World Applied Sciences Journal 18 (10): 1343-1346, 2012
ISSN 1818-4952

DOI: 10.5829/idosi.wasj.2012.18.10.1978

Field Programmable Gate Array Based Realization of S-Boxes

Muhammad H. Rais and Mohammed H. Al-Mijalli

Department of Biomedical Technology,
College of Applied Medical Sciences, King Saud University, Riyadh, Saudi Arabia

Abstract: This letter presents the comparative study between Galois Field GF (2^8) S-Box, Gray S-Box and Skipjack S-Box. The Galois Field GF (2^8), Gray and Skipjack S-Boxes implemented in Virtex-5 XC5VLX50 (package: ff676, speed grade: -1), XC5VLX50T (package: ff665, speed grade: -1), XC5VLX110 (package: ff676, speed grade: -1) and XC5VLX110T (package: ff1136, speed grade: -1) FPGA devices, using Very High speed integrated circuit Hardware Description Language (VHDL). The results obtained from Virtex-5 FPGA devices show that the Galois Field GF (2^8), Gray and Skipjack S-Boxes utilizes almost similar FPGA resources and runs at same frequency of 371.609 MHz.

Key words: Advanced Encryption Standard (AES) · Cryptography · Field Programmable Gate Array (FPGA) · Galois Field GF (2^8) S-Box · Gray S-Box · Skipjack S-Box · VHDL · Virtex-5

INTRODUCTION

The Substitution Box (S-Box) is an essential part of Advanced Encryption Standard (AES). S-Box transformation is a computationally intensive and important operation because it has the capability of attacking against differential cryptanalysis with high reliable security [1]. The cryptographic algorithms provide security for the transmission of sensitive electronic financial transactions and digital signature applications. Aside from S-box transformation, other transformations in AES are linear. Consequently, S-box is the only non-linear component of the algorithm to provide confusion capability for AES. Because of this critical role of S-box based Galois Field GF (2^8) in AES, many researchers focused on S-box improvements. Several papers have proposed to replace AES Galois Field GF (2^8) S-box by a different transformation [2-8], such as Gray S-Box, Xyi S-Box, Skipjack S-Box and Residue of Prime Number S-Box. The nonlinearity study [9] shows that, the nonlinearity of Galois Filed GF (2^8) and Gray S-Box is better than Skipjack S-box. But Skipjack S-Box is shown quite good nonlinearity strength over other reported Xyi S-box and S-box based on residue prime numbers. The contemporary field programmable gate array (FPGA) provides high flexibility with the speed and as well as physical security of traditional hardware application specific integrated circuits (ASICs) for the implementation of cryptographic algorithms. The goal of this letter is to present the comparative study of Galois Field GF (2^8) S-Box, Gray S-Box and Skipjack S-Box. For this purpose, the Galois Field GF (2^8), Gray and Skipjack S-Boxes implemented in Virtex-5 [10] XC5VLX50 (package: ff676, speed grade: -1), XC5VLX50T (package: ff665, speed grade: -1), XC5VLX110 (package: ff676, speed grade: -1) and XC5VLX110T (package: ff1136, speed grade: -1) FPGA devices using Very High speed integrated circuit Hardware Description Language (VHDL).

MATERIALS AND METHODS

The S-Boxes based Galois Field GF (2^8), Gray and Skipjack are a complete S-Box with 256 entries and the full details of these tables are given in [1-3]. In summary, the 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 Gray S-box uses the binary Gray code conversion as a pre-processing step to increase the algebraic complexity of AES S-box, the algebraic expression of Gray S-box has 255 terms. Skipjack is another block cipher algorithm was mapped to be used in fastened phones initiated by the U.S National Security

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

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

	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

Table 2: S-Box based on Gray S-Box in Hexadecimal form

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

Table 3: S-Box based on Skipjack S-Box in Hexadecimal form

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

Agency (NSA), is characterized with numerous operations, but most noteworthy is Skipjack S-box. The Table 1 shows the Galois Field GF (2^8) S-Box. Table 2 demonstrates the Gray S-Box. The Skipjack S-Box is shown in Table 3.

RESULTS

The design of S-Boxes based Galois Field GF (2^8), Gray and Skipjack is done using VHDL and implemented in a Xilinx Virtex-5 XC5VLX50 (package: ff676, speed grade: -1), XC5VLX50T (package: ff665, speed grade: -1), XC5VLX110 (package: ff676, speed grade: -1) and XC5VLX110T (package: ff1136, speed grade: -1) using the ISE 9.2i design tool [11].

DISCUSSION

The FPGA implementation results are summarized in Tables 4-7. The performance of the Galois Field GF (2^8), Gray and Skipjack S-Boxes show similar utilization of FPGA resources and runs at same frequency. This study shows that either of the S-Box could be used in AES to improve against algebraic attacks.

Table 4: Performance evaluation of a Galois Field GF (2^8), Gray and Skipjack based S-Boxes design using Virtex-5 XC5VLX50 (package: ff676, speed grade: -1)

	Galois Field GF (2^8) S-Box	Gray S-Box	Skipjack S-Box
Frequency (MHz)	371.609	371.609	371.609
Period (ns)	2.691	2.691	2.691
BRAMs	1	1	1
Occupied Slices	2	2	2

Table 5: Performance evaluation of a Galois Field GF (2^8), Gray and Skipjack based S-Boxes design using Virtex-5 XC5VLX50T (package: ff665, speed grade: -1)

	Galois Field GF (2^8) S-Box	Gray S-Box	Skipjack S-Box
Frequency (MHz)	371.609	371.609	371.609
Period (ns)	2.691	2.691	2.691
BRAMs	1	1	1
Occupied Slices	2	2	2

Table 6: Performance evaluation of a Galois Field GF (2^8), Gray and Skipjack based S-Boxes design using Virtex-5 XC5VLX110 (package: ff676, speed grade: -1)

	Galois Field GF (2^8) S-Box	Gray S-Box	Skipjack S-Box
Frequency (MHz)	371.609	371.609	371.609
Period (ns)	2.691	2.691	2.691
BRAMs	1	1	1
Occupied Slices	2	2	2

Table 7: Performance evaluation of a Galois Field GF (2^8), Gray and Skipjack based S-Boxes design using Virtex-5 XC5VLX110T (package: ff1136, speed grade: -1)

	Galois Field GF (2^8) S-Box	Gray S-Box	Skipjack S-Box
Frequency (MHz)	371.609	371.609	371.609
Period (ns)	2.691	2.691	2.691
BRAMs	1	1	1
Occupied Slices	2	2	2

CONCLUSION

We have presented the comparative study between Galois Field GF (2^8) S-Box, Gray S-Box and Skipjack S-Box. The Galois Field GF (2^8), Gray and Skipjack S-Boxes designs implemented in Xilinx Virtex-5 FPGA devices. The results obtained show that Galois Field GF (2^8), Gray and Skipjack S-Boxes uses same FPGA resources and runs at equal frequency of 371.609 MHz. This study shows that the either of the S-Box could be used in AES to improve against algebraic attacks.

ACKNOWLEDGEMENT

The authors extend their appreciation to the College of Applied Medical Sciences Research Center and the Deanship of Scientific Research at King Saud University for funding this research.

REFERENCES

1. Federal Information Processing Standards Publication (FIPS PUB) 197, National Institute of Standards and Technology (NIST). Advanced encryption standard (AES).
2. Tran, M.T., D.K. Bui and A.D. Duong, 2008. Gray S-Box for Advanced Encryption Standard, In: International Conference on Computational Intelligence and Security, pp: 253-258.
3. Skipjack, K.E.A., 1998. Algorithm Specifications, Version, 2: 1-23.
4. Rais, M.H. and M.H. Al-Mijalli, 2012. Reconfigurable Implementation of S-Box using Virtex-5, Virtex-6 and Virtex-7 based Reduced Residue of Prime Numbers. World Applied Sciences Journal. (Accepted for Publication)
5. Rais, M.H. and S.M. Qasim, 2010. Efficient FPGA realization of S-Box using reduced residue of prime numbers, IJCSNS International Journal of Computer Science and Network Security, 10: 69-73.

6. Rais, M.H. and S.M. Qasim, 2010. Resource Efficient Implementation of S-Box Based on Reduced Residue of Prime Numbers using Virtex-5 FPGA, In: Lecture Notes in Engineering and Computer Science: World Congress on Engineering 2010, pp: 979-983.
7. Al-Mijalli, M.H., 2011. Efficient realization of s-box based reduced residue of prime numbers using virtex-5 and virtex-6 FPGAs. Am. J. Applied Sci., 8: 754-757.
8. Shi, X.Y., Hu Xiao, X.C. You and K.Y. Lam, 2002. A method for obtaining cryptographically strong 8×8 S-boxes. In: International Conference on Information Network Applications, 2(3): 14-20.
9. Hussain, I., M.A. Gondal and Y. Wang, 2011. Analysis of SKIPJACK S-Box, World Applied Sciences Journal, 13(11): 2385-2388.
10. Xilinx, 2009. Virtex-5 FPGA Documentation. www.xilinx.com/support/documentation/virtex-5.htm
11. Xilinx, ISE 9.2i design tool, 2007. www. xilinx. com/prs_rls/2007/software/0786_ise92i.htm