International Journal of Engineering & Technology, 7 (1.5) (2018) 126-134

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

Analysis of power reduction and implementation on FPGA for AES-128bits using BEDT schemes

C. Sapna Kumari [1*], K. V. Prasad [2]

[1] Ph.D Research Scholar, Jain University, Bangalore
[2] Professor & HOD, Department of ECE, Bangalore Institute of Technology, Bangalore
**Corresponding author E-mail: sapnakumaric@gmail.com*

Abstract

Due to rapid improvement for innovations in cryptography, the scattered of power link in connections of cryptography contexts instigates to resist through the power disseminated via substitute mechanisms of the communication subsystem, the switches and the sub modules of cutting edge encryption standard (AES). The dynamic power dissemination in joins is real supporter of the power utilization in organize on the chip. Due to self-exchanging and cross coupling capacitance the power consumption is shirking in communications system for security aspects. In the present research work the encoding strategy the key self-exchanging is diminish by examination the exchanging change and afterward the link between the connections is patterned and guaranteed that the power utilization is lessened. To upgrade control utilization in encryption and decoding process, Bit Encryption and Decryption Transition (BEDT) information schemes went for lessening the power disseminated by the AES chiefly include round key module in AES to perform XOR operation between 128 bits plain content and secrete key. The suggested research work in this paper is main basic concept of AES due to its number of round operations and also it will allow 39% of energy sprinkling and 9% of energy utilization without having more number execution debasement and with below 11% range overhead in the other cryptography frameworks. The proposed BEDT schemes depends on both odd modified and even rearranged, and after that sending the information to receiver that will performed utilizing the kind off reversal which lessens increasingly the exchanging movement. In these proposed three schemes, utilizes an easier decoder while accomplishing a higher movement diminishment. In the prior schemes, the quantity of changes from 0 to 1 for two back to back flutters is tallied. The bit transitions reduce the number of transitions before transmitting the data to decryption.

Keywords: *AES, BEDT, Coupling switching activity, data encoding, low power, power analysis and FPGA.*

1. Introduction

An answer for the issue of diminishing the Power disseminated by an advanced framework containing a licensed innovation Core processor with over and over executes exceptional reason program. Technique depends on a novel, application-subordinate low-control address transport encoding scheme. The investigation of the execution hints of a given program permits a precise rivalry of the relationship that may exist between pieces of bits in back to back examples; this data can be effectively abused to decide and encoding which sensibly lessens the best progress action. Exploratory Results, acquired on an arrangement of uncommon reason applications, are exceptionally tasteful; lessening of transport movement up to 64.8% (41.8% by and large) have been accomplished over the first address streams. What's more, information concerning the quality and the execution of the consequently integrated in coding/translating circuits and in addition the outcomes acquired for a reasonable center based outline show the handy convenience of a proposed control Optimization system. The utilization of scholarly restrictive parts, for example, Core processor and microcontrollers as fundamental pieces for the improvement of devoted (ie; exceptional reason). Computerized framework is turning into an entrenched scheme
methodology in the microelectronics business fiscally propel this decision [1]. The dim encoding is helpful in light of the fact that the encoding of these qualities contrast by 1 bit. In the T0. Encoding and extra wire is utilized to show the back to back access mode, and no action is required in the transport. The best backwards strategy comprises of sending either the esteem it Self or its bitwise-compliment, contingent upon which would bring about fever changes. An additional wire is utilized to convey this extremity data. For uniform and autonomous dispersions, encoding strategies works better when the bit width of the incentive to be sent is isolated into littler gatherings and every one encoded freely. The transport modify method has been joined with T 0 in, along these lines getting the more effectively lessening than each of the systems without anyone else's input. Number of progress is diminished in the conceivable situation when the forecast mistake as few ones [2]. A present a non-specific encoder Decoder design and we think about its properties drive the fundamental correct and coding calculation in we out line rough variations to be utilized for minimal effort encoding translating of Fast and wide transports and in area 5 we introduce the receptive encoder Decoder engineering.
Test comes about are accounted for at least finishes up the work the transport width and the correspondence throughput in its day and age will be taken as tight imperatives seek limitation discount the likelihood of considering extra minutes repetitive code length cites. The inspiration for this supposition is that spatial excess is scarcely endured in worldwide transport association since it changes stick out and interface detail and variable length coding don't change transport width however present variable inertness in correspondence which might be unsuitable [3].

The exschemeation behind the blend of encoding and disentangling interface rationale that limits the normal number of progress on intensely stacked Global transport line at no cost in correspondence throughput (One word is transmitted at each cycle). That recognizing highlight of our approach is that it doesn't depend on architect's introduction yet it consequently builds low progress movement codes and Hardware execution of encoders and decoders give a data on word Level measurements. The Non-specific encoder Decoder design and we depict a calculation for altering and to get usage that limit change action of given a nitty gritty factual portrayal of the objective stream. We additionally presented estimate of the essential calculation that produces moderate progress codes and low multifaceted nature encoders and decoders. These codes are custom fitted for low width transports, where encoders and decoders are liable to execution and Hardware cost requirements and for surges of measurable properties are not known precisely [4]. Between lengthy wires in the circuitry the coupled Capacitance (CI) the delay few times superior extent than the best approach to-substrate capacitance. Notwithstanding its reliance rapid technology improvement and additionally auxiliary factors, for example, wire dividing, wire width, wire length, wire material, coupling length, driver quality, flag progress time et cetera, the coupled capacitance likewise relies on the information subordinate change and will increment or decline contingent on relative exchanging action between nearby transport wires. However for on-chip transports the real wellspring of vitality utilization is the entomb wire coupled capacitance and along these lines its minimization is vital for sparing vitality utilization. Decreasing the entomb wire coupling capacitance without taking out a most pessimistic scenario [5]. In PBI, just a chose sub gathering of buslines is encoded to stay away from pointless reversal of generally dormant and/or uncorrelated transport lines which are excluded in the sub gathering. In MPBI, we parcel a transport into numerous sub transports by grouping exceptionally co-related transport lines and after that encode each by sub transport freely. For apportioning a transport into sub transports for each encoding scheme, they proposed heuristic calculation. Heuristic calculation that endeavors both change co-connection and progress likelihood keeping in mind the end goal to discover a sub set of transport lines to such an extent that the aggregate number of transport advances are minimized. It additionally explores the overhead impact of encoding/deciphering circuits. It brings about the decreases in number of transport advances with both PBI and MPBI coding are substantial. The execution of the proposed sub transport choice calculation for PBI coding is practically on a par with that of reenacted tempering in the transport progress lessening [6]. Multiprocessor framework on-chip (MPSoC) utilizes various CPUs alongside other equipment subsystem to actualize a system. MPSoC speak to a vital and unmistakable class of PC engineering and furthermore overviewed on PC – added scheme issues pertinent to the outline of MPSoC. MPSoC is a framework – on – chip a VLSI framework that fuses most or every one of the parts fundamental for an application. MPSoC are broadly utilized as a part of systems administration, correspondence flag handling and interactive media among other application. If processors can supply adequate computational power, at that point the straightforwardness with which they can be modified pulls framework fashioners toward uniprocessors. In this paper, we recollected Moore's law progress as new applications that will require the advancement of new MPSoC will emerge. By utilizing these MPSoC techniques basically boundless measures of computational powers yet should likewise meat ongoing, low power, and minimal effort necessities [7].

The association of whatever is left of the setting is as per the following. After a general presentation of the impact of security and power utilization on the power framework, the convenience and the prerequisite of a cryptography limiter are exhibited to the proposed schemes which have been talked about in segment II. The customary methods for settling in control utilization framework have been examined in area III. In area IV, scheme standards, outline subtle elements, and test consequences of attractive current limiter has been introduced. The proposed idea has been finished up in segment V.

2. Methodology

The fundamental idea of the proposed work is encoder that will encodes the data with previously shifted data into the system with the objective of preventive the trading in transitions and the coupling trading action in the associates with more number of transitions in the binary data. This deduction in encoding system exploits the pipeline idea of the wormhole exchanging procedure. The encoding optimal taken at the BEDT will give a similar power sparing to all the operation of AES inward modules. For the proposed scheme, the encoder and decoder are added to the AES to reduce the power consumption. Therefore the 3 schemes are proposed in this work for reduction of power between any two bits progress. In encryption, the info flutter is given in W-1 bit with one piece for sign for encoded or not. In the event that the bit is 1 then information is encoded else no encoding is occurring for the information. The inner square graph of decoder the piece D is decoder circuit changes as per each scheme. In decoders, the backwards operation of encoder happens. There is need of just a single piece Ty to figure out which move must be made. In the scheme-II of encoder, T_y can be finding by calculating full and odd control bits to get cipher text. The full control bit changes for Type-II to Type-IV in scheme-II to scheme-IV. The scheme contrasts the present information and the past one to choose to have no inverse odd and full of the present information can offer ascent to the connection control lessening. In the encoding scheme III, even reversal to conspire II is included. The reason is that odd reversal changes over Type-I changes to Type-II schemes. Consequently, the even reversal may diminish the connection control dissemination also.

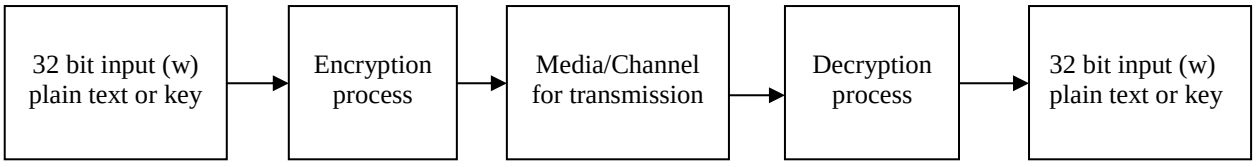


Fig. 1: Block diagram of proposed BEDT for both encryption and decryption

The novel schemes of encryption and decryption of BEDT method is to control power dissipation from coupling capacitors changes on the connections of the internal operation of the schemes. Give us initial a chance to depict the power display that contains diverse parts of the power dissemination of a connection. The active energy and power product disseminated by intersects and the driver is shown in equation (1).

$$P = [T_{0\rightarrow1} (C_s+C_l) + T_cC_c] V_{dd}^2 F_{ck} \quad (1)$$

The transition logic 0 to 1 is transistor switches from "off" condition to "on" condition or vice-versa, Tc is corresponded exchanging of connections between two physical wires/lines, substrate capacitance Cs, load capacitance C_l, coupling capacitance Cc, supply voltage V_{dd} and clock frequency $F_{ck.}$ All four variables are sorts of coupling capacitances. If one Type changes due switching action and other one is unchanged. In Type-II, if one wire voltage level changes from logic low to logic high and other one changes from logic high to logic low. In Type-III compares both Types when two lines

switches and Type-IV progress the two lines changes when changes occurs between transitions. The compelling altered capacitance shifts after transitions, and accordingly, the coupling capacitance movement, Tc, is a weighted whole of various sorts of coupling change commitments.

$$Tc= K_1T_1 + K_2T_2+ K_3T_3+ K_4T_4 \quad (2)$$

Where Ti is the normal number of Type I progress and Ki is its relating weight. As indicated by, we useK1= 1, K2= 2, and K3= K4= 0. The event likelihood of Types I and II for an irregular arrangement of information is1/2 and 1/8 individually. This prompts a higher incentive for K1T1 contrasted and K2T2 recommending that limiting the quantity of Type I change may prompt a significant power decrease. Utilizing (2), one may express (1) as

$$P = [T_{0\rightarrow1} (C_s + C_l) + (T_1+ 2T_2) Cc] Vdd^2F_{ck} \quad (3)$$

Where, Cl can be neglected

$P \alpha T_{0\rightarrow1}C_s+ (T_1+ 2T_2) C_c$

Consider a data width of w bits, where one out of w bits is reserved as the inversion bit which indicates whether the flit passing through the encoder is inverted or not. The block *E* has two inputs X and Y and the output Z. The current flit to be transmitted is given to the input X, where the incoming w bits are packed into (*w*-1) bits body flit and a "0" bit (inversion bit). The previously encoded flit is given to input Y, where the wth bit denoted by inv is used to identify its inversion or the absence thereof. The inv field is set to "1" when the previous flit is inverted and set to "0" when inversion is not performed. The incoming (previous encoded) body flits of (w-1) bits are represented by X*i* (Y*i*) where i= 0, 1, 2,…….., *w*-2. Within the encoding logic two adjacent bits of the input flits are given as the input to the sub-blocks *Ty* (e.g., X_0,X_1,Y_0,Y_1, X_1,X_2,Y_1,Y_2,……..,X_{w-1}, X_{w-2}, Y_{w-2}, Y_{w-1} where X_{w-1}=0 & Y_{w-1}=inv).When any type of the *Ty* transition is detected the output is set to "1". Such application of odd inversion over this pair of bits results in the minimization of the power dissipation. The next stage in the encoder is a majority voter block which checks for the condition. When this condition is satisfied, inversion is performed on odd bits such as X_1, X_3, X_5 etc to the final stage.

For the decoder side it checks the inversion bit, if inv bit is set to "1", it just inverts the received flit. For a random set of data, each of these thirty two transitions has the same probability. Therefore, the occurrence probability for Types I, II, III, and IV are 1/2, 1/8, 1/8, and 1/4. In the rest of this section, we present three data encoding schemes designed for reducing the dynamic power dissipation of the network links along with a possible hardware implementation of the decoder. In Scheme-I is shown in Fig.2. is concentrate on lessening the quantities of Type I changes (by changing over them to Types-III and IV advances) and Type II advances. The scheme contrasts the present information and the past one to choose whether odd reversal or no reversal of the present information can prompt the connection control decrease.

Power Model: -The dynamic power is calculated when bit changes from one transition to other, the power on the line is given by

$$P^I \alpha T^I_{0\rightarrow1} + (K_1T_1^I+ K_2T_2^I+ K_3T_3^I+ K_4T_4^I) C_C \quad (4)$$

Where $T^I_{0\rightarrow1}$, T^I_1, T^I_2, T^I_3, and T^I_4, are Types-I, II, III, and IV, respectively.

For every change, the connection of coupling progress exercises of the bounce when encrypted the data and when its bits are odd modified. Information are sorted out as takes after. The primary piece is the estimation of the bland ith line of the connection, while the second piece speaks to the estimation of its $(I + 1)^{th}$ line. For each parcel, the principal (second) line speaks to the qualities at time $t - 1$ (t).

$T_{0\rightarrow1}= T_{0\rightarrow0(odd)}+T_{0\rightarrow1(even)}$where odd/even refers to odd/even lines. Therefore, (4) can be expressed as

$$P \alpha (T_{0\rightarrow0(odd)} + T_{0\rightarrow1(even)})Cs+[K_1(T_2+T_3+T_4)+K_2T_1***+K_3T_1*+K_4T_1**]Cc \quad (5)$$

Using (4) and (5) and noting that Cc/Cs= 4, we obtain the following odd invert condition

$$1/4T_{0\rightarrow1} + T_1+ 2T_2>1/4(T_{0\rightarrow0(odd)} + T_{0\rightarrow1(even)})+T_2+ T_3+ T_4+ 2T_1.$$

In the proposed encoding scheme II, we make utilization of both odd (as talked about already) and full reversal. The full reversal operation changes over Type II advances to Type IV advances. The scheme contrasts the present information and the past one to choose whether the odd, full, or no reversal of the present information can offer ascent to the connection control diminishment.

Scheme-I: Algorithm

Step 1: Start.

Step 2: Provide "w" bit data along with the previously encoded flit to the Encoder.

Step 3: then compare current flit with previous encoded flit.

Step 4: then check the condition Ty > (w-1)/2.

Step 5: in this equation we are check for two conditions i.e., odd invert And No invert condition.

Step 6: depending on that codition we are performing inversion on odd bits.

Step 7: then for different input data the processes will be repeated.

Power Model: Let us demonstrate with P, PI, and PII the power disseminated by the connection when the flit is transmitted with no reversal, odd reversal, and full reversal, individually. The odd reversal prompts control lessening when PI< PII and PI< P. The power PII is given by

$$P^{II} \alpha T_1+2T_4 \quad (6)$$

Neglecting the self-switching activity, we obtain the condition $P^I< P^{II}$

$$T_2+T_3+T_4+2T_1 < T_1+2T_4 \quad (7)$$

Therefore, using (6) and (7), we can write

$$2(T_2-T_4) < 2Ty-\omega+1 \quad (8)$$

Based on (7) and (8), the odd inversion condition is obtained as

$$2(T_2-T_4) < 2Ty-\omega+1, Ty > ((\omega-1)/2) \quad (9)$$

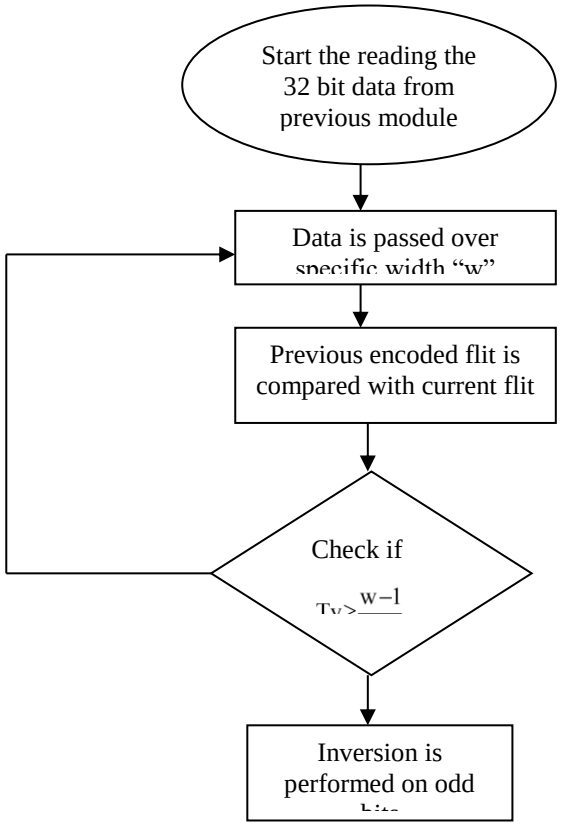


Fig. 2: Flow chart of scheme-I and specification of input data width

Encryption using Scheme-II

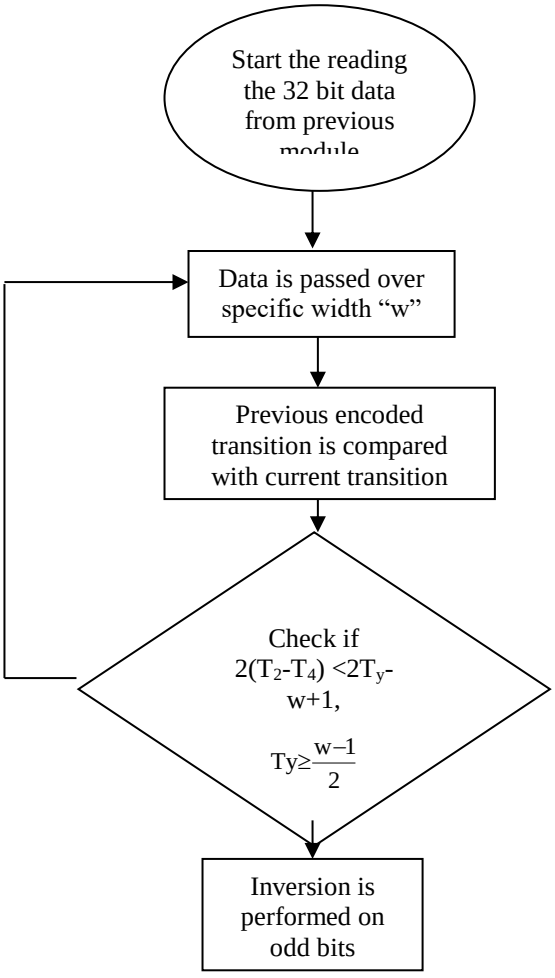


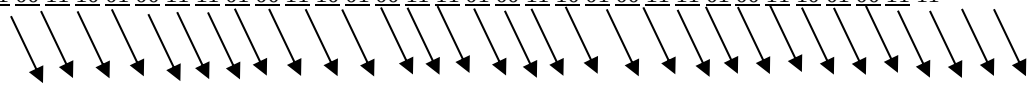
Fig. 3: Flow chart of scheme-II and specification of input data width

Scheme-II: Algorithm

Step 1: Start.
Step 2: Provide "w" bit data along with the previously encoded flit to the Encoder.
Step 3: then compare current flit with previous encoded flit.
Step 4: then check the condition 2(T2-T4**) < 2Ty-w+1, Ty > (w-1)/2.
Step 5: in this equation we are check for two conditions i.e., odd invert And No invert condition.
Step 6: depending on that codition we are performing inversion on odd bits.
Step 7: then for different input data the processes will be repeated.

x=10101011101010111010101110101011 = 24 transitions.

x=01 00 11 10 01 00 11 11 01 00 11 10 01 00 11 11 01 00 11 10 01 00 11 11 01 00 11 10 01 00 11 11



y=00 01 00 11 10 01 00 11 11 01 00 11 10 01 00 11 11 01 00 11 10 01 00 11 11 01 00 11 10 01 00 11

Ty=1 1 2 1 2 1 2 0 1 1 2 1 2 1 2 0 1 1 2 1 2 1 2 0 1 1 2 1 2 1 2 0

Ty=39=00101000 , $T_y = \frac{w-1}{2}$, T2 > T4

T2=00=00000000
T4=00=00000000

$$T_y = \frac{32-1}{2} = 15.5$$

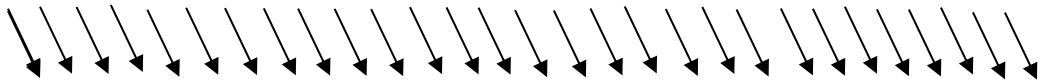
Therefore half invert (HI) = 1 and full invert (FI) = 0

$Z_0 = X_0 \oplus FI = 1 \oplus 0 = 1$
$Z_1 = X_1 \oplus FI \oplus HI = 1 \oplus 0 \oplus 1 = 0$
$Z_2 = X_2 \oplus FI = 0 \oplus 0 = 0$
$Z_3 = X_3 \oplus FI \oplus HI = 1 \oplus 0 \oplus 1 = 0$
$Z_4 = X_4 \oplus FI = 0 \oplus 0 = 0$
$Z_5 = X_5 \oplus FI \oplus HI = 1 \oplus 0 \oplus 1 = 0$
$Z_6 = X_6 \oplus FI = 0 \oplus 0 = 0$
$Z_7 = X_7 \oplus FI \oplus HI = 1 \oplus 0 \oplus 1 = 0$
$Z_8 = X_8 \oplus FI = 1 \oplus 0 = 1$
$Z_9 = X_9 \oplus FI \oplus HI = 1 \oplus 0 \oplus 1 = 0$
$Z_{10} = X_{10} \oplus FI = 0 \oplus 0 = 0$
$Z_{11} = X_{11} \oplus FI \oplus HI = 1 \oplus 0 \oplus 1 = 0$
$Z_{12} = X_{12} \oplus FI = 0 \oplus 0 = 0$
$Z_{13} = X_{13} \oplus FI \oplus HI = 1 \oplus 0 \oplus 1 = 0$
$Z_{14} = X_{14} \oplus FI = 0 \oplus 0 = 0$
$Z_{15} = X_{15} \oplus FI \oplus HI = 1 \oplus 0 \oplus 1 = 0$
$Z_{16} = X_{16} \oplus FI = 1 \oplus 0 = 1$
$Z_{17} = X_{17} \oplus FI \oplus = 1 \oplus 0 \oplus 1 = 0$
$Z_{18} = X_{18} \oplus FI = 0 \oplus 0 = 0$
$Z_{19} = X_{19} \oplus FI \oplus HI = 1 \oplus 0 \oplus 1 = 0$
$Z_{20} = X_{20} \oplus FI = 0 \oplus 0 = 0$
$Z_{21} = X_{21} \oplus FI \oplus HI = 1 \oplus 0 \oplus 1 = 0$
$Z_{22} = X_{22} \oplus FI = 0 \oplus 0 = 0$
$Z_{23} = X_{23} \oplus FI \oplus HI = 1 \oplus 0 \oplus 1 = 0$
$Z_{24} = X_{24} \oplus FI = 1 \oplus 0 = 1$
$Z_{25} = X_{25} \oplus FI \oplus HI = 1 \oplus 0 \oplus 1 = 0$
$Z_{26} = X_{26} \oplus FI = 0 \oplus 0 = 0$
$Z_{27} = X_{27} \oplus FI \oplus HI = 1 \oplus 0 \oplus 1 = 0$
$Z_{28} = X_{28} \oplus FI = 0 \oplus 0 = 0$
$Z_{29} = X_{29} \oplus FI \oplus HI = 1 \oplus 0 \oplus 1 = 0$
$Z_{30} = X_{30} \oplus FI = 0 \oplus 0 = 0$
$Z_{31} = X_{31} \oplus FI \oplus HI = 1 \oplus 0 \oplus 1 = 0$
$Z_{\_(w-1)} = FI \oplus HI = 0 \oplus 1 = 1$

The encryption output is the recorded bits from Z_{31} to $Z_{0\ i.e}$, Z = 10000000100000001000000010000000 1 = 8 transitions , the MSB bit indicates half invert or full invert. Hence the number transitions have been reduced from 24 transitions to just 8 transitions therefore the power consumption is almost reduced to 75% as compared to any another cryptography techniques.

Decryption using scheme-II

z=10000000100000001000000010000000
z=11 01 00 00 01 01 00 00 11 01 00 00 01 01 00 00 11 01 00 00 01 01 00 00 11 01 00 00 01 01 00 00



y=00 11 01 00 00 01 01 00 00 11 01 00 00 01 01 00 00 11 01 00 00 01 01 00 00 11 01 00 00 01 01 00

Ty=2 1 1 0 1 0 1 0 2 1 1 0 1 0 1 0 2 1 1 0 1 0 1 0 2 1 1 0 1 0 1 0

Ty = 24 = 00011000 $T_y = \frac{w-1}{2}$, T2 > T4

$$T_y = \frac{24-1}{2} = 11.5$$

Therefore the half invert (HI) = 1 and full invert (FI) = 0 and the decoder operation can perform as follows using just XOR operation and the original information be decrypted.

Decoder_output$_0$ = $Z_0 \oplus$ FI =1 $\oplus$ 0 = 1
Decoder_output $_1$ = $Z_1 \oplus$ FI $\oplus$ HI =0 $\oplus$ 0 $\oplus$ 1 = 1
Decoder_output $_2$ = $Z_2 \oplus$ FI =0 $\oplus$ 0 = 0
Decoder_output $_3$ = $Z_3 \oplus$ FI $\oplus$ HI =0 $\oplus$ 0 $\oplus$ 1 = 1
Decoder_output $_4$ = $Z_4 \oplus$ FI =0 $\oplus$ 0 = 0
Decoder_output $_5$ = $Z_5 \oplus$ FI $\oplus$ HI =0 $\oplus$ 0 $\oplus$ 1 = 1
Decoder_output$_6$ = $Z_6 \oplus$ FI =0 $\oplus$ 0 = 0
Decoder_output $_7$ = $Z_7 \oplus$ FI $\oplus$ HI =0 $\oplus$ 0 $\oplus$ 1 = 1
Decoder_output$_8$ = $Z_8 \oplus$ FI =1 $\oplus$ 0 = 1
Decoder_output$_9$ = $Z_9 \oplus$ FI $\oplus$ HI =0 $\oplus$ 0 $\oplus$ 1 = 1
Decoder_output$_{10}$= $Z_{10} \oplus$ FI =0 $\oplus$ 0 = 0
Decoder_output$_{11}$ = $Z_{11} \oplus$ FI $\oplus$ HI =0 $\oplus$ 0 $\oplus$ 1= 1
Decoder_output$_{12}$ = $Z_{12} \oplus$ FI =0 $\oplus$ 0 = 0
Decoder_output $_{13}$ = $Z_{13} \oplus$ FI $\oplus$ HI =0 $\oplus$ 0 $\oplus$ 1 = 1
Decoder_output $_{14}$ = $Z_{14} \oplus$ FI =0 $\oplus$ 0 = 0
Decoder_output $_{15}$ = $Z_{15} \oplus$ FI $\oplus$ HI =0 $\oplus$ 0 $\oplus$ 1 = 1
Decoder_output $_{16}$ = $Z_{16} \oplus$ FI =1 $\oplus$ 0 = 1
Decoder_output $_{17}$ = $Z_{17} \oplus$ FI $\oplus$ HI =0 $\oplus$ 0 $\oplus$ 1 = 1
Decoder_output $_{18}$ = $Z_{18} \oplus$ FI =0 $\oplus$ 0 = 0
Decoder_output $_{19}$ = $Z_{19} \oplus$ FI $\oplus$ HI =0 $\oplus$ 0 $\oplus$ 1 = 1
Decoder_output $_{20}$ = $Z_{20} \oplus$ FI = 0 $\oplus$ 0 = 0
Decoder_output $_{21}$ = $Z_{21} \oplus$ FI = 0 $\oplus$ 0 = 0
Decoder_output$_{22}$ = $Z_{22} \oplus$ FI =0 $\oplus$ 0 = 0
Decoder_output $_{23}$ = $Z_{23} \oplus$ FI $\oplus$ HI =0 $\oplus$ 0 $\oplus$ 1 = 1
Decoder_output$_{24}$ = $Z_{24} \oplus$ FI =1 $\oplus$ 0 = 1
Decoder_output$_{25}$ = $Z_{25} \oplus$ FI $\oplus$ HI =0 $\oplus$ 0 $\oplus$ 1 = 1
Decoder_output $_{26}$ = $Z_{26} \oplus$ FI =0 $\oplus$ 0 = 0
Decoder_output $_{27}$ = $Z_{27} \oplus$ FI $\oplus$ HI =0 $\oplus$ 0 $\oplus$ 1 = 1
Decoder_output $_{28}$ = $Z_{28} \oplus$ FI =0 $\oplus$ 0 = 0
Decoder_output $_{29}$ = $Z_{29} \oplus$ FI $\oplus$ HI =0 $\oplus$ 0 $\oplus$ 1 = 1
Decoder_output $_{30}$ = $Z_{30} \oplus$ FI =0 $\oplus$ 0 = 0
Decoder_output $_{31}$ = $Z_{31} \oplus$ FI $\oplus$ HI =0 $\oplus$ 0 $\oplus$ 1 = 1

Record the resultant bits from Decoder output Decoder_output $_{31}$ to Decoder_output $_0$ to get back the original data i.e X = 10101011101010111010101110101011 therefore the simplest cryptography system for power reduction for both encryption and decryption operation is BEDT best system.

Encryption using Scheme-III

Scheme-III: Algorithm

Step 1: Start.
Step 2: Provide "w" bit data along with the previously encoded flit to the Encoder.
Step 3: then compare current flit with previous encoded flit.
Step 4: then check the condition Te > (w-1)/2, Te > Ty, 2(T2-T4**) < 2Te-w+1.
Step 5: in this equation we are check for two conditions i.e., odd invert and full invert condition.
Step 6: depending on that codition we are performing inversion on odd bits.
Step 7: then for different input data the processes will be repeated.

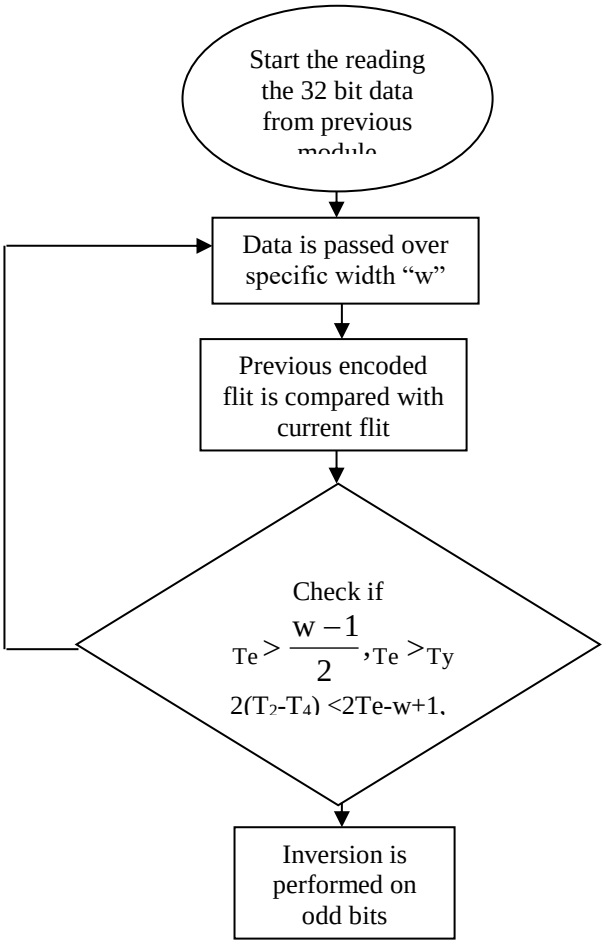


Fig. 4: Flow chart of scheme-III and specification of input data width

In the proposed encoding Scheme III, we add even reversal to Scheme II. The reason is that odd reversal changes over some of Type I (T1) advances to Type II advances. As can be seen from Table II, if the flit is even altered, the advances showed as T1/T1 in the table are changed over to Type IV/Type III advances. Along these lines, the even reversal may decrease the connection control dissemination also. The scheme contrasts the present information and the past one to choose whether odd, even, full, or no reversal of the present information can offer ascent to the connection control lessening.

Power Model: Give us a chance to show with P^{I}, P^{II}, and P^{III} the power dispersed by the connection when the flit is transmitted with no reversal, odd reversal, full reversal, and even reversal, separately. Like the examination given for Scheme I, we can surmised the condition

$P^{III} < P$ as

$$T_1+2T_2 > T_2+T_3+T_4+2T_1 \quad (10)$$

Defining

$$Te = T_2+T_1-T_1 \quad (11)$$

To obtain the condition $P^{II} < P^{I}$ as

$$Te > ((\omega-1)/2) \quad (12)$$

Hence the scheme-III can reduce the number of transitions still better as compared to scheme-I and Scheme-II, the BEDT is high performance for power reduction and this technique is also suit for any type cryptography systems to secure data and to reduce the power consumption. To perform all three schemes in a single design the 3:1 multiplexer has been used to select any one scheme as a output and the conditions of mux and schemes as follows

If mux = 00, then the scheme-1 output will be generated for the given input.

If mux = 01, then the scheme-2 output will be generated for the given input.

If mux = 10, then the scheme-3 output will be generated for the given input.

3. Results and discussion

The proposed BEDT system is designed for three different schemes and each is advanced version of previous scheme. When mux is "00" then scheme-I will be selected, "01" for scheme-II and "10" for scheme-III. Suppose if 32bit datain is 10101011101010111010101110101011, the total number transtions in the assumed datain is 24 and after encoding the number transitions have been reduced to 12 shown in the Fig.5. so the percentage of transtions reduction in scheme-I is 50% as shown in the given example

- Number of transitions in input data =24
- Encoded output =1010101110101011
- Number of transitions in encoded output =12
- Scheme 1 output = 10101011101010111010101110101011

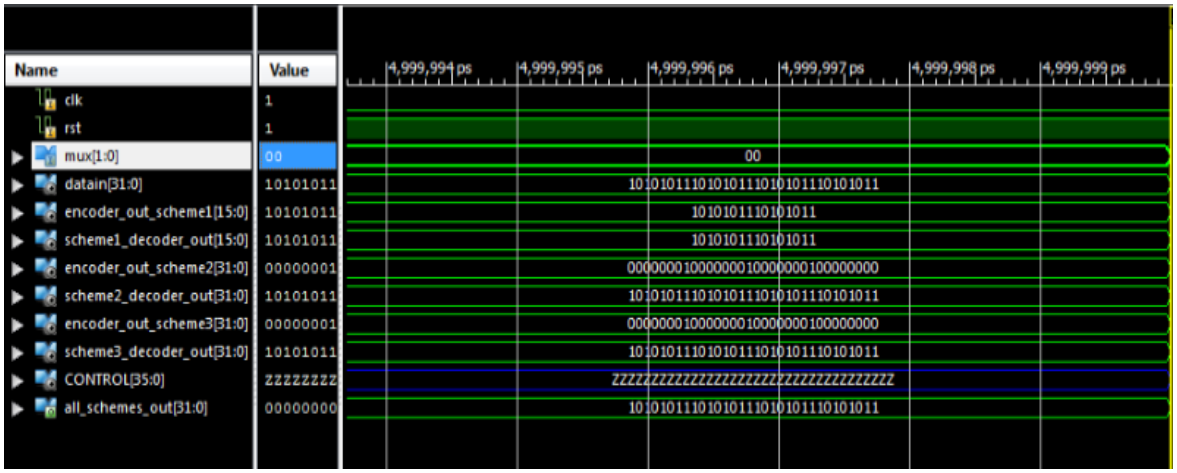


Fig. 5: Simulation resutls of Scheme-I for both encryption and decryption when mux is "00"

The scheme-II is better than scheme-I because the number of transtions are to 6 hence the percentage reduction in number of transtions is 75%. The below example is for scheme-II and its input data and output data after encryption and decryption is shown in Fig.6..

- Mux = 01
- Datain=10101011101010111010101110101011
- Number of transitions in input data =24
- Encoded output =10000000100000001000000010000000 1
- Number of transitions in encoded output =8
- Scheme 2 output = 10101011101010111010101110101011

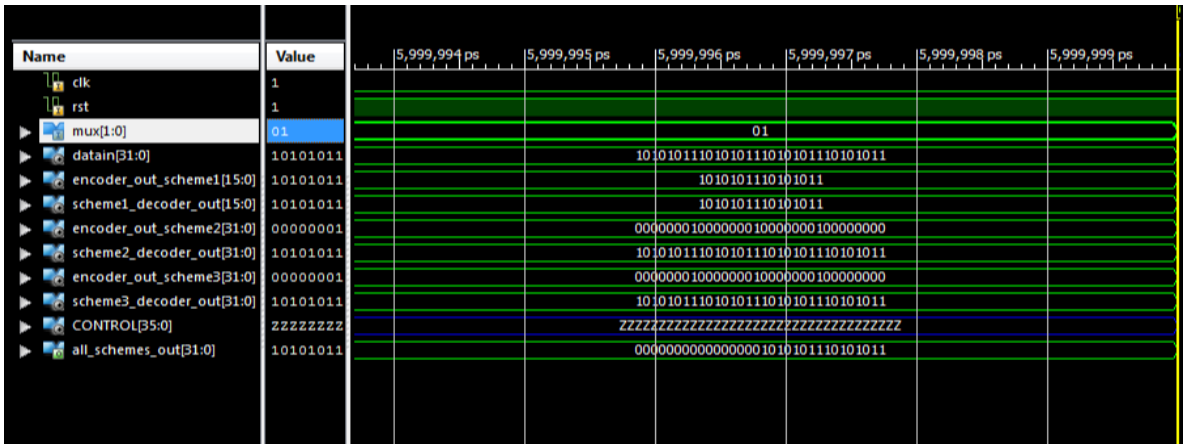


Fig. 6: Simulation resutls of Scheme-II for both encryption and decryption when mux is "10"

In scheme-III, the number of transitions is only 6; therefore the percentage of reduction in number transition is almost 85% so the scheme-III is best technique in cryptography for both security and power reduction. The below example shown the scheme-III along with encryption and decryption process.

- Mux = 10
- Datain=10101011101010111010101110101011
- Number of transitions in input data =24
- Encoded output =00000001000000010000000010000000
- Number of transitions in encoded output =6
- Scheme 3 output = 10101011101010111010101110101011

The completed design is validated using Chipscope pro software tool and the hardware results are shown in Fig.7.

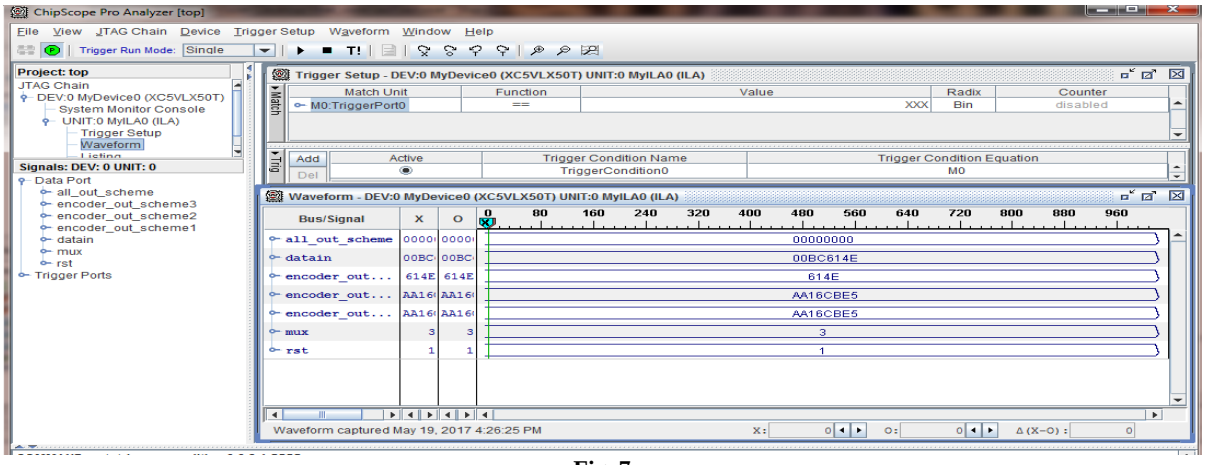


Fig. 7

4. Conclusions

In this research work, presented a set of three new data encryption and decryption schemes aimed at reducing the power dissipated in an AES sub modules pertaning to add round key. In fact, add round key process in both encryption and decrypion are responsible for a significant fraction of the overall power dissipated by the cryptography system. All schemes are producing better results in terms of power as compared to previous cryptography systems, the rationale behind the proposed schemes is to minimize not only the switching activity, but also the coupling switching activity which is mainly responsible for power dissipation in the secured systems. The proposed work is designed using verilog HDL and simulation the results are verified using Isim simulator and tested using Chipscope Pro software tool which is ingrated tool in Xilinx 14.7 ISE on Virtex-5 FPGA development board. As per results obtained from all three schemes, reduction in transtions of scheme-I, Scheme-II and Schme-III are 50%, 75% and 85% and corresponding power reductions are 51%, 41% and 31% as compared to previous results in literature.

References

[1] P. Guerrier and A. Greiner, “A generic architecture for on-chip packet-switched interconnections,” in DATE, Mar. 2000, pp. 250–256.

[2] W. J. Dally and B. Towles, “Route packets, not wires: on-chip interconnection networks,” in Proc. Des. Autom. Conf., 2001, pp. 684–689.

[3] L. Benini and G. D. Micheli, “Networks on chips: A new soc paradigm,” IEEE Comput., vol. 35, no. 1, pp. 70–78, Jan. 2002.

[4] Salminen ET AL., “Survey Of Network-On-Chip Proposals”, White Paper, ©OCP-IP, and March 2008.

[5] F. G. Moraes, N. Calazans, A. Mello, L. Mller, and L. Ost, “HERMES: An infrastructure for low area overhead packet switching networks on chip,” Integration. VLSI J., vol. 38, no. 1, pp. 69–93, 2004.

[6] Marta Ortín-Obón , Darío Suárez-Gracia,”Analysis of network-on-chip topologies for cost-efficient chip multiprocessors”,microprocessors and Microsystems,5 feb 2016,pp:1-13.

[7] D. Wiklund and D. Liu, SoCBUS: switched network on chip for hard real time embedded systems. IEEE Computer Society, 2003, p. 8.

[8] K. Goossens, J. Dielissen, and A. Radulescu, “Æthereal network on chip: Concepts, architectures, and implementations,” IEEE Des. Test Comput., vol. 22, no. 5, pp. 414–421, May 2005.

[9] C. Bobda and A. Ahmadinia, “Dynamic interconnection of reconfigurable modules on reconfigurable devices,” IEEE Des. Test Comput., vol. 22, no. 5, pp. 443–451, May 2005.

[10] L. Benini and D. Bertozzi, “Xpipes: A network-on-chip architecture for gigascale systems-on-chip,” IEEE Circuits Syst. Mag., vol. 4, no. 2, pp. 18–31, Sep. 2005.

[11] K. Lusala and J.-D. Legat, “A sdm-tdm based circuit-switched router for on-chip networks,” in Proc. Reconfigurable Commun.-centric Systems-on-Chip 6th Int. Workshop, Jun. 2011, pp. 1–8.

[12] Jara-Berrocal and A. Gordon-Ross, “SCORES: A scalable and parametric streams-based communication architecture for modular reconfigurable systems,” in Proc. Des., Autom. Test Eur.Conf., 2009, pp. 268–273.

[13] J. Lin and X. Lin, “Express circuit switching: Improving the performance of bufferless networks-on-chip,” in Proc. IEEE First Int. Conf. Network Comput., Nov. 2010, pp. 162–166.

[14] Weiwei Jiang , Kshitij Bhardwaj ,”A Lightweight Early Arbitration Method for Low-Latency Asynchronous 2D-Mesh NoC’s”, ACM 978-1-4503-3520-1/15/06,2015.

[15] Ritesh Rampal, Rajeevan Chandel, Philemon Daniel,”A Network-on-Chip Router for Deadlock-Free Multicast Mesh Routing,” 978-1-4799-9985-9/15. ©2015 IEEE.

[16] Fatemeh Nasiri , Hamid Sarbazi-azad, Ahmad Khademzadeh,” Reconfigurable multicast routing for Networks on Chip”, Microprocessors and Microsystems 42 (2016) 180–189.

[17] Akram Ben Ahmed, Abderazek Ben Abdallah,” Adaptive Fault-Tolerant Architecture and Routing Algorithm for Reliable Many-Core 3D-NoC systems”, J. Parallel Distrib. Comput. (2016).

[18] Pooria M.Yaghini, Ashkan Eghbal, Nader Bagherzadeh,” On the Design of Hybrid Routing Mechanism for Mesh-based Network-on-Chip”, INTEGRATION, the VLSI journal, S0167-9260(14)00092-3.

[19] Marcus Eggenberger, Manuel Strobel, Martin Radetzki,”Globally Asynchronous Locally Synchronous Simulation of NoCs on Many-Core Architectures”, 2016 24th Euromicro International Conference on Parallel, Distributed, and Network-Based Processing.

[20] R. Akbar , F. Safaei ,“A novel power efficient adaptive RED-based flow control mechanism for networks-on-chip”, 0045-7906/© 2015 Elsevier.

[21] N. Teimouri, M. Modarressi, and H. Sarbazi-Azad, “Power and performance efficient partial circuits in packet-switched networks-on-chip,” in Proc. IEEE 21st Euromicro Int. Conf. Parallel, Distrib. Netw. Process, Feb. 2013, pp. 509–513.

[22] Rohit Kumar and Ann Gordon-Ross, “MACS: A Highly Customizable Low-Latency Communication Architecture”, IEEE Transactions on Parallel and Distributed Systems, VOL. 27, NO. 1, January 2016, PP-237-249.

[23] J. Kim et al., “A low latency router supporting adaptively for on-chip interconnects,” in DAC, Jun. 2005, pp. 559–564.

[24] Rimpy Bishnoi , Vijay Laxmi , Manoj Singh Gaur , Mark Zwolinski,” Resilient routing implementation in 2D mesh NoC”, Microelectronics Reliability 56 (2016) 189–201.

[25] Edson i. Moreno,cesar.a.m.marcon,”arbitration and routing impact on NoC design”,978-1-4577-0660-8/11 ©2011 IEEE.

[26] H.-C. Chi and J.-H. Chen, “Design and implementation of a routing switch for on-chip interconnection networks,” in AP-ASIC, Aug. 2004, pp. 392–395.

[27] A. I. A. Jabbar, Noor .Th. AL Malah,” Design and Implementation of a Network on Chip Using FPGA”, Al-Rafidain Engineering Vol.21 No. 1 February 2013, pp: 91-100.

[28] Lu Wang, Sheng Ma,” A High Performance Reliable NoC Router," 978-1-4673-9569-4/16-©2016 IEEE.

[29] Partha Pratim Pande , Andre´ Ivanov “Performance evaluation and design trade-offs for network-on-chip interconnect architectures,” IEEE Trans. Computers, vol. 54, no. 8, pp. 1025–1040, Aug. 2005.

[30] J. Henkel, W. Wolf, and S. Chakradhar, “On-chip networks: a scalable, communication-centric embedded system design paradigm,” in VLSI, Jan. 2004, pp. 845–851.

[31] Ludovic Devaux, Sebastien Pillement, Daniel Chillet, Didier Demigny. “R2NoC: dynamically Reconfigurable Routers for flexible Networks on Chip”. 2010 International Conference on Reconfigurable Computing.

[32] T. Padmapriya and V. Saminadan, “Inter-cell Load Balancing Technique for Multi- class Traffic in MIMO - LTE - A Networks”, International Conference on Advanced Computer Science and Information Technology , Singapore, vol.3, no.8, July 2015.

[33] S.V.Manikanthan and T.Padmapriya “Recent Trends In M2m Communications In 4g Networks And Evolution Towards 5g”, International Journal of Pure and Applied Mathematics, ISSN NO:1314-3395, Vol-115, Issue -8, Sep 2017.

[34] Rajesh, M., and J. M. Gnanasekar. "An optimized congestion control and error management system for OCCEM." International Journal of Advanced Research in IT and Engineering 4.4 (2015): 1-10.