VOL. 11, NO. 21, NOVEMBER 2016 ISSN 1819-6608
ARPN Journal of Engineering and Applied Sciences
©2006-2016 Asian Research Publishing Network (ARPN). All rights reserved.
www.arpnjournals.com

FPGA IMPLEMENTATION OF PARTIALLY RECONFIGURABLE DNA CRYPTOGRAPHY METHODS THROUGH WIRELESS USING ZIGBEE

B. Murali Krishna[1], G. L.Madhumati[2] and Habibulla Khan[1]
[1]Department of ECE, K L University, AP, India
[2]Department of ECE, Dhanekula Institute of Engineering & Technology, AP, India
E-Mail: muralikrishna@kluniversity.in

ABSTRACT

Field Programmable Gate Arrays (FPGAs) are unlimited by applications, but fortunately limited with area. FPGAs can be integrated to various fields like system-on-chip, communication, cryptography, signal and image processing etc. The main purpose of this research paper is to implement multiple cryptography techniques using Partial Reconfiguration (PR) on FPGA. Partial Reconfiguration is a process of changing an area in FPGA without altering the other applications. The data will be encrypted and decrypted in wireless between transceiver through ZigBee communication. To convey the information safely several cryptography methods are used. DNA grouping mechanism is a piece of both encryption and information concealing utilizing a few properties of Deoxyribonucleic Acid (DNA) groupings. It is highlighted that DNA groupings have many more intriguing properties which are used for concealing of information. Three DNA strategies used for data encryption and decryption are: Insertion, Complimentary Pair and the Substitution Strategy. A new DNA-MRNA-Protein method was proposed based on DNA strategies. In each strategy, a specific reference DNA sequence is chosen and the message M is encrypted and a fake DNA sequence S' is generated. S' is sent to the receiver and the beneficiary can recognize and decrypt the message M covered up in sequence S'. A, C, G, and T are the four nucleotides which are considered in DNA sequence to encrypt and decrypt the information. Resource Utilization of the proposed method, consumes few resources compared with several cryptography techniques. Security level is enhanced in the proposed algorithm, which was designed using Verilog HDL, Synthesized & Simulated in Xilinx-ISE Simulator and results are tested on Spartan & Virtex FPGA architectures.

Keywords: Cryptography, DNA Sequence, FPGA, Partial Reconfiguration, ZigBee.

1. INTRODUCTION

Due to advancements in technology different sorts of information from the Internet turns out to be more easy now a days. Vital data must be disguised while being transmitted by means of the Internet. Channel security has become more vital and important factor for data transfer to receiver. The vast majority of them utilize the natural properties of DNA arrangement. The information concealing technique presented does not make utilization of organic properties; rather, it utilizes different DNA groupings which will be clarified underneath [1]. A DNA arrangement will have four nucleotides which are named as A, C, G and T elements precisely known as nucleotides. Every letter is identified with a nucleotide. Four nucleotides which form DNA sequence named as S. To encrypt and decrypt the information a specific reference DNA sequence S is chosen and the message M is encrypted with reference sequence which produces a fake DNA sequence S'.Subsequently, the cryptography method comprises two stages. In the principal stage, the mystery information is encoded by utilizing a reference DNA Sequence. In the second stage the encoded information is steganographically recovered from some reference DNA sequence. Critical job for hackers to identify the original DNA sequence among millions of DNA sequences [2].

Among all intriguing methods the information is covered up in Deoxyribo Nucleic Corrosive (DNA). In these strategies user shroud data information into DNA arrangement haphazardly utilizing certain methods [3].Three Information concealing strategies are Insertion, Complementary-Pair, and Substitution methods based upon DNA groupingare designed in Verilog HDL and implemented on FPGA. Reconfigurable silicon technology has changed the electronic industry to design, simulate and implement custom hardware functionality with less time to market. FPGAs use reprogrammable semiconductor SRAM based technology [5]. Tremendous growth in wireless communication has enabled the researchers to use portable wireless personal devices such as mobile, Wi-Fi, (ESP8266-IOT), Bluetooth, ZigBee, GSM, GPRS, data card and other wireless sensor networks to append with custom applications.

2. PARTIAL RECONFIGURATION

Partial Reconfiguration is a process of changing an area in FPGA without altering the other applications. Partial Reconfiguration flow is divided into two regions: Static and Dynamic. Static Region is a portion of the device that is programmed at start-up and never changes. Dynamic Region is a portion of the device that is reconfigured multiple times with different designs shown in Figure-1(a). Design is sliced into reconfigurable partitions where each partition is subdivided into reconfigurable modules. Partial bit files are generated using partial Reconfiguration design flow shown in Figure-1(b).

©2006-2016 Asian Research Publishing Network (ARPN). All rights reserved.

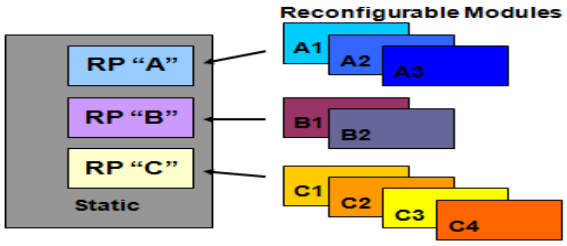

Figure-1(a). Static & dynamic region.

Cryptography forms a secure channel between sender and receiver which encrypts information at sender with key by using variety of algorithms and decrypts the encrypted data with key, and then the original message is retrieved back at receiver. Key is generated using Linear Feedback Shift Register (LFSR). LFSR generates random sequences by shift and XOR based on polynomial mechanism. Randomness in key can be enhanced by using preloaded seed value or by changing polynomial. Several types of LFSR's are available based on the application. LFSR is

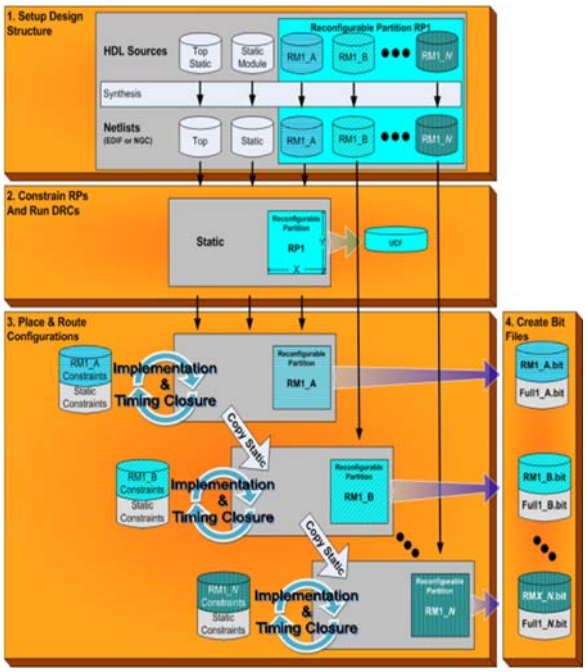

Figure-1(b). Partial reconfiguration design flow.

chosen as Pseudo Random Sequence generator. Partial Reconfiguration enhances the security level of DNA cryptography methods in runtime by changing the key using LFSR shown in Figure-1(c).

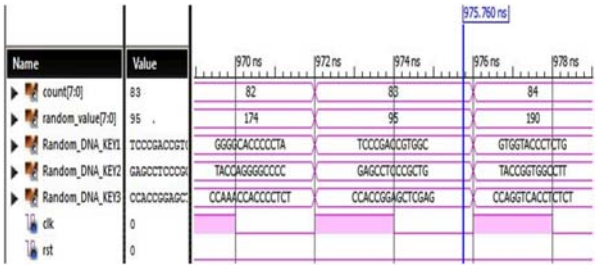

Figure-1(c). PR based dynamic key generation using LFSR.

3. ZIGBEE

ZigBee is a wireless technology suitable for short range, low power and low cost applications. ZigBee protocol is developed with IEEE 802.15.4 standard. Among different wireless technologies, ZigBee technology stands on the top as it is able to provide a communication between devices and users in a simple and efficient manner. There are many types of ZigBee devices that are being used in Wireless Sensor and Personal Area Network, home and industrial appliances. In this ZigBee S1 series module is used to control various appliances. One of its specifications is that, they work within a range of one Mile and will operate at 2.4GHz frequency. ZigBee's are used in military applications and war equipment for communicating data between robot and commander to track the enemy and deploy necessary action. Cryptography forms a secure channel between robot and commander which encrypts information with key. The proposed dynamic key generation mechanism using PR can be deployed in wireless through ZigBee. Secure Communication between two FPGAs in Wireless using ZigBee and RF is shown in Figure 14 and 15.

4. PURPOSE OF CRYPTOGRAPHY

Every security framework will be giving bundles of capacity, which can promise the information mystery of framework. Some of the important keywords are given below with their description.

•**Confidential:** making the transmitted information only available to a specific users on approved recipient.

•**Authentication:** Recognizing the message beginning effectively without false.

•**Integrity:** making the necessary adjustments to information, which is to be transmitted, is relevant only to the approved users.

•**Non repudiation:** making the sender and receiver of the message not ready to deny the correspondence.

•**Access control:** making the entry only to the specific and authorized clients as it were.

•**Availability:** making resources like PC framework are open to the approved clients whenever they require the information.

©2006-2016 Asian Research Publishing Network (ARPN). All rights reserved.

Security approaches must be adequate to handle the constantly changing information ruptures [6]. The place where the information security, encryption of information is very still and in movement, executing the client access control becomes possibly the most important factor**.** Cryptography is the specialty of changing over the message into human disjointed code, which can't be turned around to the message without proper code. Cryptography assumes an essential part in information honesty [7]. This can be represented in the three segments of the CIA triad (Confidentiality, Integrity, and Availability). CIA is the principal idea in the secured data transmission [8][9]. Resource utilization summary is compared for DES, TACIT, One Time Pad and DNA Key cryptography algorithms shown in table 1 and graphical representation is shown in Figure-13.

4.1 DNA Cryptography

DNA cryptography (Deoxyribonucleic Acid) is one of the fastest growing innovations which take a shot at thoughts of DNA figuring. Another framework for securing data was displayed using the regular structure of DNA called DNA figuring or sub-nuclear preparing or natural enrolling. The symmetric cryptosystems can be broken when the use of quantum computers came into existence. DNA cryptography plays a crucial role in future; it is more likely to replace the former cryptography techniques. Three methods of DNA Cryptography techniques are

1. Insertion Method
2. Complimentary Pair Method
3. Substitution Method

4.1.1 DNA Insertion method

DNA insertion is the first method which encrypts the message in reference DNA sequence. Insertion method uses any sequence out of million DNA sequences. DNA sequence is available in ASCII format converted into binary, and then splitted based on length of message. Message is padded with splitted DNA sequence and encrypts to fake DNA sequence consists of A, C, G, and T characters. A, C, G, and T are the four nucleotides which are considered in DNA sequence to encrypt and decrypt the information. Decryption is reverse process of encryption [5].

Encryption

DNA Insertion encryption flow chart is shown in Figure-2. Consider an input reference DNA sequence [S] which is in A, C, G, and T format. Covert sequence [S] into binary values [BS]. Depending on message length [M] split the binary sequence [BS] into segments. Length of the message is 8; so [K] is divided into 3 segments. Discard unequal binary bits in [K] "01" which appeared in violet color shown above figure 2. Binary message [BM] is generated by appending message bits in front of K segments. Convert [BM] binary values into A, C, G, and T format which generates fake DNA sequence S'. Simulation result for encryption and decryption shown in Figure-9.

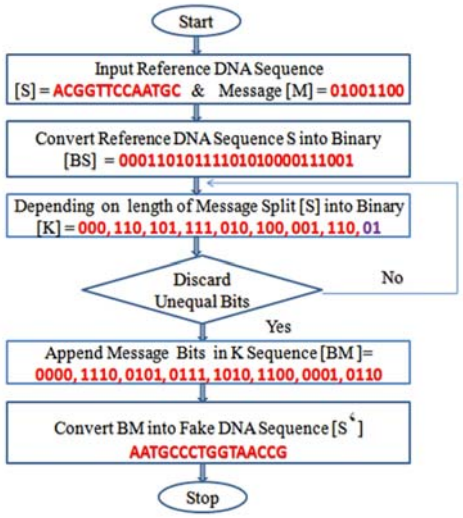

Figure-2. Flow chart for DNA insertion encryption.

Decryption

DNA Insertion decryption flow chart is shown in figure 3. Consider an input fake DNA sequence [S'] which is in A, C, G, and T format. Covert fake DNA sequence [S'] into binary values [BS']. Depending on length of binary sequence [BS'E] split into equal segments. Length of binary segment is unequal then resplit the sequence. Extract the first bits in each 4-bit binary segments. Original message [DM] is decrypted by concatenating all first bits in each 4-bit binary segments. Reference DNA sequence which considered at encryption [S] is re-generated by concatenating last three bits in each 4-bit binary segments. Simulation results for encryption and decryption of DNA Insertion method is shown in figure 9.

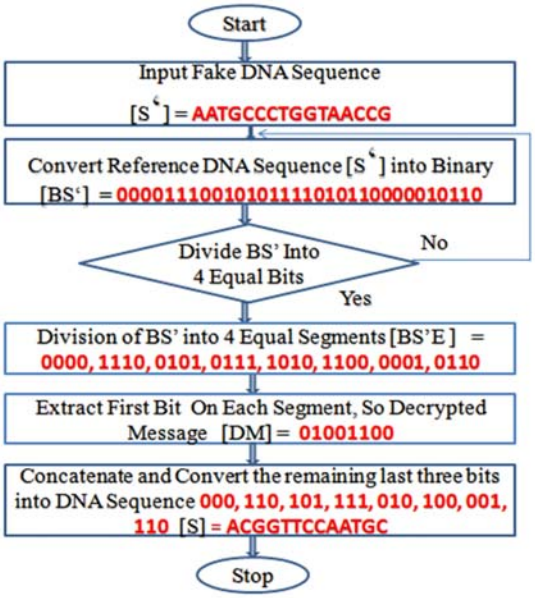

Figure-3. Flow chart for DNA insertion decryption.

©2006-2016 Asian Research Publishing Network (ARPN). All rights reserved.

4.1.2 Complimentary-Pair method

Complimentary-Pair is the second method which uses longest complimentary-pair substrings. Substrings are generated using complementary rules: ((AC) (CG) (GT) (TA)). The complimentary pair of the string AACTG will be CCGAT.

Encryption

DNA Complimentary Pair encryption flow chart is shown in figure 4. The method generates longest complementary pairs invoked in sequence along with message a fake sequence is send to receiver. Consider an input reference DNA sequence [S] which is in A, C, G, and T format. Artificially complementary substrings [CSS] is generated based on half of the message length and add one character to it for longest complementary pair. Character 'T' is padded with before and after in each substring [P] is generated. Substring sequence S1 is obtained by inserting padded bits in reference sequence [S]. Binary message bits are converted into A, C, G, and T format and inserted at positions before and after [P]. Fake DNA sequence S' is send to receiver. Recheck the no. of substring pairs are same in S' else regenerate CSS.

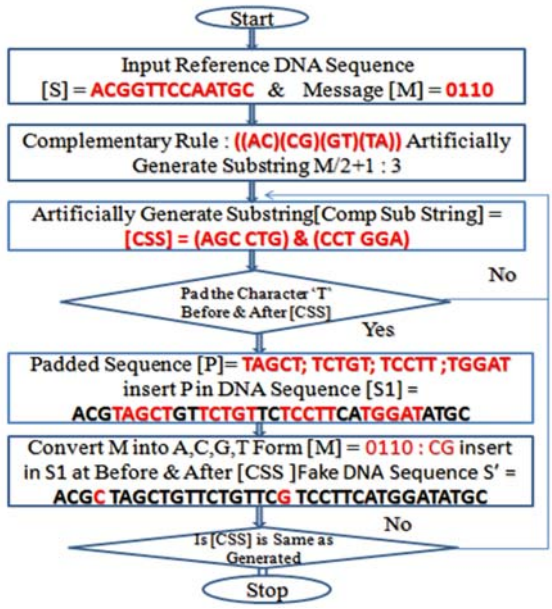

Figure-4. Flow chart for DNA complementary pair encryption

Decryption

DNA Complimentary Pair decryption flow chart is shown in Figure-5. Consider an input fake DNA sequence [S'] which is in A, C, G, and T format. HDL programming skill is used to find longest complementary substring pairs [AGS] in sequence [S']. Unpad the character 'T' before and after substrings complementary pairs [CSS] is obtained. Remove "C", "G" before and after [CSS]. Concatenating "C" and "G" converting into binary values original message is decrypted by. Deleting substrings in S' reference DNA sequence S is regenerated. Simulation results for encryption and decryption of DNA Complimentary Pair is shown in Figure-10.

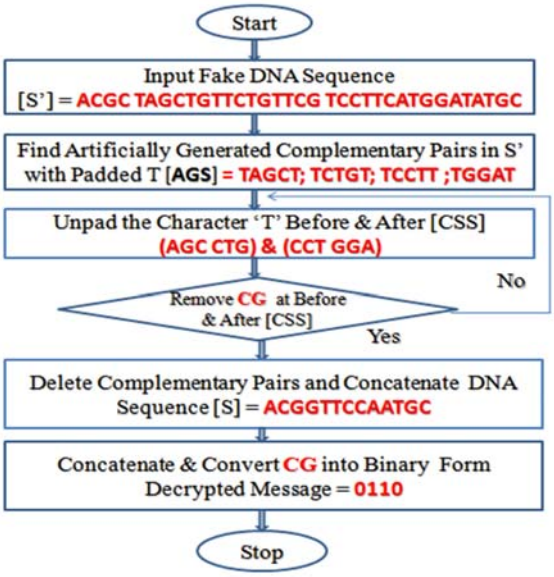

Figure-5. Flow Chart for DNA Complementary Pair Decryption.

4.1.3 Substitution method

Substitution method encrypts message in reference DNA sequence at random positions using LFSR along with complementary rules: ((AT) (CA) (GC) (TG)).

Encryption

DNA Substitution method encryption flow chart is shown in Figure-6.

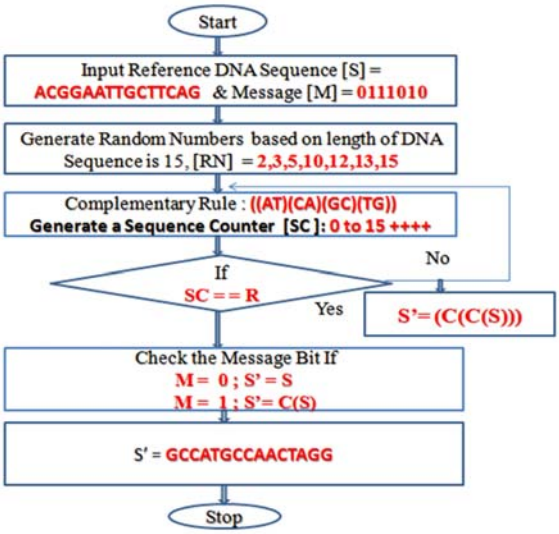

Figure-6. Flow chart for DNA substitution encryption.

The method encrypts information in variety mechanism. Depending on the length of reference DNA sequence and message bits random values [RN] are generated and arrange them in increasing order. Sequence counter [SC] in incremented and compares with random number if the current value of [RN] not equal to [SC] but

©2006-2016 Asian Research Publishing Network (ARPN). All rights reserved.

number is available in [RN] it verifies the message [M]. If M value is'0'no complement, else perform complementary rule once on reference DNA sequence. SC value does not matches perform complementary rule twice, fake DNA sequence S' is generated. Send S' and S to receiver.

Decryption

DNA Substitution method decryption flow chart is shown in Figure-7. Consider an input DNA sequence [S] and fake DNA sequence [S'].

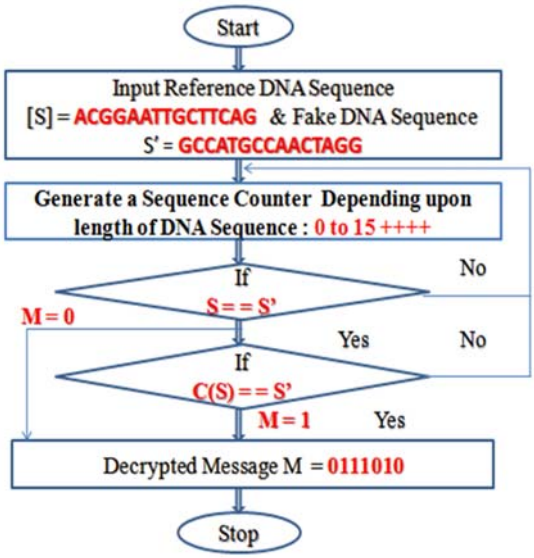

Figure-7. Flow chart for DNA substitution decryption.

Depending on the length of DNA sequences Sequence counter [SC] is incremented and compares S with S'.If both are equal message value is '0' else perform complementary rule once on reference DNA sequence and again compare S with S,' if both are equal message value is '1'. If S! = S' then SC is incremented and compared for all values then the final message is decrypted. Simulation results for encryption and decryption of DNA Substitution method is shown in Figure-11.

4.1.4 Proposed DNA-MRNA-protein method

DNA-MRNA-Protein method consumes fewer resources which encrypts the original message (M_n) in reference DNA sequence. Method uses any DNA sequence out of million DNA sequences. DNA sequence is available in ASCII format converted into binary, and then splitted based on length of message. Complemented Message $C_n(M)$ is padded with splitted DNA sequence (DNA_n)and converts to fake DNA Sequence S1. Based on Length of S1 DNA sequence is sliced into two parts MSB is shifted by circular right and LSB is shifted by circular left named as fake DNA Sequence S2 shown in flow chart Figure-8.

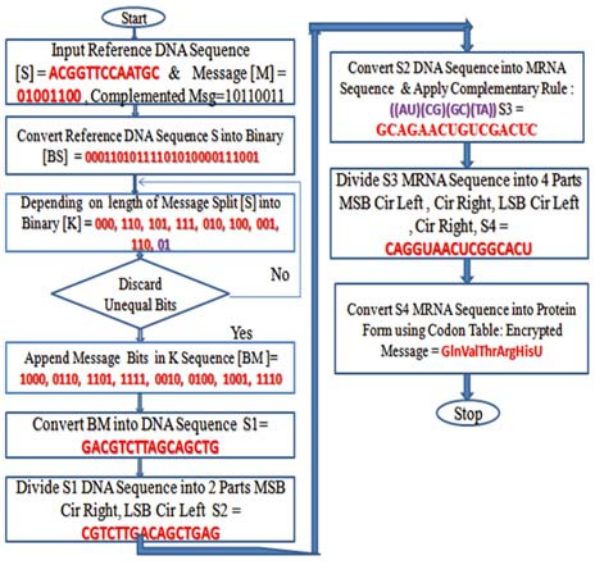

Figure-8. Flow chart for DNA-MRNA-protein encryption.

To secure data from hackers apply complementary rule on S2 and convert to MRNA sequence is generated named as S3. MRNA sequence is splitted into 2 parts MSB & LSB, again each splitted part subdivided into 2 parts is shifted by circular left ,circular right and LSB is shifted by circular left ,circular right named as S4. MRNA sequence obtained at S4 is converted to Protein form mapping of ($MRNA_n$) codon to amino acid shown in Table-2, which is final Encrypted message for n-bit, E_n (M). Decryption is a reverse process of encryption. Security analysis is for proposed method. Simulation result for encryption and decryption of DNA-MRNA-Protein method is shown in Figure-12.

Encrypted message E_n (M) = {(M_n), $C_n(M)$, DNA_n[S1, S2], $MRNA_n$[S3, S4],Protein Form}.

Decrypted message D_n (M) = {Protein Form,$MRNA_n$[S3, S4],DNA_n[S1, S2], $C_n(M)$, (M_n)}.

5. SIMULATION RESULTS

The simulation results for four different DNA Cryptography techniques Insertion Method, Complimentary-Pair Method, Substitution Method and Proposed DNA-MRNA-Protein Method are presented in this section.

©2006-2016 Asian Research Publishing Network (ARPN). All rights reserved.

Table-1. Summary of resource utilization comparison for several cryptography techniques.

CRYPTOGRAPHY TECHNIQUES	DES ENCRYPTION STANDARD		TACIT	ONE TIME PAD	DNA-KEY CRYPTOGRAPHY	
Logic Utilization	ENCRYPTION	DECRYPTION	ENC & DEC	ENC & DEC	ENCRYPTION	DECRYPTION
Number of Slice LUTs	16	16	18	17	6	9
Number of fully used LUT-FF pairs	29	16	32	28	11	17
Number of bonded IOBs	16	17	88	112	56	88
No of Message Bits	8	8	8	8	8	8

CRYPTOGRAPHY TECHNIQUES	DNA INSERTION	DNA COMPLEMENTARY-PAIR	DNA SUBSTITUTION	PROPOSED DNA_MRNA INSERTION
Logic Utilization	ENC & DEC	ENC & DEC	ENC & DEC	ENC & DEC
Number of Slice LUTs	5	6	36	4
Number of fully used LUT-FF pairs	0	0	41	0
Number of bonded IOBs	146	288	264	144
No of Message Bits	8	4	8	8

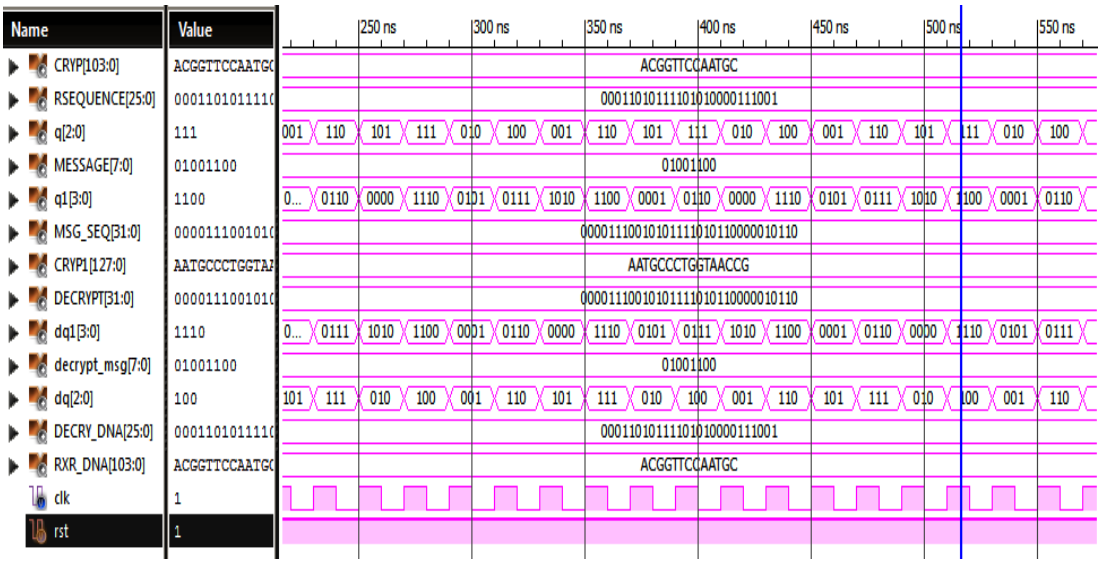

Figure-9. DNA Insertion method – Encryption & decryption.

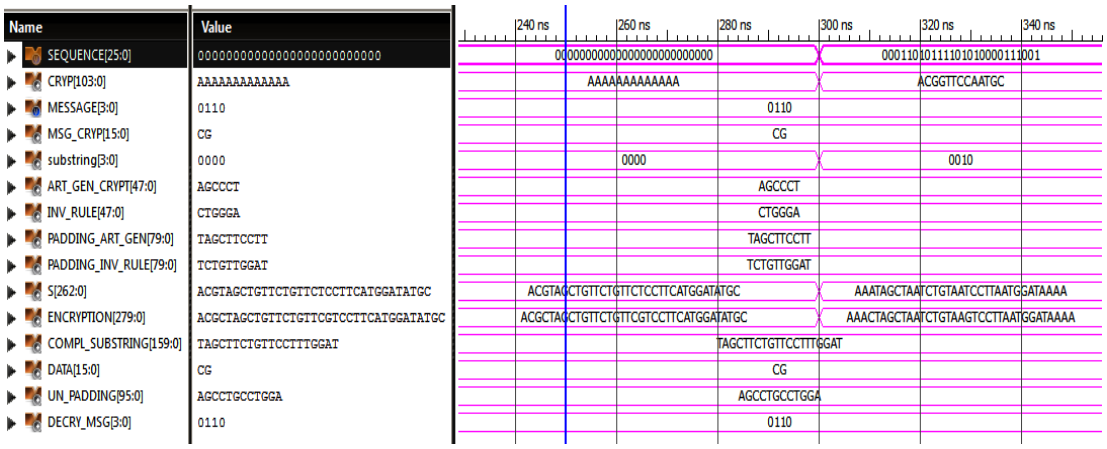

Figure-10. DNA Complementary-pair method – Encryption & decryption.

©2006-2016 Asian Research Publishing Network (ARPN). All rights reserved.

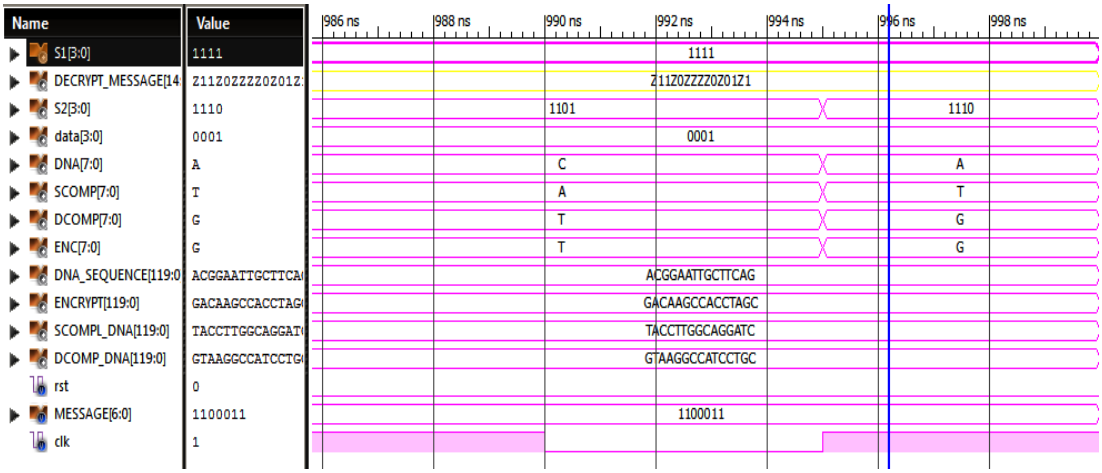

Figure-11. DNA Substitution method – Encryption & decryption.

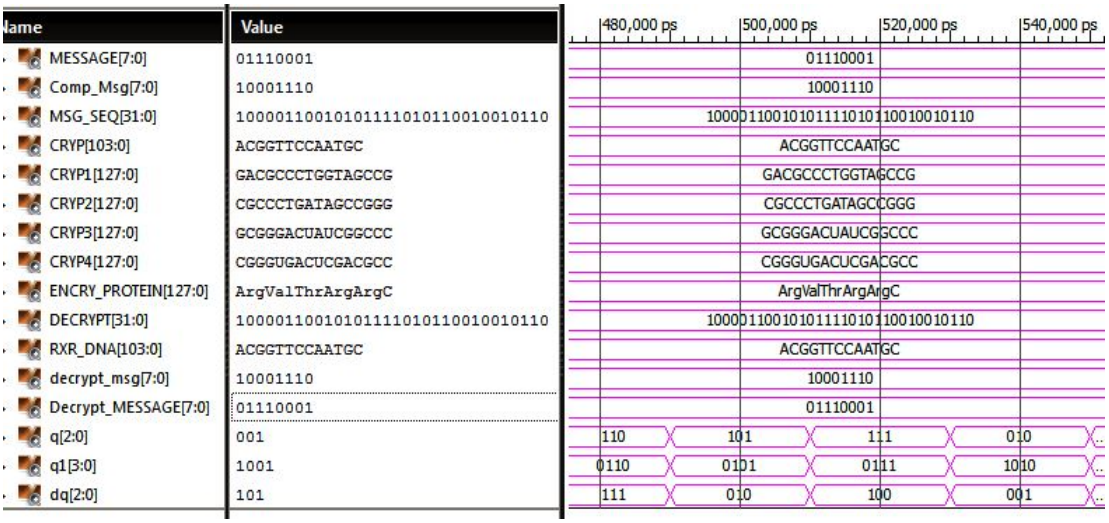

Figure-12. DNA-MRNA-protein Method – Encryption & decryption

Table-2. Mapping of (MRNA Sequence) codon to amino acid.

First letter	Second letter: U	C	A	G	Third letter
U	UUU, UUC: Phe; UUA, UUG: Leu	UCU, UCC, UCA, UCG: Ser	UAU, UAC: Tyr; **UAA Stop**; **UAG Stop**	UGU, UGC: Cys; **UGA Stop**; UGG Trp	U C A G
C	CUU, CUC, CUA, CUG: Leu	CCU, CCC, CCA, CCG: Pro	CAU, CAC: His; CAA, CAG: Gln	CGU, CGC, CGA, CGG: Arg	U C A G
A	AUU, AUC, AUA: Ile; AUG: Met	ACU, ACC, ACA, ACG: Thr	AAU, AAC: Asn; AAA, AAG: Lys	AGU, AGC: Ser; AGA, AGG: Arg	U C A G
G	GUU, GUC, GUA, GUG: Val	GCU, GCC, GCA, GCG: Ala	GAU, GAC: Asp; GAA, GAG: Glu	GGU, GGC, GGA, GGG: Gly	U C A G

©2006-2016 Asian Research Publishing Network (ARPN). All rights reserved.

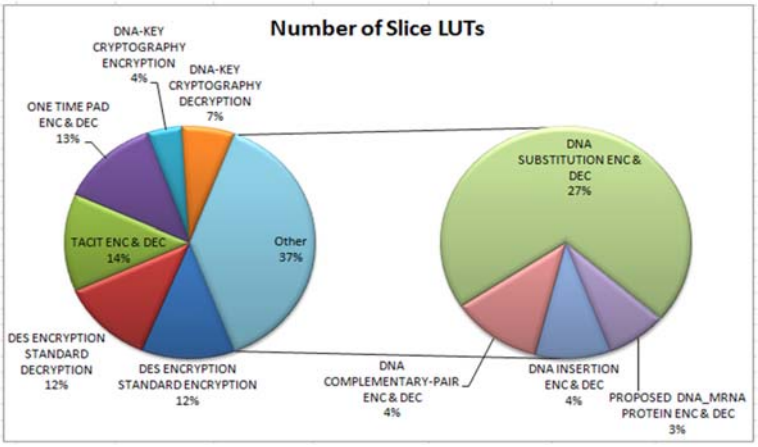

Figure-13. Graphical representation of resource utilization for several cryptography techniques.

6. FPGA Implementation

Figure-14. Secure communication between two FPGAs in wireless using ZigBee.

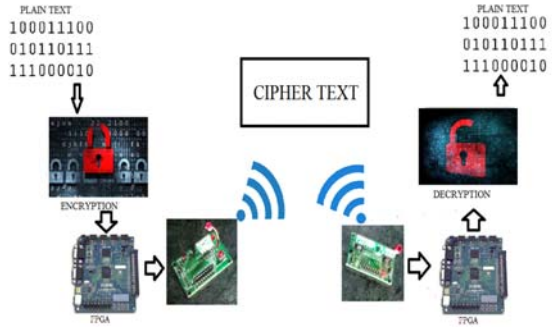

Figure-15. Secure communication between two FPGAs in wireless using RF.

7. CONCLUSION

DNA cryptography system approach is a new approach, which utilizes the deoxyribonucleic acid arrangement property for encryption and decryption. Deoxyribonucleic acid cryptosystem is safer and solid than the customary cryptography systems. Partial Reconfiguration enhances the security level of several cryptography techniques with LFSR based key generation in runtime. ZigBee and RF Interface, supports wireless data acquisition from sender and deploy the commands at receiver to configure the dynamic key generation mechanism in runtime. Cryptography techniques was implemented and tested in Spartan & Virtex FPGA architectures.

REFERENCES

[1] H.J. Shiu, K.L. Ng, J.F. Fang, R.C.T. Lee, C.H. Huang. 2010. Data hiding methods based upon DNA sequences. Information Sciences Volume 180, Issue 11, 1 June, pp. 2196-2208.

[2] S. Manna S. Roy P. Roy S. K. Bandyopadhyay: Modified techniques of insertion method. 2014. First International Conference on Automation, Control, Energy and Systems (ACES) : 1 - 5.

[3] C.-C. Chang, T.-C.Lu, Y.-F.Chang and C.-T. Lee, Reversible data hiding schemes for deoxyribonu- cleic acid (DNA) medium, International Journal of Innovative Computing, Information and Control, vol.3, no.5, pp.1145-1160.

[4]I.Rama Satya Nageswara Rao, B. Murali Krishna, Syed Shameem, Habibulla Khan, G. L. Madhumati. 2016. Wireless Secured Data Transmission using Cryptographic Techniques through FPGA, International Journal of Engineering and Technology (IJET), e-ISSN: 0975-4024, Vol. 8, Issue No. 1, Feb-Mar, pp. 332-338.

[5] ShizhuangLin; JingyuLiu; YanjunFang. 2007. ZigBee Based Wireless Sensor Networks and Its Applications in Industrial, IEEE International Conference on Automation and Logistics 18-21 Aug, pp. 1979-1983.

[6] A. Gehani, T. H. LaBean, and J. H. Reif. 1999. DNA-based cryptography," in Proceedings 5th DIMACS Workshop on DNA Based Computers, pp. 233-249.

©2006-2016 Asian Research Publishing Network (ARPN). All rights reserved.

[7] T. Head, Splicing schemes and DNA. 1992. in Linden-mayer Systems; Impact on Theoretical Computer-science and Developmental Biology, pp. 371-383.

[8] G. Cui, L. Qin, Y. Wang and X. Zhang. 2008. An encryption scheme using DNA technology, Bio-Inspired Computing: Theories and Applications, 2008. BICTA 2008. 3rd International Conference on, Adelaide, SA, pp. 37-42.

[9] M. Hirabayashi, A. Nishikawa, F. Tanaka, M. Hagiya, H. Kojima, K. Oiwa. 2011. Analysis on Secure and E ective Applications of a DNA-Based Cryptosystem," in Sixth International Conference on Bio-Inspired Computing: Theories and Applications, pp. 205-210.