ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 4, April 2017

TACIT Secured Comprehensive Data Transmission Scheme for On-chip Communication Network

Pinky Rajendrakumar[1], Gokul P.G[2]

PG Scholar, Dept. of ECE, TKM Institute of Technology, Kollam, Kerala, India[1]

Asst.Professor,Dept. of ECE, TKM Institute of Technology, Kollam, Kerala, India[2]

ABSTRACT: Network on chip is a communication subsystem on an integrated circuit typically between cores in a system on chip (SOC). Application of encoding and decoding techniques tends to reduce energy consumption. We propose a new standard-basis based encoding/decoding method to increase the performance and cost of CDMA NoCs in area, power assumption, and network throughput. In the transmitter module, source data from different senders are separately encoded with an orthogonal code of a standard basis and these coded data are mixed together by an XOR operation. Then, the sums of data can be transmitted to their destinations through the on chip communication infrastructure. In the receiver module, a sequence of chips is retrieved by taking an AND operation between the sums of data and the corresponding orthogonal code. Original data can be reconstructed in the receiver. The Walsh code-based (WB) encoding/decoding technique is also implemented andis compared with the proposed method in terms of power, area and throughput. A TACIT algorithm based security could be provided for the standard-basis based transceiver as a framework to secure a NoC, addressing in particular the protection from power/EM attacks of a system containing non-secure cores as well as secure ones.

KEYWORDS: Network on chip; standard-basis based encoding/decoding method; The Walsh code-based (WB) encoding/decoding technique; TACIT algorithm

I. INTRODUCTION

Network on chip is a communication subsystem on an integrated circuit typically between cores in a system on chip(soc).Network on chip is feasible and advantageous over traditional bus based architectures because they exhibit high levels of parallelism and scalability.The CDMA technique functions at the principle of encoding the original data with a set of orthogonal codes. The encoded data from different users are then added together for transmission without interfering with each other due to the orthogonal property of the spreading codes. The meaning of being orthogonal is that the normalized auto-correlation of the spreading codes is 1. However the cross-correlation value of the spreading codes is 0. The receiving user can then extract or decode the original data by multiplying the received sum with the corresponding unique spreading code used for encoding.Several types of spreading codes have been proposed for CDMA communication, such as M-sequence, Gold sequence, and Kasami sequence, etc.But these the spreading codes used in the CDMA NoC does not balance both the required orthogonal and balance properties.

Several techniques were proposed to provide a low energy reliable communication scheme for network on chip. Application of encoding and decoding techniques tends to reduce energy consumption. Encoding is the process of putting a sequence of characters into specialized format for efficient transmission or storage. Decoding is the opposite process, the conversion of an encoded format back into the original sequence of characters. The concept of code division multiple access(CDMA) can also be applied for on chip packet switch communication network.CDMA is form of multiplexing, which allows numerous signals to occupy a single transmission channel.Thus CDMA can provide better signal quality and reduced fading during encoding and decoding when used in network on chip.

A standard basis based encoding/decoding method of CDMA NOC to improve performance and cost is proposed.The standard-basis-based method is compared with the walsh-code-based encoding and decoding technique.Different parameters like power, area and throughput are studied under both the coding schemes.A cryptographic security based on TACIT encryption and decryption algorithm is provided for the most relevant communication scheme under comparative study.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 4, April 2017

II. RELATED WORK

In [2]to overcome the limitations of traditional TDMA-I, a number of new interconnect schemes have been investigatedto greatly increase the aggregate data rate and concurrency as well as to reduce latency and power consumption. In [3] anon chip packet-switched communication network which applies Code-Division Multiple Access (CDMA)technique has been developed and implemented inRegister-Transfer Level (RTL) using VHDL. In [4] the chip implementation of thenew technique of securing data in NoC routers is proposed. Many algorithms have been anticipated already for secured NoC routing butlimited to their key size and block size. In the paper, NoC architecture is integrated with modified TACIT security algorithm onVirtex-5 FPGA. In [5] a cryptographic algorithm is considered to be computationallysecured if it cannot be broken with standard resources, either current or future and apart from the algorithm distribution of keys also more important is to make an efficient cryptosystem. TACIT Encryption Algorithm can produce best possible results if key size is the size of the packet expected to pass through the network is small. This paper gives the comparison of the various algorithms with TACIT Encryption Algorithm on the basis of parameters like key length, block size, type and features.

In [6] A cryptographic algorithm is considered to be computationally secured if it cannot be broken with standard resources, either current or future and apart from the algorithm distribution of keys also more important is to make an efficient cryptosystem. TACIT Encryption Algorithm can produce best possible results if key size is the size of the packet expected to pass through the network is small. This paper gives the comparison of the various algorithms with TACIT Encryption Algorithm on the basis of parameters like key length, block size, type and features. In [7] In this paper a new block cipher cryptographic symmetric key algorithm is proposed named "TACIT Encryption Technique" which has a unique independent approach by using some suitable mathematical logic along with a new key distribution system which is being applied on a secure policy based routing. In [8] a novel Network-on-Chip (NoC) architecture that is based on Code Division Multiple Access (CDMA) techniques. The orthogonal properties of a Walsh code are used to route data packets between resources. A star network topology allows a hierarchical switching platform to be constructed which can be scaled to handle large systems.

PROPOSED ALGORITHM

A. *Design Considerations:*

- Walsh code generation using walsh generator circuit.
- Walsh code based transceiver coded.
- Standard basis based code generated using code generator.
- Standard basis based transceiver coded.
- Tacit based encryption algorithm
- Cryptographic security is provided to standard basis based transceiver based on TACIT algorithm

B. *Description :*

Aim of the project is to find the most reliable communication scheme under CDMA for network on chip. The most reliable method is to be provided with security using TACIT encryption/decryption algorithm.

1: Walsh code generator circuit:

Walsh code is generated from a walsh matrix or hadamard matrix. Each row of hadamard matrix represents the walsh code. The walsh matrix is usually generated from a seed which may generate larger matrix seeds for higher matrices and larger walsh code generation.

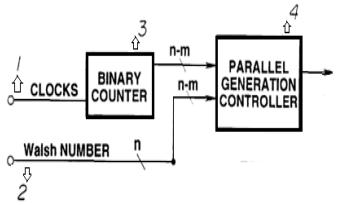


Figure1. Walsh code generator circuit

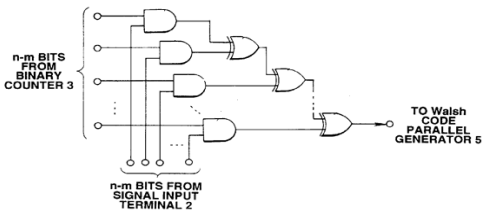


Figure2. Parallel generation controller

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 4, April 2017

Figure1. shows the walsh code generator circuit.The clock signals entering an input terminal 1 is sent to a binary counter3. The binary counter 3 is controlled on the basis of the clock signals. To a signal input terminal 2 is supplied a signal representing Walsh number. Upper (n-m) bits and lower m bits of the signal representing the n-bit Walsh number are sent to the parallel generation controller 4.

2: Walsh code based encoder:

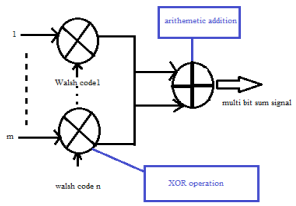


Figure 3. Walsh code based encoder circuit

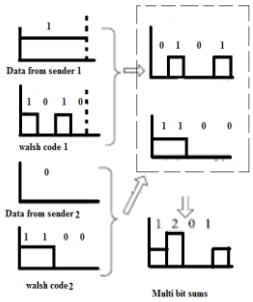


Figure 4. Walsh code based encoding scheme

Figure 3 shows the walsh based encoder circuit. TheN number of signal are collected from n number of sources. These signals are given as input to the encoder in bit by bit manner. So it is a discrete form of signal processing. S bit of spreading code is generated by using walsh sequence generator. For each message signal unique spreadingcode is used. An original data bit is first encoded with a Walsh code by taking an XOR operation. Then, these encoded data are added up to a multibit sum signal by taking arithmetical additions. Each sender needs an XOR gate, and multiple wires are used to express the sum signal if we have two or more senders. Moreover, the number of wires increases as the number of senders increases.

3: Walsh code based decoder:

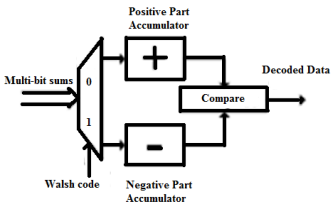


Figure 5. Walsh code based decoder circuit

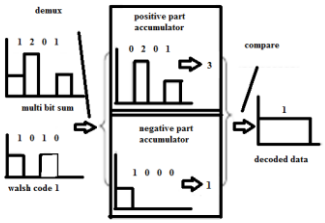


Figure 6. Walsh code based decoding scheme

According to the bit value of data chips spreading code are to be used for decoding operation. For decoding operation the spreading code which is used is same as the spreading code which is used for encoding scheme of that data bit. The data bit is either 0 or 1. The spreading code is playing very vital role in accumulator selection. According to the chip value of Walsh code, the received multibit sums are accumulated into positive part (if the chip value is 0) or negative part (if the chip value is 1). Therefore, the two accumulators in the WB decoder separately contain a multibit adder to accumulate the coming chips and a group of registers to hold the accumulated value. Through the comparison module after the two accumulators, the original data is reconstructed. If the value of positive part is large, the original data is 1. Otherwise, the original data is 0.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 4, April 2017

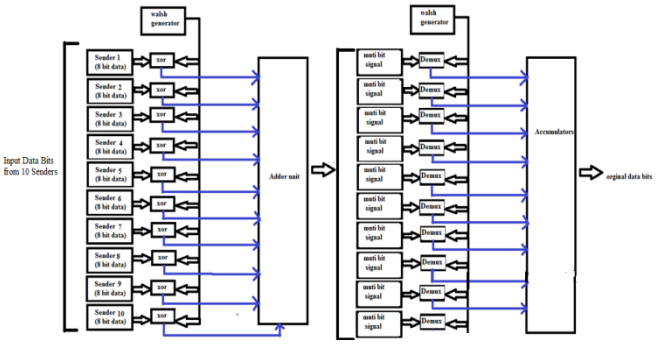


Figure 7. Walsh code based transceiver

4: Standard basis based code generator:

Any code with a single high value or a single '1' is called a standard orthogonal code.

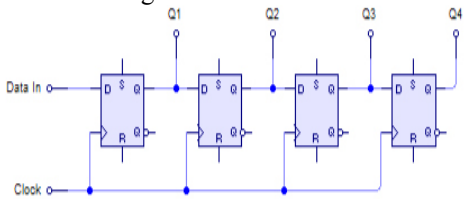


Figure 8.Standard basis code generator

5: Standard basis based encoder:

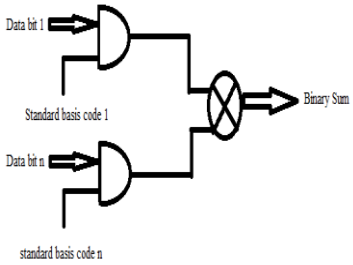


Figure 9. Standard basis based encoder circuit

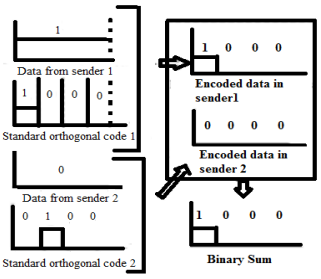


Figure10. Standard basis based encoding scheme

An original data bit from a sender is fed into an AND gate in a chip-by-chip manner, and it will be spread to n-chip encoded data with an orthogonal code of a standard basis. Then, the encoded data from different senders are mixed together through an XOR operation, and a binary sum signal is generated. Therefore, the output signal is always a sequence of binary signal transferred to destination using one single wire.

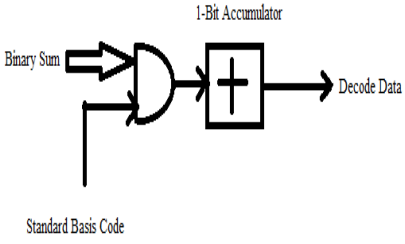


Figure11. Standard basisbased decoder circuit

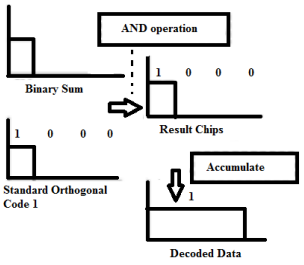


Figure12. Standard basis based decoding scheme

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering
(An ISO 3297: 2007 Certified Organization)
Website: www.ijircce.com
Vol. 5, Issue 4, April 2017

6: Standard basis based decoder:

When the binary sum signal arrives at receivers, an AND operation is taken between the binary sum and the corresponding orthogonal code in chip-bychip manner. Then, the result chips are sent to an accumulator. After m-chipsare accumulated (m is the length of the orthogonal code), the output value of the accumulator will be the corresponding original data.

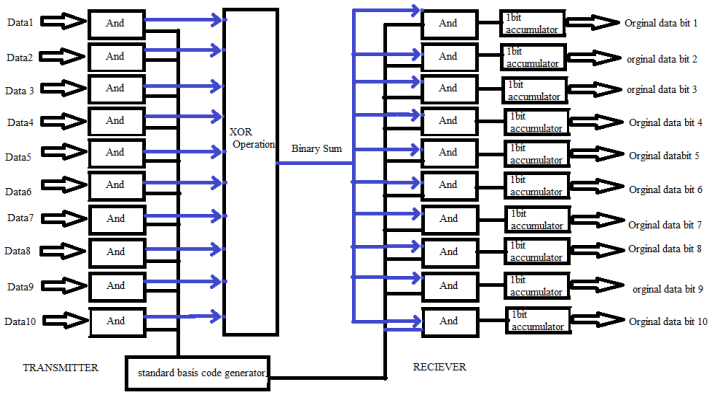


Figure 13 Standard basis based transceiver

7: Comparative study of walsh code based transceiver and standard basis based transceiver

Parameter	Walsh Code Transceiver	Standard Basis Code Transceiver
Number Of Slice Registers	503-utilisation 4%	59-utilisation 0%
Number of slice LUTs	1420-utilisation 24%	99-utilisation 1%
Number of fully used LUT-FF pairs	275-utilisation 16%	21- utilisation 2%
Memory usage	289056 kilobytes	219100 kilobytes
Timing Details	7.664ns	3.984ns
Real Time to XST completion	27.00 seconds	16.00 seconds
Real Time to CPU Time Completion	26.55 seconds	15.77 seconds

Table1. Comparative study

8:TACIT Based Security on SB Transceiver- Key Generation

Security has gained increasing relevance in the development of embedded devices. Towards the aim of a secure system at each level of the design, NoCs offer more resistance to bus probing attacks. But power/EM attacks and network snooping attacks are becoming more relevant.The network level framework for security is based on symmetric key cryptography, where each secure core communicates each other using symmetric key cryptography. Many cryptographic algorithms were proposed, out of which TACIT algorithm proves to be the best in terms of security and key size. TACIT Encryption/ Decryption Technique have a unique independent approach by using some suitable mathematical logic along with a new key distribution system.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 4, April 2017

Generation of random strings by sender and receiver

↓

Classifier for M,N,U,V,n

M=no:of lower case letters

N=no:of numerical characters

U=no:of uppercase character

V=no:of special characters

n=n of hash table

↓

Comparator to find the largest among M,N,U,V

↓

Use the modified hash function table to find function values for both sender and receiver

↓

Find the function values, P for sender, Q or receiver

↓

Average of P and Q is the key

The random strings are generated by the sender and receiver. Each of the strings are studied to find the number of upper case letters, number of lower case letters, number of numerical characters and number of special characters within the string. In each of the string these values are compared to find the largest among M,N,U,V. According to the largest variable found and 'n' value, a modified hash function table is used to find the function values of both sender and receiver whose average generates the symmetric key for the cryptographic security.

Hash Table

n	Hash Functions			
	H1	H2	H3	H4
	$m_g = m > (n,u,v)$	$n_g = n > (m,u,v)$	$u_g = u > (m,n,v)$	$v_g = v > (m,n,u)$
0	m^n-m.n	n^u+n.u	u^v+u.v	v^m+v.m
1	m^u+(m+u)	n^v+(n+v)	u^m+(m+v)	v^n+(u+v)
2	m^v-(u+v)	n^m-(m+n)	u^n-(u+n)	v^u-(v+m)
3	n^u+(v.m)	m^v+(u.n)	u^n+(v.m)	v^m+(v.m)
4	n^v+(n.m)	m^u+(u.v)	u^n+(v.n)	v^m+(n.u)
5	n^m-m	m^n-n	u^v-v	v^u-v
6	u^m-m	v^n-n	m^u-u	n^v-v
7	u^n+(n+m-u)	v^m+(m+n-v)	n^v+(v-n-m)	m^u+(u-m-n)
8	u^v+(n+m+v-u)	v^u+(v+u+m-n)	m^n+(m+n+v-u)	n^m+(m+u+n-v)
9	m.n.v+(m.u)	n.u.v+(n.v)	m.n.u+(u.v)	u.v.n+(v.m)

Table2. Modified Hash Function table

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 4, April 2017

9: TACIT Encryption /Decryption Algorithm

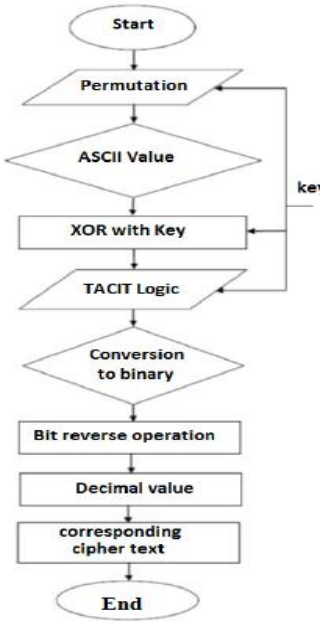


Figure14. TACIT encryption algorithm

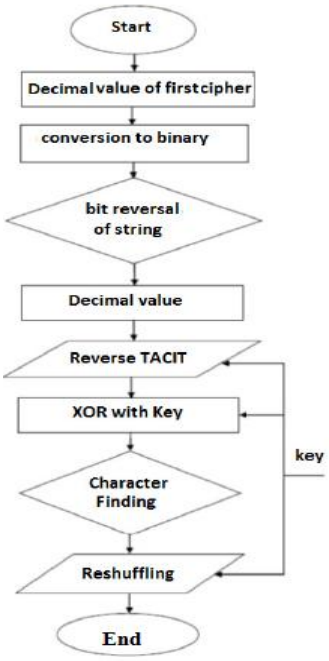


Figure15. TACIT decryption algorithm

TACIT Encryption Algorithm: Fig. 16 shows the flow of the encryption algorithms

Step 1: First, read the text file and apply the concept of initial permutation approach to shuffle the position of each character with the help of key value.
Step 2: Read the character from the text file corresponding to the text and get the ASCII value of that character.
Step 3: specific n-bit key value is XORed with corresponding text.
Step 4: Apply TACIT Logic which is $n^k xor k$ along with some specific operations.
Step 5: It is needed to convert the resulted value from step 4 into binary one.
Step 6: Perform reverse operation on resulted value from step 5 on the binary string.
Step 7: Find the corresponding decimal value.
Step 8: Formation of unicode character corresponds to the decimal value, which is nothing other than the cipher text.
Step 9: Continue all steps 1 to 7 for the next characters and complete until End of File (EoF) is achieved.

TACIT Decryption Algorithm: Fig. 17 shows the flow of the decryption algorithms.

Step 1: Encode text in encryption algorithm is cipher text. Get the corresponding decimal value of cipher text, after reading the first character from the cipher text.
Step 2:.Evalute the corresponding binary value and reverse it.
Step 3: Perform the inverse operation of the tacit logic.
Step 4: Perform XOR logical operation with next key value or n-bit key value.
Step 5: Determine the character corresponds to it.
Step 6: Now, reshuffling is needed with the help of key value.
Step 7: Repeat the steps (1 to 6) till EoF is achieved.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

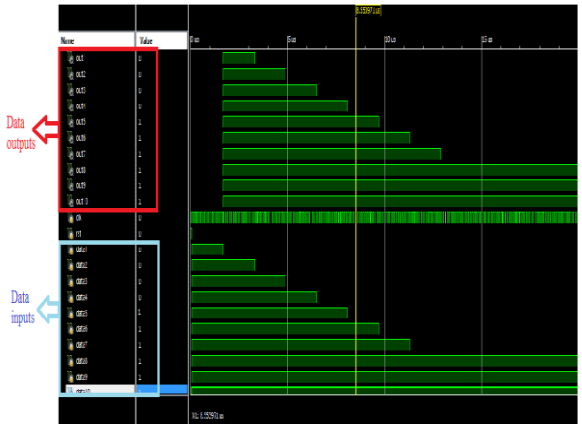
Website: www.ijircce.com

Vol. 5, Issue 4, April 2017

III.SIMULATION RESULTS

The simulation studies involve the outputs of standard basis based transceiver and walsh code based transceiver for 10 senders sending 8bit data each. The coding is done in Verilog HDL and is simulated in Xilinx ISE 14.1.

Figure 16. Walsh code based transceiverFigure



17 Standard basis based transceiver

In both the transceivers, the inputs given are obtained at the output of the receiver. On comparing both the transceivers, the standard basis based transceiver is found to be five times better than walsh code based transceiver in terms of area, timing margins and throughput.

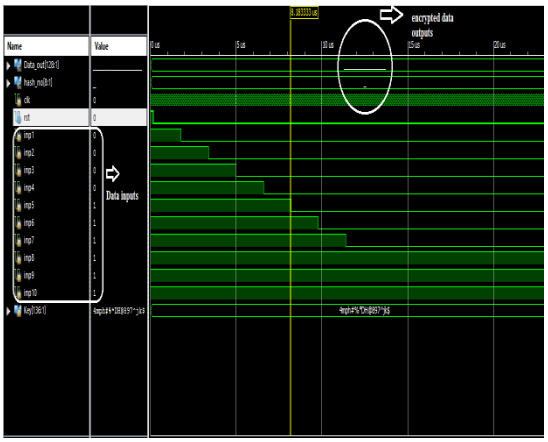


Figure 18SB Transmitter Secured With

TACIT Encryption Algorithm

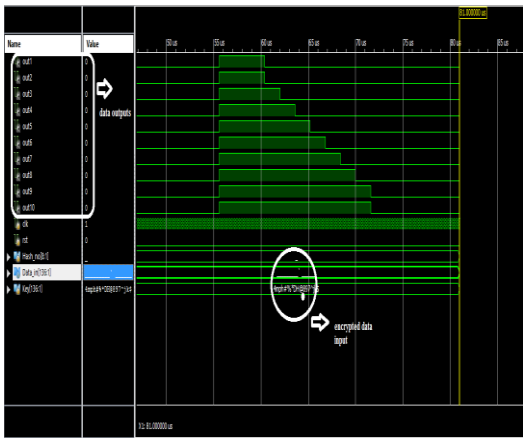


Figure 19SB Transmitter Secured With

TACIT Decryption Algorithm

The standard basis based transceiver is further provided with a cryptographic security using TACIT algorithm to secure the communication subsystem from any external attacks. Thus the input data given, encoded by the standard basis based transmitter is encrypted into cipher text. This cipher text given as an input to the standard basis based receiver is decrypted and then decoded by which the data input given is retrieved at the output of the receiver.

IV.CONCLUSION

CDMA concept is based on the concept that transferring the data from nodeto node in bit by bit format. Modelling of network on chip structure by using the principle ofCDMA is better way for data transferring in chip level. By using

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 4, April 2017

CDMA NOC concept the datatransfer latency has increased in node to node communication process. Application of encoding and decoding technique helps in more reliable data communication scheme for network on chip. The walsh codes are generated using a walsh code generator unitApplication of encoding and decoding techniques tends to reduce energy consumption. A Walsh and the standard code-based encoding/decoding techniques based transmitter and receiver are proposed. The original data is retrieved at the output of both the transceivers. The transceivers are compared in terms of area, throughput and timing details. The standard basis based transceiver is found to be five times better that Walsh code based transceivers in terms of all parameters. The SB transceiver is secured using TACIT encryption/decryption algorithms.

REFERENCES

1. Jian Wang, Zhonghai Lu, and Yubai Li," A New CDMA Encoding/Decoding Method for on-Chip Communication Network, "in *IEEE transactions on very large scale integration (vlsi) systems, vol. 24, no. 4, April 2016.*
2. M. Frank Chang**, "**CDMA/FDMA-Interconnects for Future ULSI Communications",in *High Speed Electronics Laboratory, Department of Electrical Engineering University of California, Los Angeles, CA 90095-1594, December 2015.*
3. Xin Wang, JariNurmi*"* An On-Chip CDMA Communication Network " in *Institute of Digital and Computer Systems, Tampere University ofTechnology, Tampere, Finland, December 2014.*
4. Adesh Kumara, PiyushKuchhalb ,SonalSinghalc, "Secured Network on Chip (NoC) Architecture and Routing with Modified TACIT Cryptographic Technique," *in International Conference on Intelligent Computing, Communication & Convergence (ICCC-2014 Conference Organized by Interscience Institute of Management and Technology, Bhubaneswar.*
5. *ManmeetKaur ,ManjitKaur , Gurmohan Singh ,* "Comparison of TACIT Encryption Algorithm with Various Encryption Algorithms," in *International Journal of Electronics and Computer Science Engineering.*
6. A.Arun, Dr P Nirmal kumar and A. Kwasinski, "Modified TACIT algorithm based on 4H key distribution for secure routing in noc architectures," in *IEICE electronics express*,pp. 636–639, *May 2012.*
7. W. Lee and G. E. Sobelman, "An Efficient Cryptographic Approach for Secure Policy Based Routing (TACIT Encryption Technique)," in *Proc. IEEE Int. Symp. Circuits Syst.*,pp. 1349–1352, *May 2009*.
8. X. Wang, T. Ahonen, and J. Nurmi, "Applying CDMA technique to network-on-chip," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst., vol. 15, no. 10, pp. 1091–1100, Oct. 2007.*
9. X. Wang and J. Nurmi, "Modeling a code-division multiple-access network-on-chip using SystemC," in *Proc. Norchip,, pp. 1–5, Nov. 2007.*