Critical Analysis of Cryptography Methods Used for Secure Data Transmission

Sangeeta Kumari
Dept of Computer Engineering and Application,
NITTTR,
Bhopal, India
sangeetak2606@gmail.com

Sonal Pawar
Dept of Computer Engineering and Application,
NITTTR,
Bhopal, India
sonalpawar890@gmail.com

Rakhi Emelaya
Dept of Computer Engineering and Application,
NITTTR,
Bhopal, India
rakhisports@gmail.com

Dr. Sanjay Agrawal
Dept of Computer Engineering and Application,
NITTTR,
Bhopal, India
sagrawal@nitttrbpl.ac.in

Abstract— Cryptography technologies provide best mechanism of protecting the information from unauthorized access without putting the business on risk, this paper focus on the concept of different cryptography method likewise hierarchical visual cryptography in this method expansion ratio is reduced to one ratio two from one ratio four. Another method is accelerating block cryptography application which is used with procedure level mechanism; here also describe the lightweight key which is used in Wireless Sensor Network (WSN).Cryptography used in many fields for network and information security.

Keywords- *wireless sensor network; rsa algorithm; elliptic curve cryptography; block cryptography; AES encryption algorithm*.

*****

I. INTRODUCTION

In Cryptography encryption and decryption are used for securing of our data, encryption are rarely used by public but are largely a military tool, there is secret key for symmetric cryptography and for asymmetric cryptography public/private key are used. In digital signature RSA algorithm are used it involves swapping the role of public and private key. For controlling the unauthorized access digital certificates and certificate authorities are used, certificate authorities basically are a trusted third party. There are still many applications in the area of cryptography, here we take the overview of different methods which are used by researchers to encrypt and decrypt our data. In this paper we have analyze encryption and decryption, users always want security, confidentiality, integrity and authentication of data with the help of public and private key or secret key. Likewise, lightweight key establishment in wireless sensor network based on elliptic curve cryptography [1] in which key distribution mechanism are used whose objective is to provide reliable and secured communication it is widely used in education, medical treatment, military, traffic and also collect the information about light intensity, pressure and temperature and detect danger. Additionally, hierarchical visual cryptography is used, the main motive of this cryptography is secret sharing. As the number of levels in hierarchy visual cryptography increases, the secrecy of data tends to increase [2].

Encryption method has been divided into two categories: substitution cipher and transposition cipher. AES encryption algorithm is used as a symmetric algorithm. AES block cipher [3] as acting in plaintext in groups of each bit time which are called blocks and in block cipher encryption algorithm takes input an n-bit plaintext M and k- bit key K and output as n-bit cipher text C, and in decryption algorithm takes input an n-bit cipher text C, k-bit key K and output n-bit plaintext M. In cryptography, many applications are written for uniprocessors but it has no benefit from single- chip multiprocessors and these applications could be paralyzed into threads which contain data and control flow dependences which is a challenging task especially for poor –understood legacy code and to overcome these problem Thread-Level Speculation proposed mechanisms for optimistically execute non-analyzable serial codes in parallel. Block cryptography [3] applications are computing-intensive application which used in network and information security fields. And in procedure level speculation mechanism for accelerating block cryptography applications which include execution model, synchronization strategy and analysis method [4] etc. It takes RC 5 and AES to analyze their potential speedups and memory accessing characteristics. Foe secured messages joint channel coding & cryptography is used which is extension of soft input decryption with feedback. Recently, Bellare and Rogaway showed in the ideal cipher model, the triple encryption is more secure than single and double encryption.

II. RELATED WORK

In recent years, the research of sensor network has made a great progess.Song Ju [1] has found in his research work that some researchers believe that Public Key Cryptography(PKC) is not realizable(feasible) in Wireless Sensor Network(WSN) because of limitation of resource and battery power but still PKC is the main base of many security technology and application. But after that researchers found PKC is feasible to

WSN. In PKC, elliptic curve cryptography(ECC) [1],is the best choice due to its small size and fast computation, for example, to offer the same degree of security to 1024 bit RSA,there is only need 160 bit ECC.And then Song Ju proposed lightweight key establishment protocol based on ECC,this protocol combines Elliptic Curve Diffie-Hellmann(ECDH) with symmetric cryptography and hash chain, in this protocol an initial key as initial trust is used as symmetric cryptography which is vastly facilitate the protocol and is foundation to make it lightweight, there is also a node join scheme which support different size of network and flexible against the increase of network

Here initial key K_n is treated as initial trust and it is the last one of hash chain,K={K_1,K_2,K_3,…..K_n}, K_{i+1}=H(K_i), and H() is one way hash function. At the same time all nodes produces its own public key P_A and private key k_A. In figure 1. [2], two nodes will use their initial key to perform pairwise key establishment in following steps [2]:

1) Firstly divide nodes into two work mode i.e. old mode and new mode. All nodes broadcast their own message and receive other's broadcast messages.

2) Then assume A and B are nodes. In new mode, broadcast message is NEW ID_A E_K(ID_A P_A K_n).When node turns into old mode flag will be OLD.E_{Kn}(ID_A P_A K_n) means using AES to encrypt ID_A P_A K_n with K_n.

3) When node B receives A's message, receiver will use Kn to decrypt the E_{Kn}(ID_A P_A K_n).

4) At the same time B takes P_A and calculate P_{BA}(P_{BA}=P_A×k_B). According to assumption communication between nodes is symmetrical,so A can receives B's message and the pairwise key P_{AB}(P_{AB}=P_B×k_A)

5) So, here ECDH use for P_{AB}=P_{BA}, where G is the base point on elliptic curves.

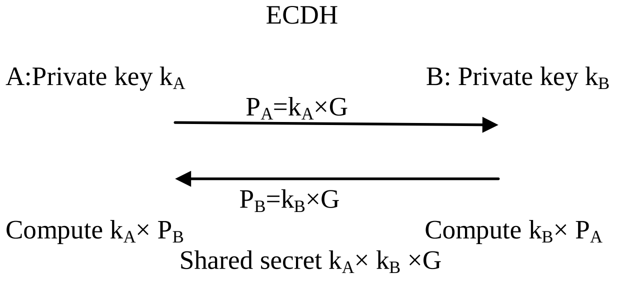

Figure1. Elliptical Curve diffie-Hellmann [2]

According to Pallavi V.Chavan and Dr Mohammad Atique.Hierarchical visual cryptography [2] is based upon the concept of visual cryptography. It encrypts the secret in number of levels. Firstly the secret is divided into exactly two shares called share 1 and share 2.Then each share is encrypted in the independently in four shares: share 11, share 12, share 21 and share 22 as shown in Figure 2. After these four shares any three shares are generates the key shares, the superimposition of key share with the remaining share reveals the secret information, the superimposition is logically performed by the X-OR operation [2]

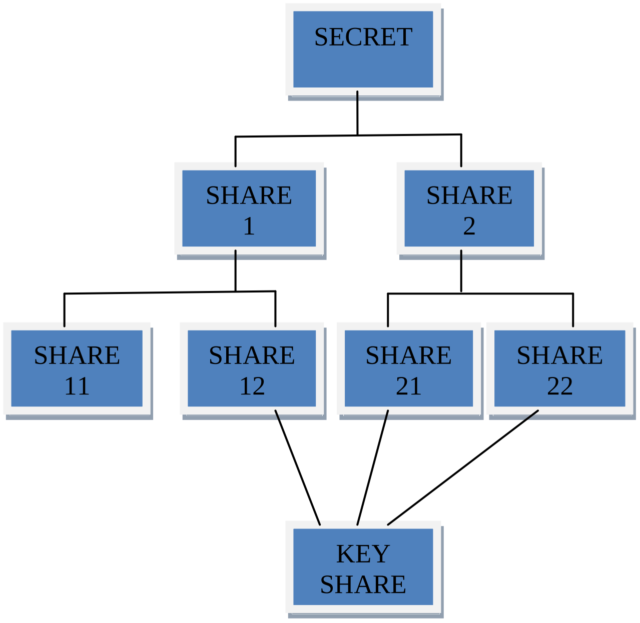

Figure 2. Concept of hierarchical visual cryptography [2]

In visual cryptography, each pixel information in original secret is represented by 4 pixels in shares and the pixel expansion ratio is 1:4. Size of original secret is n×m and size of shares become 2n×2m,it is a combination of black and white pixels which shown in figure 3.[2].

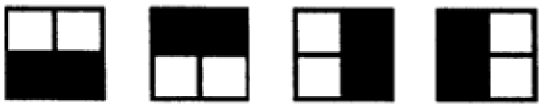

Figure 3. Encoding of Pixel [2]

METHODOLOGY FOR KEY SHARE GENERATION

- Share 1 and share 2 are inputs.
- Share 1 is encrypted in two shares S11& S12
- Share 2 is encrypted in two shares S21& S22
- S12, S21 & S22 are combined to form a key.

TABLE I. ENCODING OF PIXEL [2]

No	S12 Pixel	S21Pixel	S22Pixel	Encode
1	Black	Black	Black	Black
2	White	Black	Black	White
3	White	Black	White	White
4	Black	White	White	Black
5	Black	White	Black	Black
6	White	White	Black	White
7	Black	Black	White	Black
8	White	White	White	White

Ashwak M.AL Abiachi, Faudziah Ahmad, Ku Ruhana proposed model providing secure and flexible cryptography mechanism for analyzing and comparing different algorithm for the aim of enhancing the security during the encryption process. In block cipher cryptography mechanism managing the key sequentially encryption-secret- key, decryption-secret-key and shared-secret –key, these keys are working dependently for extracting and generating the content relation to manage later by the key manage that helps to communicate and share information.

Yaobin Wang, Hong An, Zhiqin Liu, Kang Xu, Wanli Dong [4] proposed how to accelerate block cryptography application in procedure level speculation mechanism which include the execution model, synchronization strategy. The inter –thread data dependence is the most critical TLS technical factors affecting the performance, in the data dependence violation, there are two terms “produce-distance” and “consume-distance”.

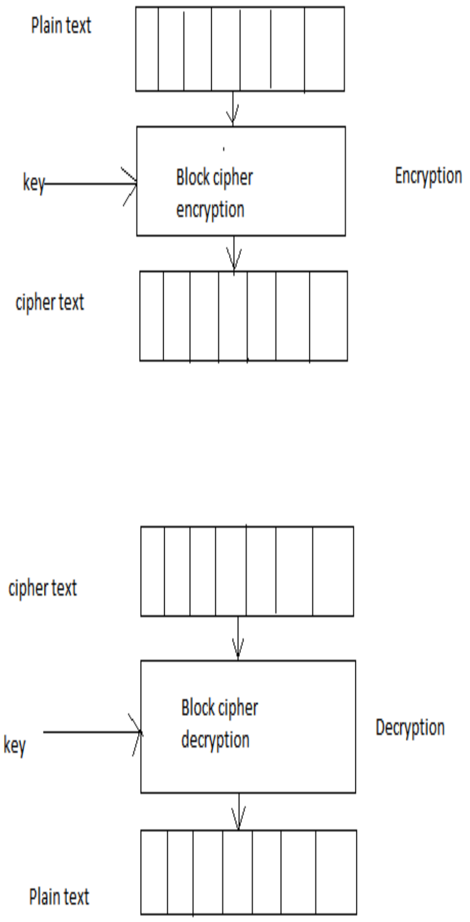

Fig.ure 4. Encryption and Decryption operations in block cipher algorithm [2]

- Produce-Distance: the instruction numbers from the beginning of the threads for the last write operation for a specific memory address [4].
- Consume-Distance: the instruction numbers from the beginning of the thread to the first read operation for a specific address [4].

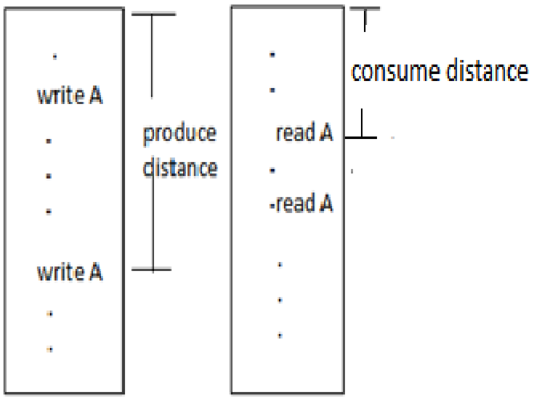

Figure 5. Produce distance and Consume distance [4]

For thread ‘i’ and its successor thread i+1, starting at the same time. If i thread takes more time for produce distance as compare to i+1 thread consume distance than the dependence violation under the assumption of all processors execute instructions at the same speed.

III. PROPOSED WORK

Quantum cryptography [5] is used to transmit and receive a photon between two parties only for communicating over relatively short distances (tens of kilometers), any farther, the photon signals become faded. Quantum is the standard cryptography in which keys are used to encrypt/unscramble message.Todays, the more popular algorithm is RSA algorithm for public key cryptography which is publicly available key that is the product of two large prime numbers and to create a gibberish –like cipher text, then combine a message with the public key. Once the message is encrypted and sent then second private key is applied to decipher the message.

TABLE II. POLARIZATION OF STATE [5]

No.	Polarization	Angle	State
1.	Rectilinear	$\Theta=0^0$ =state|0 >	+(0)=↔
		$\Theta=90^0$ =state| 0>	+(1)=↕
2.	Diagonal	$\Theta=45^0$ =state| 0>	× (0)=^{0}
		$\Theta=135^0$ =state|0>	× (1)=^{0}

It is difficult to derive the private key from the public one because its calculation could be a flaw in the long run. It is only secure if factoring is a hard problem [6] explains physicist Daniel Gottesman of the Perimeter Institute. That turns out to be very hard on a classical [6] computer, whereas a quantum computer could run new [5] kinds of algorithm that can efficiently factor large numbers. So if you had big quantum computers RSA [5] would not be secure.

In quantum cryptography, users communicate securely by generating and exchange a shared, secret key. This key is also known as ‘one time pad’ that used as only once and is as long as the message itself. This key opposes the relatively short 128 bit or 156 bit keys used in today’s system, if a message is encrypt with one time pad and send to another one receiver who used the same key to unscrambled this text.

The most common method of quantum aspect for generating and exchanges that key known as prepare and measure. If one user sends a photon of light to another user, in this case photon assumes as the number of states like different spins and polarization used for represent different bits. For bit 1 photon might stand with a vertical orientation, while the photon with horizontally oriented could correspond to 0. For example if Alice sends the message then he prepares each photon and collapsed it into a particular state then he send to Bob who attempts to measure the result.

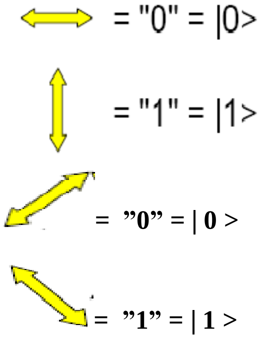

Fig.ure 6. Polarization of a states [5]

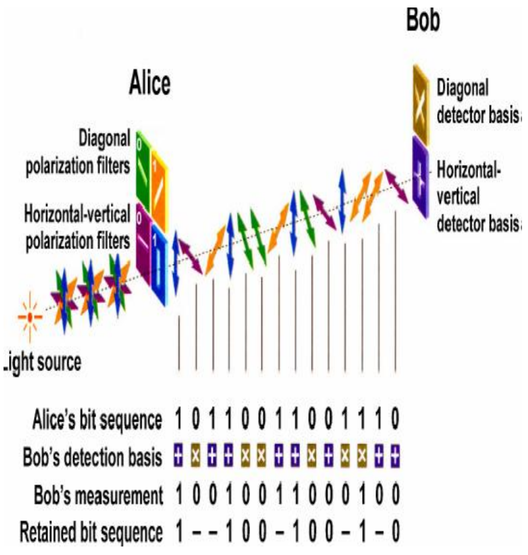
Bob
Alice
Diagonal detector basis
Horizontal-vertical detector basis
Diagonal polarization filters
Horizontal-vertical polarization filters
Light source
Alice's bit sequence 1 0 1 1 0 0 1 1 0 0 1 1 1 0
Bob's detection basis
Bob's measurement 1 0 0 1 0 0 1 1 0 0 0 1 0 0
Retained bit sequence 1 - - 1 0 0 - 1 0 0 - 1 - 0

Figure 7. Transmission of message in polarization form [5]

Each of them translates what both are seen into key bits and also compare their results. If any unauthorized access intercept the photon in route then Alice and Bob who send the message and also who receive will notice too many discrepancies and finally they conclude that their communication is insecure but if measurement match are often enough, then both are left it with matching string of random bits, in this case they used it as shared, secret key for encryption and decipher the message. Each of this photon is in a state which is denoted by four following

symbols [5] —, |, ⁄, \,.

According to quantum cryptography [5], the first

two photon states are emitted by a polarizer which is set with a Rectilinear orientation and the other two states are Emitted by a polarizer which is set with a diagonal orientation. For example:

+(0)= — , +(1)= | , x(0)= ⁄, x(1)= \

If Alice sends a random sequence of photons:

++xx++xxx++xx

The binary number represented by these states is 1110010110010

Now, if Bob wants to obtain a binary number [5] sent by Alice, he needs to receive each photon on the same basis as shown in figure 7 [5].

IV. COMPARISON

A comparison of popular encryption algorithms [7] based on block size, key size, number of rounds and attacks if occurred as shown on Table III [7].

TABLE III. COMPARISION OF ALGORITHM [7] [8] [9]

Algorithm	DES	AES	RSA
Block Size	64 bits	128bits	512bits
Key Size	56 bit	128,192,256 bit	1024 to 4096 bit
Created By	IBM in 1975	Joan Daeman in 1998	Rivest, Shamir and Adleman 1977
Algorithm Structure	Fiestel Network	Substitution Permutation Network	Recursively Defined Structure
Round	16	9,11,13	1
Attack	Brute Force Attack	Side Channel Attack	Subtle Attack

A. Data Encryption Standard (DES)

DES was the most widely used standard all across the world [7]. Block cipher encrypts 64 bit plaintext at a time and uses 56 bit key. This was based on symmetric key algorithm [7] which means that the same key will be used for both encryption and decryption. DES has 16 rounds which mean a total of 16 processing steps are being applied on the input plaintext to produce cipher text [7]. First, 64 bit data is passed through the initial permutation phase and then 16 rounds of processing takes place and finally the last step of final permutation is carried out on the input plain text which results in 64 bit cipher text. In DES there are only 2^{56} possible combinations which are quite easy to crack [7].

B. Advanced Encryption Standard (AES)

AES [7] is a variable bit block cipher and uses variable key length of 128, 192 and 256 bits [7]. If both the block length and key length are 128 bits, AES will perform 9 processing rounds. If the block and key are of 192 bits [7], AES performs 11 processing rounds. If the block and key are of length 256 bits then it performs 13 processing rounds [7].

C. Ron Rivest, Adi Shamir and Leonard Adleman (RSA)

RSA is a cryptosystem, which is known as one of the first practicable public-key cryptosystems and is widely used for secure data transmission. In such a cryptosystem, the encryption key is public and differs from the decryption key which is kept secret. In RSA, this asymmetry is based on the practical difficulty of factoring the product of two large prime numbers, the factoring problem.

V. CONCLUSION

We have analyzed some papers and found that Quantum cryptography is the best secure communication technology which is used for a short distance or point to point communication, when long term secrecy is essential. The successful hacks are not a proof that quantum cryptography itself [6] is flawed. This is a necessary step in the process to make the technology secure, Once the implementation loopholes are found and closed, then we have a really secure technology [6]. Quantum cryptography is going through this process right now [6].

References

[1] Song Ju, "A lightweight key establishment in wireless sensor network based on elliptic curve cryptography," in *Intelligent Control, Automatic Detection and High-End Equipment (ICADE),*

[2] P.V. Chavan and M. Atique, "Design of hierarchical visual cryptography," in *Engineering (NUiCONE), 2012 Nirm University International Conference on,Dec2012,pp.1-3.*

[3] A.M. Al-Abiachi, F. Ahmad, and K. Ruhana, "A Competitive Study of Cryptography Techniques over Block Cipher," in *Computer Modelling and Simulation (UKSim), 2011 UkSim 13th International Conference on*, March 2011, pp. 415-419.

[4] Yaobin Wang, Hong An, Zhiqin Liu, Kang Xu, and Wan Lin Dong, "Accelerating Block Cryptography Algorithms in Procedure Level Speculation," in *Computational Intelligence and Security (CIS), 2011 Seventh International Conference on*, Dec 2011, pp. 874-877.

[5] M.S. Sharbaf, "Quantum cryptography: An emerging technology in network security," in *Technologies for Homeland Security (HST),2011 IEEE International Conference on,Nov 2011,pp.13-19.*

[6] (2013) Communication ACM. [Online]. http://cacm.acm.org/magazines/2013/11/169023- future-

[7] Monika Agrawal and Pradeep Mishra, "A Comparative Survey on Symmetric Key Encryption Techniques," *International Journal on Computer Science and Engineering (IJCSE)*, vol. 4, pp. 877-882, May 2012.

[8] Prashant Singh Yadav, Pankaj Sharma, and K.P Yadav, "Implementation of RSA Algorithm using Elliptic curve algorithm for Security and Performance Enhancement," *International Journal of Scientific & Technology Research*, vol. 1, no. 4, pp. 102-105, may 2012.

[9] Isil Dillig, "Discrete Structures," *More on Cryptography and Mathematical Introduction,2012.*