(12) PATENT APPLICATION PUBLICATION (21) Application No.202141006425 A

(19) INDIA

(22) Date of filing of Application :16/02/2021 (43) Publication Date : 19/02/2021

(54) Title of the invention : A NOVEL METHOD OF POWER REDUCTION IN MODIFIED AES USING BIT ENCRYPTION AND DECRYPTION TRANSITION SCHEME ON FPGA

(51) International classification	:H04L0009060000, H04L0029060000, H04L0009000000, H04B0010850000, H04L0001160000	(71)**Name of Applicant :** **1)Mr.Gajja Prasad** Address of Applicant :Assistant Professor, Department of Electrical and Electronics Engineering, GIT, GITAM (Deemed to be University), Visakhapatnam, Andhra Pradesh, India. Pin Code:530045 Andhra Pradesh India **2)Dr.Gouse Baig Mohammad** **3)Dr.Devasish Pal** **4)Dr. S.Karthick** **5)Dr.Piyush Kumar Shukla**
(31) Priority Document No	:NA	**6)Mr.Shaik Karimullah**
(32) Priority Date	:NA	**7)Dr.Rokesh Kumar Yarava**
(33) Name of priority country	:NA	**8)Mr.Shaik Johny Basha**
(86) International Application No Filing Date	:NA :NA	**9)Dr.G.Sambasiva Rao** **10)Mr.Pijush Dutta**
(87) International Publication No	: NA	(72)**Name of Inventor :**
(61) Patent of Addition to Application Number Filing Date	:NA :NA	**1)Mr.Gajja Prasad** **2)Dr.Gouse Baig Mohammad** **3)Dr.Devasish Pal**
(62) Divisional to Application Number Filing Date	:NA :NA	**4)Dr. S.Karthick** **5)Dr.Piyush Kumar Shukla** **6)Mr.Shaik Karimullah** **7)Dr.Rokesh Kumar Yarava** **8)Mr.Shaik Johny Basha** **9)Dr.G.Sambasiva Rao** **10)Mr.Pijush Dutta**

(57) Abstract :
The data such as text, Image, and Video can be transmitted by the communication systems from one node to another node. While transmitting the data, the security is utmost concern and is obtained by the Data Encryption and Data Decryption. The increased Speed of Data transmission and the less utilization of power are the factors to be considered while designing the communication system with VLSI Technology. The implementation of Advanced Encryption Standard (AES) on the Field Programmable Gate Array (FPGA) is highly flexible and efficient method for high secured data encryption and decryption system. The implementation of Modified AES on FPGA is having more number of transitions due to continuously receiving data and continuously transmitting the data. The power consumption is more in implementation of Modified AES on FPGA, can be optimized and reduced with the Bit Encryption and Decryption Transition Scheme. The present invention disclosed here is a Novel Method of Power Reduction in Modified AES using Bit Encryption and Decryption Transition Scheme on FPGA comprising of: Data Input (201); Key Input (202); BEDT Scheme (203); S-Box Generation (204); Row Shift (205); Steller Matrix (206); Inverse BEDT (207); Inverse S-Box (208); Row Shift (209); Steller Matrix (210); Decrypted Data (211); reduces the power in modified Advanced Encryption Standard implemented on FPGA. The present invention disclosed here reduces the power to 0.42mw for 325 flip flop pairs in the design. The present invention is implemented on the Verilog HDL programming on the Virtex-5 FPGA Development Board.

No. of Pages : 15 No. of Claims : 5