Wireless Secured Data Transmission using Cryptographic Techniques through FPGA

I.Rama Satya Nageswara Rao *[1], B.Murali Krishna[2], Syed Shameem[3]
Habibullah Khan[4] , G.L.Madhumati[5]

[*1] PG Student Department of ECE in K.L.University Green fields-522502, AP, India
irsnrao435@gmail.com
[2] Assistant Professor Department of ECE in K.L.University Green fields-522502, AP, India
muralikrishna@kluniversity.in
[3] Associate Professor Department of ECE in K.L.University Green fields-522502, AP, India
shameemsyed@kluniversity.in
[4]Professor & Dean (SA), Department of ECE, KL University Green fields-522502, AP, India
[5]Professor & Head, Department of ECE, DIET Vijayawada - 521139; AP, India

Abstract— The need to protect the data disturbances and unauthorized access in communication has led to development of several cryptographic algorithms. Current issue in modern world as popularity of internet, e-commerce and communication technologies has emerging and they became the medium to security threats. Due to advancement in cryptographic techniques the DNA technique is a new crypto algorithm to encrypt and decrypt data. It consists of two stage encryption based on DNA sequence enhances the data security compared to conventional methods. In encryption process the former stage will encrypt the data (plain text) with a random key generated by random DNA sequence generator. Latter and final stage the encrypted data is re-encrypted with DNA translation to generate cipher. The cryptographic techniques (symmetric algorithm) is designed and simulated using Xilinx ISE and targeted on Spartan-3E FPGA interfaced with ZigBee for wireless communication.

Keyword- encryption, decryption, Spartan-3E FPGA, DNA sequence, ZigBee.

I. INTRODUCTION

Security is essential factor during communication among the people and in e-commerce for the internet user applications such as private communication, password protection and secured e-commerce [1]. The need of secure communication i.e., with Cryptography techniques provides high security like internet banking, ATM's and Satellite transmission etc. Cryptography concept provides the security to store secret and sensitive data, to transmit to receiver by sender and vice versa .Cryptography is the concept of mixing the complex mathematics and logical functions for the process of encryption and decryption of the message. The degree of security is dependent on the key and strength of the algorithm which are used to encrypt and decrypt the plaintext (message).the cryptography is classified into mainly two types and they are based on the key. Two types of cryptography namely secret (symmetric) and public (asymmetric) key cryptography and the following Fig1 shows the classification

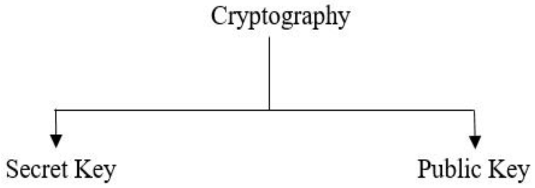


Fig1: Classification of Cryptography

A. *Secret key Cryptography*: in this process we use same key to encrypt and decrypt data of the message i.e., the symmetric key hence it is also termed as symmetric key cryptography.

B. *Public key Cryptography*: in this process we use different keys for encrypt and decrypt data of the message i.e., the asymmetric key hence it is also termed as asymmetric key cryptography.

Among the both cryptography techniques secret key cryptography is the widely used technique due its implementation and other factors comparing to public key cryptography. Present day scenario Cryptography plays a major role in providing security for at most people in the world who are using internet and online shopping etc. the main issue comes is the security at payment gateway communication between online transaction and banking sites. A Field Programmable (FPGA) is reprogrammable logic device which can act as alternative to ASIC's. For developing and acquiring algorithm in VLSI we use Verilog HDL and for simulation purpose ISE simulator. The FPGA is to act as the security provider as main processes like the encryption and decryption are done in FPGA.

The following sections will discuss the concepts of purpose of the cryptography, about the uses and applications of FPGA, concepts of the ZigBee and its features, DNA cryptography and process of implementation cryptography technique, simulation results and finally the conclusion.

II. PURPOSE OF CRYPTOGRAPHY

Each security system should provide package of functions which can guarantee the data secrecy of the system [2].

- Confidentially: making the transmitted data is accessible to particular or targeted authorized receiver
- Authentication: assured and correctly identifying the message origin without false.
- Integrity: making modifications to data received or transmitted is applicable to authorized users.
- Non Repudiation: making the sender and receiver of the message not able to deny the communication.
- Access Control: making the access to particular and authorized users only.
- Availability: making assets like computer system are accessible to authorized users when needed.

III. FPGA

ASICs offer significant in size (transistors count), complicatedness and realization , design of an ASIC is time exhausting and costly mechanism, and the main deprivation is that finishing design may be " frozen in silicon " which cannot be altered and we have to create a different variant of equipment or device [3]. Need of new devices that functionality can be customized(PLDs) and should offer flexibility to implement extremely extensive and convoluted functions (ASICs) by providing thousands of logic gates and be used they are FPGAs and take up intermediate field ground between ASICs and PLDs. FPGAs offers " Fred-in-the-shed " operations process i.e., it allows individual and small organizations of engineers to implement their design concepts (hardware and software concepts) on an FPGA-based test platform which reduces the nonrecurring engineering (NRE)costs beyond the having to provoke the excessive non-recurring engineering (NRE) expenditures or less tool sets compared to ASIC architectures.

A. Application of FPGA:

During the middle of 1980s the first family of FPGAs were arrived and they mainly used to work out the medium complex state machines, adhesive logics and limited data processing functions. After the decade the FPGAs erudition and size started to take impact and targeted to great markets at that time like telecommunication and networking which both of them are mainly operated on data processing.

The advancement the FPGA technology they come to consumer, industrial and automotive applications. These are often prototyped for designs of ASIC to construct hardware stage to study the physical workout of new approaches and algorithms. These find way to final products as their development cost and time to market are low compared ASICs.

The present FPGA technology has been advanced and provides millions of gates to implement the complex functions and high performance. The present day trend in FPGAs is that they can be able to implement cores of embedded microprocessor, high speed IO devices and any devices like SDR, communication and DSP related applications and these leads to form SOC components which has both hardware and software.

IV. ZIGBEE

Present day wireless technology has developed rapidly and technology progression in electromechanical systems has assimilation with RF capability, signal processing and sensing. All types of small applications are able to communicate wirelessly. The main moto of wireless communication is to collect information from nodes or to execute task [4]. A sensor node consists of three c's they namely Communication, Computation and Collection blocks. The main causes to use ZigBee are as follows

- Massive number of nodes.
- Simple to expand
- Consumes low power
- Provides security
- Cheaper cost
- Globally usable

ZigBee is the most utilized WSN standard technology with low power and data rate, cheaper price easy to develop and distribute and offers the rich preservation and high data authenticity. Name ZigBee is derived from zigzag patterns followed by bees in blossom, acts as the connection in a mesh organization among nodes [5].

V. DNA CRYPTOGRAPHY

DNA cryptography (Deoxyribonucleic Acid) is the upcoming and emerging field with research in computational DNA. Due to its energy efficiency, information density and especially its massive parallelism the DNA was studied for information sciences. It provides different advantages of its features DNA cryptography plays a vital role in the future cryptography techniques. The symmetric cryptosystems like DES, AES and etc. are can be broken when the use of quantum computers came into existence. DNA cryptography is more likely to replace the former techniques [6].The main reason behind the DNA computing is that the it can be used to direct Hamiltonian path issue which is demonstrated by Ad leman [7] has been the first step to DNA in information era. Later this concept is used by Lipton and extended to solve NP-complete problem [8].The main concept behind the DNA cryptography is its computing and two stage encryption process. In general the binary coding for digital applications which represents the data in two states 1 or 0 and a sequence of 1 and 0.in DNA cryptography, the DNA consists of mainly four bases and they are Adenine, Cytosine, Guanine and Thymine in DNA sequence and these represented by first letter of their name i.e., A, C, G and T respectively. These bases are represented in digital coding form as shown in the following table1.

TABLE1: DNA NUCLEOTIDE BASES

NUCLEOTIDES	BINARY	HEXA
A	00	0
C	01	1
G	10	2
T	11	3

The main advantages of binary digital coding of sequenced DNA are

- Improved coding efficiency.
- Convenient for logical and mathematical operation.
- Adapted to present computers and provides direct conversion between biological and encryption information
- It can be used to pre-process the plaintext. [9]

The DNA cryptography mainly consists of three basic processes. They are mainly

1) Encryption

2) Key Encryption Decryption

3) Decryption

In the DNA cryptography both the cipher text and key are send to the receiver by the sender and these two thing s are encrypted by DNA cryptography technique and send through secured channel [10]. The main thing in this cryptography is that it sends both the cipher text and key in the encrypted form i.e., in DNA sequence form. Now we will discuss each one in detail in the remaining session of DNA cryptography.

A. DNA encryption

The DNA encryption process is two staged encryption process in which first stage is Xored with operation between the plain text and the randomly generated key (OTP) and then encrypted data in the first stage is re-encrypted based on the DNA bases . The flow diagram for the encryption process is as shown in the following Fig2.

The encrypted message of the encryption process is encrypted to DNA sequence ACGT by the following encryption process based on the hiding the message in ATCG bases for the corresponding alphabets based on the table2.

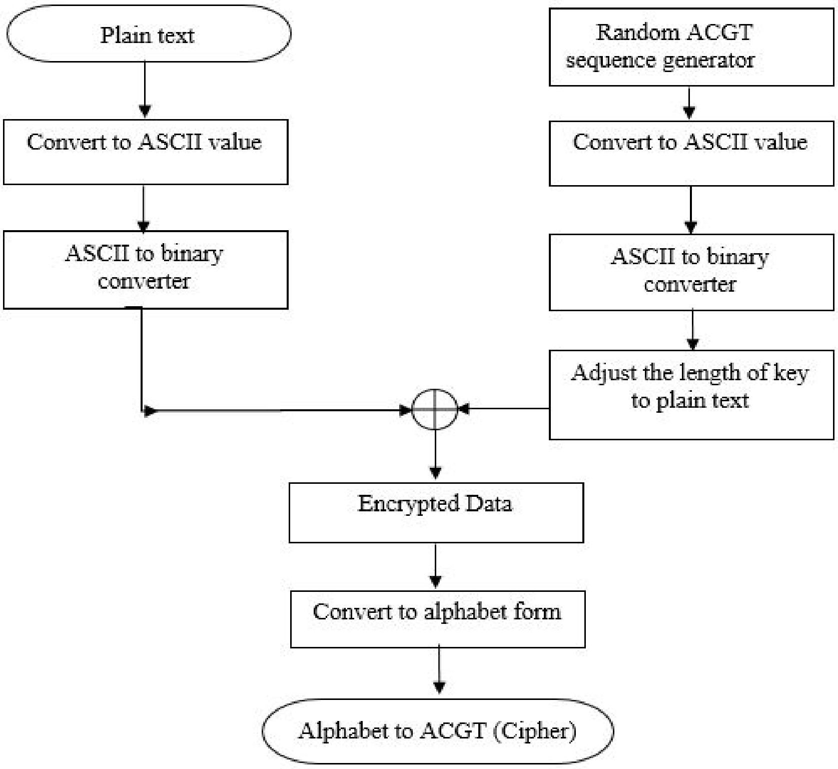

Plain text
Convert to ASCII value
ASCII to binary converter
Random ACGT sequence generator
Convert to ASCII value
ASCII to binary converter
Adjust the length of key to plain text
Encrypted Data
Convert to alphabet form
Alphabet to ACGT (Cipher)

Fig2: DNA Encryption Process

The data hiding of the plaintext in the DNA sequence is done by representing the alphanumeric and punctuations into the DNA bases i.e. nucleotides A, C, G and T. the DNA nucleotide sequence for the alpha numeric and punctuations is as follows

TABLE2: DNA BASES FOR ALPHA NUMERIC AND PUNCTUATIONS

A=CGA	H=CGC	O=GGC	V=CCT	2=TAG	9=GCG
B=CGA	I=ATG	P=GGA	W=CCG	3=GCA	.=ATA
C=GTT	J=AGT	Q=AAC	X=CTA	4=GAG	,=TCG
D=TTG	K=AAG	R=TCA	Y=AAA	5=AGA	*=GAT
E=GGT	L=TGC	S=ACG	Z=AAT	6=GGG	:=GCT
F=ACT	M=TCC	T=TTC	0=TTA	7=ACA	;=ATT
G=TTT	N=TCT	U=CTG	1=ACC	8=AGG	-=ATC

B. Key Encryption

The main part in the DNA cryptography is that key generation and encryption of the key. Primarily the key is generated randomly the ACGT sequence and this sequence is converted into binary format and the key is adjusted to the length of the plaintext for the first stage of encryption process. This key is get transferred to the receiver by encrypting the key by the process as shown in the following Fig3.

First the length of the is calculated in order to create dummy key for the encryption process of the key the dummy key creation is shown in the Fig 3. At this stage also the encryption process is done in two phases, first phase encryption is done by XOR operation between the original key and dummy key. The encrypted key which we got in the above is again converted to the DNA sequence by using the table2.

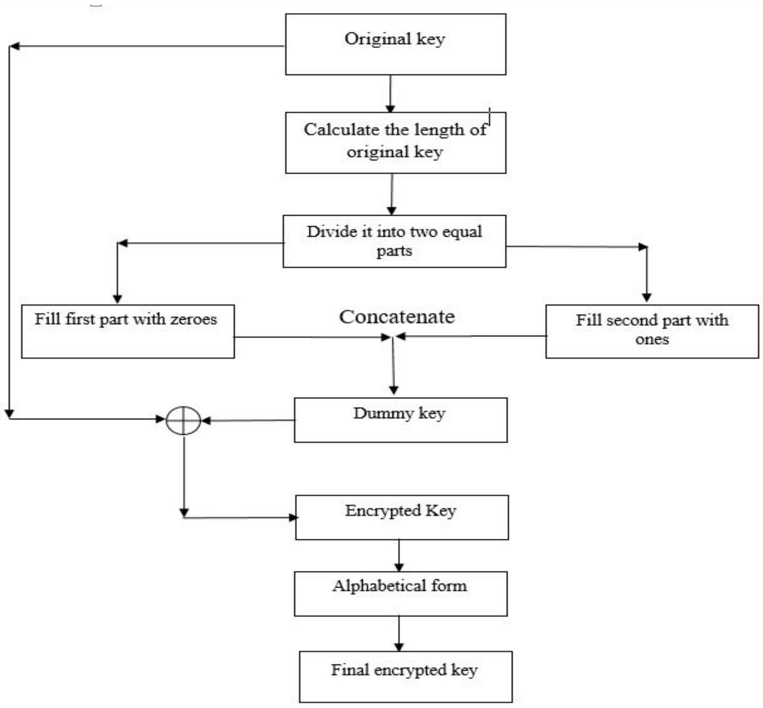

Original key
Calculate the length of original key
Divide it into two equal parts
Fill first part with zeroes
Concatenate
Fill second part with ones
Dummy key
Encrypted Key
Alphabetical form
Final encrypted key

Fig3: DNA Key Encryption Process

C. *DNA Decryption*

In the decryption process the reverse encryption process will be done .The received DNA (ACGT) sequence is converted to the alphabetical form and to required binary format. The received key is also to be is get decrypted in the same by using the table and dummy key for the original key. The original key is then Xored with data by the process of decryption. The decryption process and procedure can be followed is as shown in the Fig4.

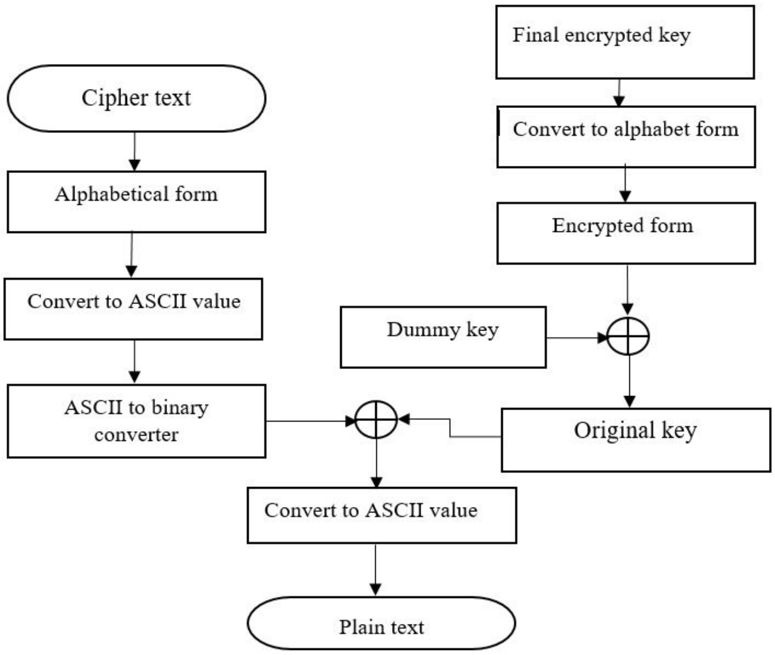
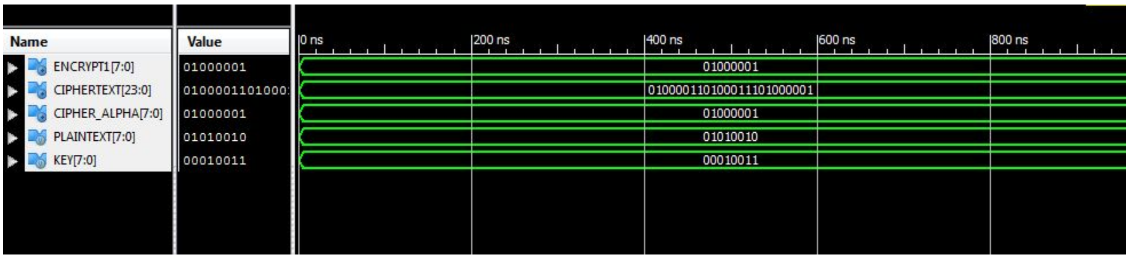


Fig4: DNA Decryption Process

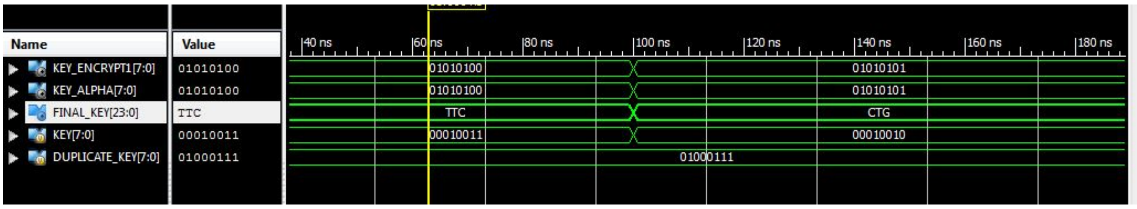
VI. SIMULATION RESULTS

The simulation results for the encryption, decryption and key encryption are as follows



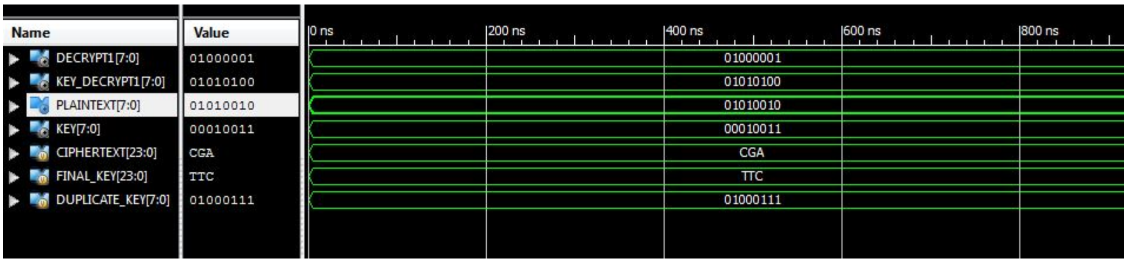
Name	Value
ENCRYPT1[7:0]	01000001
CIPHERTEXT[23:0]	0100001101000:
CIPHER_ALPHA[7:0]	01000001
PLAINTEXT[7:0]	01010010
KEY[7:0]	00010011

Fig5: DNA Encryption



Name	Value
KEY_ENCRYPT1[7:0]	01010100
KEY_ALPHA[7:0]	01010100
FINAL_KEY[23:0]	TTC
KEY[7:0]	00010011
DUPLICATE_KEY[7:0]	01000111

Fig6: DNA Key encryption



Name	Value
DECRYPT1[7:0]	01000001
KEY_DECRYPT1[7:0]	01010100
PLAINTEXT[7:0]	01010010
KEY[7:0]	00010011
CIPHERTEXT[23:0]	CGA
FINAL_KEY[23:0]	TTC
DUPLICATE_KEY[7:0]	01000111

Fig7: DNA Decryption

VII. CONCLUSION

DNA cryptography technique approach for the symmetric key cryptosystem is new approach which uses the DNA sequence property for key generation and cryptography process. The special properties of DNA sequence lead to utilization of DNA sequence for data hiding and cryptography processes. The key generated in the process goes two level encryption process as well as the cipher text generated also goes two level encryption process. The second level of the encryption process is mainly depends on the transaction table (table2) for the alphabet, digit and letter. Complexity and security is achieved by random generation of the key which is used to encrypt and decrypt data. DNA cryptosystem is more secure and reliable than the traditional encryption techniques as the computational complexity may high for DNA technology.

REFERENCES

[1] Sangapu Venkata Appaji & Dr. Gomatam V S Acharyulu "Recent Advancements on Symmetric Cryptography Techniques -A Comprehensive Case Study" Global Journal of Computer Science and Technology: F Graphics & Vision, Volume 14 Issue 2 Version 1.0 Year 2014.

[2] William Stallings "Cryptography and network security 4/E".

[3] Clive "Max" Maxfield FPGAs: World Class Designs, 1st Edition.

[4] ShizhuangLin; JingyuLiu; YanjunFang;" ZigBee Based Wireless Sensor Networks and Its Applications in Industrial", IEEE International Conference on Automation and Logistics18-21Aug.2007, Pg1979-1983.

[5] Ramya, C.M.; Shanmugaraj, M.; Prabakaran, R., "Study on ZigBee technology," in Electronics Computer Technology (ICECT), 2011 3rd International Conference on , vol.6, no., pp.297-301, 8-10 April 2011.

[6] Lu MingXin, Lai XueJia, Xiao GuoZhen, Qin Lei "Symmetric-key cryptosystem with DNA technology" Science in China Series F: Information Sciences June 2007, Volume 50, Issue 3, pp 324-333.

[7] LM Ad leman "Molecular computation of solutions to combinatorial problems" Science 11 November 1994:Vol. 266 no. 5187 pp. 1021-1024.

[8] R. J. Lipton, "Using DNA to solve NP-complete problems," Science, vol. 268, pp. 542-545, 1995.

[9] Guangzhao Cui; Limin Qin; Yanfeng Wang; Xuncai Zhang, "An encryption scheme using DNA technology," in Bio-Inspired Computing: Theories and Applications, 2008. BICTA 2008. 3rd International Conference on, vol., no., pp.37-42, Sept. 28 2008-Oct. 1 2008.

[10] Asish Aich , Alo Sen, Satya Ranjan Dash, Satchidananda Dehuri," A Symmetric Key Cryptosystem Using DNA Sequence with OTP Key" Information Systems Design and Intelligent Applications Volume 340 of the series Advances in Intelligent Systems and Computing pp 207-215.

AUTHOR PROFILE

I.Rama Satya Nageswara Rao is pursuing M. Tech VLSI Design in K L University. His research interests include FPGA Implementation, Low Power VLSI and Testing for VLSI Circuits.

B.Murali Krishna is working as Assistant Professor in K L University. His research interest focuses on FPGA implementation, Partial Reconfiguration, and Testing of VLSI circuits.

Syed Shameem is working as Associative Professor in K L University. His research interest focuses on Biological sensors and MEMS.

Dr. Habibullah khan presently working as Professor & Dean (SA), Department of the ECE at K L University. His research interested areas includes Antenna system designing, microwave engineering, Electromagnetic and RF system designing.

Dr. G.L.Madhumati presently working as Professor &Head, Department of the ECE at Dhanekula Institute of Engineering & Technology. Her research interested areas includes FPGA Implementation, Low Power VLSI.