A Novel FPGA Implementation of AES-128 using Reduced Residue of Prime Numbers based S-Box

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

Summary
In this paper, we present a novel Field Programmable Gate Array (FPGA) implementation of advanced encryption standard (AES-128) algorithm based on the design of high performance S-Box built using reduced residue of prime numbers. The objective is to present an efficient hardware realization of AES-128 using very high speed integrated circuit hardware description language (VHDL). The novel S-Box look up table (LUT) entries forms a set of reduced residue of prime number, which forms a mathematical field. The S-Box with reduced residue of prime number adds more confusion to the entire process of AES algorithm and makes it more complex and provides further resistance against attacks. The target hardware used in this paper is state-of-the-art Virtex-5 XC5VLX50 FPGA from Xilinx. The proposed design achieves a throughput of 3.09 Gbps using only 1745 slices.

Key words:
Advanced Encryption Standard (AES), Very High Speed Integrated Circuit Hardware Description Language (VHDL), Field Programmable Gate Array (FPGA), Virtex-5.

1. Introduction

Since its inception, encryption has evolved within many fields especially in the field of communications and security networks. For security and fast transmission of data over an insecure path, cryptography methods have been used so far. For this reason, many researchers [1-3] are trying to implement secure, fast and efficient cryptographic algorithms in hardware using very high speed integrated circuit hardware description language (VHDL) or Verilog. Advanced Encryption Standard (AES) algorithm was developed by Vincent Rijmen and Joan Daeman and named as Rijndael cipher algorithm [4]. 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 computationally intensive and consumes more than 75% of FPGA resources [1]. The S-Box is based on the Galois Field GF (256), and it is the only non-linear component of the AES algorithm which provides confusion capability [5]. The new approach reported in [6] uses residue of prime numbers, which adds more confusion than the normally used Galois Field GF (256). S-Box based on Galois Field GF (256) is constructed by performing two transformations; first taking a multiplicative inverse in the Galois Field GF (256) and then applying a standard affine transformation over Galois Field GF (256). The S-Box is one of the most time consuming process because it is required in every round [7]. There are other fast and memory efficient algorithms that have been reported [1, 3, 8-10] but such methods are insecure and potential threat to the security of the data [6]. Other issues pertaining to this which were not given due importance is to accelerate the process, and in order to do that, a reduced residue of prime numbers can be utilized, which results in table entries similar to S-Box based on Galois Field GF (256) [6]. In this paper, a new S-Box algorithm which provides more confusion based on reduced residue of prime number is coded using VHDL and targeted to Xilinx Virtex-5 FPGA. To the best of our knowledge there exists no previous work of implementing AES using FPGA based on S-Box using reduced residue of prime numbers till date.

The rest of the paper is organized as follows: Section 2 present the details of AES algorithm. S-Box design using residue of prime number and its reduced version is described in section 3. The target FPGA technology is described briefly in section 4. Section 5 presents the related work of AES algorithm implementation in hardware. The FPGA implementation results and concluding remarks are provided in sections 6 and 7 respectively.

2. Advanced Encryption Standard

The AES was selected in 2000 by the US National Institute of Standards and Technologies (NIST) as a

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

replacement to the Data Encryption Standard (DES) block cipher. AES has grown in popularity over the past few years and has been accepted as the defacto standard in the cryptographic community. 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 focus on the 128-bit version with 10 rounds. Each round mixes the data with a round key, which is generated from the encryption key. Figure 1 illustrates the encryption round operations. 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 exclusive-ored with the encryption key.

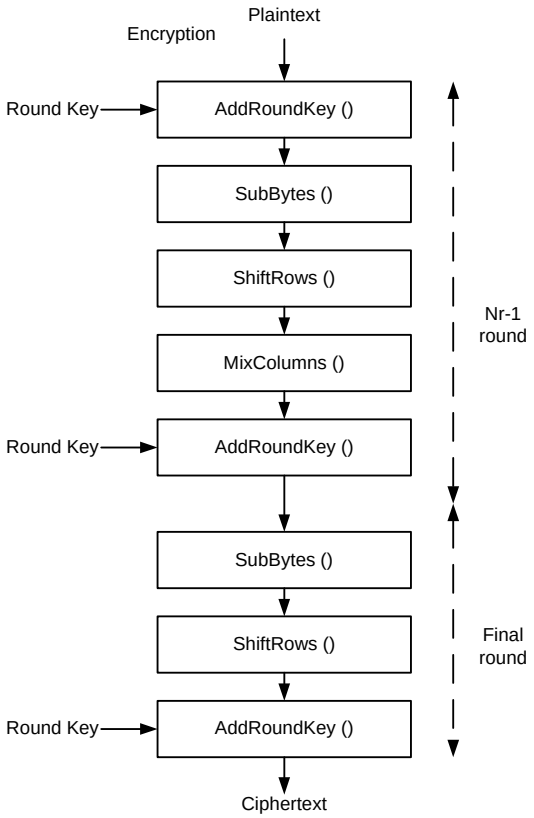

Figure 1 AES Encryption Round operations

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 tables called S-box.

SubBytes can be implemented either by computing the substitution or using 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.

3. S-Box using residue of prime numbers

The S-Box based on residue of prime numbers is a complete S-Box with 256 entries. The entries shown in Table 1 are the residue of the prime number 257. The row and column headers of Table 1 are hexadecimal digits. The Table 2 shows the reduced version of Table 1. As presented in Table 2, the eliminated half entries are unknown, so it creates more confusion to the S-Box implementation which is not present in Galois Field GF (256) based S-Box as presented in Table 3 [6]. Research efforts are underway in this area where researchers have been trying to implement other fast and efficient algorithms to generate S-Box [1-3, 8-10].

4. Field Programmable Gate Array

An FPGA is a digital integrated circuit that can be programmed after it is manufactured rather than being limited to a predetermined, unchangeable hardware function. Latest FPGAs 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 algorithms [11]. Implementation of security protocols on FPGA leads to the various advantages such as low cost, availability of sophisticated design and debugging tools, ability of in-circuit reprogramability and short time to market which leads to the lower financial risk in comparison to the fully customized ASICs and potentially much higher performance than software implementations.

5. Related work

Major effort led towards the implementation of AES using ASICs by many leading research groups [11-13]. McLoone et al. [14] 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. [15] presented and analyzed the results of implementations of all five AES finalists using Xilinx FPGAs.

Gielata et al. [16] investigates hardware implementation of AES-128 cipher standard on FPGA technology. Since in many network applications software implementations of cryptographic algorithms are slow and inefficient, in order to solve those problems custom architecture in

Table 1 S-Box based on residue of prime number 257

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

Table 2 S-Box based on reduced version of residue of prime number 257

	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**a**	**b**	**c**	**d**	**e**	**f**
0	00	01	81	56	c1	67	2b	93	e1	c8	b4	bb	96	b2	ca	78
1	f1	79	64	e6	5a	31	de	be	4b	48	59	ee	65	c3	3c	c7
2	f9	94	bd	eb	32	84	73	91	2d	a3	99		6f		5f	af
3	a6			7e	ad	61	77	f3	b3	f8	e2	3d			e4	66
4	fd	57	4a	ea	df	95	f6	b5		a9			ba	f7	c9	f4
5	97	a5	d2	60	cd	7f			b8			d1	b0	98	d8	
6				87					d7	a4	b1	f5	bc	e0	fa	
7	da	74	7c			86	9f				9e	8c		dc		
8	ff		ac	ce		8f			f0	f2	cb	62		90	db	
9			d5								fc	c2	e5	ef		
a	cc	ae	d3					ed	e7		c0	fe				
b							e9	bf		e8						
c					c6	e3										dd
d	ec				d9		fb									
e																
f																

Table 3 S-Box based on Galois Field GF (256)

	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

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.

Saleh et al. [17] 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. Rady et al. [18] presented a 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. Standaert et al. [19] addressed various approaches for efficient Virtex-E FPGA implementations of the AES Algorithm.

In embedded applications, it is required to minimize the area rather than to maximize the throughput. Therefore, several implementations with small logic requirements have been published [10]. Pramstaller et al. [20] 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.

Therefore, FPGAs are considered one of the integral part of the cryptographic hardware implementation in order to achieve further acceleration in throughput and efficient utilization of memory and other hardware resources [1, 21-22].

6. Implementation results

The design of AES using reduced residue of prime number based S-Box 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. Table 4 shows the FPGA implementation results of AES using reduced residue of prime number based S-Box. It describes the selected target Xilinx FPGA device, encryption throughput achieved, timing reports and the overall device utilization.

7. Conclusions

In this paper, we have presented a novel FPGA implementation of AES utilizing high performance S-Box which uses reduced residue of prime numbers. The proposed design was implemented on Xilinx Virtex-5 XC5VLX50 FPGA device. The objective is to use a novel S-Box based on LUT whose entries are set of residue of prime number. The S-Box with reduced residue of prime number adds more confusion to the entire process of AES algorithm and makes it more complex and provides further resistance against attacks. Our implementation achieves a throughput of 3.09 Gbps and uses a total of 1745 slices of a Virtex-5 FPGA.

Table 4 Implementation Results

Target FPGA device	Virtex-5 XC5VLX50
Encryption throughput	3.09 Gbps
Timing Report	
Speed grade	-3
Max. clock frequency	242.153 MHz
Min. period	4.130 ns
Min. input arrival time before clock	2.254 ns
Max. output required time after clock	2.622 ns
Device Utilization	
Number of Slice LUTs	5256 / 28800 18%
Number of occupied Slices	1745 / 7200 24%
Number of fully used LUT-FF pairs	260 / 5258 4%
Total equiv. gate count for design	44689
Block RAMS	Zero

Acknowledgement

The authors acknowledge the assistance and the financial support provided by the Research Center in the College of Engineering under their Research Grant 39/429 at King Saud University.

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] E. S. Abuelyman and A. A. S. Alsehibani, "An optimized implementation of the S-Box using residue of prime numbers", International Journal of Computer Science and Network Security, Vol. 8, No. 4, pp. 304-309, 2008.

[7] I. Harvey, "The effects of multiple algorithms in the Advanced Encryption Standard", nCipher Corporation Ltd., 2000.
[8] 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.
[9] 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.
[10] 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.
[11] 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.
[12] A. Satoh, S. Morioka, K. Takano and S. Munetoh, "A Compact Rijndael Hardware Architecture with S-Box Optimization", in Proc. 7th International Conference on Theory and Application of Cryptology and Information Security: Advances in Cryptology, pp. 239-254, 2001.
[13] 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.
[14] 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.
[15] 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.
[16] 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.
[17] 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.
[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] 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.
[20] 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.
[21] 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.
[22] 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.

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.