Efficient Hardware Realization of Advanced Encryption Standard Algorithm using Virtex-5 FPGA

Muhammad H. Rais and Syed M. Qasim
King Saud University, College of Engineering, Department of Electrical Engineering, Riyadh 11421, Saudi Arabia

Summary
This paper presents an efficient hardware realization of Rijndael Advanced Encryption Standard (AES) cryptographic algorithm using state-of-the-art Field Programmable Gate Array (FPGA). The design is coded in Very High Speed Integrated Circuit Hardware Description Language (VHDL). Timing simulation is performed to verify the functionality of the designed circuit. Performance evaluation is also done in terms of throughput and area. The design implemented on state-of-the-art Xilinx Virtex-5 (XC5VLX50FFG676-3) FPGA achieves a throughput of 4.34 Gbits/s using a total of 399 slices.

Key words:
Advanced Encryption Standard (AES), FPGA, VHDL, Virtex-5.

1. Introduction

Transmission of sensitive electronic financial transactions and digital signature applications have emphasized the need for fast and secure digital communication networks to achieve the requirements for secrecy, integrity, and non reproduction of exchanged information. Cryptography provides a method for securing and authenticating the transmission of information over insecure channels. To achieve high performance it is highly recommended to implement the cryptographic algorithms in hardware. Since modern security protocols are increasingly defined to be algorithm independent, a high degree of flexibility with respect to the cryptographic algorithms is desirable. A promising solution that combines high flexibility with the speed and physical security of application specific integrated circuits (ASICs) is the implementation of cryptographic algorithms on state-of-the-art reconfigurable devices such as field programmable gate array (FPGA).

Reconfigurable hardware such as FPGA offer math functions, embedded memories and storage elements, which makes the design of cryptography easier and provides reasonably cheap solution for designing and implementing various cryptographic algorithms.

Implementation of security protocols on FPGA leads to various advantages such as low cost, availability of sophisticated design and verification tools, ability of in-circuit reprogramability and short time to market which leads to the lower financial risk as compared to fully customized ASICs and potentially much higher performance than software implementations. Research efforts are underway to implement secure, fast and efficient cryptographic algorithms in hardware [1-3]. Vincent Rijmen and Joan Daeman [4] proposed and developed a new algorithm for Advanced Encryption Standard (AES). AES consists of 128 block length of bits and supports 128, 192 and 256 key length bits. The 128 bits are organized into state matrix which is of the size of 4×4. This algorithm starts with initial transformation of state matrix followed by nine iteration of rounds. A round consists of four transformations: Byte Substitution (SubBytes), Row Shifting (ShiftRows), Mixing of columns (MixColumns) and followed by addition of Round Key called (AddRoundKey). From each round, a round key is generated from the original key through key scheduling process. The last round consists of SubBytes, ShiftRows and AddRoundKey transformation.

SubBytes transformation is implemented using S-Box, which is highly computationally intensive and consumes more than 75% of FPGA resources [1]. The S-Box is based on the *Galois Field* GF (2^8), and it is the only non-linear component of the AES algorithm which provides confusion capability [5]. S-Box based on *Galois Field* GF (2^8) is constructed by performing two transformations; first taking a multiplicative inverse in the *Galois Field* GF (2^8) and then applying a standard affine transformation over *Galois Field* GF (2^8).

The S-Box is one of the most time consuming process because it is required in every round [6]. There are other fast and memory efficient algorithms that have been reported for the generation of S-Box [1, 3, 7-9]. Dedicated embedded memory blocks available in modern FPGAs are suitable for implementing S-Boxes [1]. The objective of this paper is to present an efficient hardware realization of AES algorithm using state-of-the-art reconfigurable hardware (Virtex-5 FPGA).

This paper is organized into five sections. Section 2 discusses the AES algorithm. Section 3 highlights on the past and current progress in the area of FPGA implementation of AES. Section 4 discusses the FPGA implementation results of our design. Finally, section 5 gives the concluding remarks.

Manuscript received September 5, 2009
Manuscript revised September 20, 2009

Table 1: S-Box based on Galois Field GF (2^8)

	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**a**	**b**	**c**	**d**	**e**	**f**
0	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
1	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
2	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
3	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
4	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
5	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
6	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
7	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
8	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
9	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
a	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
b	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
c	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
d	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
e	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
f	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

2. Advanced Encryption Standard

AES is based on Rijndael algorithm which is a symmetric block cipher that processes fixed data of 128-bit blocks. It supports key sizes of 128, 192 and 256 bits and consists of 10, 12 or 14 iteration rounds, respectively. In this paper, we will present the 128-bit version of AES with 10 rounds. Each round mixes the data with a round key, which is generated from the encryption key. The AES encryption structure is shown in Figure 1. The cipher maintains an internal, 4×4 matrix of bytes referred to as State, on which the operations are performed. Initially, State is filled with the input data block and XOR-ed with the encryption key.

Regular rounds consist of operations called SubBytes, ShiftRows, MixColumns and AddRoundKey. The last round bypasses MixColumns transformation. SubBytes transformation uses 16 identical 256-byte substitution table called S-box as shown in Table 1.

SubBytes can be implemented either by computing the substitution or using look-up-table (LUT). ShiftRows is a cyclic left shift of the second, third and fourth row of State by one, two, and three bytes, respectively. MixColumns performs a modular polynomial multiplication on each column. During each round, AddRoundKey performs XOR with State and the round key. Round key generation (key expansion) includes S-box substitutions, word rotations, and XOR operations performed on the encryption key. Depending on the security level required for the application, AES uses different key lengths.

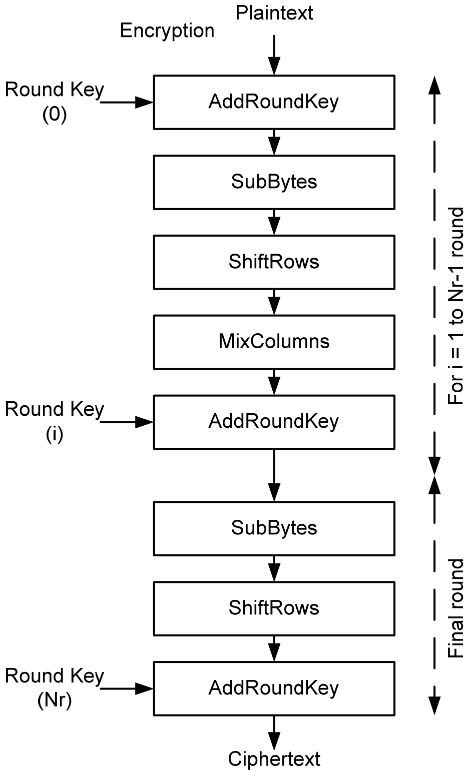

Fig. 1 AES Encryption Structure

3. Literature Review

Since 2001, many implementations have been presented showing different possible design to achieve highest throughput as well as compact area [10]. For embedded applications, the focus is on the reduction of area rather than the throughput. Therefore, several implementations with small logic requirements have also been published [9]. Research efforts to achieve further acceleration in throughput along with efficient utilization of memory and other FPGA resources are also underway [1, 11-12]. Numerous efforts to implement AES using ASICs are also presented [13-14]. Gielata et al. [15] presented hardware implementation of AES-128 cipher standard on FPGA technology. Since in many network applications software implementations of cryptographic algorithms are slow and inefficient, so to solve those problems, custom architecture in reconfigurable hardware was proposed to speed up the performance and flexibility of Rijndael algorithm implementation. They have reported to achieve the maximum speed and efficiency of cipher process, and have rather proposed pipeline architecture of AES modules using simulations and synthesis of VHDL code utilizing Virtex-4 series of Xilinx FPGA.

McLoone et al. [16] discussed high performance single chip FPGA implementations of the Rijndael. These designs were implemented on the Virtex-E FPGA family of devices. Gaj et al. [17] presented and analyzed the results of implementations of all five AES finalists using Xilinx FPGAs. Rady et al. [18] presented hardware implementation of optimized area for the block cipher AES-128 using FPGA. The proposed architecture was implemented in Spartan-3 XC3S400-5 chip with area utilization of 2699 slices and achieving a throughput of 10 Mbps. Pramstaller et al. [19] presented a compact implementation of AES encryption and decryption with all key lengths using a novel State representation, which solves the problem of accessing both rows and columns of the State.

Saleh et al. [20] proposed new hardware architecture for AES algorithm over GF (256) and has compared it against two AES hardware structures which were iterative looping and ten rounds pipeline approach respectively. Standaert et al. [21] addressed various approaches for efficient Virtex-E FPGA implementations of the AES Algorithm.

From the studies presented above, FPGAs are considered one of the important hardware platforms and integral part for the cryptographic algorithms implementation. FPGAs offer much easier and reasonably cheap solution for the implementation of cryptographic algorithm [10].

4. Implementation Results

The design of AES is done using VHDL and implemented in a Xilinx Virtex-5 XC5VLX50 (package: ffg676, speed grade: -3) FPGA using the ISE 9.2i design tool. Figure 2 and 3 shows the block diagram of AES and FPGA layout respectively. Figure 4 illustrates the timing simulation of AES. Table 2 summarizes the FPGA implementation results of AES using modular approach. It describes the selected target Xilinx FPGA device, encryption throughput achieved, timing reports and the overall device utilization.

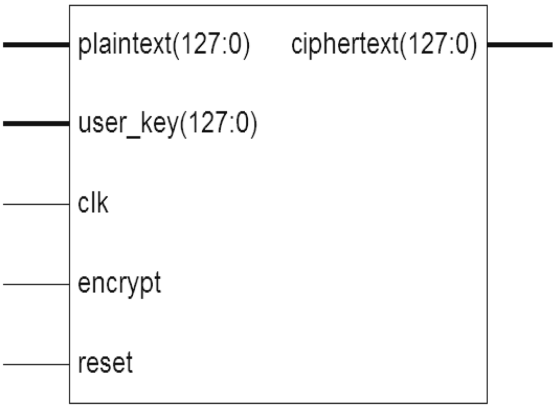

Fig. 2 Block diagram of AES

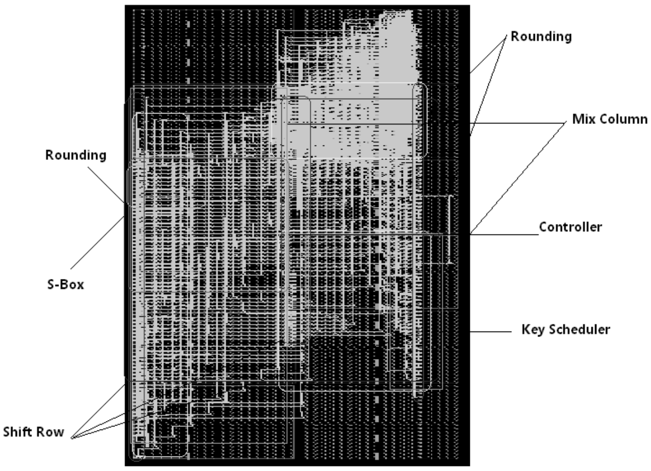

Fig. 3 FPGA Layout of AES

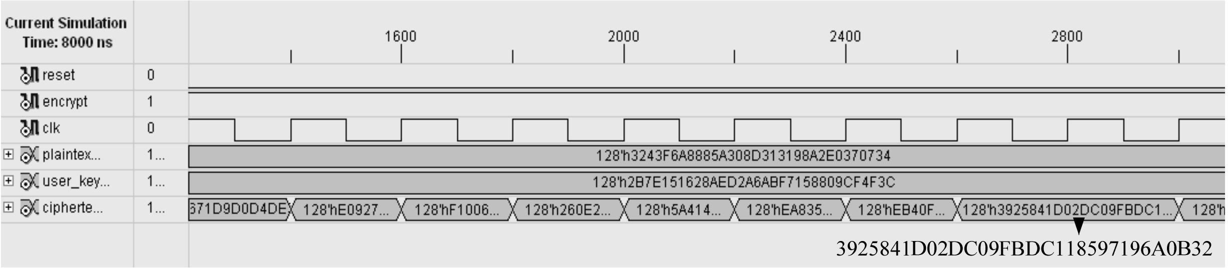

Fig. 4 Timing simulation of AES

Table 2: Implementation Results

Target FPGA device	Virtex-5 XC5VLX50
Encryption throughput	4.34 Gbps
Timing Report	
Speed grade	-3
Max. clock frequency	339.087 MHz
Min. period	2.949 ns
Min. input arrival time before clock	1.983 ns
Max. output required time after clock	2.610 ns
Device Utilization	
Number of Slice LUTs	1338 / 28800 4%
Number of occupied Slices	399 / 7200 5%
Number of fully used LUT-FF pairs	260 / 1338 19%
Total equiv. gate count for design	11926
Block RAMS	Zero

5. Conclusions

In this paper, a high performance and highly optimized hardware realization of Rijndael AES Algorithm has been designed and implemented on Xilinx Virtex-5 XC5VLX50 FPGA device. The design has been coded using modular approach by using VHDL Language. The design operates correctly as shown in the simulation result. The performance of the presented design is evaluated based on throughput and area. Our design utilizes a speed of 339.087 MHz, which translates to throughput of 4.34 Gbps using an area of 399 slices of a Virtex-5 FPGA.

Acknowledgement

The authors acknowledge the assistance and the financial support provided by the Research Center in the college of Engineering, King Saud University vide their Research Grant No. 39/429.

References

[1] A. Aziz and N. Ikram, "Memory efficient implementation of AES S-boxes on FPGA", Journal of Circuits, Systems, and Computers, Vol. 16, No. 4, pp. 603-611, 2007.

[2] E. L-. Trejo, F. R-. Henriquez and A. D-. Perez, "An efficient FPGA implementation of CCM using AES", in Proc. of the 8th International Conference on Information Security and Cryptology, Lecture Notes in Computer Science, Springer-Verlag, pp. 208-215, 2005.

[3] F. R-. Henriquez, N. A. Saqib and A. D-. Perez, "4.2 Gbits/s single chip FPGA implementation of AES algorithm", Electronics Letters, Vol. 39, No. 15, pp. 1115-1116, 2003.

[4] J. Daemen and V. Rijmen, "The design of AES-The Advance Encryption Standard" Springer-Verlag, 2002.

[5] M. T. Tran, D. K. Bui and A. D. Duong, "Gray S-Box for Advanced Encryption Standard", in Proc. of International Conference on Computational Intelligence and Security, Vol. 1, pp. 253-258, 2008.

[6] I. Harvey, "The effects of multiple algorithms in the Advanced Encryption Standard", nCipher Corporation Ltd., 2000.

[7] I. A-. Badillo, C. F-. Uribe and R. C-. Para, "Design and implementation of an FPGA-based 1.452 Gbps non pipelined AES architecture", in Proc. of the International Conference on Computational Science and its applications, Lecture Notes in Computer Science, Springer-Verlag, Vol. 3982, pp. 446-455, 2006.

[8] J. Zambreno, D. Nguyen and A. Choudhary, "Exploring area/delay tradeoffs in an AES FPGA implementation", in Proc. of International Conference on Field Programmable Logic and its Applications, Lecture Notes in Computer Science, Springer-Verlag, Vol. 3203, pp. 575-585, 2004.

[9] D. S. Kundi, S. Zaka, Q. Ain and A. Aziz, "A compact AES encryption core on Xilinx FPGA", in Proc. of 2nd International Conference on Computer, Control and Communication, pp.1-4, 2009.

[10] K. Järvinen, M. Tommiska, and J. Skyttä, "Comparative survey of high-performance cryptographic algorithm implementations on FPGAs", in Proc. of IEE on Information Security, Vol. 152, pp. 3-12, 2005.

[11] P. Chodowiec and K. Gaj, "Very compact FPGA implementation of the AES algorithm", in Proc. of Cryptographic hardware and embedded systems workshop, pp. 319-333, 2003.

[12] G. Rouvroy, F. -X. Standaert, J. -J. Quisquater, and J. -D. Legat, “Compact and efficient encryption/decryption module for FPGA implementation of the AES Rijndael very well suited for small embedded applications”, in Proc. of International Conference on Information Technology: Coding and Computing, Vol. 2, pp. 583-587, 2004.

[13] S. Mangard, M. Aigner and S. Dominikus, “A Highly Regular and Scalable AES Hardware Architecture”, IEEE Transaction on Computers, Vol. 52, No. 4, pp. 483-491, 2003.

[14] H. Kuo and I. Verbauwhede, “Architectural Optimization for a 1.82 Gbits/sec VLSI Implementation of the AES Rijndael Algorithm”, in Proc. of Cryptographic hardware and embedded systems workshop, Vol. 2162, pp. 51-64, 2001.

[15] A. Gielata, P. Russek and K. Wiatr, “AES hardware implementation in FPGA for algorithm acceleration purpose”, in Proc. of International Conference on Signals and Electronic Systems, pp. 137-140, 2008.

[16] M. McLoone and J. V. McCanny, “Rijndael FPGA implementations utilizing look-up tables”, Journal of VLSI Signal Processing Systems, Vol. 34, pp. 261-275, 2003.

[17] K. Gaj and P. Chodowiec, “Comparison of the Hardware Performance of the AES Candidates Using Reconfigurable Hardware”, in Proc. of Third Advanced Encryption Standard Candidate Conference, 2000.

[18] A. Rady, E. ElSehely, and A. M. ElHennawy, “Design and implementation of area optimized AES algorithm on reconfigurable FPGA”, in Proc. of International conference on Microelectronics, pp. 35-38, 2007.

[19] N. Pramstaller and J. Wolkerstorfer, “A universal and efficient AES co-processor for field programmable logic arrays”, in Proc. of 14th International Conference on Field-Programmable Logic and its Applications, pp. 565-574, 2004.

[20] A. H. Saleh and S. S. B Ahmed, “High performance AES design using pipelining structure over GF $((2^4)^2)$”, in Proc. of IEEE International Conference on Signal Processing and Communications, pp. 716-719, 2007.

[21] F.-X. Standaert, G. Rouvroy, J. -J. Quisquater and J. -D. Legat, “Efficient Implementation of Rijndael Encryption in Reconfigurable Hardware: Improvements and Design Tradeoffs”, in Proc. of Cryptographic hardware and embedded systems workshop, Lecture Notes in Computer Science, Vol. 2779, pp. 334-350, 2003.

Muhammad H. Rais received the Ph.D. degree in Electronics Engineering from the University of Western Australia, in 2000. He is an Assistant Professor in Department of Electrical Engineering at King Saud University. His major interest includes microelectronics, logic design, FPGA, VHDL, and characterization and modeling of semiconductor devices. He is member of IEEE and Institution of Engineers, Australia.

Syed M. Qasim received B.Tech and M.Tech Degrees in Electronics Engineering from Zakir Hussain College of Engineering and Technology, Aligarh Muslim University, India in 2000 and 2002 respectively. Currently he is working as a researcher at Electrical Engineering Department, King Saud University. His areas of interest include Digital VLSI System Design and Reconfigurable computing using FPGAs. He is a member of the Institution of Electronics and Telecommunication Engineers, India and International Association of Engineers, Hong Kong.