Proceedings of the 2010 International Conference on Industrial Engineering and Operations Management
Dhaka, Bangladesh, January 9 – 10, 2010

A Compact FPGA Implementation of Triple-DES Encryption System with IP Core Generation and On-Chip Verification

Prasun Ghosal, Malabika Biswas and Manish Biswas
Department of Information Technology
Bengal Engineering and Science University
Shibpur, WB 711103, India

Abstract

This paper presents a fast and compact FPGA based implementation of the Data Encryption Standard (DES) and Triple Data Encryption Standard (TDES) algorithm, widely used in cryptography for securing the Internet traffic. The main objective of this paper is to provide the reader with a deep insight of the theory and design of a digital cryptographic circuit, which was implemented in a Vertex 5 series (XCVLX5110T) target device with the use of VHDL as the hardware description language. In order to confirm the expected behavior of these algorithm, the proposed design was extensively simulated, synthesized for different FPGA devices both in Spartan and Virtex series from Xilinx viz. Spartan 3, Spartan 3AN, Virtex 5, Virtex E device families. The novelty and contribution of this work is in three folds: (i) Extensive simulation and synthesis of the proposed design targeted for various FPGA devices, (ii) Complete hardware implementation of encryption and decryption algorithms onto Virtex 5 series device (XCVLX5110T) based FPGA boards and, (iii) Generation of ICON and VIO core for the design and on chip verification and analyzing using Chipscope Pro. The experimental as well as implementation results compared to the implementations reported so far are quite encouraging.

Keywords
Data Encryption Standard, Triple DES encryption, Encryption system, FPGA Implementation

1. Introduction
Beyond any doubt, the need for secure storage or transfer of information is an inextricable part of human history. Nowadays, the rapid evolution of communication systems offers, to a very large percentage of population, access to a huge amount of information and a variety of means to use in order to exchange personal data. Therefore, every single transmitted bit of information needs to be processed into an unrecognizable form in order to be secured. This enciphering of the data is necessary to take place in real time and for this procedure cryptography is the main mechanism to secure digital information. Due to the heavy increase in the volume of information data, a variety of encryption algorithms have been developed [1-7]. Among the different cryptographic algorithms, the most popular example in the field of symmetric ciphers is the Data Encryption Standard (DES) algorithm, which was developed by IBM in the mid-seventies.

The DES algorithm is popular and in wide use today because it is still reasonably secure and fast [2, 5-7, 9-11]. There is no feasible way to break DES, however because DES is only a 64-bit (eight characters) block cipher, an exhaustive search of 255 steps on average, can retrieve the key used in the encryption. A much more secure version of DES called Triple-DES (TDES), which is essentially equivalent to using DES three times on plaintext with three different keys. Naturally, it is three times slower than the original form of DES but it is way more secure.

This paper examines the full procedure of implementing a DES and Triple DES algorithm using a high-level hardware description language, VHDL, combined with the usage of FPGA technology. The complete design was synthesized for various FPGA devices of Spartan and Virtex series, viz Spartan 3, Spartan 3AN, Virtex E, Virtex 5 etc. The design is implemented and verified on a Virtex 5 FPGA development board from Xilinx using device XCVLX5110T. Next, ICON and VIO type of core was developed and the total implementation of DES and TDES was verified on chip using Chipscope Pro. The rest of the paper is organized as follows: Section II describes previous works and implementation of Cryptography algorithm i.e. DES and Triple DES, also give a brief introduction to the Data Encryption Standard and Triple Data Encryption Standard algorithm respectively. Section III will give experimental framework and results. Section IV will give the conclusions.

2. Background

2.1 Previous Work

A lot of research & development are going on over DES & Triple DES. DES and Triple-DES are already implemented in Spartan –II devices [6]. The design and implementation of DES and TDES processors was reported in [7, 12]. DES is also developed using the Handel-C. Others are reported in [3, 13, 14].

2.2 Data Encryption Standard

Complete function of DES algorithm can be described briefly as follows [1, 11]. DES is a block cipher. It operates on blocks of 64-bits in size. A 64-bit input block of plaintext will be encrypted into a 64-bit output block of cipher text. It is a symmetric algorithm, which means the same algorithm and key are used for encryption and decryption. The security of DES rests in the 56-bit key. The DES algorithm functions as follows [1-7, 11, 20]. The plaintext block is taken in and put through an initial permutation. The key is also taken in at the same time. The key is presented in a 64-bit block with every 8th bit being a parity check. The 56-bit key is then extracted ready for use. The 64-bit plaintext block is split into two 32- bit halves, named the right half and left half. The two halves of the plaintext are then combined with data from the key in an operation called Function F. There are 16 rounds of Function f, after which the two halves are recombined into one 64-bit block, which is then put through a final permutation to complete the operation of the algorithm and a 64-bit cipher text block is outputted. The detailed procedure is omitted due to paucity of space and is represented with a flowchart in Figure 1.

C. Data Encryption Standard Decryption

The decryption method is similar and omitted due to the paucity of the space.

D. Triple Data Encryption Standard

A concise representation of Triple Data Encryption Algorithm is described.

TDES is a block cipher operating on 64-bit data blocks. There are several forms, each of which uses the DES cipher three times. TDES can however work with one, two or three 56-bit keys. This means that the plaintext is, in effect, encrypted three times [2][5-7][9-11]. A number of modes of TDES have been proposed:

• DES-EEE3: Three DES encryptions with three different keys.

• DES-EDE3: Three DES operations in the sequence encrypt-decrypt-encrypt with three different keys.

• DES-EEE2 and DES-EDE2: Same as the previous formats except that the first and third operations use the same key.

Let $E_K(I)$ and $D_K(I)$ represent the DES encryption and decryption of I using DES key K respectively. Each TDEA encryption/decryption operation is a compound operation of DES encryption and decryption operations. The following operations are used:

1. TDEA encryption operation: the transformation of a 64-bit block I into a 64-bit block O that is defined as follows: $O = E_{K3}(D_{K2}(E_{K1}(I)))$.
2. TDEA decryption operation: the transformation of a 64-bit block I into a 64-bit block O that is defined as follows: $O = D_{K1}(E_{K2}(D_{K3}(I)))$.

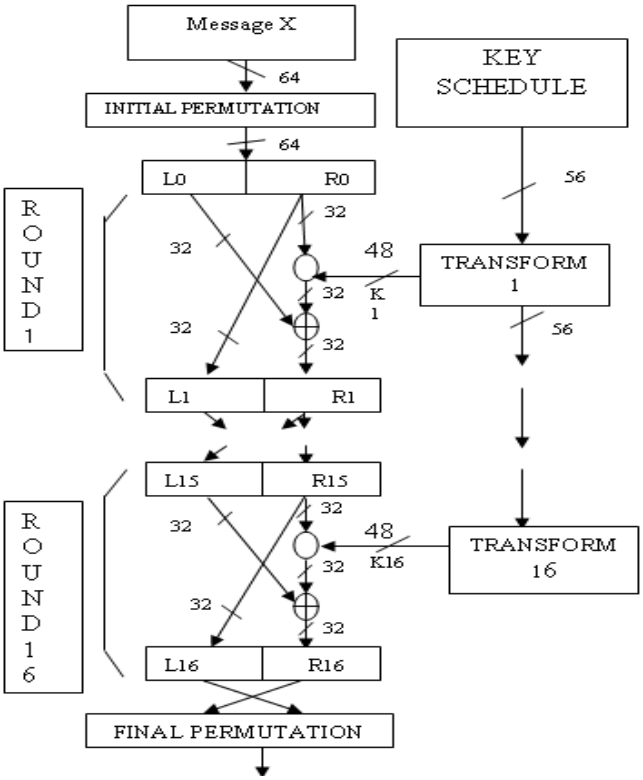

Figure 1: DES Encryption

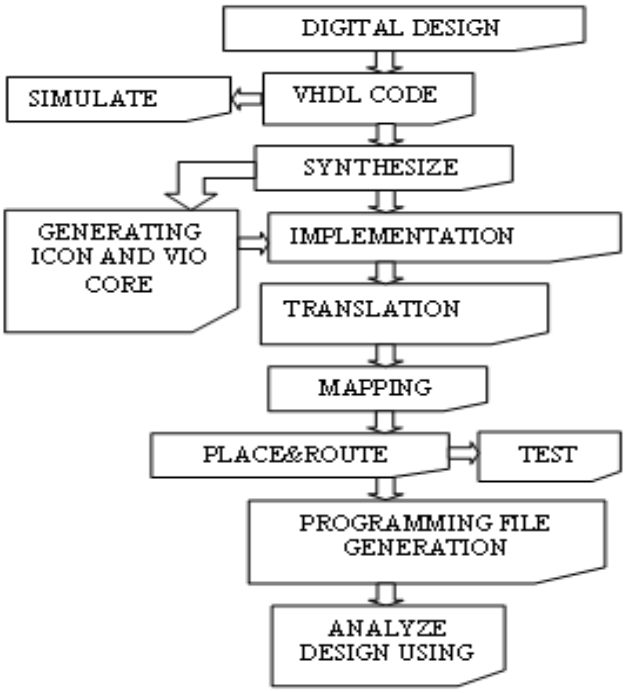

Figure 2: Implementation Course

3. Experimental Framework and Results

A. Synthesis and Implementation

The complete design was synthesized and implemented with the use of VHDL using ISE Foundation. Simulation was done by ISE simulator and Modelsim XE simulator. Core generation and on-chip verification was done by Chipscope Pro. Figure 2 represents the course that was followed for the digital implementation. The RTL architecture of DES and TDES is shown in Figure 3 and 4 respectively.

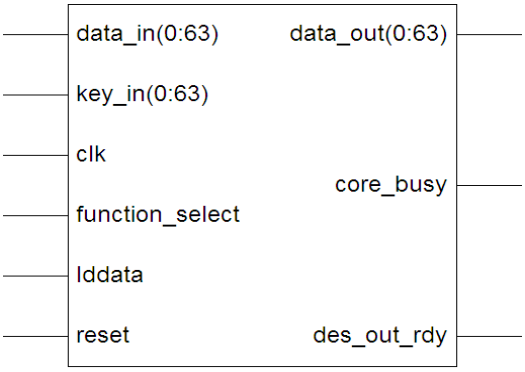

Figure 3: RTL Schematic of DES

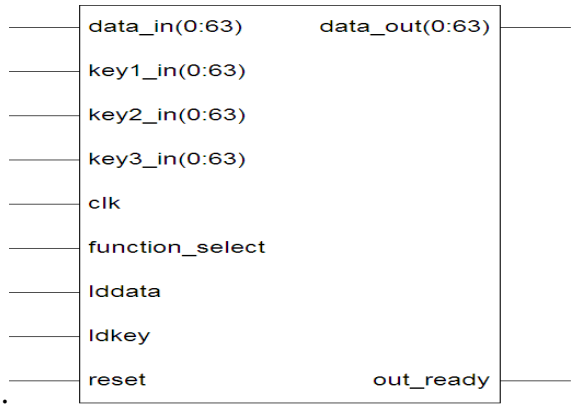

Figure 4: RTL Schematic of TDES

Figures 5 and 6 illustrate the implemented components inside the chip. Additionally, the interconnections of the components are shown.

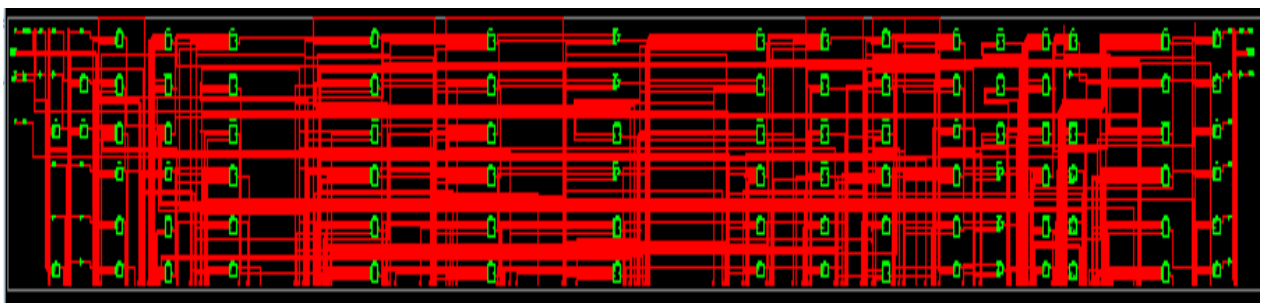

Figure 5: Technology Schematic of DES

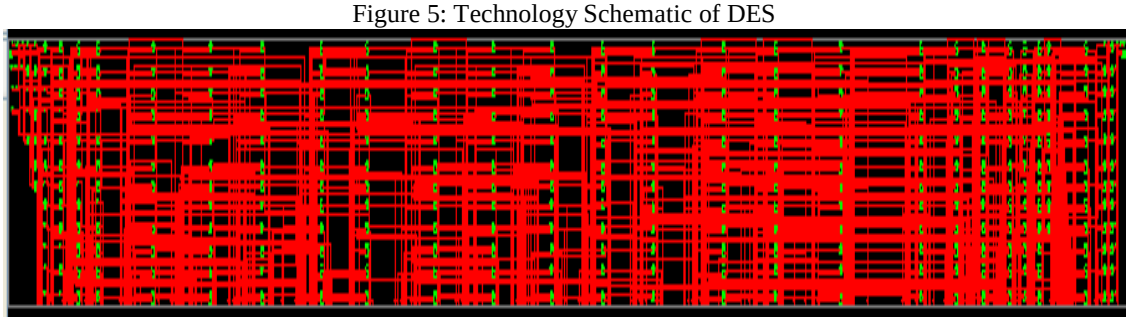

Figure 6: Technology Schematic of TDES

FPGA implementation of DES algorithm and TDES algorithm were accomplished on a Virtex5 device XCVLX5110T using Xilinx ISE Foundation 10.1i. Table 1 and Table 2 show the performance figures for DES hardware implementations. Table 3 and Table 4 show synthesis results of Triple DES implementations. The comparison between achieved results of DES for vertex E series and the existing implementations for Vertex E series [7] in Table 5.

Table 1: DES Synthesis result for Spartan series devices

	Spartan 3 (Target device xc3s400,Package fg320,Speed -5)		Spartan 3AN (Target device xc3s700AN,Package fgg484,Speed -5)	
Logic Utilization	Used	Utilization	Used	Utilization
Number of Slices	442 out of 28800	5%	461 out of 11264	4%
Number of Slice Flip Flops	281 out of 28800	1%	273 out of 22528	1%
Number of 4 input LUTs	789 out of 15681	5%	827 out of 22528	3%
Number of bonded IOBs	190 out of 391	48%	190 out of 502	37%
Number of GCLKs	1 out of 8	12%	1 out of 24	4%

Table 2: DES Synthesis result for Vertex series devices

	Vertex 5 (Target device XC5VLX50,Package ff1676,Speed -1)		Vertex 5 (Target device XC5VlX110T, Package f1136,Speed -1)	
Logic Utilization	Used	Utilization	Used	Utilization
Number of Slice Registers	266 Out of 28800	0%	266 Out of 69120	0%
Number of Slice LUTs	527 Out of 28800	1%	527 Out of 69120	0%
Number of fully used LUT-FF pairs	112 Out of 681	16%	112 Out of 681	16%
Number of bonded IOBs	190 Out of 440	43%	190 Out of 640	29%
Number of BUFG/BUFGCTRLs	1 Out of 32	3%	1 Out of 32	3%

Table 3: Triple-DES Synthesis result for Spartan series Devices

	Spartan 3 (Target device xc3s1000,Package fg676,Speed -5)		Spartan 3AN (Target device xc3s1400AN,Package fgg676,Speed -5)	
Logic Utilization	Used	Utilization	Used	Utilization
Number of Slices	1585 out of 7680	20%	1622 out of 11264	14%
Number of Slice Flip Flops	1254 out of 15360	8%	1230 out of 22528	5%
Number of 4 input LUTs	2494 out of 15360	16%	2593 out of 22528	11%
Number of bonded IOBs	302 out of 391	77%	302 out of 502	37%
Number of GCLKs	1 out of 8	12%	1 out of 24	4%

Table 4: Triple-DES Synthesis result for Vertex series Devices

	Vertex 5 (Target device XC5VLX50,Package ff1676,Speed -1)		Vertex 5 (Target device XC5VlX110T, Package f1136,Speed -1)	
Logic Utilization	Used	Utilization	Used	Utilization
Number of Slice Registers	1206 out of 28800	4%	1,206 Out of 69120	1%
Number of Slice LUTs	1690 out of 28800	5%	1,692 OUT OF 69120	2%
Number of fully used LUT-FF pairs	447 out of 2449	18%	632 Out of 2,266	27%
Number of bonded IOBs	302 out of 440	68%	302 Out of 640	47%
Number of BUFG/BUFGCTRLs	1 out of 32	3%	1 Out of 32	3%

Table 5: Triple-DES Synthesis result for Vertex E series Devices

	Triple-DES Implementation Result		Triple-DES Existing Implementation Result	
	Vertex E (Target device XCV1600E,Package bg560,Speed -8)		Vertex E (Target device XCV1600E,Package bg560,Speed -8)	
Logic Utilization	Used	Utilization	Used	Utilization
Number of Slices	1481 out of 15552	9%	12635 out of 14039	90%
Number of Slice Flip Flops	1256 out of 31104	4%	20505 out of 31104	65%
Number of 4 input LUTs	2396 out of 31104	7%	15518 out of 31104	49%
Number of bonded IOBs	302 out of 404	74%	243 out of 408	59%
Number of GCLKs	1 out of 4	25%	1 out of 4	25%

It is clear from the comparison result the proposed implementation is very much compact and efficient in all respects. The synthesis is carried out with the same Virtex E series device resulting in very less consumption of hardware components.

B. Core Generation, Analysis and On-chip Verification using Chipscope Pro

Xilinx Core Generator Tool provides core generation capability for the Integrated Controller core (ICON), Integrated Logic Analyzer core (ILA), Virtual Input/Output core (VIO), Integrated Bit Error Ratio core (IBERT), Agilent Trace Core 2 (ATC2). ChipScope Pro tools integrate key logic analyzer hardware components with the target design inside the supported devices. The ICON core provides a communication path between the JTAG Boundary Scan port of the target FPGA whereas the VIO core is a customizable core that can both monitor and drive internal FPGA signals in real time. In this design, after generating programming file three primary steps are: 1.Generate ICON & VIO cores using ChipScope Pro Generator, 2. Analyze & Implement the Design in ISE, 3. Drive & observe design inputs & outputs using ChipScope Pro Analyzer.

4. Conclusion

The proposed implementation of DES and TDES provide high-speed performance with very compact hardware implementation. It is a flexible solution for any cryptographic system and security layers of wireless protocol. Measurement results and comparisons between the proposed and previous hardware implementations are presented that shows quite encouraging results.

Acknowledgement

This research work was supported in part by the grant from All India Council for Technical Education (AICTE) under Research Promotion Scheme (RPS) by grant no. 8023/BOR/RID/RPS-92/07/08 dated 05.03.2008.

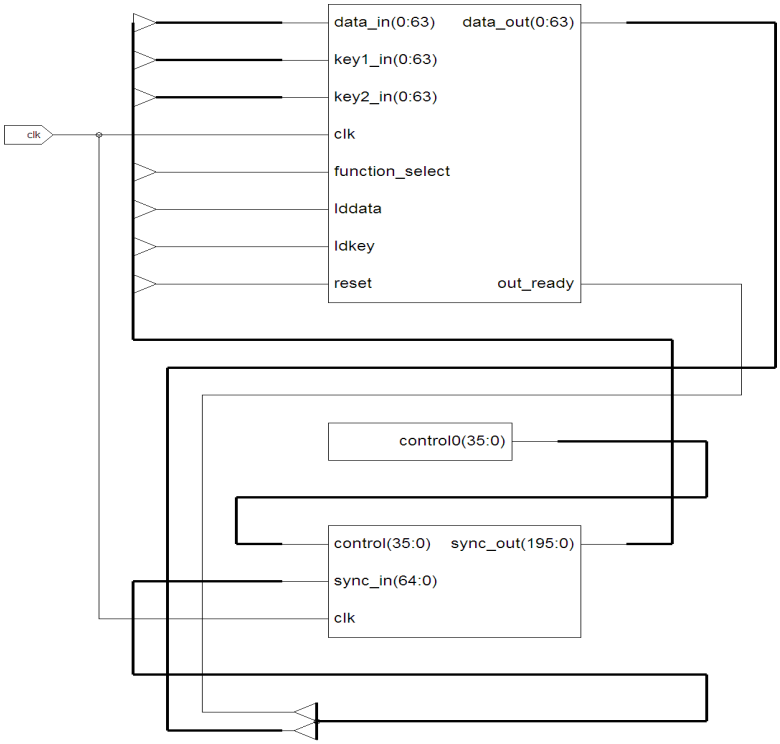

Figure 7: RTL Schematic of the VIO core of Triple-DES using ChipScope Pro

References

[1] "Data Encryption Standard (DES) ", Federal Information Processing Standard Publication, FIPS PUB 46-3, National Bureau of Standards, 1977.

[2] C. B. William, "Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher", Revised 19 May 2008, NIST Special Publication 800-67, Version 1.1.

[3] V. Kamakoti, G. Ananth and U.S. Karthikeyan, "Cryptographic Algorithm Using a Multi-Board FPGA Architecture", Nios II Embedded Processor Design Contest—Outstanding Designs 2005.

[4] F. D. Pereira, E. D. M. Ordonez, R. B. Chiaramonte, "VLIW Cryptoprocessor: Architecture and Performance in FPGAs", IJCSNS International Journal of Computer Science and Network Security, VOL.6 No.8A, August 2006.

[5] V. Pasham and S. Trimberger, “High-Speed DES and Triple DES Encryptor/Decryptor”, Xilinx Application Note: Virtex-E Family and Virtex-II Series, XAPP270 (v1.0) August 03, 2001.

[6] A. Dhir , "Data Encryption using DES/Triple-DES Functionality in Spartan-II FPGAs", White Paper: Spartan-II FPGAs, WP115 (v1.0) March 9, 2000.

[7] F. Antonios, P. Nikolaos, M. Panagiotis, A. Emmanouel, "Hardware Implementation of Triple-DES Encryption/ Decryption Algorithm", International Conference on Telecommunications and Multimedia, 2006.

[8] http://www.tropsoft.com/

[9] http://en.wikipedia.org/

[10] D. Stinson. “Cryptography: Theory and Practice”, 2nd Edition, Chapman and Hall/CRC, 2002.

[11] A. S. Tanenbaum, “Computer Networks”, 2003.

[12] T. Schaffer, Member, Alan Glaser, Member, and Paul D. Franzon, "Chip-Package Co-Implementation of a Triple DES Processor", IEEE Transactions on Advanced Packaging, Vol. 27, No. 1, February 2004.

[13] P. Kitsos, N. Sklavos, M. D. Galanis and O. Koufopavlou, “An FPGA-Based Performance Comparison Of The 64-Bit Block Ciphers”, Fifth International Symposium on Intelligent Automation and Control Seville, Spain June 28th-July 1st, 2004.

[14] F. Hoornaert, J. Goubert, and Y. Desmedt, “Efficient hardware implementation of the DES,” in Proc. Adv. Cryptol. (CRYPTO’84), 1984, pp. 147–173.