ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2015

Implementation of Scalable Encryption Algorithm in ETI for High Security Purpose

P.Vyshnavi [1], G. Mary Sowjanya [2]

P.G. Student, Department of Electronics and Communication Engineering, VR Siddhartha Engineering College, Kanuru, Vijayawada, India[1]

Assistant Professor, Department of Electronics and Communication Engineering, VR Siddhartha Engineering College, Kanuru, Vijayawada, India [2]

ABSTRACT: Embedded transition inversion (ETI) is proposed to reduce bit transitions in Serializing parallel buses. Implies power can be reduced further. The ETI coding scheme helps to avoid the problem of extra indication bit by using the phase difference between the clock and data in serial data transmission. Using pipelining this technique is implemented in optimized fashion with only a slight compromise in performance it can used in practical systems. This is achieved by doing the encoding and by calculating the decision bit as the data is loaded on to the buffer. Further this project can be enhanced using Scalable Encryption Algorithm. SEA provides more reliable and secured communication between transmitter and receiver. Low complexity and more security is major advantage with this algorithm, since it consists of low hardware architecture.

KEYWORDS: Phase encoder, Flip Flop, Buffer, Power.

I. INTRODUCTION

In digital electronics systems low power design is the main aspect in a system perspective. It is almost done from the top most software design to the lower most device level but in the intermediate levels it consumes more effort to make the system run at low power and achieving high performance. In many cases if the performance of the system is high but it consumes more power it will become a drawback in such cases. In this project proposes to reduce the power compared to previous technique. According to the moore's law the mounting density of integrated circuits makes vital to have low power systems because if the size of integrated circuit is more then it consumes more power[1]. For such integrated circuits may not keep track in size, so the size of electronic components is miniaturization is necessary. Hence on this concept the research is being made system track at all levels. A system is designed by multiple components they can be broadly classified and a communication framework designed work.

II. EXISTING TECHNIQUE TO DESIGN BUS

To reduce the switching activity TIC technique is used and it is also used to detect errors. Transition inversion coding technique initially receives the parallel data and converts the data in to serial data and transmits data to the encoder block. In this encoder block it consists of check transition block that counts the number of transitions in a given data word and generates a decision bit if the number of transitions is more than the threshold value. In this scheme an extra bit is sent through the data word to indicate whether the transitions is high or low. While coming to ETI this problem is solved the transitions is indicated the phase difference but not by the decision bit because of the elimination of extra indication bit the power consumption also reduces. In TIC scheme the extra bit increases the transitions and latency. Here in this technique we adopted the serialization data transmission to a larger interconnects width and reduces number of wires and reduces spacing. Coupling capacitance is one of the main problem in data transmission to avoid that large interconnect spacing is adopted in this technique and the resistivity is reduced by wider interconnects. By applying various coding techniques and their proposed multiplexing techniques improvement in

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2015

interconnect energy dissipation is achieved. If the degree of multiplexing increases then the power reduction decreases. The ETI coding scheme is mainly proposes to avoid the drawback in the TIC scheme nothing but the extra indication bit problem[2]. By embedding inversion information in between encoded data and clock then the phase difference is generated. Otherwise, no phase difference is generated between clock and data and the data word remains unchanged. ETI transition reduction is improved 20% compared with that TIC.

III. PROPOSED TECHNIQUE

The transitions in word exceeds threshold value Nth, the bits should be encoded in the data word. Otherwise, data word remains same. If the transitions in data word is more than or equal to threshold value then encoding is needed in a data word, this method checks every two bit in the data word. In a serial stream every two bit is combined as a base to be encoded. In such case the b11 b21 is one base and b31 b41 is another base. b1 b2 is denoted as two bit in a base and be1 be2 is denoted as encoded output[3]. In a data word when Nt is less than N(th)then b1 b2 remains unchanged. Otherwise, perform the inversion coding and phase coding. The bit streams for inversion coding is 10 and 01 are mapped to 11 and 00, the bit streams 11 and 00 are mapped to 10 and 01. If the inversion is takes place in word data then we embed the phase difference of serial data in between the clock and data. If the input data is eight bit then the data is divided in to four sets and counts the number of transitions in a given data and checks whether the number of transitions is more than or equal to threshold value. If the number of transitions is more than threshold value then the every second bit of the input data gets inverted to reduce the number of transitions.

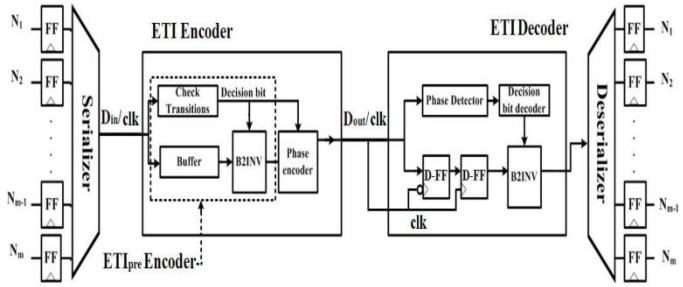


Fig 1: Architecture of the ETI scheme.

The operation of the inversion coding can be expressed as

$$b_{e1=b_1}$$

$$b_{e2} = \begin{cases} b_2 \ with \ N_t < N_{th} \\ !\, b_2 \ with \ N_t \geq N_{th} \end{cases}$$

Phase Coding: Difference of the phase between the clock and data is used in the ETI coding scheme to encode the information.

ETI Decoder: It receives the data coming from ETI encoder and decodes data with the help of phase difference

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2015

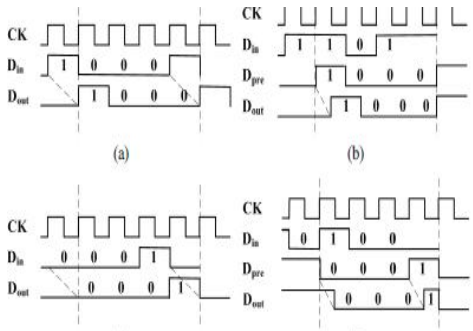


Fig.2: Dout "1000" obtained from (a) Din "1000" without encoding, (b) from Din "1101" with encoding. Dout "0001" obtained from (c) Din"0001" without encoding, and (d) Din "0100" with encoding.

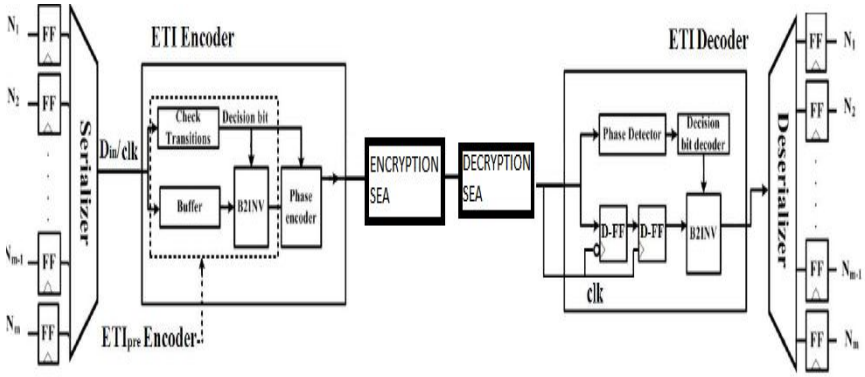


Fig 3: Overall architecture of the ETI scheme.

IV. SCALABLE ENCRYPTION ALGORITHM

SEA is mainly used for small embedded applications. Basically it is designed for software applications because of its simplicity and low cost factor it is using in various applications like controllers, smart cards and processors. It is a loop like structure its designing and operation is very simple and gives high performance[5]. Now a days compared to other algorithms it is one of the best algorithm in terms of performance, simplicity, cost. It is a loop like structure and perfomes many operations like Modulo addition, bit wise xor, word wise xor, substitution operation. SEA is called a simple algorithm because of its small operations performed inside the algorithm.

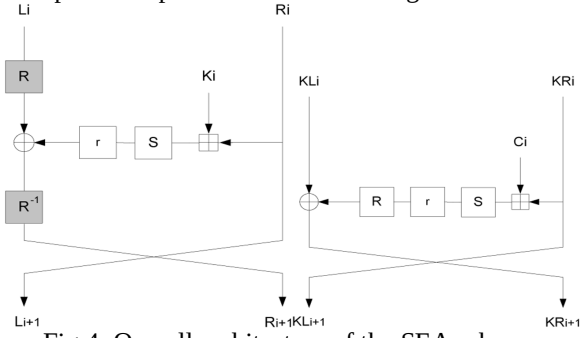


Fig 4: Overall architecture of the SEA scheme

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

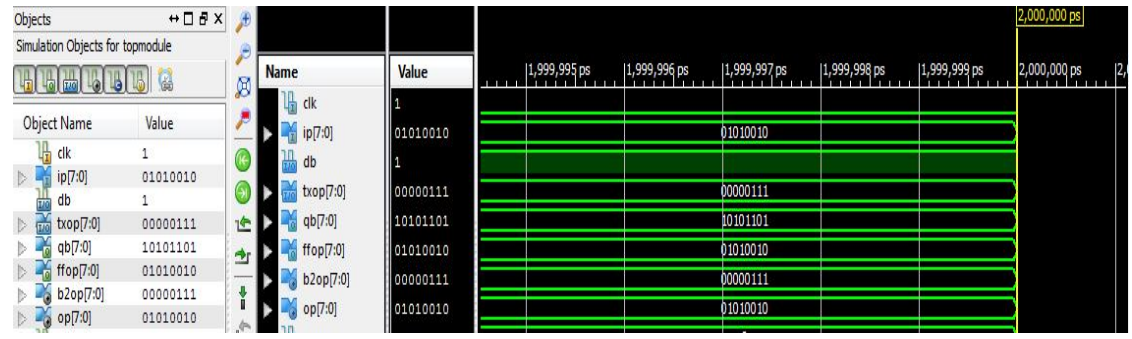
Vol. 4, Issue 7, July 2015

V. ETI WITH SEA

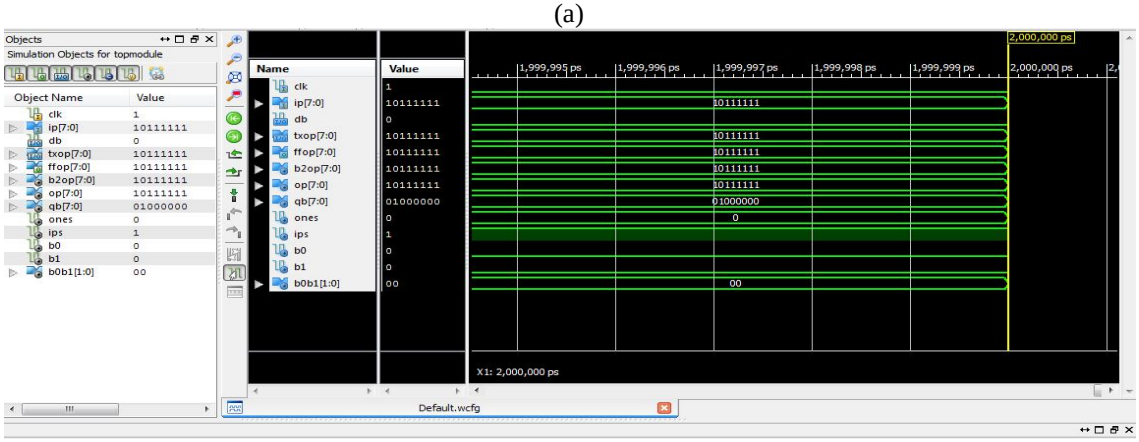
The algorithm is targeted to design at low memory requirements, small code size, and limited instruction set. In addition, the efficient combination of encryption and decryption and deriving sub keys on the fly. SEA structure is based on feistel structure with a variable number of rounds, depends on the plaintext size, key size, and processor size. SEA encryption involves basic elementary operations such as Bit wise XOR, Substitution Box S, Word rotation R, Bit rotation r, and mod 2^b. The structure of the SEA was secured against various attacks such as linear and differential cryptanalytic attacks, square attacks, truncated and impossible differential attack, Interpolation attack, slide attacks, related key attacks and algebraic attacks. The SEA was implemented with a block size and key size of 96 and 96 bits and occupies an area of 3758 GE with a throughput of 103 Kbps at a clock rate of 100 KHZ.SEA algorithm is placed in between the ETI encoder and ETI decoder blocks as shown in the figure. Our main aim of this project is to reduce power and provide security. SEA provides high security. As SEA is placed in between the encoder and decoder blocks the encoded data is given to the SEA encryptor. SEA performs some operations on the encoded data and transmits the encrypted data through the channel so that no third party can hack the data because the third party member doesn't know the key and which operations performed on the key. The encrypted data is transmitted through the channel and given to the SEA decryptor to decrypt the data. In SEA decryptor reverse operations are performed on the encoded data and the data is given to the ETI decoder ETI decoder decodes the data.

VI .RESULT ANALYSIS

The result analysis for ETI scheme is done using Xilinx 13.4 by coding in VHDL language below figures show the simulation results of ETI technique with and with out decision bit.



(a)



(b)

Fig 5: Simulation results of ETI scheme (a) with decision bit. (b) without decision bit.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2015

The result analysis for ETI scheme with SEA is done using Xilinx 13.4 by coding in VHDL language below figure shows the simulation results of ETI technique with SEA.

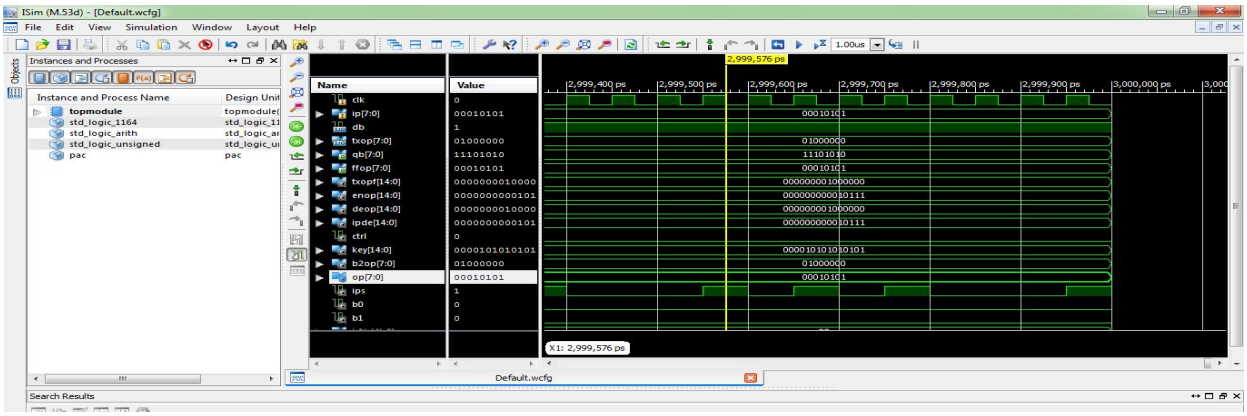


Fig 6:Simulation results of ETI scheme with SEA

The below table shows the comparison between power and delay of ETI scheme and ETI with SEA scheme. The time has reduced to 8.8% and delay has reduced to 27.5%.

TABLE 1: Power and Delay comparison

PARAMETER	ETI Scheme	ETI with SEA
POWER	0.125W	0.114W
DELAY	4 ns	2.9 ns

VII. CONCLUSION

Extra bit problem is solved in ETI. Power is reduced in ETI compared to TIC. High security is provided in serial communication by using Embedded Transition Inversion scheme with Scalable Encryption Algorithm.

REFERENCES

[1]C.JacobEbbipeni1N. Bamakumari, "Design and Implementation of Area and Power Efficient Embedded Transition Inversion Coding For Serial Links", in Feb.2004.
[2] Francois-XavierStandaert,GillesPiret, "A Scalable Encryption Algorithm for Small Embedded Applications", in 2006.
[3] J. Jenifa, C.Jacob Ebbipeni," Bus Energy Minimization for a Serial Link by Modified EmbeddedTransition Inversion Coding" International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, Issue-3, March 2014.
[4]Abinesh R "Transition Inversion based Low Power Coding for Buffered Bus Systems",2010.
[5]System on Chip Design and Modelling University of Cambridge Computer Laboratory Lecture Notes Dr. David J Greaves (C) 2011 All Rights Reserved DJG Part II Computer Science Tripos Easter Term 2011.
[6]Ching-te chiu, wen-chih huang, "embedded transition inversion coding with Low switching activity for serial links" ieee transactions on very large scale integration systems, vol. 21, no. 10, october 2013.