OPEN ACCESS INTERNATIONAL JOURNAL OF SCIENCE & ENGINEERING

DESIGN AND IMPLEMENTATION OF A DIGITAL SECURE CODE-SHIFTED REFERENCE UWB TRANSMITTER AND RECEIVER

Ch.Swetha[1], Mr.M.Sundar rao[2], Y.David Solomon Raju[3]

PG Scholar, *Dept of Electronics and Communication Engineering, Holymary Institute Of Technology And Science, Bogaram(V), Keesara (M),Hyderabad -501 301*

Assistant Professor *Dept of Electronics and Communication Engineering, Holymary Institute Of Technology And Science, Bogaram(V), Keesara (M),Hyderabad -501 301*

Associate Professor, *Head of Dept, Electronics and Communication Engineering, Holymary Institute Of Technology And Science, Bogaram(V), Keesara (M),Hyderabad -501 301*

Email-Id [1] , *Email-Id* [2]

Abstract ***This article presents the first compact hardware implementation of a digital code-shifted reference (CSR) ultrawideband (UWB) transceiver. The security of the transmission is based on changing the physical properties of the transmission without the use of higher level security options. The software models of the designed transceiver are simulated and verified in both floating-point and fixed-point numerical representations. The synthesizable Verilog description of the transceiver architecture is simulated and verified against its fixed-point simulation model. The secure transceiver is implemented on our custom-developed field-programmable gate array (FPGA) board. The characteristic and implementation results of the secure transceiver architecture on the FPGA are presented. The bit error rate performance of the transceiver is measured in realtime on the FPGA using an accurate on-chip Gaussian noise generator and is compared with that of the software simulation model. An ASIC architecture of the CSR-UWB transceiver is estimated to occupy 0.019 mm2 and dissipate .63 mW from a 1-V supply while operating at 82 MHz in a standard 32-nm CMOS technology.***

Keywords: *Code-shifted reference ultra-wideband (CSRUWB), field-programmable gate array (FPGA), baseband architecture*

----------∴∴∴----------

I INTRODUCTION

For applications in which the transceiver must manage sensitive data, it is important for the transceiver to offer robust protection from both passive and active potential adversaries. The passive adversary would be considered an eavesdropper that would attempt to collect the transmitted information intended for the receiver. An active adversary would attempt to mimic the transceiver and send its own messages to the receiver while posing as the transmitter. The addition of the security scheme is intended to prevent unwanted eavesdropping while also deterring the mimicry of the legitimate transmitter. Computational security conventionally uses a security key to encrypt data before it is transmitted. The strict size and power requirements of certain devices, such as brain-implantable transceivers, prevent the use of conventional cryptography algorithms. In an effort to drastically reduce the power consumed, the security strategy relies on the changing of the physical properties of the transmission scheme to mask the transmitted data. Ultra-wideband (UWB) is considered to provide some inherent advantages when it comes to the security of its transmissions because of the extremely large bandwidth. The security of the transmitted reference (TR) trasnceiver

in [1] is based on separating a data and a reference pulse in time so only a legitimate receiver would be able to locate the data pulse. For the receiver to interpret the data received, the receiver must know the separation and use an exact timing delay to correlate the data with its reference. A precise timing delay is difficult to implement in digital hardware, especially with strict area limitations. In the code-shifted reference (CSR) scheme [2], [3], the transmitter sends groups of data pulses simultaneously with a reference pulse added together in the time domain. Orthogonal codes allow data and reference pulses to be separated in the code domain in a way that is only discernible by the legitimate receiver.

Fortunately, physical properties of the CSR scheme can be manipulated to resemble the security provided in [1] by a precise timing offset that is impractical to implement. For a compact and low complexity architecture, the CSRUWB transceiver is designed as a non-coherent transceiver [5] using the energy collection method [6]. Choosing the CSR scheme provides the transmission with additional inherent security. The low probability of detection as well as the masking of the number of bits transmitted simultaneously are basic properties of CSR-UWB before the inclusion of a security key. Incorporating the security key into the CSR scheme bolsters security by allowing only the intended receiver to know the separation in the code domain between the data and reference. The transceiver is implemented to stay as compact as possible while introducing a way to vary the separation between transmitted data and reference pulses [1]. We first modeled the secure IR-UWB transceiver in floatingpoint representation in Matlab. The fixed-point representation of the transceiver is then modeled using a custom-developed library of parameterizable fixed-point operations in MEX-C. The Verilog description of the transceiver is developed and the cycle-accurate bit-true implementation of the transceiver is analyzed and verified against its fixed-point model. The transceiver is implemented on a custom-developed field programmable gate array (FPGA) board hosting a relatively small Xilinx Spartan-6 FPGA. The on-chip bit error rate performance measurement of the transceiver using our accurate GNG [7] is compared with the fixed-point software simulation.

II LITERATURE SURVEY

2.1 Over-burden CDMA transport topology for MPSoC interconnects:

Intra-chip correspondence is a noteworthy bottleneck in present day multiprocessor framework on-chip (MPSoC) outlines. The transport topology is the most well-known on-chip interconnects innovation and transport conflict in one of the significant issues in transport based MPSoC plans. Code division different access (CDMA) has been proposed as a transport sharing system to defeat the transport conflict issue. In CDMA, a predetermined number of symmetrical spreading codes can share the medium because of the Multiple Access Interference (MAI) issue. In remote interchanges, over-burden CDMA has been considered to expand the framework limit by including additional non-symmetrical spreading codes with particular qualities. We propose a novel CDMA transport design utilizing the over-burden CDMA ideas to expand the most extreme number of centers having the same CDMA transport in MPSoC by 25% at a negligible Improved Overloaded CDMA Interconnect (OCI) Bus Architecture for On-Chip Communication: On-chip interconnect is a noteworthy building square and a principle execution bottleneck in current complex System-on-Chips (SoCs). The transport topology and its subsidiaries are the most sent correspondence structures in contemporary SoCs. Space exchanging exemplified by cross bars and multiplexers, and time sharing are the key empowering influences of different transport structures. The cross bar has quadratic multifaceted nature while asset sharing altogether debases the general framework's execution. In this work we rouse utilizing Code Division Multiple Access (CDMA) as a transport sharing methodology which offers numerous points of interest over other topologies. Our work looks to supplement the regular CDMA transport includes by applying over-burden CDMA practices to expand the transport usage effectiveness. We propose the Difference-Overloaded CDMA Interconnect (D-OCI) transport that use the adjusting Parallel over-burden CDMA interconnect (OCI) transport engineering for on-chip interchanges On-chip interconnects are the execution bottleneck in present day System-on-Chips (SoCs). Transport topologies and Networks-on-Chip (NoCs) are the fundamental methodologies used to actualize on-chip correspondence. The interconnect texture empowers asset sharing by Time or potentially Space Division Multiple Access (T/SDMA) strategies. Code Division Multiple Access (CDMA) has been proposed to empower asset partaking in on-chip interconnects where every datum bit is spread by a one of a kind symmetrical spreading code of length N. Not at all like T/SDMA, in remote CDMA, can the correspondence channel limit be expanded by defeating the Multiple Access Interference (MAI) issue. Accordingly, we present two over-burden CDMA interconnect (OCI) transport structures, in particular TDMA-OCI (T-OCI) and Parallel-OCI (P- OCI) to expand the traditional CDMA interconnect limit. We execute and approve

2.2 Over-burden CDMA interconnect for Network-on-Chip (OCNoC)

Systems on Chip (NoCs) have supplanted on-chip transports as the foremost correspondence methodology in vast scale Systems-on-Chips (SoCs). Code Division Multiple Access (CDMA) has been proposed as an interconnect texture that can accomplish high throughput and settled exchange inertness because of the CDMA transmission simultaneousness. Over-burden CDMA Interconnect (OCI) is a compositional development of the customary CDMA interconnects that can twofold their transfer speed at marginalcost. Utilizing OCI in CDMA-based NoCs has the capability of giving higher transfer speed at low-power and-territory overheads contrasted with otherNoC structures. Besides, settled idleness and unsurprising execution

accomplished by the inalienable CDMA simultaneousness can lessen the exertion and overhead required to actualize QoS. In this work, we advance the Overloaded CDMA interconnect for Network on Chip.

2.3 Over-burden CDMA transport topology for MPSoC interconnects:

Intra-chip correspondence is a noteworthy bottleneck in present day multiprocessor framework on-chip (MPSoC) outlines. The transport topology is the most well-known on-chip interconnect innovation and transport conflict in one of the significant issues in transport based MPSoC plans. Code division different access (CDMA) has been proposed as a transport sharing system to defeat the transport conflict issue. In CDMA, a predetermined number of symmetrical spreading codes can share the medium because of the Multiple Access Interference (MAI) issue. In remote interchanges, over-burden CDMA has been considered to expand the framework limit by including additional non-symmetrical spreading codes with particular qualities.We propose a novel CDMA transport design utilizing the over-burden CDMA ideas to expand the most extreme number of centers having the same CDMA transport in MPSoC by 25% at a negligible Improved Overloaded CDMA Interconnect (OCI) Bus Architecture for On-Chip Communication: On-chip interconnect is a noteworthy building square and a principle execution bottleneck in current complex System-on-Chips (SoCs). The transport topology and its subsidiaries are the most sent correspondence structures in contemporary SoCs. Space exchanging exemplified by cross bars and multiplexers, and time sharing are the key empowering influences of different transport structures. The cross bar has quadratic multifaceted nature while asset sharing altogether debases the general framework's execution. In this work we rouse utilizing Code Division Multiple Access (CDMA) as a transport sharing methodology which offers numerous points of interest over other topologies. Our work looks to supplement the regular CDMA transport includes by applying over-burden CDMA practices to expand the transport usage effectiveness. We propose the Difference-Overloaded CDMA Interconnect (D-OCI) transport that use the adjusting Parallel over-burden CDMA interconnect (OCI) transport engineering for on-chip interchanges On-chip interconnects are the execution bottleneck in present day System-on-Chips (SoCs). Transport topologies and Networks-on-Chip (NoCs) are the fundamental methodologies used to actualize on-chip correspondence. The interconnect texture empowers asset sharing by Time or potentially Space Division Multiple Access (T/SDMA) strategies. Code Division Multiple Access (CDMA) has been proposed to empower asset partaking in on-chip interconnects where every datum bit is spread by a one of a kind symmetrical spreading code of length N. Not at all like T/SDMA, in remote CDMA, can the correspondence channel limit be expanded by defeating the Multiple Access Interference (MAI) issue. Accordingly, we present two over-burden CDMA interconnect (OCI) transport structures, in particular TDMA-OCI (T-OCI) and Parallel-OCI (P- OCI) to expand the traditional CDMA interconnect limit. We execute and approve Over-burden CDMA interconnect for Network-on-Chip (OCNoC) Systems on Chip (NoCs) have supplanted on-chip transports as the foremost correspondence methodology in vast scale Systems-on-Chips (SoCs). Code Division Multiple Access (CDMA) has been proposed as an interconnect texture that can accomplish high throughput and settled exchange inertness because of the CDMA transmission simultaneousness. Over-burden CDMA Interconnect (OCI) is a compositional development of the customary CDMA interconnects that can twofold their transfer speed at marginalcost. Utilizing OCI in CDMA-based NoCs has the capability of giving higher transfer speed at low-power and-territory overheads contrasted with other NoC structures. Besides, settled idleness and unsurprising execution accomplished by the inalienable CDMA simultaneousness can lessen the exertion and overhead required to actualize QoS. In this work, we advance the Overloaded CDMA interconnect for Network on Chip.

III PROPOSED SYSTEM

CSR-UWB TRANSMITTER ARCHITECTURE

For a compact CSR implementation, the designed transceiver only uses the security key to change the reference pulse, while keeping the shifting codes fixed. By keeping the value of the shifting codes constant, the control logic to manage the security key is simplified and a multiplexer is removed for each bit transmitted simultaneously. Fig. 5 shows the architecture of the secure CSR transmitter. The security key determines the reference code used to create the reference pulse orthogonal to all four of the bits transmitted simultaneously. This implementation uses four possible reference codes that can be specified using a two-bit section of the security key. Updating only the reference code reduces the size of the transceiver while maintaining overlaps available at the output of the transmitter. In addition to the presence of the overlaps at the transmitter, changing the reference code impacts the detection codes used at the time of decoding. The fixed location of the pulse train at the start of the frame period allows the transmitter to be made of a storage location for the waveform samples along with a scalar generator. The hardware seen in Fig. 1 prior to the final multiplier serves as a generator of a scalar by which to multiply the pulse train in every frame. The waveform scalar is generated using the group of transmitted bits, the shifting codes, and the reference code. The scalar is multiplied by the

samples of the pulse train to determine the amplitude of the samples seen at the output of the transmitter. Key Rotation provides a portion of the security key that changes at every symbol boundary. Rotating which portion of the key is used provides the transmitter with a new reference code used during the transmission.

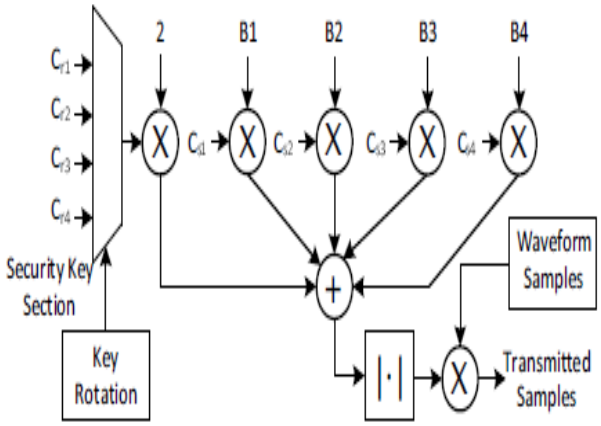

Fig. 1. Secure CSR transmitter architecture

With a fixed four bits per group, the multiplier for the reference pulse is a constant value of two. The limitation of the orthogonal codes as well as the presence of the absolute value allow for additional simplifications of the transmitter. Given that the reference code is always a one or a negative one, the contribution of the reference to the final scalar can only ever be a two or a minus two. Because the possible output can only be two values, it is simpler to represent the outputs using a single bit. The single bit of the reference code uses a one to indicate the addition of a negative two while a zero to indicate the addition of a positive two. This simplification is accounted for when the reference is passed to the addition with the data pulses. Fig. 2 shows the utilization of a combinational logic tree made of XNOR gates as well as NOR gates to replace all of the multipliers as well as the two adders required to sum the multiplication results together in the transmitter datapath. To make the transmitter more compact, the shifting and reference codes are passed in as a single bit using the zero to represent the negative one. Each of the XNOR gates along the top row takes in one element of a shifting code as well as one of the bits in the group of bits transmitted simultaneously. The possible inputs to the multipliers are either one or negative one, which limits the possible output to a one or negative one. The addition of each two of the multiplication results can result in a two, negative two, or zero. Even though the range of these results span from negative two to two, the presence of only three possible output values allows the result of the addition to be expressed using two bits.

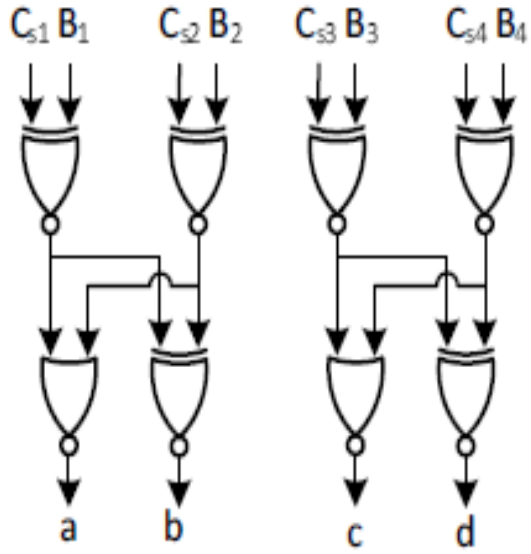

Fig. 2. Combinational logic for the reduction of the multiplier bank and first round of additions

The remainder of calculating the scalar used when generating the pulse is done by the addition of both of the two bit results from the multiplier and adder replacement a, b, c, and d, as well as the single bit e from the reference code as shown in Fig 3. The combinational logic in Fig. 3 reduces the two adders needed to combine the reference and two multiplication results, where e denotes the impact of the reference and S1 and S2 represent the final scale calculated for multiplication with the sample values. The use of the absolute value block restricting the possible scalar to zero, two, four, or six allows the final scalar to be represented using two bits.

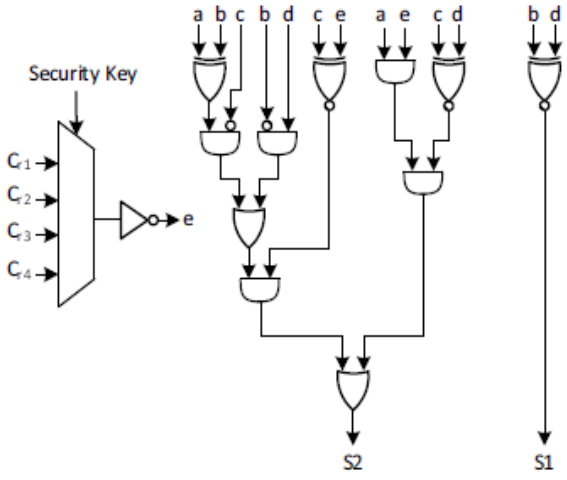

Fig. 3. Adder reduction datapath.

The implementation of the CSR-UWB transceiver is based on our basic non-coherent transceiver presented in [6]. The performance of the design is improved using cutset retiming. Cutset retiming is a transformation technique used to add pipeline registers and/or change the location of the delay elements without affecting the input/output characteristics of the design [9]. A cutset intersects a set of edges of a graph such that if these edges are removed from the graph, the graph becomes disjoint. The block diagram of our designed secure CSR receiver is shown in Fig. 9. Incoming samples are first squared in the autocorrelator to increase the separation between signal and noise values. The detector integrates the incoming data to find the preamble and the frame boundaries. The synchronizer finds the symbol boundaries that determine which frames are used to constitute one group of four bits transmitted simultaneously. The receiver requires both frame level and symbol level synchronization in order to correctly decode the received samples. Symbol level synchronization is necessary to evaluate which security key section is used, while frame level synchronization determines which element of the detection codes to use. In order to adapt to secure CSR, the security key is now an input to a code generator in the decoder. The code generator uses a two-bit section of the security key to determine the reference code for the current incoming data. The reference code is then multiplied by each of the shifting codes to make the detection codes for the decoder. The detection codes created by the code generator allow the decoder to create the bit stream of output data. The decoder includes a module to identify the reception of the Barker code, allowing the decoder to differentiate between the preamble and transmission data. The finite state machine (FSM) controls the operations of components of the receiver. To better manage power consumption, the FSM is responsible for making some components of the receiver idle while waiting for samples to become

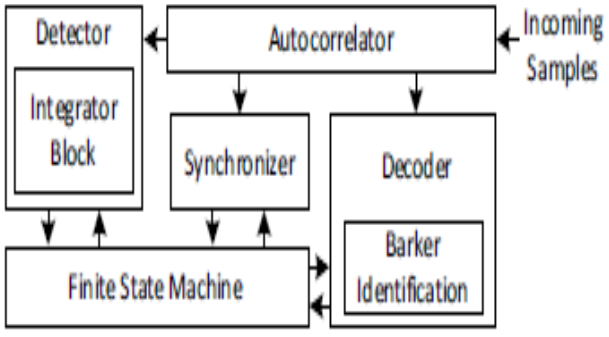

Fig. 4. Block diagram of the secure receiver.

A. Detection

The detection process establishes the presence of a transmission as well as the start of each frame within the symbol period. The architecture of the detector for the CSR transceiver is based on the detection process described in [6]. The preamble used to indicate the presence of a packet is a block of transmitted ones at the beginning of the transmission. The detection of the preamble is done using sweeping integration phases that integrate over the different sections of the frame space. Each section of the frame space is accumulated over one full symbol period. The detector is looking for the maximum integration phase over several symbol periods. The detector determines if it has found a preamble when one integration phase has the highest integration value in 6 out of 11 symbol periods. The detector resets if no phase has met this threshold after evaluating 11 symbol periods. The presence of multiple integration phases inside of a frame period gives the detector a reasonable approximation of the start of the frame period, within 22 samples. The detection process essentially synchronizes to the frame period prior to the start of the symbol synchronization stage.

The detector is made up of an integrator block, a rotating shift register, and phase comparison logic to determine if a preamble has been detected. The integrator block and rotating shift register manage the collection of overlapping phases for comparison. The architectures of the integrator block and rotating shift register are described in [6] and are updated for the bitwidths necessary for secure CSR. The datapath is adapted to use a (10,1) autocorrelator output and (15,1) rotating shift register, where (WI, WF) denotes the number of integer bits WI and the number of fractional bits WF of a signal. The detector in this implementation sweeps 9 integration phases over each frame. The integration windows are separated by a phase space of 22 samples. Fig. 10 shows the datapath of the detector after the integration block and the rotating shift register. The detector continually updates the maximum integration phase as they are presented by the integrator block. The comparator is responsible for determining the maximum integration phase and indicating the index inside of the rotating shift register. The rough synchronization to the boundary of the frame is done by evaluating which integration phase has been a maximum over a series of symbol periods and storing the

maximum index. When the preamble has been detected, the detector stores the value of the maximum phase index in a register, Waste Cycles. The detector informs the FSM that it has found the preamble only when the phase counter returns to the value of the maximum integration phase. The addition of this delay means that the starting point of the synchronizer will roughly match the frame boundary.

B. Synchronization

The main challenge of the CSR transceiver is synchronizing the transmitter and receiver so the same shifting and reference codes are used in the appropriate part of the transmission. The synchronization stage finds the symbol boundaries within the transmission data. For this implementation, the reference

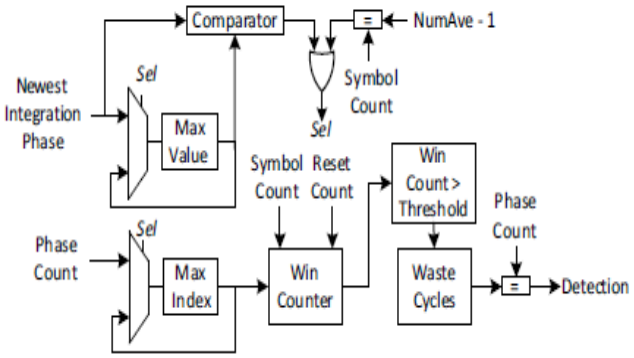

Fig. 5. Datapath of the detection evaluation and frame synchronization

C. Decoder

To interpret a symbol period of incoming samples, the receiver must first generate detection codes by multiplying the shifting codes with the reference code. Because four bits are received simultaneously, the decoder generates a detection code for each bit in the group using its shifting code. The detection codes match the length of the shifting and reference codes. The detection codes are made of eight elements that are each applied to one frame of the symbol period. As shown in Algorithm 2, the detection codes are applied to the total of one accumulated frame. These frames are accumulated to create a total for the symbol period of each bit in the group. The sign of each symbol period accumulation is used to determine the transmitted bits.

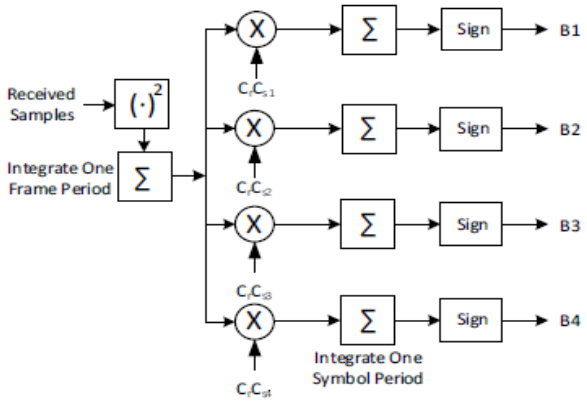

Fig. 6. Block diagram of the CSR-UWB decoder.

IV SIMULATION RESULTS AND DISCUSSION

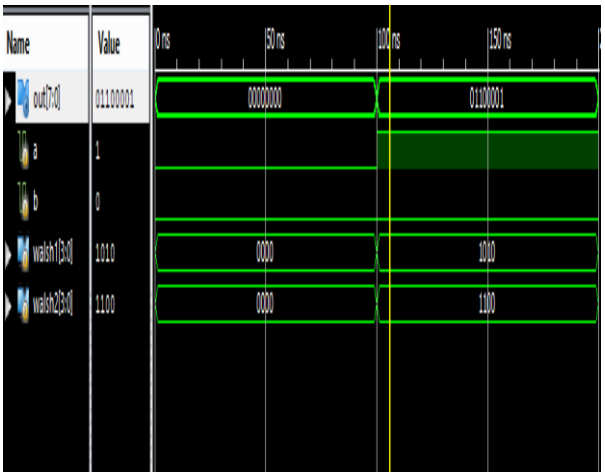

Fig.7. wb encoder

From fig.1 and fig.2The encoded data from two senders are mixed together through 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. The progression of both the encoding schemes are depicted from fig.1. and fig.2. In WB decoding scheme the chip value of walsh code, the received multi bit sums are accumulated positive part or negative part by using comparator we have to compare positive and negative parts, if positive is greater than negative then the original data is 1, otherwise the original data is 0.

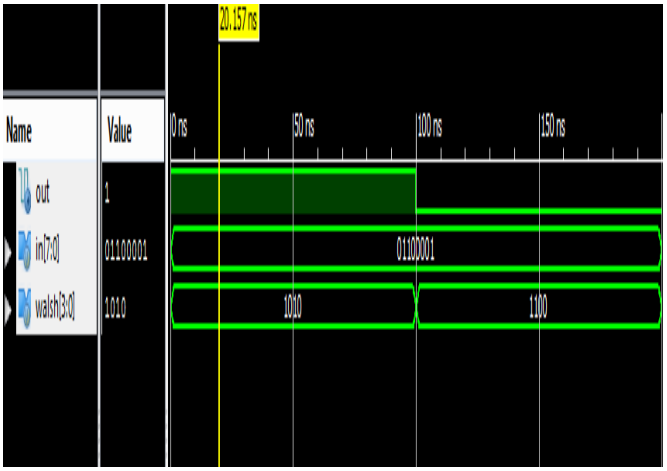

Fig.8.wb decoder

From fig.3 and fig.4 in SB encoding scheme original data bit from a sender is fed into an AND gate in chip by chip manner and encoded data from a different senders are mixed together by an xor operation and a binary sum signal is generated. In sb decoding scheam the binary sum signal arrives at recevers,an AND operation is taken between binary sum and corresponding sum then the result is send to an accumulator

the output of the accumulator will be the corresponding original data.

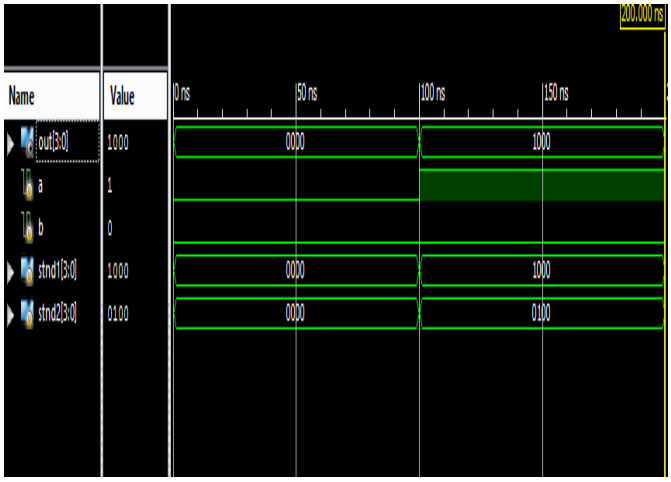

Fig.9. sb encoder

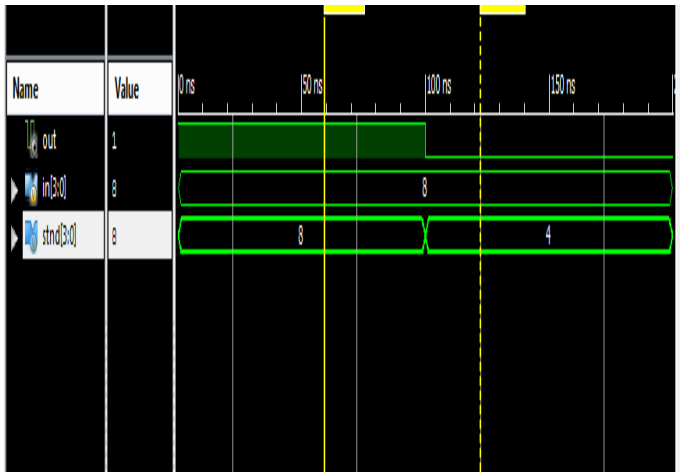

fig.10. Sbdecoder

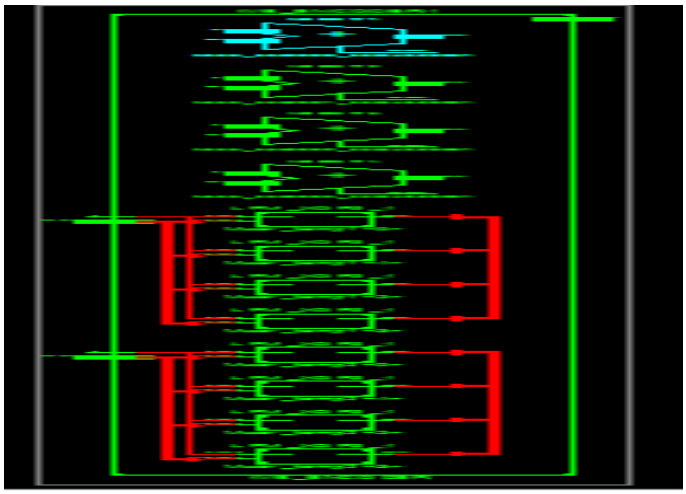

Fig.11. Rtl schrmatic

Design summary

Device Utilization Summary (estimated values)			
Logic Utilization	Used	Available	Utilization
Number of Slices	4	5888	0%
Number of 4 input LUTs	8	11776	0%
Number of bonded IOBs	18	372	4%

VI CONCLUSION

In this paper, we introduced the concept of overloaded CDMA crossbars as the physical layer enabler of NoC routers. In overloaded CDMA, the communication channel is overloaded with nonorthogonal codes to increase the chan-nel capacity. Two crossbar architectures that leverage the overloaded CDMA concept, namely, T-OCI and P-OCI, are advanced to increase the CDMA crossbar capacity by 100% and 2*N*× 100%, respectively, where *N* is the spreading code length. We exploited featured properties of the Walsh spread-ing code family employed in the classical CDMA crossbar to increase the number of router ports sharing the crossbar without altering the simple accumulator decoder architecture of the conventional CDMA crossbar. Generation procedures of nonorthogonal spreading codes are presented along with the reference and pipelined architectures for each crossbar variant. The T-/P-OCI crossbars were implemented. The performance of the OCI crossbars is compared with that of the conventional CDMA crossbar. The dynamic power is reduced by 45% for the T-OCI crossbar but increased by 133% for the P-OCI crossbar. The T-OCI crossbar utilizes 31% fewer resources, while the P-OCI crossbar uses 400% more resources compared with the conventional CDMA crossbar. The OCI crossbar suitability for NoCs has been established by analytically and experimentally evaluating a fully working OCI-based NoC. A 65-node OCI-based star NoC was realized and compared with an SDMA-based torus NoC generated by CONNECT. The evaluation results demonstrate the superiority of the OCI-based NoCs in terms of area and throughput.

REFERENCES

[1] M. Ko and D. Goeckel, “Wireless physical-layer security performance of UWB systems,” in Military Communications Conf., 2010, pp. 2143– 2148.

[2] H. Nie and Z. Chen, “Code-shifted reference transceiver for impulse radio ultra-wideband systems,” Physical Communication, vol. 2, no. 4, pp. 274–284, 2009.

[3] K. Aldubaikhy, “Differential code-shifted reference impulse-radio ultrawideband receiver: Timing recovery and

digital implementation," Master's thesis, Dalhousie University, 2012.
[4] H. Nie and Z. Chen, "Performance analysis of code-shifted reference UWB radio," in IEEE Radio and Wireless Symp., Jan 2009, pp. 396– 399.
[5] S. Vitavasiri, "A non-coherent ultra-wideband receiver: Algorithms and digital implementation," Master's thesis, Dept. Elect. Eng. Comp. Sci., Massachusetts Inst. Technol., Cambridge, 2007.
[6] A. Hennessy, "Implementation of physical layer security of an ultrawideband transceiver," Master's thesis, Dept. Elect. Eng., San Diego State Univ., San Diego, CA, 2016.
[7] A. Alimohammad, S. Fard, B. Cockburn, and C. Schlegel, "A compact and accurate Guassian variate generator," IEEE Trans. Very Large Scale Integr. (VLSI) Syst., vol. 16, no. 5, pp. 517–527, 2008.
[8] H. Nie and Z. Chen, "Performance evaluations for differential codeshifted reference ultra-wideband (UWB) radio," in IEEE Int. Conf. Ultra-Wideband, Sept. 2009, pp. 274–278.
[9] K. K. Parhi, VLSI Digital Signal Processing Systems: Design and Implementation. New York, N.Y., USA: John Wiley & Sons, 1999.
[10] P. Pace, Detecting and Classifying Low Probability of Intercept Radar, 2nd ed. Boston, Mass., USA: Artech House Books, 2008.
[11] D. Goeckel and Q. Zhang, "Slightly frequency-shifted reference ultrawideband (UWB) radio," IEEE Trans. Commun., vol. 55, no. 3, pp. 508–519, Mar. 2007.