encryption: Diffie-Hellman Key Exchange, and the Massey-Omura Encryption. Ther are many methods which can be used for decryption.

There are many in-depth implementation details that are done in research by a company by the name Certicom. Elliptic curve cryptography is vulnerable to a modified Shor's algorithm for solving the discrete logarithm problem on elliptic curves [8].

A. *Various schemes of cryptography based upon elliptic curves are also available these days:*

a.) The elliptic curve Diffie-Hellman (ECDH) based upon Diffie-Hellman scheme.

b.) The elliptic curve Integrated Encryption scheme (ECIES) also known as Elliptic curve Augmented Encryption scheme.

c.) Elliptic curve digital signature algorithm (ECDSA) based upon digital signature algorithm.

d.) ECMQV key agreement based upon MQV key agreement.

e.) ECQV implicit certificate scheme.

IV. **Quantum Cryptography**

Just like LBC, Quantum cryptography [3] performs the cryptographic tasks while breaking the cryptographic systems. It describes the use of quantum mechanical effects particularly used as quantum communication and quantum computation. Quantum cryptography can be used in quantum communication to securely exchange a key i.e. for key distribution or for hypothetical use of quantum computers. Both of these implementations allow the breaking of various popular public-key encryption and signature schemes. Quantum cryptography has been proven advantageous over the classical (non quantum) crypto graphical constructs. An example for this could be that quantum mechanisms guarantee that measuring quantum data disturbs that data, this can be used to detect eavesdropping in quantum key distribution.

A. *Quantum Key Distribution:*

Quantum Key Distribution is practically available commercial application of quantum cryptography. Quantum communication is implemented to establish a shared key between two parties. Any eavesdropper can know about the ongoing communication between the sender and receiver but it would never come to know about the key shared among them because the sender (Alice) encodes the key bits into quantum data and sends them to the receiver (Bob).Any malicious invader if wishes to interrupt and know this key, his such kind of attempts will result in changes in the message and eventually the sender and receiver will come to know of it. The key is then typically used for encrypted communication. Security of QKD can be proven mathematically something that can't be done through classical key algorithms. But the condition here is that the minimal assumptions required as well as the laws of quantum mechanics are applied and both the sender and receiver should be able to authenticate each other. Any intermediate invader must not be able to impersonate as the designated sender and receiver.

B. *Commitment value and protocols promising security:*

The unconditional security provided by QKD is supported by the commitment, where under this commitment scheme the sender (Alice) is supposed to commit over some value and it is not allowed to change this value until the secure cryptographic task is completed. One more thing is assured here that the intended receiver is not made to learn about this value until Alice reveals it. This commitment scheme enhances the security aspect in QBC. Crepeau and Kilian worked upon the commitment scheme and proposed that given a quantum channel and a proper commitment scheme one can perform secure multiparty computation. Another researcher Mayers came with a view that quantum commitment is impossible, a computationally unlimited attacker can break any quantum commitment protocol but later it was resolved by the fact that assumptions are supposed to be weaker when such attacks are proved prominent otherwise a significant commitment value and an efficient commitment scheme will never let you down. There are two implementations of QBC: a.) *Bounded Quantum Storage Model:* Since there is commitment protocols and another new Oblivious Transfer

(OT) protocol to provide the most secure cryptographic tasks. But despite of using such security perspectives the eavesdropper as opposed by 'Mayers' can learn about the quantum data anyhow. So, in order to prevent the cryptosystem from this, a specific limit say 'Q' is applied on the amount of the quantum data an adversary can store. No such limit is imposed on classical i.e. non-quantum data for an adversary.

Using BQSM, Commitment and Oblivious Transfer can be well implemented. So, the intended parties exchange more than 'Q' quantum bits formally known as 'qubits'. Since, the dishonest party is compelled to store only 'Q' bits therefore it can't store all the exchanged bits hence a state of complete intrusion and information loss or modification are avoided.

b.) Noisy Storage Model: This scheme disagrees with the limit implication on the quantum memory of the adversary but allows them to have an imperfect quantum storage device of arbitrary size. This imperfection is measured by some noisy quantum levels. Those noise levels determine how crucially some primitives like BQSM need to be implemented. It is sometimes not possible to limit the adversary's storage device and capacity. Therefore, more effort is applied on the techniques for resolving high enough noise levels implemented through BQSM where it forms a special case of the noisy-storage model.

C. More forms of quantum cryptography:

i.) *Position-based quantum cryptography:* The main task here is of position verification where in this quantum cryptography the intended sender has to locate the specified receiver and then the receiver's position needs to be verified by using some verification protocol.

ii.*) Post-quantum cryptography*: As quantum computers are increasingly being realistic, it is important to study cryptographic schemes that can prove to be secure even against adversaries with access to quantum computers. The study of such schemes is known as post-quantum cryptography. Need for this comes from the fact that many popular encryption and signature schemes can be broken using Shor's algorithm for factoring and computing discrete logarithms on a quantum computer. Schemes that are secure against quantum adversaries are McEliece and Lattice-based schemes as discussed earlier in this paper.

V. **Threshold Cryptography**

Threshold-the word itself signifies meaning. In case of cryptography it suggests that when you have those minimum number or threshold value of the secret (key or message) then only you could be able to access it or produce it to the fullest of its form. Actually threshold cryptography [4] creates the bridge of that threshold value while keeping its initial requirement as chopping the secret key into little bits.

For e.g. let us assume that we have 4 copies of a key and then we break the key into 3 pieces or subsets of bits and distribute one such piece to each of 12 people. Then 2 consequences arise while we tend to use these pieces/subsets in threshold cryptography:

a.) *Random Distribution*: It would probably take 5 people for using the key, threshold minimum here would be '3' and maximum number of servers to contact would be '9'.

b.) *Algorithm, non-random alphabetic distribution:* The alphabetically lowest four would get piece 1, next alphabetic group would get piece 2 and so on. This approach would be more optimal and would require exactly 3 successful contacts to the server to find the whole key. Algorithms are available which can suggest the structure of subsets into which the key must be broken and distributed over severs. For reconstruction of that key 'M' out of 'N' servers who possess those subsets need to give their approval as well as their partial secret key in order to compute the complete secret key. Say 3 out of 12 or 5 out of 12.Where selecting 3 specific servers out of 12 would implement more effort and consequently more cost. A secret key must be broken into C(N,M-1) pieces each of the holders is given with(N-M+1)/N parts of the complete key.

Where, C is the combinator function, N is the total number of holders of subsets of secret, M is the number of holders to be selected who would be required to give their approval and secret key when needed to generate the key to its fullest form.

A. Security aspects of threshold cryptography:

i.) Designated systems/holders of piece of key must be compromised or equipped with special schemes so that they can control the secret key cooperatively.

ii.) The participating systems must be inherently resistant to the spoofing attacks by the eavesdropper or some super users of the computation resource. Distributed nature of this system prevents the complete loss of secret key or information because they are not available to the attacker at the same place and collecting that from all probable holders as well as computation of such probability are both difficult to attempt.

iii.) It provides the secret redundancy therefore we can guarantee that loss of secret would be less probable since any copy would be there for sure and from that subset copy the entire key would be generated.

iv.) Even if the nodes/servers are lost then the other one's are supposed to surely have the copy of secret key's piece and hence key generation is possible somehow, till we have that 'M' out of 'N' condition working.

v.) In case when the attacker or simply any normal user wants the authorization to access a different system, then the systems are also split into threshold numbers and specifically particular number of systems needs to be compromised, then selection of those particular systems becomes problematic. If we have to have the approval of 3 out of 12 systems then at random any 3 systems can be compromised but that won't work. Actually this all happens through combinatorial representation where the possibilities come out to be huge and selecting from such a huge collection is really hectic.

VI. Visual Cryptography

Visual cryptography [5] is a real advancement in the field of encryption and decryption where the secret information is hidden in images and the information can be decrypted by the human vision if the correct key image is used. It was proposed by Moni Naor and Adi Shamir in 1994.Working of visual cryptography is shown in figure 1 [11]. Two concepts are employed under this.

1.) One time pad system: Here we use two transparent images where one image is supposed to actually have the secret information while the other to have truly random pixels, when those two images are overlapped then only the secret is decrypted. The number of the participating images can be more than 2 because the degree of complexity of encryption and the amount of data transmission both need to be really high.

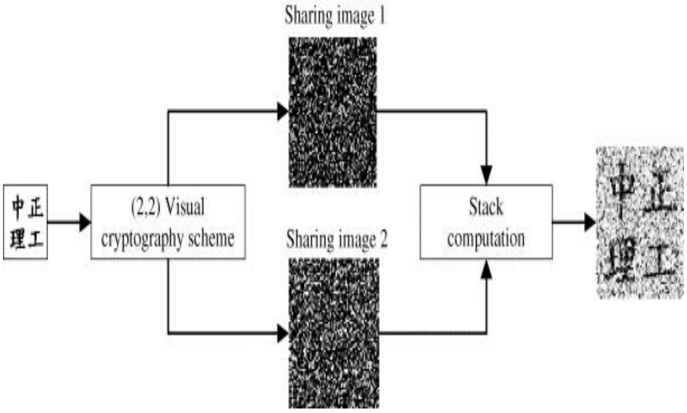

Figure 1: Working of visual cryptography

2.) Secret Sharing: This is the case when we use more than 2 images or when one image is cryptographically broken into any number of shares say 'n' and overlapping all those shares can only decrypt the image and secret information in that. As shown in figure 2 [10]. It is also suggested here that even if some adversary or attacker manages to intrude and collect (n-1) shares of the image, no possible information could be derived from that and hence the intrusion would be a waste to do until it can manage to collect all shares of image, hence security has been given more significant and high levels.

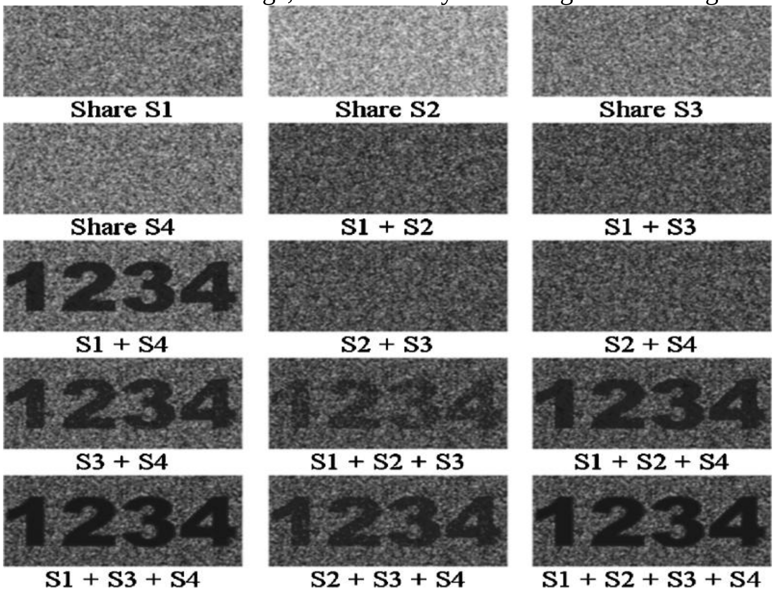

Figure 2: Secret sharing

For practical implication the major requirements would be:

a.) The two images should be printed on same type of transparent sheet and such that overlapping of the images is done correctly.

b.) The program must be such that it can depict and display the black and white pixels correctly and set the printer so that all pixels are printed correctly being aligned on each other correctly for those 2 information hiding images.

A. Advantages:

i.) If the pixel states in layer '1' are truly random then according to the need of information to be decrypted, the states of the pixels of layer '2' has to be similarly unpredictable and random. So, if on one side this unpredictability is difficult to implement or program through protocols on the other side if it is implemented it is eventually impossible for the attacker to predict the states because in order to know the state patterns of layer '2' the state patterns of layer '1' must be known first but since those are random, so its not possible to predict them, hence security is enhanced further.

ii.) For secure communication sender will in advance distribute a few copies of layer '1' probably more than one copy to its receiver. If it has more than one intended receivers like if it is a server for LAN or any such network, it will distribute such copies to all of them. When it has some secret information to be sent to its intended receivers it will generate an appropriate layer '2' and the receivers would carefully overlay those two layers and decrypt the information. The proper alignment of the layers needs to be preprogrammed there on the participating parties.

For any adversary to succeed in decrypting the information all the participating layers or images are must to be achieved otherwise there is no way to decrypt the information with incomplete set of those layers, not even with just one missing layer. Where the attacker can't decrypt the actual information without having all the intended layers between the sender and receiver but somehow they can intrude and get the intended layer '2' and maliciously modify it and therefore can cause the consequences like loss of information and transmission of wrong information at the receiver.

VII. **White Box Cryptography**

In the earlier cryptographic schemes it was assumed that the attacker or adversary is only aware about the input to the cryptographic system, implemented algorithm and the output from all this. This was termed as Black-Box cryptography and later on it was assumed that the attacker can intrude to some more internal levels like it can learn the channel configuration, the cryptography which could deal with such scenarios was termed as Grey-Box cryptography.

These terms came into existence for the Digital Rights Management (DRM) implementations. Here the cryptographic algorithms are a part of security solutions employing a known, strong algorithm while relying on secrecy of the cryptographic key. When such applications needed to be executed on the systems which are subject to the control of potentially hostile end-users then came a requirement that if the attackers are so effective that they can monitor each and every execution occurring, they can know about every single detail in many cases even about the secret key, a more significant cryptographic technique must be evolved. This gave birth to the concept of White-Box cryptography [6].

Where white box cryptography keeps into consideration that the attacker can intrude deep inside and therefore the cryptographic schemes and the implemented applications should be programmed such that they can overcome all those malicious activities and help execute the cryptographic transmission as well as other software implications efficiently.

A. Challenges in front of White-Box Cryptography:

Operating in the fully transparent environment and still keeping the valuable information such as licensing and other trade secrets hidden is a challenging task because:

a.) How to encrypt or decrypt the content without directly revealing any portion of key or data while it is assumed to be all visible to the attacker.

b.) How to perform strong encryption mechanism knowing that attackers can observe and or alter the code during execution.

Attackers have full visibility of: The dynamic code execution & Intended algorithm details, both these are alterable and knowing this fact the cryptographic schemes are designed. White box cryptography integrates the cipher in such a way that does not reveal the key.

i.) Here the key will be hard-coded in the code.

ii.) The key will be embedded in the algorithm and instantiated.

iii.) When these hard-coded instances of key are used for encryption and decryption on demand, there would be least chances of loss of this key through the attacks.

iv.) Just as in RSA, the protection of key is done through simple multiplication through large numbers and it is harder to factor the result into its prime integers which is the requirement in RSA for being a cryptographic key. Decryption function will be implemented in these cryptographic applications or software but through function which is hard-coded, the key can't be extracted and decryption cannot be reversed to produce encryption and then decrypt back the desired value.

VIII. **Steganography**

Steganography [7] basically means hiding one piece of data/information into other piece of information/data. Cryptography makes the data unreadable for the adversary where as steganography tends to hide the data from the third party. Data can be hidden in many different forms:

i.) Covert channels, like some tools use ICMP as the communication channel between the adversary and the system compromised by it.

ii.) Hiding text within web pages.

iii.) Hiding files in plain sight e.g. hiding data in important sounding file like C:\winnt\system 32 directory?

iv.) Null ciphers e.g. using the first letter of each word to form a hidden message in an otherwise innocuous text. Steganography provides dual security by first encrypting the data and making it unreadable for the adversary and then hiding it in some other data form. The intruder has first to find the hiding data object that is itself a difficult task and then if somehow it manages to do that, it has to decrypt that.

A. Steganography Applications:

1.) Digital watermarking: Replicating any image, logo or text on paper stock for the sake of atleast partial authentication of source document .e.g. any graphic artist can hide the signature in his creations and post them. So that any copyright issues can be resolved with that signature.

2.) For communication, images can be used to depict any type of message secretly hidden in the image.

Steganography works upon the following formulation:

Fe(cover_medium(C)+hidden_data(M)+Stego_key(K) = Stego_Medium(S)

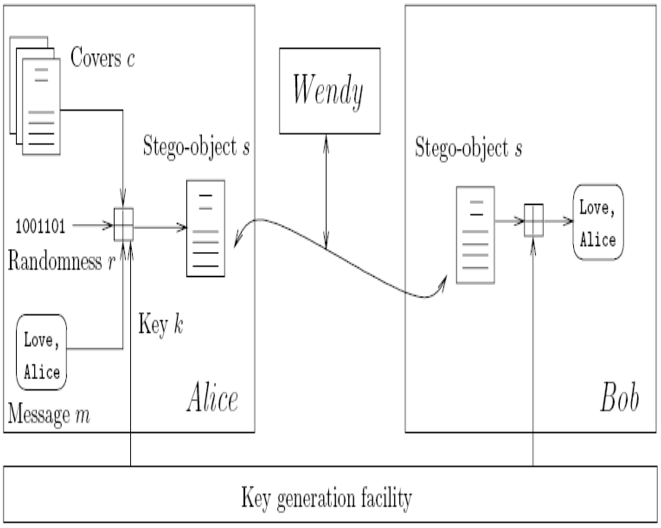

Figure 3: Working of steganography

Where cover_medium(C) is the file into which the data will be hidden, it can be any image or audio file. Hidden_data (M) is the secret message to be hidden. Stego_key (K) is the key with the help of which the message to be hidden can be encrypted first. Stego_medium is the output file which has the hidden and encrypted message/data, it is similar to cover_medium. The stego function 'Fe' will operate on all the required elements and produce 'S', the stego_medium.

While the inverse Fe^{-1} will decode all these elements back to the initial state. Figure 3 [9] showcase the working of steganography.

B. Some modern techniques of steganography:

Plaintext: a.) Using the selected characters of the cover text will help generate message. The sender will transmit to the receiver an integer key and the receiver is in agreement with the sender that the received key is the respective positions of those keywords in the cover text whose 1st alphabets would generate the secret message.

b.) Using extra white spaces of cover text: Extra white spaces are inserted between the consecutive words in the cover text and counting that spaces would give a number which is going to map to a hidden data available in a lookup table which is actually an agreement between the two parties. The number will be mapped with the index of that lookup table and the data at that index value will be the hidden message.

Still imagery steganography: The information is hidden in the digital image, Human vision system can't detect the variation in luminance of color vector at high frequency side of visual spectrum. That shortcoming is exploited in this type of steganography. In a 24-bit bitmap each color i.e. red, blue and green will get an equal share of 8-bits.So,info can be hidden in the images with the help of these 8-bits,changes in the LSB (Least Significant Bit) would be the requirement for hiding the message/secret. And altering that small single bit is very difficult for intruder to detect.

Audio and Video Steganography: Secret information is embedded in the digitized audio file here and that is done through altering the binary sequence of the respective audio file. It can be implemented through various techniques while the primary requirement being the conversion of the analog audio signal into digital binary sequence which can be an easy format for embedding secret message. Sampling and quantization performs this conversion.

IP datagram steganography: Here, the information to be hidden is placed in the IP header of a TCP/IP datagram. Some of the fields of IP header and TCP header in IPV_4 network are chosen for data hiding. The objective is to make the stego datagram undetectable by any kind of adversary, sniffer etc.

IX. **Conclusions**

In this paper seven major types of cryptography is described. Lattice based cryptography is based on lattice which is a set of vectors. This scheme is yet not deployed securely in practical. Elliptic curve cryptography depends on the algebraic structure of elliptic curve. It provides a complex cryptographic structure and widely explored these days. Quantum based cryptography is mainly in demand now a days. Threshold cryptography keeps a set of threshold value of the secret. It is redundant and distributed in nature. Visual cryptography uses the concept of hiding secrets in images. It is vulnerable to eavesdropper and intruder can modify the information during transmission. White box cryptography keeps into consideration the attackers possibility and help in executing the transmission as well as software implementation simultaneously and efficiently. Steganography used to hide one piece of data into another piece of data.

References

[1] Available:http://www.di.ens.fr/~lyubash/papers/signaturechess.pdf
[2] Available:http://bithin.wordpress.com/2012/02/22/simple-explanation-for-elliptic-curve-cryptography-ecc/
[3] Bennett CH, Bessette F, Brassard G, Salvail L, Smolin J, '*Experimental quantum cryptography'*.

[4] Available: http://groups.csail.mit.edu/cis/cis-threshold.html

[5] M. Naor and A. Shamir, ‘*Visual cryptography*,’ Advances in Cryptography

[6] Available: http://www.cs.colorado.edu/~jrblack/class/csci7000/s05/project/oorschot-whitebox.pdf

[7] Gary C Kessler, ‘*Hiding data within data’*

[8] Nielsen et al., ‘*quantum copmutation and quantum information’.*

[9] Available: http://scien.stanford.edu/pages/labsite/2005/psych221/projects/05/vvikram/stego.htm

[10] Available: http://opticalengineering.spiedigitallibrary.org/article.aspx?articleid=1076972#Introduction

[11] Available: http://www.sciencedirect.com/science/article/pii/S0920548906000225