American Journal of Applied Sciences 8 (8): 754-757, 2011
ISSN 1546-9239

Efficient Realization of S-Box based reduced Residue of Prime Numbers using Virtex-5 and Virtex-6 FPGAs

Mohammed H. Al Mijalli
Biomedical Technology Department, College of Applied Medical Sciences, King Saud University, Riyadh, Saudi Arabia

Abstract: Problem statement: The S-Box transformation is a computationally intensive and important operation of the Advanced Encryption Standard (AES). **Approach:** This study presents the comparative study between reduced Residue of Prime Numbers and Galois Filed GF (2^8) based S-Boxes using Virtex-5 and Virtex-6 FPGA devices. The implementation of S-Boxes is done using Very High speed integrated circuit Hardware Description Language (VHDL). **Results:** The results obtained from Virtex-6 FPGA show that the proposed method runs at a clock frequency of 0.785ns, which is three times faster than S-Box based on Galois Filed GF (2^8). **Conclusion:** The reduced version of the S-Box based on prime number shows promising results as compared to Galois Field GF (2^8) based S-Box, which could be used in AES to increase its complexity and add more confusion.

Key words: Advanced Encryption Standard (AES), Field Programmable Gate Array (FPGA), Galois Field GF (2^8), reduced residue of prime number, Virtex-5, Virtex-6, VHDL

INTRODUCTION

The National Institute of Standards and Technology (NIST) has adopted a block cipher, which was subsequently developed by Belgian researchers Vincent Rijmen and Joan Daemen and named as Rijndael cipher algorithm Advanced Encryption Standard (AES) (FIPS-197, 2001; Daemen and Rijmen, 2002). The transmission of sensitive electronic financial transactions and digital signature applications heavily rely on cryptographic algorithms. Cryptographic algorithms offer secrecy, integrity and non-reproduction of exchanged information over the fast and insecure digital communication networks. The implementation of cryptographic algorithms on the Field Programmable Gate Array (FPGA) provides a promising solution that combines with high flexibility with the speed and as well as physical security of traditional hardware Application Specific Integrated Circuits (ASICs) (Mangard *et al*., 2003).

The substitution box (S-Box) is a computationally intensive and requires more than 75% of the FPGA resources (Aziz and Ikram, 2007). The S-Box is a non-linear component of the AES algorithm based on the Galois Field GF (2^8) provides confusion capability (Tran *et al*., 2008). 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 based on residue of prime numbers (Abuelyman, and Alsehibani, 2008) adds more confusion than the S-Box based Galois Field GF (2^8), because it exploits most of the resources since it is required in every round (Harvey, 2000). To date, researcher (Aziz and Ikram, 2007; Henriquez *et al*., 2003; Zambreno *et al*., 2004; Badillo *et al*., 2006; Talwar and Rajpal, 2006; Li *et al*., 2007; Kundi *et al*., 2009; RezaeiPour and Said, 2009; Mirvaziri *et al*., 2009; Kundi *et al*., 2010) have reported S-Box based fast and efficient algorithms, but no one has look at the importance of data security, which is also very important. The acceleration of the process is also one of the prime factors and the security of the data is another. Looking at these important parameters a S-Box based on reduced Residue of Prime Numbers can be used, which results in similar table entries to S-Box based on Galois Field GF (2^8) (Abuelyman and Alsehibani, 2008).

Advanced Encryption Standard: The AES is a symmetric block cipher that processes fixed data of 128-bit blocks. It supports key sizes of 128, 192-256 bits and consists of 10, 12 or 14 iteration rounds.

Corresponding Author: Mohammed H. Al Mijalli, Biomedical Technology Department, College of Applied Medical Sciences, King Saud University, Riyadh, Saudi Arabia

Table 1: 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																

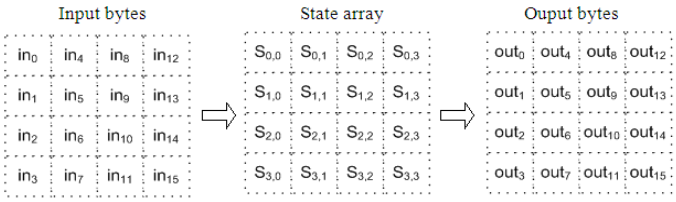

Fig. 1: Mapping of Input bytes, State array and Output bytes

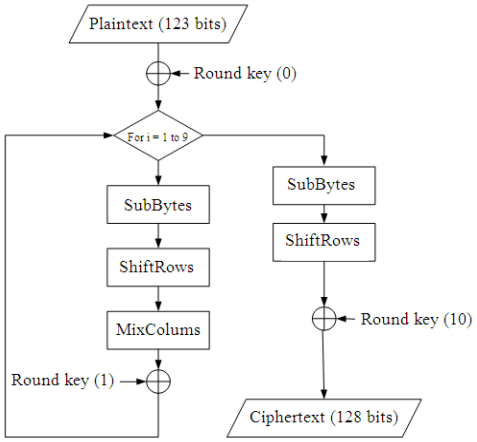

Fig. 2: AES algorithm structure

The AES algorithm's internal operations are performed on a two dimensional array of bytes called State. The 128 bits are organized into state matrix which is of the size of 4×4. State is filled with the input data block and XOR-ed with the encryption key. At the start of encryption the array of input bytes is mapped to the State array as shown in Fig. 1. The 128-bit block can be expressed as 16 bytes: in0, in1, in2, …, in15. Encryption process is performed on the State and then State values are mapped to the output bytes array out0, out1, out2,…, out15.

The AES algorithm is an iterative algorithm and each iteration is called a round. Each round mixes the data with a round key, which is generated from the encryption key. Figure 2 presents AES algorithm structure with round operations. As shown in Fig. 2, each of the nine rounds consists of four transformations: SubBytes, ShiftRows, MixColumns and AddRoundKey with the exception of MixColumns transformation in the last round. SubBytes can be implemented either by computing the S-box, which is consists of 16 identical 256-byte substitution table or using Look-Up-Table (LUT).

MATERIALS AND METHODS

The S-Box based on Residue of Prime Numbers is a complete S-Box with 256 entries and the full details of this table is given in (Abuelyman and Alsehibani, 2008; Rais and Qasim, 2010). The Table 1 shows the reduced version of S-Box based on Residue of Prime Numbers. As it is reported in (Abuelyman and Alsehibani, 2008; Rais and Qasim, 2010) S-box based on reduced Residue of Prime Numbers produces more confusion, which is not present in Galois Field GF (2^8) based S-Box.

Table 2: Performance evaluation of a Galois Field GF (2^8) and reduced Residue of Prime Number based S-Box design using Virtex-5 (Rais and Qasim, 2010)

	Galois field GF (2^8) / Residue of Prime Numbers	Reduced version of Residue of Prime Numbers
Frequency (MHz)	371.609	512.821
Period (ns)	2.691	1.950
BRAMs	1	Zero
Occupied slices	2	31

Table 3: Performance evaluation of a Galois Field GF (2^8) and reduced Residue of Prime Numbers based S-Box design using Virtex-6

	Galois field GF (2^8) / Residue of Prime Numbers	Reduced version of Residue of Prime Numbers
Frequency (MHz)	402.739	1273.885
Period (ns)	2.483	0.785
BRAMs	1	Zero
Occupied Slices	1	43

RESULTS

The design of Galois Field GF (2^8) and reduced Residue of Prime Numbers based S-Box is done using VHDL and implemented in a Xilinx Virtex-5 XC5VLX50 (Xilinx, 2009) (package: ffg676, speed grade: -1) and Virtex-6 FPGA XC6VLX75T (Xilinx, 2011) (package: ffg484, speed grade: -1) using the ISE 12.1 design tool (Xilinx, 2010).

DISCUSSION

The performance of the proposed design is evaluated based on the FPGA implementation results. Table 2-3 present the FPGA implementation results of both the designs using Virtex-5 and Virtex-6 FPGA devices. Compared with the design using Galois Field GF (2^8), reduced Residue of Prime Numbers based S-Box operates at a maximum clock frequency of 512.821 MHz using Virtex-5 and 1273.885 MHz using Virtex-6. The proposed design utilizes only 31 occupied slices of Virtex-5 FPGA and 43 occupied slices of Virtex-6 FPGA as compared to 2 occupied slices and 1 block RAM (BRAM) used in Galois Field GF (2^8) based S-Box design for Virtex-5 and 1 occupied slice and 1 BRAM for Virtex-6 FPGAs.

CONCLUSION

In this study we have presented a resource efficient and much faster S-Box design based on the reduced Residue of Prime Numbers. The proposed design is implemented in Xilinx Virtex-5 and Virtex-6 FPGAs and the results are compared with that of Galois Field GF (2^8). The reduced version shows promising results which could be used in AES to increase its complexity and add more confusion in order to provide further resistance against algebraic attacks.

ACKNOWLEDGEMENT

The researcher acknowledges the assistance and the financial support provided by the Cornea Research Chair, College of Applied Medical Sciences, King Saud University. In particaular, I would like to thank Dr. Muhammad H. Rais for his vaulable support in this study.

REFERENCES

Abuelyman, E.S. and A.A.S. Alsehibani, 2008. An optimized implementation of the S-Box using residue of prime numbers. IJCSNS Internat. J. Comput. Sci. Network. Security, 8: 304-309. http://paper.ijcsns.org/07_book/200804/20080443.pdf

Aziz, A. and N. Ikram, 2007. Memory efficient implementation of AES S-boxes on FPGA. J. Circu. Syst. Comp., 16: 603-611. DOI: 10.1142/S0218126607003873

Badillo, I.A-., C.F-. Uribe and R. Cumplido, 2006. Design and implementation of an FPGA-based 1.452 Gbps non pipelined AES architecture, Proceedings of the International Conference on Computational Science and its applications, Lecture Notes in Computer Science, Springer, pp: 456-465. DOI: 10.1007/11751595_49

Daemen, J., V. Rijmen, 2002. The design of Rijndael AES-The Advanced Encryption Standard. 1st Edn., Springer, ISBN: 3540425802, pp: 255.

FIPS-197, 2001. Federal Information Processing Standards Publication FPIS-197, Advanced Encryption Standard (AES). http://csrc.nist.gov/publications/fips/fips 197/fips-197.pdf

Harvey, I., 2000. The effects of multiple algorithms in the Advanced Encryption Standard, nCipher Corporation Ltd. http://csrc.nist.gov/archive/aes/round2/conf3/papers/06-iharvey.pdf

Henriquez, F.R., N.A. Saqib and A.D. Perez, 2003. 4.2 Gbits/s single chip FPGA implementation of AES algorithm. Electro. Lette., 39: 1115-1116. DOI: 10.1049/eI: 20030746

Kundi, D.S., A. Aziz and N. Ikram, 2010. Resource efficient implementation of T-Boxes in AES on Virtex-5 FPGA, Information Processing Letters 110: 373-377. DOI: 10.1016/j.ipl.2010.03.004

Kundi, D.S., S. Zaka, Q. Ain and A. Aziz, 2009. A compact AES encryption core on xilinx FPGA. Contr. Commun. (IC-4), 1: 1-4. DOI: 10.1109/IC4.2009.4909251

Li, M., G. Dai, H. Liu and W. Hu, 2007. Design of an instruction for fast and efficient S-box implementation. Proceedings of the International Conference on Computational Intelligence and Security, IEEE Computer Society Washington, DC, USA., pp: 623-626. http://portal.acm.org/citation.cfm?id=1333055

Mangard, S., M. Aigner and S. Dominikus, 2003. A highly regular and scalable AES hardware architecture. IEEE Trans. Comput., 52: 483-491. DOI: 10.1109/TC.2003.1190589

Mirvaziri, H., K.J.M. Ismail and Z.M. Hanapi, 2009. Message based random variable length key encryption algorithm. J. Comput. Sci., 5: 573-578. DOI: 10.3844/jcssp.2009.573.578

RezaeiPour, D. and M.R.M. Said, 2009. New directions in cryptanalysis of block ciphers. J. Comput. Sci., 5: 1091-1094. DOI: 10.3844/jcssp.2009.1091.1094

Rais, M.H. and S.M. Qasim, 2010. Efficient FPGA realization of s-box using reduced residue of prime numbers. IJCSNS Intern. J. Comp. Sci. Netw. Security, 10: 69-73. http://paper.ijcsns.org/07_book/201001/20100110.pdf

Talwar, Y., C.E.V. Madhavan and N. Rajpal, 2006. On partial linearization of byte substitution transformation of Rijndael-the AES. J. Comput. Sci., 2: 48-52. DOI: 10.3844/jcssp.2006.48.52

Tran, M.T., D.K. Bui and A.D. Duong, 2008. Gray S-box for advanced encryption standard. Comput. Intell. Security., 1: 253. DOI: 10.1109/CIS.2008.205

Xilinx, 2009. Virtex-5 FPGA Documentation. http://www.xilinx.com/support/documentation/virtex-5.htm

Xilinx, 2010. ISE 12.1 design tool. http://www.xilinx.com/support/documentation/dt_ise12-1.htm

Xilinx, 2011. Virtex-6 FPGA family overview. http://www.xilinx.com/support/documentation/virtex-6.htm

Zambreno, J., D. Nguyen and A. Choudhary, 2004. Exploring area/delay tradeoffs in an AES FPGA implementation field programmable logic and its applications. Lectu. Note.Compu. Scien. Sprin., 3203: 575-585. DOI: 10.1.1.92.6824