Advances and Applications in Mathematical Sciences
Volume 20, Issue 11, September 2021, Pages 2535-2541

DESIGN AND IMPLEMENTATION OF LOW POWER 128 BIT AES PIPELINED ENCRYPTION USING CLOCK GATING ON 28nm FPGA

V. PRASANTH[1], K. BABULU[2] and NAGESH DEEVI[3]

[1,3]Associate Professor
ECE Department
Pragati Engineering College India
E-mail: varasalaprasanth@gmail.com
nagesh.deevi417@gmail.com

[2]Professor
ECE Department
JNTUK, Vizianagaram, India
E-mail: kapbbl@gmail.com

Abstract

Advanced encryption standard (AES) with clock gating using 28nm FPGA is implemented in this paper to achieve low power consumption for wireless applications. AES coprocessor with optimized architecture is considered for integrating columns and keys for encryption process using clock gating technologies. The proposed mechanism is designed on 28n Technology where the power consumption is 167mW, throughput is 12.8Gbps for 100Mhz Clock frequency. Based on the results the above architecture is highly suitable for advanced 5G wireless applications. Compared to conventional design process proposed algorithm shows 35% reduction in terms of power dissipation t at a frequency of 100Mhz frequency.

I. Introduction

In present scenario, due to advancement in technology massive integration of different technology platform is being taken place. Artificial intelligence and cryptography are playing vital role in providing facilities and security to user respectively [1]. Cryptography deals with the secured

2010 Mathematics Subject Classification: 68P25.
Keywords: Advanced Encryption Standard (AES), Clock gating, Power Consumption, Throughput.
Received October 13, 2020; Accepted November 7, 2020

mechanism keeping message information confidential. Encryption and decryption are very much essential for communication networks and processing systems where secured data or information is involved [2]. Encryption is defined as transformation of plain text with the help of cipher key to encrypted data. In the both encryption and decryption key plays a major role for secured data transmission. Its physical properties show direct impact on the encryption length and data recovery time between transmitter and receiver. Among the available standards, advanced encryption standard is considered to be the best in terms of confidentiality and personal privacy. This mechanism comes under symmetric cryptography. The security levels provided by the AES is dependent on different key sizes [3]. It is widely used in security protocols, security applications with optimization in modern communication systems. Full parallel architectures and pipeline architectures are the most commonly used very high-performance AES algorithms [4]. In general, AES algorithms suffers with low throughput and high-power consumption on hardware implementation. AES is a symmetric cryptography which increases the consumption of power and energy. In general, there is a tradeoff between power/energy consumption, cost, throughput for AES which are difficult to satisfy. To overcome this clock gating algorithm for low power consumption is implemented in 65nm CMOS process.

In this article, based on VLSI clock gating mechanism low power optimization on AES algorithm on FPGA is implemented. In this sub bytes and mixcolumns mechanism is applied for power optimization and resource sharing to synthesize encryption and decryption. S-box includes low power design methodologies for circuit size optimization and gate count. This shows direct impact on power consumption. In addition to this, clock gating mechanism used in the implementation of AES algorithm will shows power optimization at architectural level. This paper comprises of section 2 as implementation of clock gating over AES algorithm on 28nm CMOS technology, section 3 with results and discussion and section 4 as conclusion. This document is a template.

II. Implementation

AES algorithm is an encryption standard which uses 256 bit/192 bit/128-bit cipher key for symmetric mechanism which results in 10, 12 and 14 rounds of operation [5]. In general, AES block consists of data with encryption and decryption with array of bytes called the state. There are mainly four major AES transformations: Sub Bytes, Add Round Key, Mix Columns and Shift Rows. The reverse process is being followed for the decryption of AES algorithm that is being followed for encryption standards [6]. In general, Sub Bytes transformation is operated independently as a non-linear byte substitution of each byte state that substitution table (*S*-box) with a transformation of multiplicative inverse in finite field GF and affine transformation over GF [7]. The *S*-box transformation of sub Bytes transformation is shown in Figure 2(a). Shift Rows transformation process states that the bytes in last three rows are shifted cyclically over different bytes. The process is shown in Figure 2(b). The values in the state are substituted by other values according to a lookup table called *S*-box.

Table 1. *S*-Box.

	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

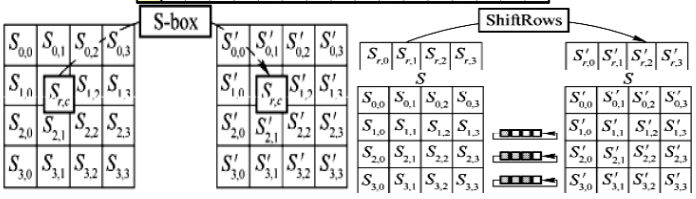

Figure 2. AES Transformations (a) Sub Bytes (b) Shift Rows.

Four-term polynomial treats with Mix Columns transformation on the state column-by-column by treating each column and considers a polynomial by multiplying with fixed polynomial as shown in Figure 2(c). Round Key is a simple bit wise XOR operation with Add Round Key transformation. It consists of words from key schedule and those words are added into the columns of the state which is illustrated as shown in Figure 2(d).

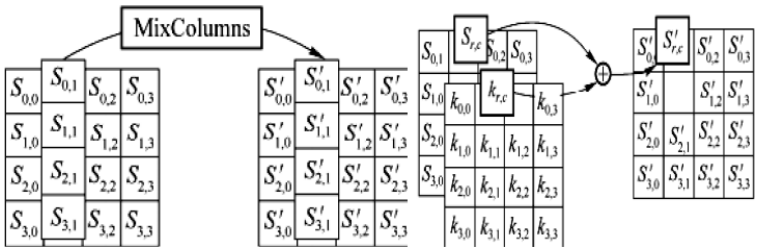

Figure 2. AES Transformations (c) Mix Columns (d) Add Round Key.

In AES transformations, we used to implement Sub Bytes/Inv Sub Bytes, Sift Rows/Inv Shift Rows, Mix Columns/Inv Mix Columns and Add Round Key. In addition to this key expansion which is independent of *S*-box. Cipher key plays an important role and clock gating mechanism is applied to optimize the power consumption and cost [8].

In AES coprocessor, encryption and decryption procedures do not run simultaneously. Whole procedures and transformations run with same clocking gate in order to reduce power consumption. The general AES hardware coprocessor architecture of encryption and decryption is shown as below.

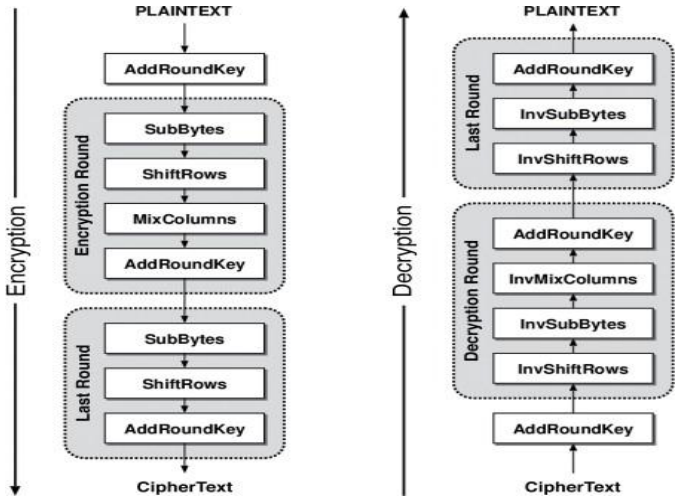

Figure 3. AES Encryption and decryption.

III. Results and Discussion

AES Encryption is implemented on 28nm technology FPGA and used Clock gating for reducing dynamic power consumption. Clock Gating reduces use of clock on regular intervals and activated when signal or data is active. As frequency increases dynamic power consumption increases with number of signals, so effective gating of clock will prevent consumption of power.

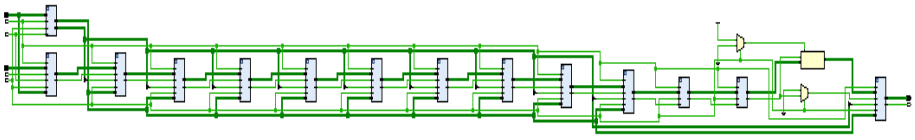

Figure 4. Schematic diagram of AES.

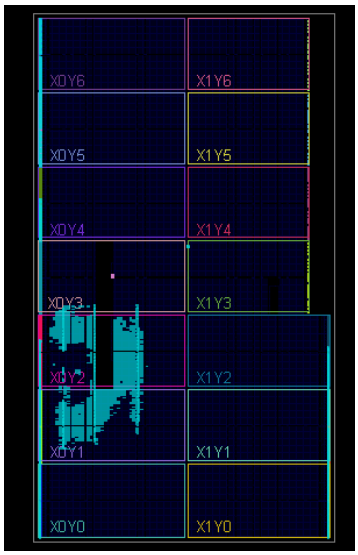

Figure 5. Implementation on Trgeted FPGA (Knitex 7).

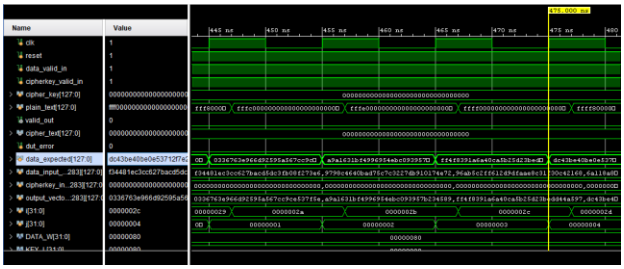

Figure 6. Simulation Result of AES Encryption Algorithm.

Table 1. Power analysis of ASE with and without clock gating.

Power		Without clock gating	With latch-based clock gating	With data driven clock gating
Static		163mw	163mw	163mw
Dynamic	Signals	78mw	72mw	47mw
	Logic	50mw	42	19w
	BRAM	7mw	7mw	23mw
	I/O	56mw	32mw	7mw
Total Power		**354mw**	**316mw**	**259mw**

IV. Conclusions

The designed AES Pipelined encryption is implemented with clock gating to improve its speed and Power reduction. Its functionality has been verified

using Vivado HDL. This design is verified on Kintex 7 FPGA. In Digital wireless applications transmitted data is vulnerable for external attacks therefore in present paper we have introduced pipelining and clock gating in AES encryption in *S*-Box output to make it more secure. On total power 35% of power is reduced using clock gating with a throughput of 12.8GbpsThe conclusions should be written here.

References

[1] LI. Zhen-rong, Zhuang Yi-qi, Zhang Chao and JIN Gang, Low-power and area-optimized VLSI implementation of AES coprocessor for Zigbee system The Journal of China Universities of Posts and Telecommunications 16(3) (2009), 89-94.

[2] D. Kamel, F. Standaert and D. Flandre, Scaling trends of the AES S-box low power consumption in 130 and 65 nm CMOS technology nodes, 2009 IEEE International Symposium on Circuits and Systems, Taipei, 2009, pp. 1385-1388, doi: 10.1109/ISCAS.2009.5118023.

[3] Kirat Pal Singh and Shivani Parmar, Low Power encrypted MIPS processor based on aes algorithm, Journal of Global Research in Computer Science 3(4) (2012).

[4] V. P. Hoang, V. L. Dao and C. K. Pham, Design of ultra-low power AES encryption cores with silicon demonstration in SOTB CMOS process, ELECTRONICS LETTERS 9th November 53(23) (2017), 1512-1514.

[5] V. Hoang, V. Dao and C. Pham, An ultra-low power AES encryption core in 65nm SOTB CMOS process, International SoC Design Conference (ISOCC), Jeju, doi: 10.1109/ISOCC.2016.7799747 (2016), 89-90.

[6] S. Morioka and A. Satoh, An Optimized S-Box Circuit Architecture for Low Power AES Design. In: Kaliski B.S., Koç .K., Paar C. (eds) Cryptographic Hardware and Embedded Systems - CHES 2002. CHES 2002. Lecture Notes in Computer Science, vol 2523. Springer, Berlin, Heidelberg (2003).

[7] Duy-Hieu Bui, Diego Puschini, Simone Bacles-Min, Edith Beigné and X.-T. Tran, AES Datapath Optimization Strategies for Low-Power Low-Energy Multisecurity-Level Internet-of-Things Applications, IEEE Transactions on Very Large-Scale Integration (VLSI) Systems, IEEE 25(12) (2017), 3281-3290.

[8] Panu Hämäläinen, Timo Alho, Marko Hännikäinen and Timo D. Hämäläinen, Design and Implementation of Low-area and Low-power AES Encryption Hardware Core, Proceedings of the 9th EUROMICRO Conference on Digital System Design (DSD'06)