FPGA - HARDWARE BASED DES & BLOWFISH SYMMETRIC CIPHER ALGORITHMS FOR ENCRYPTION & DECRYPTION OF SECURED WIRELESS DATA COMMUNICATION

[1] MR. C. R. PATEL, [2] PROF. N. B. GOHIL , [3] PROF. VANDANA SHAH

[1]M.E.[Electronics & Communication] Student, Department Of Electronics & Communication Engineering, Shantilal Shah Engineering College, Bhavnagar, Gujarat
[2] Asst.Professor, Department Of Electronics & Communication Engineering, Shantilal Shah Engineering College, Bhavnagar, Gujarat
[3] Asst.Professor, Department Of Electronics & Communication Engineering, Sarvajanik College Of Engineering & Technology, Surat, Gujarat

chirag_pro7@yahoo.com, icc_narendra@yahoo.co.in, vandshah@gmail.com

ABSTRACT: *Now a days internet and wireless networks growing rapidly, information and network security becomes a vital process to protect commerce secret and evaluation privacy. Earlier security was a major issue for military applications but now a days the area of communication applications has been enhanced since most of the communication takes place over the web. Hence, the principal goal of any encryption algorithm is to provide security against any unauthorized attacks as well as to make communication network smoother without any hurdle. In this paper, we demonstrated performance of the most communication network data encryption algorithms: DES and Blowfish in terms of speed and power consumption. In this paper, we also demonstrated simulation results of DES encryption and decryption algorithm in VHDL coding with the help of Xilinx 9.2i ise and practical implementation of DES encryption and decryption algorithm in System C coding on FPGA - Spartan 3 XC3S200 with the help of Xilinx Platform Studio. We have also practically implemented Blowfish encryption and decryption algorithm in System C coding on FPGA - Spartan 3 XC3S200 with the help of Xilinx Platform Studio. We could also show that Blowfish encryption and decryption algorithm simulation results in VHDL coding with the help of Xilinx 9.2i ise in future. The study of DES and Blowfish algorithms shows that Blowfish algorithm runs faster than DES algorithm and the power consumption is almost same.*

JIKRECE

Keywords— Encryption Algorithm, Decryption Algorithm, DES, Blowfish, Cryptography, Performance Evaluation.

I: INTRODUCTION

In recent years, there emerged a lot of communication and networking applications based on internet such as on line shopping, stock trading, web based banking, e-commerce, m-commerce and electronic bill payment. Such a confidential transactions over wired or wireless public networks demand end to end secure connections to ensure data authentication, privacy, integrity, non repudiation, access control and confidentiality[1].

Cryptography converts the original message in to the non readable format and sends the message over an insecure noisy channel. The attacker who are unauthorized to read the message try to break the non readable message but it is almost hard to do it so. Only the authorized person has the capability to convert the non readable message to readable one.

Data Encryption algorithm plays an important role for information security guarantee. Encryption is the process of transforming the plaintext data into the cipher text in order to conceal its meaning and so preventing any unauthorized recipient from retrieving the original data means forming highly secured data communication networks. The main task of encryption is to ensure secrecy as well as privacy, data authentication, integrity and non repudiation. Companies usually encrypt their data before transmission to ensure that the data is secure during transit. The encrypted data is sent over the public network and is decrypted by the intended recipient only and by other it will be the garbage data.

A. *Classification Of Cryptography:*

Encryption algorithms can be classified into two broad categories - Symmetric key encryption and Asymmetric key encryption.

1. Symmetric Key Encryption:

   Symmetric key encryption may also be referred to as *shared key* or *shared secret* encryption.

   In symmetric key cryptography, the key used for encryption is similar to the key used in decryption. Hence, the key distribution has to be made prior to the transmission of information. The key plays a very important role in symmetric key cryptography since their security directly depends on the nature of the key i.e. key length etc. There are various symmetric key encryption algorithms such as DES, 3DES, AES, RC4, RC6, UMARAM, UR5 and BLOWFISH. 3DES and AES are commonly used in IPsec and other types of VPNs. RC4 has seen wide deployment on wireless networks as the base encryption used by WEP and WPA version 1.

Symmetric key encryption algorithms can be extremely fast and their relatively low complexity allows for easy implementation in hardware. However, the requirement is that all the hosts participating in the encryption process have already been configured with the secret key through some external means.

2. Asymmetric Key Encryption:

Asymmetric key encryption is also known as public-key encryption. In asymmetric key encryption, two different keys are used for encryption and decryption public key and private key. The public key is meant for general use so it is available to anyone on the network. Anyone who wants to encrypt the plaintext should know the public key of receiver. Only the authorized person can be able to decrypt the cipher text through his own private key. Private Key is kept secret from the outside world. The most common asymmetric key encryption algorithms are RSA and digital signature.

For example, user A wants to send message to user B, the following steps are involved,

- User A and user B should know public key of each other but private keys are kept secret.
- User A encrypts a plain text message for user B by using B’s public key.
- User A transmits the encrypted message (cipher text) to user B.
- User B receives the cipher text and decrypts it using its own private key.
- User B gets the original plain text message .

As compared to symmetric key encryption, asymmetric key encryption imposes a high computational burden and tends to be much slower. Thus, it isn't typically used to protect payload data. Instead, its major strength is its ability to establish a secure channel over a non secure medium (e.g. internet). This is accomplished by the exchange of public keys, which can only be used to encrypt data. The complementary private key, which is never shared, is used to decrypt the data. Public key encryption is based on mathematical functions, and is not very efficient for small mobile devices.

B. *Objectives Of Cryptography:*

Cryptography provides a number of security objectives to ensure the privacy of data, non alteration of data and many more. Following are the various objectives of cryptography for it’s increasing demand now a days[12],

- Confidentiality: Information in computer is transmitted and has to be accessed only by the authorized party and not by anyone else.
- Authentication: The information received by any system has to check the identity of the sender that whether the information is arriving from a authorized person or a false identity.
- Integrity: Only the authorized party is allowed to modify the transmitted information. No one in between the sender and receiver are allowed to alter the given message.
- Non Repudiation: Ensures that neither the sender, nor the receiver of message should be able to deny the transmission.
- Access Control: Only the authorized parties are able to access the given information.

As we know that high security is the basic requirement of data encryption algorithm whereas the encryption algorithms are known to be computationally intensive. They consume a significant amount of computing resources such as CPU time, memory, and battery power. Especially for a wireless devices, usually with very limited resources (e.g. battery) is subject to the problem of energy consumption due to encryption algorithms. Therefore, it is essential to evaluate the performance of encryption algorithms so as to ensure various applications. Elminaam et al. and Nadeem et al. proposed a performance evaluation of the most common encryption algorithms: AES (Rijndael), DES, 3DES, RC2, Blowfish, and RC6. They gave a comparison for those encryption algorithms at different settings such as different sizes of data blocks, different data types, battery power consumption, different key size and finally encryption/decryption speed[2, 4]. Prasithsangaree and Krishnamurthy evaluated the energy consumption of AES and RC4, which are commonly used in WLANs. They show that RC4 is more suitable for large packets and AES for small packets [3]. Wander et al. quantified the energy cost of authentication and key exchange based on two public-key cryptographies: RSA and Elliptic Curve Cryptography (ECC)[5]. Karri et.al identified the various sources of energy consumption during the setup, operation and tear down of a secure wireless session. Furthermore, they developed techniques based on compression, protocol optimization and hardware acceleration to reduce the energy consumed[1].

DES and Blowfish are extensively used for security of communication system network like wireless network, portable terminal etc.

In this paper, we firstly study the basic algorithms of common DES and Blowfish. Both of them are block ciphered symmetric key encryption algorithms block. Referencing the encryption process methods, we analyse their security. We give a comprehensive performance evaluation which includes three aspects: security analysis, encryption speed, and power

JIKRECE

consumption.

The remainder of this paper is organized as follows. We review the two encryption algorithms: DES and Blowfish and analyse their security in section 2. We introduce the evaluation method in section 3 and hardware and software requirement in section 4. Finally we show VHDL simulation results and System C practical implementation results on FPGA for DES and System C practical implementation results on FPGA for Blowfish in section 5, followed by conclusion & future work in section 6.

II: DES AND BLOWFISH ENCRYPTION ALGORITHMS DESCRIPTION

In this section, we have study an overview for both common DES and Blowfish algorithms follows security analysis for both of them.

A. *DES Algorithm*

DES was the first encryption standard to be recommended by NIST (National Institute of Standards and Technology). It was developed by an IBM team around 1974 and adopted as a national standard in 1997 [7]. The flow of DES algorithm is shown in Fig.1. DES is a 64 bit block cipher uses 56 bit key. The algorithm processes with an initial permutation, sixteen rounds block cipher and a final permutation. DES application is very popular in commercial, military, and other domains in the last decades. There are variants like 3DES [8], AES [9] by enhancing DES function[11].

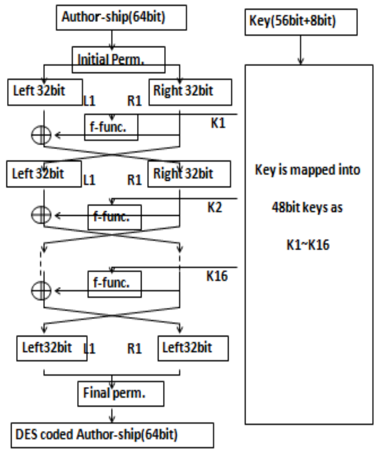


Fig.1 DES Algorithm

B. *Blowfish Algorithm*

Bruce Schneier, one of the world's leading cryptologists, designed the Blowfish algorithm [10] and made it available in the public domain. Blowfish is a variable length key from 32 bits to 448 bits, 64 bit block cipher. The algorithm was first introduce in 1993, and has not been cracked yet. It can be optimized in hardware applications due to its compactness.

The flow of Blowfish algorithm is shown in Fig.2. It consists of two parts: 1. key expansion part and 2. Data encryption part. Key expansion converts a key of at most 32 to 448 bits into several sub key arrays totalling 4168 bytes. Data encryption occurs via a 16 round (commonly) network. Each round consists of a key dependent permutation, and a key and data dependent substitution. All operations are XORs and additions on 32 bit words. The only additional operations are four indexed array data look ups per round[11].

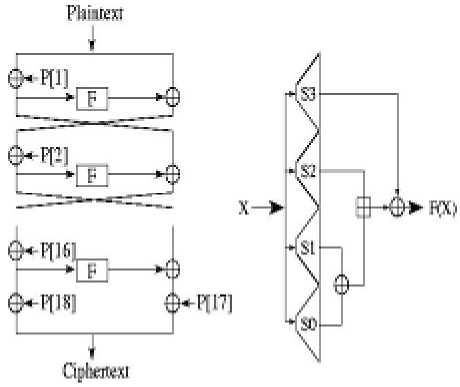


Fig.2 Blowfish Algorithm

C. *Security Analysis*

In this section, we analyse the algorithms strength against attacks from two aspects: differential cryptanalysis and linear cryptanalysis.

Eli Biham and Adi Shamir introduced differential cryptanalysis in 1990. They found a chosen plaintext attack against DES which was more efficient than brute force. The best attack against full 16 round DES requires 247 chosen plaintexts. This can be converted to a known plaintext attack, but requires 255 known plaintexts. And 237 DES operations are required during analysis. The attack is heavily dependent on the structure of the S-boxes which happen to be optimized against differential cryptanalysis in DES. In addition, the resistance of DES can be improved by increasing the number of rounds [13].

Linear cryptanalysis is another type of cryptanalytic attack invented by Mitsuru Matsui. The attack uses linear approximations to describe the action of a block cipher [14]. Against full 16 round DES, this attack can recover the key with an average of 243 known plaintexts. A software implementation of this attack recovered a DES key in 50 days using 12 HP9000/735 workstations which is the most effective attack so far [15]. Linear cryptanalysis is newer than differential cryptanalysis and it is efficient against reduced round DES variants.

From above analysis, DES can provide a certain security guarantee in some degree by optimizing the construction of S-boxes.

Bruce Schneier show differential cryptanalysis on Blowfish is possible either against a reduced number of rounds or with the piece of information which describes the F function. However, the boxes are well designed to resist to an attacks while they are randomly generated in Blowfish [16]. As we know, there is no successful cryptanalysis against Blowfish.

III: EVALUATION METHOD

Any Encryption algorithm plays a vital role in network information and communication security. It is essential to evaluate the performance of encryption algorithms in terms of security analysis, encryption speed, power consumption etc. We already analysed the differential cryptanalysis and linear cryptanalysis resistance for both DES and Blowfish algorithms in section 2. In this section, we study evaluation method for encryption speed and power consumption of the DES and Blowfish algorithms.

A. Encryption Speed Evaluation

Encryption algorithms are known computationally intensive, hence the encryption speed is considered as an important factor of the encryption performance. The encryption speed is considered the computation measures that an encryption algorithm employed to produce a cipher text from a given plaintext. Encryption speed is used to measure the throughput per unit time of an encryption scheme. The encryption speed is calculated as the total plaintext in bytes divided by the encryption time in BPS. The main task for encryption speed evaluation is to observe the performed encryption time for certain plaintext. In general the decryption speed can be considered the same as encryption speed. Based on this terminology, we only choose encryption speed for the algorithm performance evaluation in this work[11].

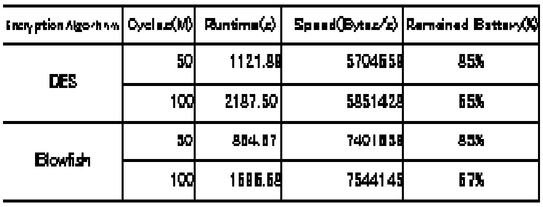
B. Power Consumption Evaluation

Energy consumption is another important performance factor of cipher, especially for application of portable wireless devices. Energy consumption has been extensively studied in previous task. An evaluation for power consumption of an Itsy pocket computer has been conducted in [17]. The study is only intended to evaluate power consumption of different parts of the pocket computer under normal operations. Another research about computational complexity of public key encryption has been studied on an embedded processor in [5]. The work quantified the energy cost of authentication and key exchange based on public key cryptography on an 8 bit microcontroller platform. They showed the efficiency in their experimental results. They showed ECC to have a significant advantage over RSA as it reduces computation time and also the amount of data transmitted and stored.

In this work, we implement the encryption operation repeatedly for millions of times on a laptop without impressing power supply. We calculate encryption speed and power consumption by observing encryption run time and the remained battery power percentage after the encryption process[11].

Prasithsangaree et.al has studied the distribution of packet sizes of packets typically transmitted and received by a wireless device over a wireless LAN. They used a wireless sniffer to capture 802.11 network packets over one hour and obtained their packet size distribution. It is shown that most of packets have a small size between 64 to 127 bytes [3]. In order to evaluate the performance in wireless network application for both algorithms, we randomly generated plaintext in 128 byte size block for the experiment. We implemented the program on the laptop without impressing power supply for millions of times to obtain the encryption speed and power consumption. The experimental result is shown in Table 1[11].

Table 1 Performance Of DES And Blowfish Algorithms



Encryption Algorithm	Cycles(M)	Runtime(s)	Speed(Bytes/s)	Remained Battery(%)
DES	50	1121.88	5704658	85%
	100	2187.50	5851428	65%
Blowfish	50	864.87	7401838	85%
	100	1686.69	7544145	67%

As per the above table, Blowfish run faster than DES, about 7.4~7.5 Mbytes per second to 5.7~5.8 Mbytes per second. The remained battery percentage of Blowfish and DES was almost the same, 15% for 50M cycles and about 35% for 100M cycles. Hence it is proved that Blowfish encryption algorithm may be more suitable for wireless network application which exchanges small size packets[11].

IV: SOFTWARE AND HARDWARE REQUIREMENT

In order to simulate DES on laptop, We have used Xilinx 9.2i ise software in Windows 8 32 bit Operating System and VHDL Coding Language for simulation purpose. The test platform is Sony Vaio Laptop with Intel Core i5-2430M Processor 2.40 GHz and 4 GB Memory.

In order to practically implement DES and Blowfish on FPGA, We have used Xilinx Platform Studio software in Windows XP 32 bit operating system and System C Coding Language for implementation purpose. The test platform is HP Desktop with Intel Core 2 Duo Processor 2.40 GHz, 4 GB Memory and FPGA - Spartan 3 XC3S200 Kit.

V: EXPERIMENTAL RESULTS

The experimental results of DES are of two types: A. VHDL Simulation Results and B. System C Practical Implementation Results on FPGA.

A. VHDL Simulation Results Of DES:

Fig.3 shows DES encryption Results to generate cipher text(encrypted data).

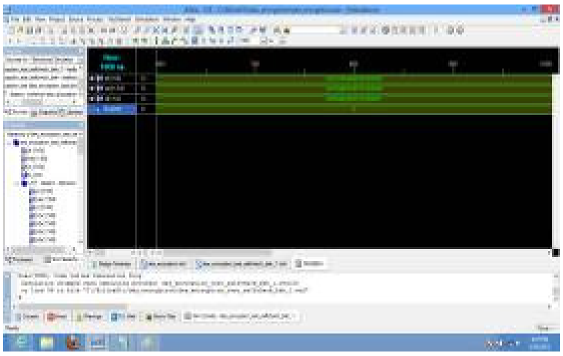


Fig.3 DES Encryption

Fig.4 shows DES decryption results to generate plain text(original data).

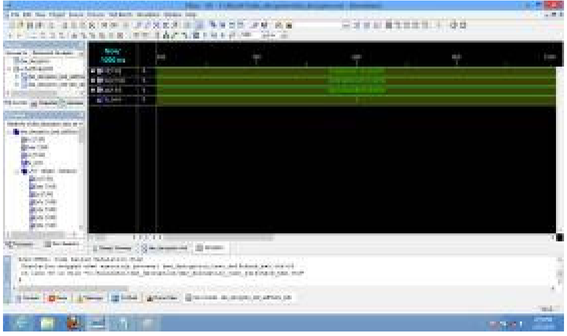
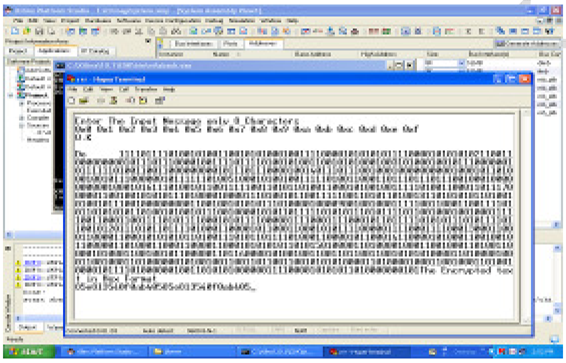


Fig. 4 DES Decryption

B. System C Practical Implementation Results Of DES And Blowfish On FPGA:

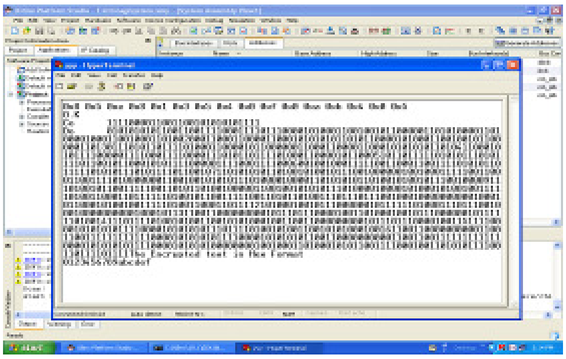
Fig. 5 shows DES encryption practical implementation results on FPGA to generate cipher text.



```
Enter The Input Message only 8 Characters
```

Fig.5 DES Encryption

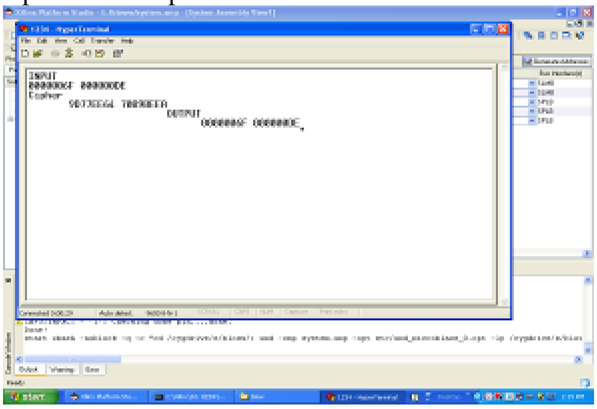
Fig. 6 shows DES decryption practical implementation results on FPGA to generate plain text.



```
The Encrypted text is Hex Format
0123456789abcdef
```

Fig. 6 DES Decryption

Fig. 7 shows Blowfish encryption and decryption practical implementation results on FPGA to generate cipher text and plain text.



```
INPUT
0000006F 000000DE
Cipher
        9D73EE64 780987FA
                        OUTPUT
                              0000006F 000000DE
```

Fig. 7 Blowfish Encryption and Decryption

VI: CONCLUSION AND FUTURE WORK

Encryption algorithm plays a vital role for information security guarantee in recent growing internet and communication network applications. In this paper, we studied two symmetric key encryption algorithms: DES and Blowfish. We evaluated encryption speed and power consumption for their performance. Here, We have simulated DES for encryption and decryption with the help of VHDL coding as well as practically implemented DES and Blowfish on FPGA Spartan 3 XC3S200 for encryption and decryption with the help of System C coding.

In our future research, we are going to simulate Blowfish encryption and decryption algorithm using VHDL coding. Finally, we are planning to compare performance measures of both algorithms DES and Blowfish in terms of encryption speed and power consumption for wireless communication applications.

REFERENCES

[1] Karri, R. and Mishra, "Minimizing the secure wireless session energy," Journal of Mobile Network and Applications (MONET) 8, 2 (April), pp. 177-185.

[2] Diaa Salama Abdul. Elminaam, Hatem Mohamed Abdul Kader and Mohie Mohamed Hadhoud3, "Performance Evaluation of Symmetric Encryption Algorithms," in IJCSNS International Journal of Computer Science and Network Security, vol.8 No.12, December 2008, pp. 280-286.

[3] P. Prasithsangaree and P. Krishnamurthy, "Analysis of Energy Consumption of RC4 and AES Algorithms in Wireless LANs," Globecom 2003, pp. 1445 – 1449.

[4] Nadeem, A. and Javed, M.Y., "A Performance Comparison of Data Encryption Algorithms," IEEE Information and Communication Technologies, 2005. ICICT 2005. First International Conference, February, 2006, pp. 84- 89.

[5] A. Wander, N. Gura, H. Eberle, V. Gupta, and

S. Chang, .Energy analysis for public-key cryptography for wireless sensor networks,. In IEEE PerCom'05, Pisa, Italy, Mar. 2005.

[6] Bruce Schneier. Applied Cryptography: Protocols, Algorithms, and Source Code in C. John Wiley & Sons, 2nd edition, 1995.

[7] "Data Encryption Standard," Federal Information Processing Standards Publication No. 46, National Bureau of Standards, January 15, 1977.

[8] William C. Barker, "Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher," NIST Special Publication 800-67 Version 1.1, May 2008.

[9] Daemen, J., and Rijmen, V. "Rijndael: The Advanced Encryption Standard." D r. Dobb's Journal, March 2001, pp. 137-139.

[10] Bruce Schneier. The Blowfish Encryption Algorithm Retrieved October 25, 2008, http://www.schneier.com/blowfish.html

[11] Tingyuan Nie, Chuanwang Song, Xulong Zhi, Communication and Electronic Engineering Institute Qingdao Technological University, Qingdao, China - **''Performance Evaluation Of DES And Blowfish Algorithms'',** Supported by Shandong Province Natural Science Foundation (ZR2009GL007) & A Project of Shandong Province Higher Educational Science and Technology Program (J09LG10).

[12] O.P Verma, Ritu Agarwal, Dhiraj Dafouti and Shobha Tyagi, "Peformance Analysis Of Data Encryption Algorithms",IEEE Delhi Technological University India, 2011.

[13] E. Biham and A. Shamir, "Differential Cryptanalysis of the Full 16- Round DES," Advances in Cryptology-CRYPTO '92 Proceedings, Springer-Verlag, 1993, pp. 487-496.

[14] M. Matsui, "Linear Cryptanalysis Method for DES Cipher," Advances in Cryptology-EUROCRYPT '93 Proceedings, Springer-Verlag, 1994, pp. 386-397.

[15] M. Matsui, "The First Experimental Cryptanalysis of the Data Encryption Standard," Advances in Cryptology-CRYPTO '94 Proceedings, Springer-Verlag, 1994, pp. 1-11.

[16] S. Vaudenay, "On the Weak Keys in Blowfish," Fast Software Encryption, Third International Workshop Proceedings, Springer-Verlag, 1996, pp. 27-32.

[17] M.A. Viredaz and D.A. Wallach, "Power Evaluation of a Handheld Computer: A Case Study," WRL Research Report, 2001/1.

[18] P. Ruangchaijatupon, P. Krishnamurthy, "Encryption and Power Consumption in Wireless LANs-N,'' The Third IEEE Workshop on Wireless LANs - September 27-28, 2001- Newton, Massachusetts.

[19] http://www.xilinx.com, Fundamentals to FPGA Design.

[20]http://www.xilinx.com/itp/xilinx9/books/docs/xst/xst.pdf, ISE User Guide.

JIKRECE