Reconfigurable Encryption System: Encrypt Digital Data

Md. Jobayer Hossain[1], Md. Billal Hossain[2], Khaled Mahbub Morshed[3]

[1, 2, 3]#*Electronics and Communication Engineering Department,*
Khulna University of Engineering and Technology,
Khulna—9203, Bangladesh
[1]jobayer.ece@gmail.com, [3]kmm_ece@yahoo.com, [2]billal.0709018@gmail.com

Abstract—**This paper presents a reconfigurable system that can encrypt digital data. The system provides the option of choosing one of familiar encryption methods DES, 3 DES and AES to the user. All these methods are symmetric type block cipher cryptography. DES takes 64 bit key to encrypt each 64 bits block of the entire message. AES on the contrary takes 128 bit key to encrypt each 128 bits block. Providing reconfigurability, the architecture enables the user to choose one of the existing techniques according to the level of security required. So the designed architecture is both flexible and reliable enough for the user to secure their privacy of conversation or e-commerce transaction. The architecture is designed using Verilog hardware description language, synthesized in Xilinx Synthesis Tool (XST) and Simulated by Verilogger Pro 6.5. It may be implemented in commercially available FPGAs.**

Keywords—**Encryption, Symmetric key cryptography, DES, AES, 3 DES, RTL schematic, timing diagram, FPGA.**

I. Introduction

The tremendous spreading out of the communication networks has evoked increased dependency on digitized information in our society. So information is more vulnerable to abuse now. The generic e-commerce often involves the transfer of sensitive information such as credit card details over the network. This is a dangerous thing since someone can easily eavesdrop on the network and read all the packets that fly by. Cryptographic techniques allow users to disguise the data (*encryption)* so that an intruder can obtain no information from the intercepted data [1]. It is also effective in securing e-mail, virtual private networks [2, 3] and IPSec [4]. This can be accomplished by one of three types of cryptographic algorithms [5]: symmetric key algorithms, public key algorithms, and hashing algorithms. Symmetric key algorithms are the quickest and most commonly used type of encryption [6]. Here, a single key is used for both encryption and decryption. DES, Triple DES and AES are three most common types of symmetric key public cryptography [7].

Data Encryption Standard (DES) was an excellent encryption technique previously. But it was proved vulnerable to brute force attack. So this is no longer in use today [7]. However, DES can be used in association with A5 algorithm for enhancing security in GSM network as outlined in [8] and [9]. The security level provided by DES is also found sufficient and cost effective in RFID [10-12]. The triple DES algorithm is a modification of DES algorithm. It is capable of avoiding brute force attack [13]. So it is widely used in commerce industries, embedded systems applications, non-classified secure defence data as well as secure communication protocols such as SSH, SFTP, and SHTTP [14]. It can also serve secure communication in GPRS, EDGE, WAP, UMTS and HIPERLAN/2 and ATM [15]. The most recent algorithm of interest is Advanced Encryption Standard (AES). It is also a symmetric block cipher. But it is of larger key and plaintext size and solely different from the other two [16-19]. It is stronger and more efficient than triple DES. It may be suitably used in ATM networks, voice & satellite communications, HDTV, B-ISDN and wireless IP network [20]. All of DES, 3DES and AES serve confidentiality in data communications [21].

A user may be served with encryption in two ways: software or hardware implementation. Actually DES, Triple DES and AES can be implemented in Java package 'javax.crypto' [8]. But it is not speedy enough. In addition to resolving this, a dedicated hardware like FPGA is more secure and consumes less power [22].

The choice of encryption technique depends upon the order of security required, cost allowable and time allocation for encryption operation. Again people are looking forward to using same device in different applications today. To fulfil this demand we have designed a reconfigurable encryption device that can encrypt digital data and offer the bliss of reconfiguration ability to users when required. A brief description about that design is given below.

II. Design Preliminaries

DES algorithm is a block cipher. It means that it works on fixed-sized blocks of data [23-26]. It encrypts 64 bit data by 56 bit key. There are three major sections in DES structure. The first section, initial permutation rearranges 64 bit plaintext block according to a fixed transposition operation. Then this data block is passed through 16 successive rounds. Each round does the same operation but with different sub key. As stated before, DES uses 56 bit key. This 56 bit key is expanded into 64 bits by adding an extra parity bit after each seven bits. After that, sixteen sub keys (k1, k2,…,k16) are generated from this 64 bits. This is done by parity drop, compression P-box and left shift operation. Each sub key is of 48 bits. They are subsequently used in successive round operations of DES algorithm i.e. k1 is used in round 1, k2 in round 2 and so on.

978-1-4673-4836-2/12/$31.00 ©2012 IEEE

ISBN 978-1-4673-4834-8

After doing all these, final permutation is done. It is nothing but the initial permutation in the reverse order. The DES operation is illustrated in Fig. 1.

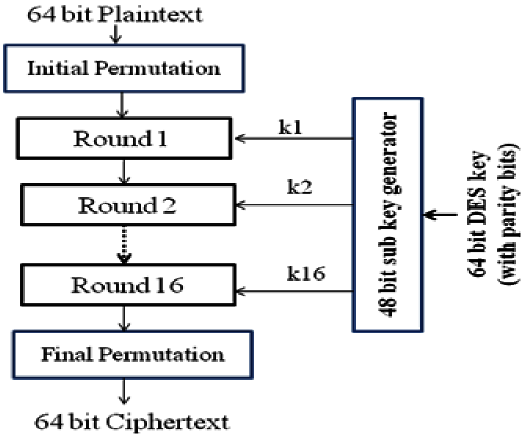

Fig. 1. Overall schematic diagram of DES

Triple DES (3 DES) is a modification of simple DES encryption approach. It uses two 56 bit keys instead of one to encrypt 64 bit data block. Firstly, 64 bit plaintext is encrypted by the first key (DES key, k1). Then this ciphertext is decrypted by the second key (3DES key, k2). The outcome is again encrypted by the first key. This result is the triple DES ciphertext. The triple DES operation is illustrated in Fig. 2

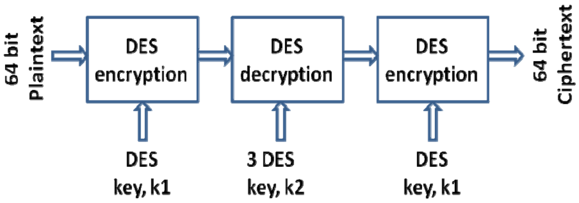

Fig. 2. Triple DES operation

The third and most efficient data encryption technique is AES. It is also a block cipher with fixed block size of 128 bits. Key size may be of 128, 192 or 256 bits. We used 128 bits key size that is more than enough in securing high security communications. In the structure, at first the plaintext bits are arranged in a 4×4 matrix form. Each element of this matrix is an eight bit block of plaintext. This matrix set is called a state. This state is then passed through the rounds operations. AES-128 uses 10 rounds. Each round of AES has the four distinct functions: SubBytes, ShiftRows, MixColumns, and AddRoundKey. An overall schematic representation of such a round is given in Fig. 3. In SubBytes operation, one byte is substituted into another according to a substitution table s-box. This adds confusion to the state. ShiftRows is a circular left shifting operation. Row 1 is shifted 1 byte, row 2 is shifted 2 bytes, and row 3 is shifted 3 bytes. In Mixcolumns operation, every column of state is multiplied by a constant matrix

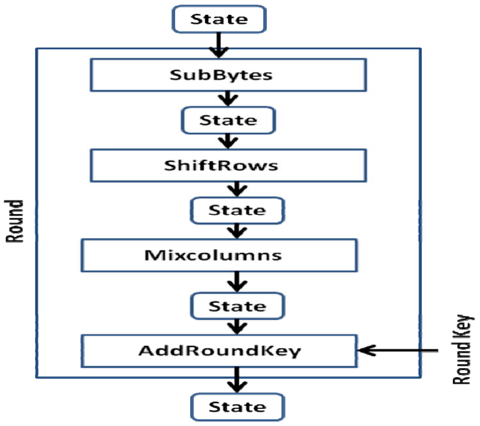

Fig. 3. Overall schematic diagram of an AES round

The resultant column is placed in the previous column position. The final step is addRoundKey. Here each byte in the State is XORed with the sub key. The sub key is derived from the 128 bit AES key according to a key expansion schedule.

III. Model Development Strategy

A. Architecture

We have focused on three encryption techniques DES, 3DES and AES. Both DES and 3 DES have 64 bit input plaintext and 64 bit output ciphertext. DES requires 64 bits key (k1) and 3 DES requires additional 64 bit key (k2) for encryption operation. On the other side AES encrypts 128 bit plaintext by 128 bit key input to get 128 bit ciphertext output. The brief design of the architecture is delineated in Fig. 4.

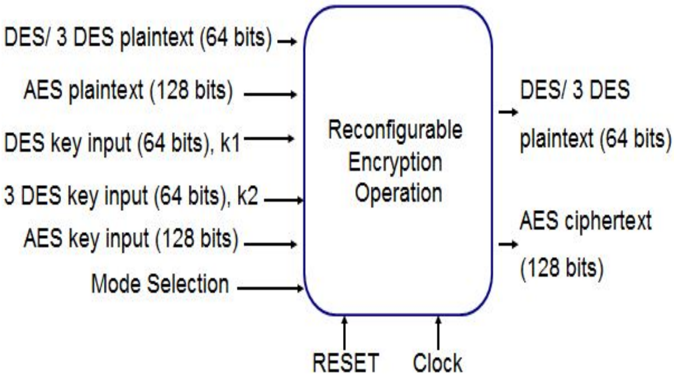
DES/ 3 DES plaintext (64 bits)
AES plaintext (128 bits)
DES key input (64 bits), k1
3 DES key input (64 bits), k2
AES key input (128 bits)
Mode Selection
Reconfigurable Encryption Operation
DES/ 3 DES plaintext (64 bits)
AES ciphertext (128 bits)
RESET
Clock

Fig. 4. Concise illustration of reconfigurable encryption system

Fig. 4 shows that there are eight types of input in the reconfigurable encryption device. DES and 3 DES data input-output ports are merged as they require same number of bits. AES input and output are defined as different input and output ports as it has different number of input and output bits. External RESET and clock input are devised for proper controlling operations in the device. Mode selection is used for selecting desired encryption method from all three methods. It requires 2 bits for selecting a technique from 3 techniques. The mode selection process is shown in TABLE I.

If mode selection input is 00, the processor does DES operation taking plaintext and key as input and passes cipher text as output.

TABLE II
MODE SELECTION CRITERIA

Mode Selection Input	Method
00	DES
01	3 DES
10	AES

If selection input is 01 then the processor takes plaintext and DES input key, runs encryption, decrypts this ciphertext with the second key (3 DES key inputs) and finally encrypts it again by the first key. Fig. 5 reveals a bit more about the encryption operation. Direct data flow is shown as direct lines and feedback data flow (in case of 3 DES) is shown as dashed lines. An internal register A is required for storing present output and fetching this data in the next operations. In 3 DES, DES encoded data is stored in register A. Then it is fetched from register A and inputted to DES decoder in the next instruction cycle. Decoding is done with the second key and the output is again stored in register A. In the next instruction, this is fetched and inputted to the DES encoder. Encoding is done with the first key and output is passed through the final output line.

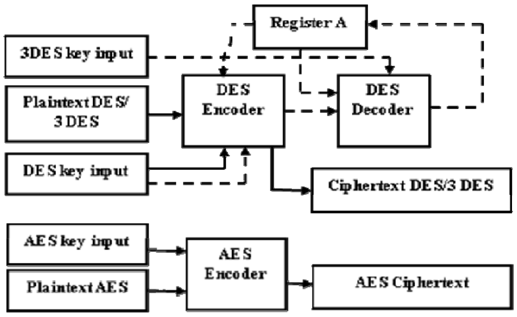

Fig. 5 Illustration of reconfigurable encryption operation

To handle all these operations properly a control unit is required. The control unit generates a control word leaving each one bit position for managing each block. So when a positive edge of clock signal appears, all the logic blocks become active or inactive according to the control signal. A program counter (PC) is required to drive the control unit. For synchronous operation of all the blocks, A Pro PC is also required. It activates the PC block after a fixed number of clock cycles. In addition to this, five input registers and two output registers are required for storing input and output data. An external reset is also an inevitable part of the system structure. It is used for clearing all the logic blocks at the user's will.

B. Instruction

The architecture necessitates total thirty two instruction cycles to give final output. This includes taking key and data inputs, program execution, getting and storing data from and in internal register A and giving ciphertext as output.

IV. OVERVIEW OF THE ARCHITECTURE

The overall construction of the reconfigurable encryption system is illustrated in Fig. 6. It consists of input and output pins, control unit, PC, Pro PC, input and output registers, internal register A, mid logic block, DES encoder, DES decoder, AES encoder clock and external reset pins. The clock signals are shown as dotted line and data flow as general line.

Control unit is the heart of the architecture. It handles all other logical units. The structure needs in total 23 control signals. So control bus consists of 23 lines. A detailed description of all these control sequences is outlined in TABLE III. Control signals are shown as thick blue coloured line in Fig. 6. A program counter (PC) is needed to drive the control unit. The architecture involves thirty instruction cycles for total encryption operation. Consequently, to attain this, the PC output is designed consisting of five bits. A Pro PC is also required for proper synchronization.

TABLE IV
DETAILED DESCRIPTION OF CONTROL BUS FROM CONTROL UNIT TO MODULES

Module name	Control Bus name	Bus No.
DES input	ena(DES input), out(DES input)	1, 2
DES key input	ena(key input DES), out(key input DES)	3,4
3DES key input	ena(3DES input), out(3DES input)	5,6
AES key input	ena(key input AES), out(key input AES)	7,8
AES text input	ena(AES input), out(AES input)	9,10
DES/3DES output	ena(DES/3DES output), write(DES/3DES output)	11,12
AES output	ena(AES output)	13
DES	Chip select bar (DES), RST(DES)	14,15
3DES	Chip select bar (3DES), RST(3DES)	16,17
AES	ld(AES), rst(AES)	18,19
reg A	ena(reg A),write1(reg A), ena2(reg A), write2(reg A)	20,21,22, 23

Input and output registers are used to store input (plaintext, key) and output (ciphertext) data. Register A is an internal register that temporarily stores outcome of an operation. This stored data is taken from the register and used in another operation.

The DES encoder block takes 64 bit plaintext, 64 bit key and gives 64 bit ciphertext. Similarly the AES block takes 128 bit plaintext, 128 bit key and gives 128 bit ciphertext. DES decoder is used in case of triple DES encryption. In this case DES encoded ciphertext is decoded by a second key, key input 3DES. This is again DES encoded by the first key. The final outcome is the Triple DES ciphertext. All the passive operations in the form of fixed information like s box, initial permutation, final permutation, p box etc are designed as ROM to reduce the computational burden and increase speed of the system. The mid is a simple block that performs logical OR of two 64 bit inputs. The output of the mid block is set as the input of the DES encoder.

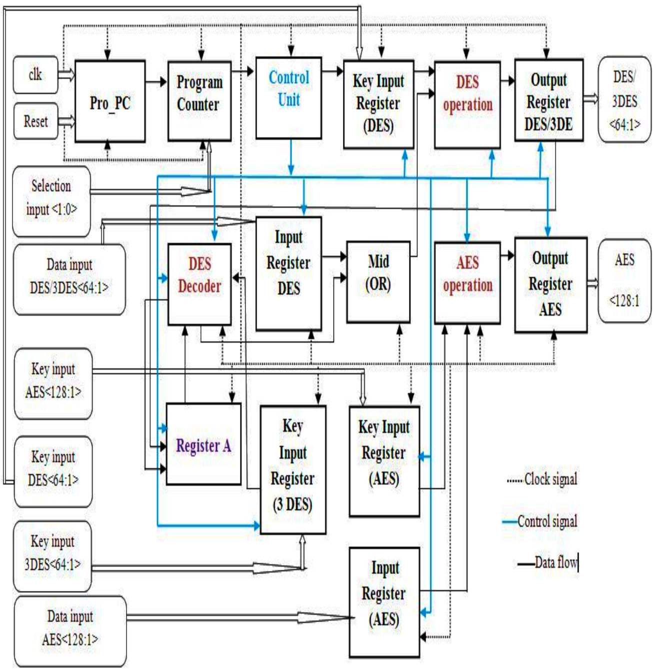

Fig. 6 Reconfigurable encryption system architecture

The reason behind insertion of mid block is simple; DES and Triple DES plaintext input do not appear simultaneously

V. Synthesis Results

The model is designed at Xilinx System Generator. Then it is synthesized in Xilinx Synthesis Tool (XST). The synthesis results are illustrated in Fig. 7.

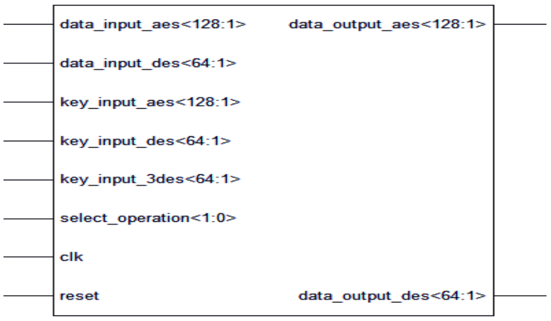

Fig. 7(a) Synthesised top module of reconfigurable encryption system

Fig. 7(a) shows the top module of the reconfigurable encryption system. It contains eight input pins and two output pins. AES data and key input are of 128 bits. On the contrary DES and 3DES have 64 bit data and key input each. There is a 2 bit select pin that is used for encryption method selection. External reset pin is helpful for clearing all the states in the system. The clk pin takes input clock signal into the system. The top module consists of some other smaller building blocks. It comprises control unit, input and output registers, DES encryption architecture, DES decryption architecture (required for 3 DES), AES encryption architecture, PC and Pro PC. These are interconnected as demonstrated in fig 7(b).

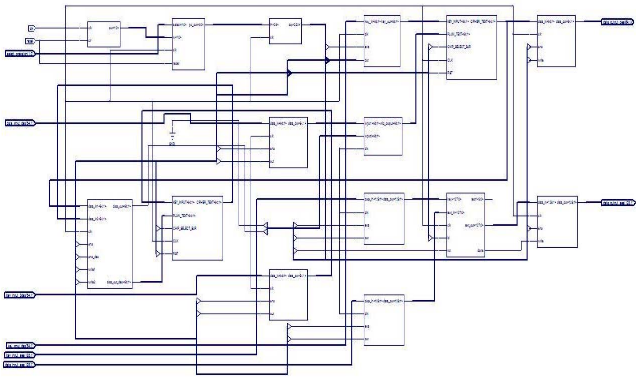

Fig. 7(b) Schematic diagram of reconfigurable encryption system

Schematic diagram of Fig. 7(b) is actually identical with our pre-synthesis design of Fig. 6. It comprises all the registers, required logical blocks and input-output ports. Fig. 7(c) demonstrates the DES structure that encrypts 64 bit plaintext by a 64 bit key and gives the ciphertext as output. Here we can notice sixteen distinct stages numbered from 1 to 16. These perform sixteen round operations of DES algorithm.

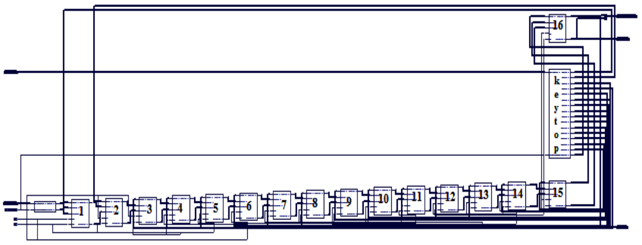

Fig. 7(c) Schematic diagram of Data Encryption Standard (DES)

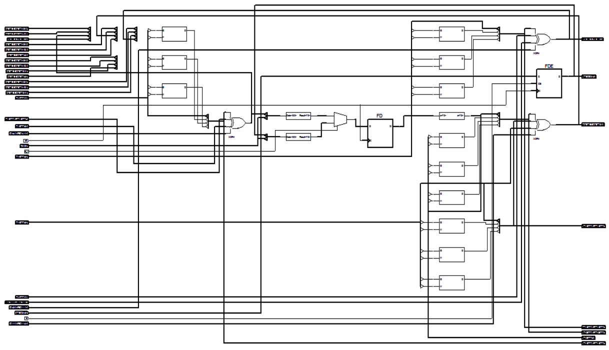

Fig. 7(d) Schematic diagram of Advanced Encryption Standard (AES)

The structure that performs AES encryption is shown in Fig. 7(d). It consists of 128 bit plaintext input, 128 bit key input, necessary logical units and 128 bit ciphertext output. DES decoder is an essential part in triple DES encryption. It is shown in Fig. 7(e). It performs the inverse operation of a DES encoder shown in Fig. 7(c). It also has 16 blocks numbered from 1 to 16. These blocks are associated with sixteen round operations of DES decryption algorithm. Every part of a DES decoder is identical with a DES structure but they act in reverse ordering.

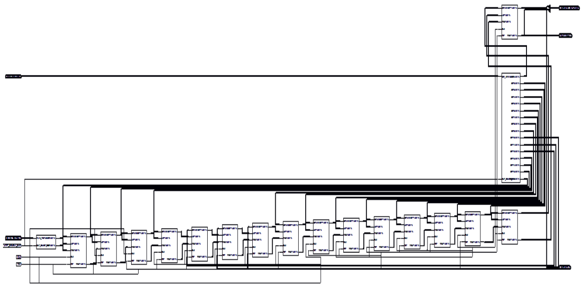

Fig. 7(e) Schematic diagram of DES decoder

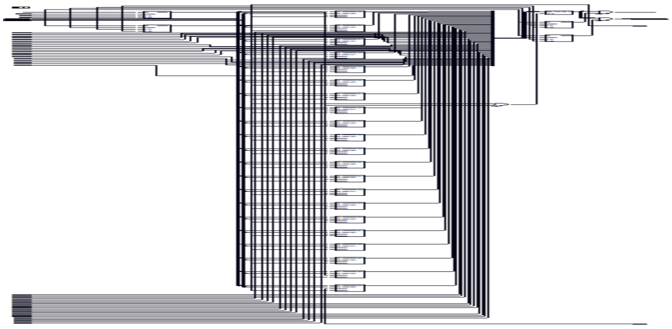

Fig. 7(f) Schematic diagram internal register A

The structure of internal register is shown in register A. The major components of this block are several D flip-flops. The mid block of Fig. 7(g) is nothing but an OR gate that can perform the logical OR operation of two 64 bit inputs.

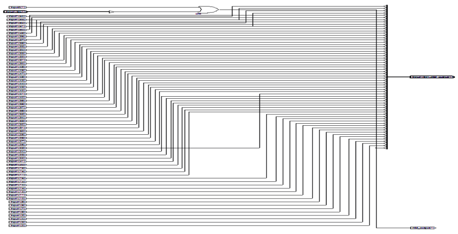

Fig. 7(g) Schematic diagram of mid logic (OR)

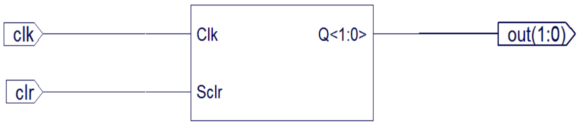

Fig. 7 (h) Schematic diagram of Pro PC

Fig. 7(h), 7(i) and 7(j) demonstrate the structure of Pro PC, PC and control unit correspondingly. Pro PC takes clock and clear signal as input and outputs two bit signal that drives program counter. The clear signal is identical with external reset of the system. PC is a very important part in any processor architecture. The synthesized PC gives 5 bit count sequences to the control unit. Its input pins are clk, reset, 2 bit mode selection and 2 bit Pro PC output. The vital part of the arrangement, the control unit has two input lines: clk and 5 bit PC output. The 5 bit control input (PC output) is enough for 30 combinations (instructions). The output of the unit is a 23 bit control word. To satisfy all these, the logical structure uses a 32×23 RAM. Each bit of the control word runs one of 23 control buses. Thus the logical operations are performed.

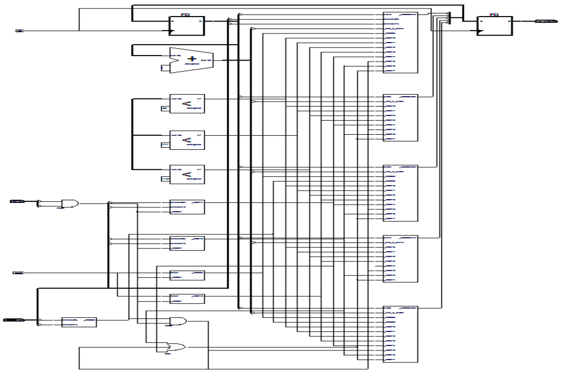

Fig. 7(i) Schematic diagram of Program Counter (PC)

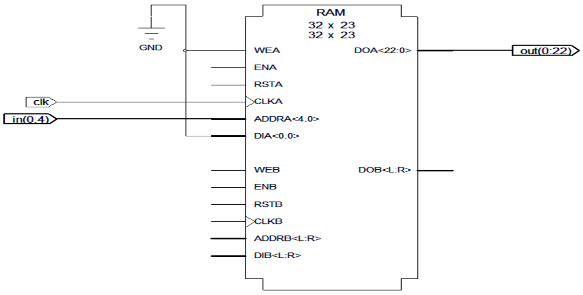

Fig. 7(j) Schematic diagram of control unit

VI. Simulation Results

Simulation is useful for verifying that all the sections of the processor architecture operate logically. We used Textbench Verilogger Pro 6.5 as a simulation tool. The outcomes were found identical to the logical states.

Fig. 8(a) illustrates the functions of reconfigurable encryption architecture. At the first twenty five clock cycles, External reset is at high state. So whatever the inputs, the device is inactive. After that, reset=0; so the device is ready for encryption operation. As Selection input is 00, so the device is now prepared for DES operation according to TABLE I. For 64 bit plaintext 12345ABCD132536 (hexadecimal) and 64 bit DES key AABB09182736CCDD it shows DES encrypted output D19CC746581BC403.

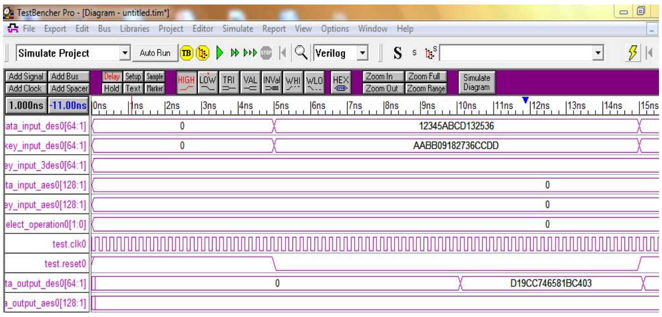

Fig. 8(a) Timing diagram of reconfigurable encryption system operation

Noticeable that, the time interval between providing inputs and getting ciphertext output is about twenty four clock cycles.

This time is required for storing inputs in the input registers, transferring data through the busses, DES encryption operation and storing outputs in the output registers. Other input situations like 3 DES key input, AES data and key input are insignificant as only DES operation is permitted here (select input=00).

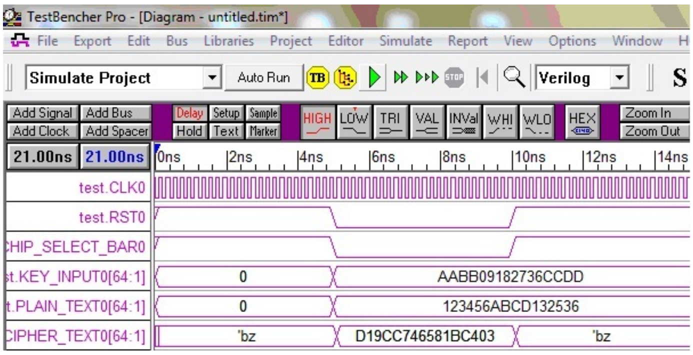

Fig. 8(b) Timing diagram of DES

To verify the operation of each logical unit, we simulated them one by one. The first thing to state is DES encoder. The simulation result of DES block is outlined in Fig. 8(b). When RESET and chip select bar are at low state, the block can encrypt plaintext by the assigned DES key. In the figure, plaintext is 123456ABCD132536 and key input is AABB09182736CCDD. As a result, the ciphertext output is D19CC746581BC403.

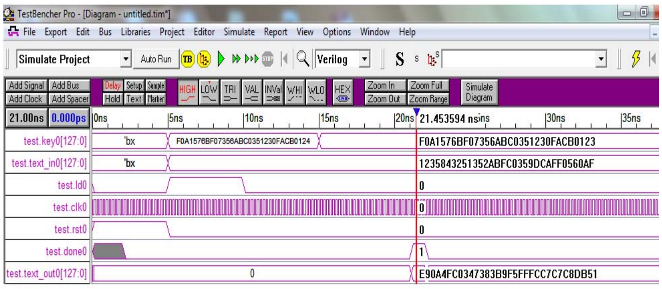
TestBencher Pro - [Diagram - untitled.tim*]
21.00ns
0.000ps
21.453594 nsins
test.key0[127:0]
'bx
F0A1576BF07356ABC0351230FACB0123
F0A1576BF07356ABC0351230FACB0123
test.text_in0[127:0]
'bx
1235843251352ABFC0359DCAFF0560AF
test.ld0
0
test.clk0
0
test.rst0
0
test.done0
1
test.text_out0[127:0]
0
E90A4FC0347383B9F5FFFCC7C7C8DB51

Fig. 8(c) Timing diagram of AES

AES encryption operation is illustrated in Fig. 8(c). An action is worthy only when reset is at low state. When ld (permission of loading) is at low state, the data busses transfers 128 bit plaintext and 128 bit AES key to the AES encryption section. It requires almost 30 clock cycles to encrypt in AES mode. In the first case of Fig. 8(c), everything is okay. But the input state is experimentally kept unchanged for less than 30 instruction cycles. So AES operation did not occur. In the second case, 128 bit plaintext 1235843251352ABFC0359DCAFF0560AF and 128 bit key F0A1576BF07356ABC0351230FACB0123 are passed to the AES encryption device. After about 30 clock cycles, the 'done' signal goes high from low state and the 128 bit ciphertext E90A4FC0347383B9F5FFFCC7C7C8DB51 is transferred to the output terminal. After that 'done' signal goes to low state; that means the device is now ready for further AES operation.

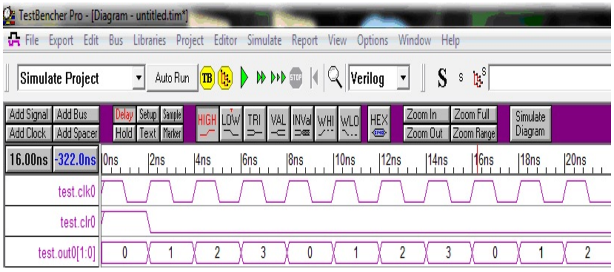

Fig. 8(d) Timing diagram of Pro PC

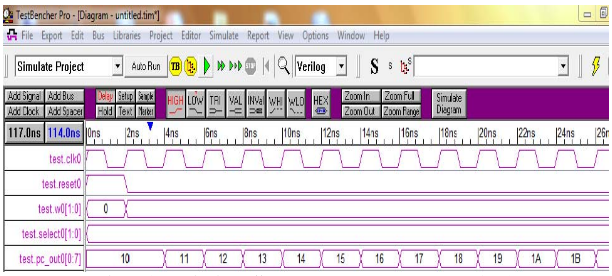

Fig. 8(e) Timing diagram Program Counter (PC)

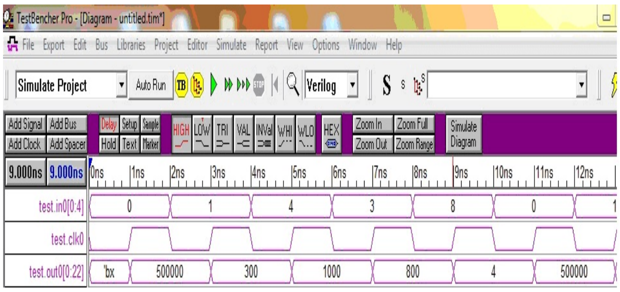

Fig. 8(f) Timing diagram of control unit

Fig. 8(d), 8(e) and 8(f) illustrate Pro PC, PC and control unit operations correspondingly. Pro PC is an independent counter that changes its states from 0 to 3 at each positive edge of clock pulses. PC is also a counter that gives count sequences depending upon Pro PC output and mode selection input. This occurs when reset=0. The control unit takes 5 bit input and provide a 23 bit control word. As an example, in the figure, when control input is 0, it delivers control word 50000. The time delay incurred is about half clock cycle.

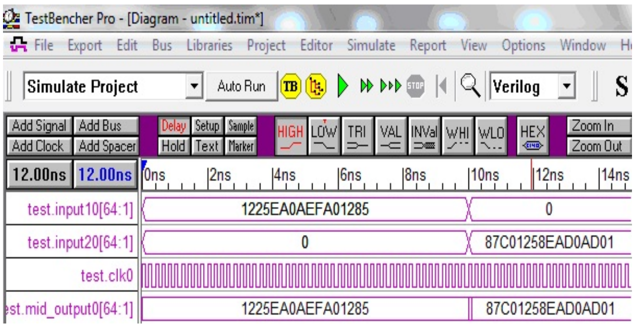

Fig. 8(g) Timing diagram of mid block

The operating behaviour of mid block is evident from Fig. 8(g). It shows that it can successfully perform logical OR operation of two 64 bit inputs. In the figure, the OR operation between 1225EA0AEFA01285 and 0 results to 1225EA0AEFA01285. The time delay for this is almost zero.

VII. Discussion

The configuration has two plaintext input ports and two ciphertext output ports. The first set is for 64 bit plaintext and ciphertext for DES and triple DES. The second set is for AES 128 bit plaintext and ciphertext. But users would like one input port and one output port only to reap the bliss of reconfigurability. This is kept for simpler design of PC and control unit and higher processing speed of the system.

After verification in RTL synthesis and Textbench simulation, the design was implemented in FPGA device SPARTAN 4 (model no: TM4XC4VLX25CES).

A further simplification of the architecture is also possible. It is expected to reduce the complexity and cost of implementation. That is the current research interest of the authors.

VIII. Conclusion

A reconfigurable encryption system for digital data encryption is introduced. It is designed in XST, simulated by Textbench and implemented in FPGA device SPARTAN 4. It may provide different levels of security to the user depending upon the order of safety required, delay tolerated and expense allowed by only one device. Therefore it is expected to be cost effective to use this device for multiple communications by using a single device.

References

[1] Paul C. van Oorschot, Alfred J. Menezes and Scott A.Vanstone, "Handbook of applied cryptography", CRC press Inc., Florida, 1996

[2] "*VPN Security",* February, 2008©The Government of the Hong Kong Special Administrative Region, www.infosec.gov.hk/english/technical/files/vpn.pdf

[3] Roy Hills, "Common VPN Security Flaws", NTA Monitor Ltd. white paper, January 2005, www.nta-monitor.com/posts/2005/01/VPN-Flaws-Whitepaper.pdf

[4] R. Atkinson. Security architecture for the internet protocol. *IETF Draft Architecture ipsec-arch-sec00*, 1996.

[5] Larry L. Peterson and Bruce S. Davie, *" Computer networks- A systems approach",* 3rd edition, page 580

[6] Ayushi, "*A Symmetric Key Cryptographic Algorithm",* ©2010 International Journal of Computer Applications (0975 - 8887), Volume 1 – No. 15

[7] Hamdan.O.Alanazi, B.B.Zaidan, A.A.Zaidan, Hamid A.Jalab, M.Shabbir and Y. Al-Nabhani, "*New Comparative Study Between DES, 3DES and AES within Nine Factors*", Journal Of Computing, Volume 2, Issue 3, March 2010, ISSN 2151-9617

[8] Majithia Sachin, Dinesh Kumar, *"Implementation and Analysis of AES, DES and Triple DES on GSM Network",* International Journal of Computer Science and Network Security, VOL.10 No.1, January 2010

[9] Neeraj Kumar, "Investigations in Brute Force Attack on Cellular Security Based on Des and Aes", IJCEM International Journal of Computational Engineering & Management, Vol. 14, October 2011 ISSN (Online): 2230-7893

[10] Marius Cristian Cerlinca, Adrian Graur, "Some considerations regarding software/hardware implementation of DES algorithm for an RFID enabled device", www.cybermova.com/uasoiro/files/Zbirnyk/2006/8/p_57.pdf

[11] Marius Cerlinca, Adrian Graur, Valentin Popa, "FPGA Implementation of an RFID Hub", 13th INTERNATIONAL SYMPOSIUM on POWER ELECTRONICS, Novi Sad, 2005, printed in Electronics, Banjaluka, 2005, ISSN 1450-5843, pp.57-59

[12] Marius Cerlinca, Adrian Graur, Valentin Popa, " FPGA Implementation of an RFID Dedicated SoC", ECUMICT, Gent, 2006, ISBN 9-08082-552-2, pp.201-204

[13] W. C. Barker, "Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher", NIST Special Publication 800-67, May 2004

[14] Andrew Watts and Anton Wanio, " *FPGA Implementation of Triple DES",* Copyright © 2008 Center for Systems Integration, Florida Atlantic University.

[15] P. Kitsos, S. Goudevenos and O. Koufopavlou, "VLSI Implementations Of The Triple-Des Block Cipher" ICECS-2003© 2003 IEEE

[16] National Inst. Of Standards and Technology, "Federal Information Processing Standard Publication 197, the Advanced Encryption Standard (AES)," Nov. 2001

[17] Xinmiao Zhang and Keshab K. Parhi, "Implementation Approaches for the Advanced Encryption Standard Algorithm," *IEEE Circuits and systems Magazine*, vol. 2, no. 4, pp. 24–46, 2003

[18] G. Rouvroy, F.-X. Standaert, F.-X.J.– J. Quisquater, J.-D. Legat, "Compact and Efficient Encryption/Decryption Module for FPGA Implementation of the AES Rijndael Very Well Suited for Small Embedded Applications," *Proc. ITCC-04 Conf.*, pp. 583-587, 2004

[19] Chih-Chung Lu and Shau-Yin Tseng, "Integrated Design of AES (Advanced Encryption Standard) Encrypter and Decrypter," *Proc. IEEE Int. Conf. on Application-Specific Systems, Architectures, and Processors, (ASAP'02)*, pp. 277-285, 2002

[20] Alina Stan*,* "Jericho Project, Secure communications: 'End-to-end encryption' in Jericho networks*" www.few.vu.nl/en/Images/stageverslag-stan_tcm39-90706.pdf*

[21] Christos Xenakis *, Nikolaos Laoutaris, Lazaros Merakos, Ioannis Stavrakakis, "A generic characterization of the overheads imposed by IPsec and associated cryptographic algorithms" © 2005 Elsevier B.V

[22] Shuenn-Shyang Wang and Wan-Sheng Ni, "An Efficient FPGA Implementation of Advanced Encryption Standard Algorithm", ISCAS 2004 © 2004 IEEE

[23] Fred Halsall, *"Computer Networking and the Internet"* , 5th edition

[24] Larry L. Peterson and Bruce S. Davie, *" Computer networks- A systems approach",* 3rd edition, page 580

[25] Andrew S. Tanenbaum, *"Computer Networks"*- 4th edition

[26] James F. Kurose, Keith W. Ross, *Computer Networking: A town approach",* 4th edition