IOSR Journal of VLSI and Signal Processing (IOSR-JVSP)
Volume 6, Issue 4, Ver. I (Jul. - Aug. 2016), PP 26-31
e-ISSN: 2319 – 4200, p-ISSN No. : 2319 – 4197
www.iosrjournals.org

FPGA Implementation of Crypto-System based Wireless communication system

Shruthi B[1], U B Mahadevaswamy[2]
[1]*(ECE Department, SJCE College/VTU, Karnataka, India)*
[2]*(Associate Professor, ECE Department, SJCE College/VTU, Karnataka, India)*

Abstract**:** *Single input and single output (SISO) is the technology in communication and is a new and emerging generation and is predicted to play a completely vital position in 4g Wi-Fi structures. The prototyping of SISO systems through the usage of Field programmable gate arrays (FPGA) or ASIC'S presents an opportunity trying out surroundings for SISO structures[2]. A crucial challenge for the SISO generation will be the design of the transmitter and receiver sections which includes complicated algorithms at each sections[4]. Encryption and Decryption is the process of cryptography technique which provides secrecy of the data over the network. To secure the data transmission Crypto system with embedded encryption algorithm is used. The system supports data security and reliability. The layout and trying out element can be simplified through designing the circuits by the use of hardware description languages (HDL) and included software environment (ISE) which gives accurate simulations of the layout. This paper presents the area optimization for SISO with noise by using the Artrix 7 FPGA, and the obtained results are compared with alimohammad and Fard [7] for area constraints.*

Keywords: *FPGA, HDL, ISE,SISO.*

I. Introduction

Single input and single output (SISO) is the technology in communication and is a new and emerging generation and is predicted to play a completely vital position in 4g Wi-Fi structures [1]. This technique also allows increasing the quantity of bits transmitted. SISO systems are also utilized in wired power line communications for 3-cord installations. Using FPGA's, evaluation of numerous common systems or circuits or frameworks can be done [3]. FPGA's incorporates enormous scope of decision making ability entryways and memory squares (ram pieces) to put into impact confused computerized calculations.

The proposed wireless communication system consists of transmitter and receiver. The transmitter section consists of Convolution encoder, puncturing, interleaver and modulator. The receiver part consists of de-modulator, deinterleaver, depuncturing and Viterbi decoder. To provide security encryption and decryption algorithm is used. The encrypted data is given as input to the encoder in the transmitter section. Our proposed design is system independent and we have designed efficient system with high security.

A SISO system is realized on a Field Programmable Gate Array. The dissertation is used in developing an efficient software simulation of transceiver system and a realistic channel called as Additive white Gaussian Noise (AWGN) channel which can mimic the real world noisy communication channel.

II. Literature survey

2.1 SISO, MIMO and FPGA

Alimohammad and Fard [7]: In this paper the improvement and testing of an FPGA primarily based bit error rate tester for virtual base band conversation structures have been developed. the bit error rate tester is advanced for both MIMO and SISO digital communication systems. The transmitter system makes use of golay coding method for channel encoding, accompanied with the aid of a pseudorandom interleaver phase and a 16-qam modulation approach. The receiver segment consists of ml detector, pseudorandom de-interleaver and decoder. The paper also discusses the issues of noisy channels and methods of data reception through noisy channels.

Numan et al. [8]: this paper gives an efficient hardware cognizance of a 2×2 MIMO machine which is designed and implemented on a xilinx virtex -four xc4vlx60 area programmable gate array (FPGA).This paper discusses the usage of Matlab and VERILOG for the improvement of the device where both mat lab and VERILOG simulations are accomplished and each are in comparison to test for the similarities. the synthesis is executed using VERILOG.

Heejung et al. [10]: This paper discusses the design of a transmission structure primarily based on twin band and SISO -OFDM schemes and media get admission to manipulate (mac) layer the usage of the improved disbursed channel get admission to (edca) including a block acknowledgement approach (ack). the complete device is synthesized in an FPG

A and tested. this paper discusses the development of a 2×2 MIMO system with Convolutional coding on the transmitter and viterbi decoding technique at the receiver.

Paulraj et al. [11]: On this paper the technique of SISO is mentioned in detail, the blessings, risks of SISO are briefed. The paper additionally demonstrates using SISO in wireless generation and suggests that excessive information switch quotes in Gb/s can be finished. The paper proves the excessive capacity of SISO system over single antenna structures through making use of the shannon's channel potential components.

Murphy et al. [12]: In this paper the layout of an SISO examined in a virtex-ii. Fast prototyping of SISO transceivers for wideband channel is mentioned. Here the circuit is designed to allow maximum flexibility for research and layout purposes. Also the implementation of two wireless structures ieee 802.11b and Alamoutti's transmit range scheme the usage of the designed FPGA primarily based SISO examined.

1.2. For encryption and WSN:

Padmini et al. [9]: This paper proposes a new embedded encryption algorithm based on Linear feedback shift register. The algorithm is composed by some basic operations such as the XOR and displacement. The architecture is synthesized and implemented on the Xilinx Spartan-3.

Chan et al. [13] proposed the Pre-distribution schemes with Random Key used for Sensor Networks. The present three new mechanisms for key establishment, Q-composite keys scheme, multipath-reinforcement scheme, this shows how to strengthen the security between any two nodes by leveraging the security of other links.

Jolly et al. [14] given the energy efficient protocol for key management of WSN. The proposed cryptographic key administration convention, which depends on the IBSK plan, however just two symmetric keys are required to be pre-sent at every sensor. The convention bolsters the ousting of the bargained hubs. Recreation demonstrates that the vitality utilization overhead presented by the key administration is astoundingly low on account of the multi-level system design in which just sensor-to-door secure sessions are permitted, and reports request of-size change in vitality sparing when contrasted with the first IBSK plan, and Kerberos-like plans.

Siddeeq et al. [15] This paper presents the design of an Adaptive Viterbi decoder that uses survivor path with parameters for wireless communication in an attempt to reduce the power & cost and increase the speed. The design was coded in VHDL and implemented on Spartan-3.

Zhao et al. [16] have given the image encryption topology based on RSA for WSN. Image Encryption is the image processing in the field of a new branch. The simulation experiments illustrate that it is workable to utilize the existing WSN to transmit the sensitive information covertly with the characteristics of lower energy costs and invisibility, and it is suitable for stream data in sensor nodes.

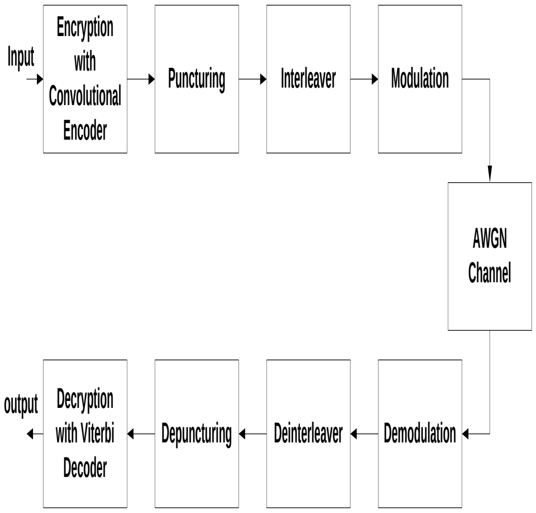
Othman et al. [17] have given the encryption algorithm to evaluate the performance of WSN. The growth in applications for resource limited WSNs, the need for reliable and efficient security mechanisms for them has increased manifold but its implementation is a non-trivial task. The cost of security, however, still mostly remains an unknown variable.

III. Proposed Method

The block diagram of proposed system is shown in Fig.1. The system consisting of transmitter (having processes encryption, puncturing, interleaver, modulation), receiver (having process like De-interleaver, de-punching and decryption) and channel (having Additive white Gaussian noise). The transmitter involves a source that produces the symbols as information and an encoder that performs encoding of the source images. The encoder is trailed by an interleaver which is utilized for blunder revision amid burst mistake situations in the channel. The interleaver is trailed by a modulator that adjusts the images and makes them reasonable for transmission through a boisterous channel. The channel is acknowledged through an Additive white Gaussian noise (AWGN) where noise is introduced by Xoring the 32 bit data with single bit error. The recipient segment comprises of a de-interleaver that performs the converse of interleaver lastly a decoder deciphers the data.

3.1 Encryption

The block diagram of Encryption algorithm is shown in Fig.2. To Encrypt, the original data is fed into algorithm as input. Key performs the parameterization of Cryptographic operation. Key length for 8-bit block size is 16-bit. The subkey is generated by splitting an 16-bit key to mask1 of 8–bit and mask2 of 8-bit. The PN sequence is generated by using Linear feedback shift register. Here two linear feedback shift registers are used since main input key is split into two equal bits then each split key's is replaced by the PN sequence generated by LFSR[1] and LFSR[2]. The output of LFSR[1] and LFSR[2] is connected to SIPO where parallel output replaces MSB and LSB of mask1 and mask2 to generate a new mask1 and mask2 so that each time different subkey is generated which is Xor'd with input to generate the encrypted data.[9]



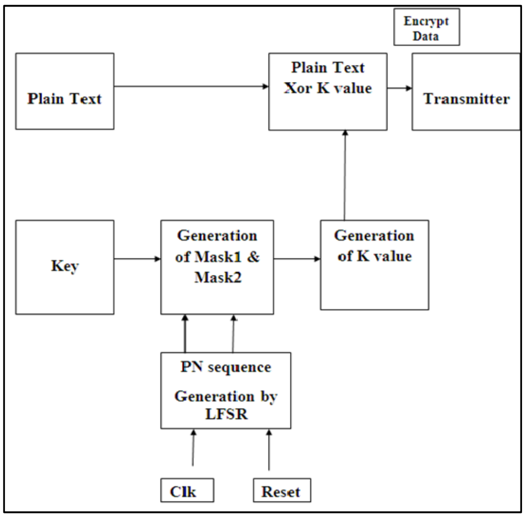


Fig.1 Block diagram of Proposed System **Fig.2** Block diagram of Encryption module[9]

3.2 Transmitter section:

The transmitter section comprises of a source an encoder that performs encoding of the source symbols. The encoder is followed by an interleaver which is used for error correction during burst error scenarios in the channel. The interleaver is followed by a modulator that modulates the symbols and makes them suitable for transmission through a noisy channel. The output bits from the transmitter are added with error bits to corrupt the signal which normally happens in a noisy channel. Now let us consider the individual blocks in detail.

3.2.1 Convolutional Encoder

An encoder in a communication system will generally take the message bits as the inputs and change the input bits by adding more redundant bits so that error correction and error detection can be done. Convolutional encoder is a forward error correction encoder, where the encoded output bits will not only depend on the current input bits but also on the preceding message bits. Convolutional encoders are best known for its error correcting properties. Encoding of Convolutional codes can be accomplished using simple shift registers.
In general a Convolutional encoder is represented using three digits (n,k,m) where
n = the number of outputs or number of code words generated.
K= is the number of input bits entering at any time.
m= is the total number of shift registers or number of flip-flops required to realize the encoder.
Here we are using 1/3 code rate for the design.

3.2.2 Puncturing

Puncturing is the process of increasing the rate and reducing the redundancy of the coded bits, this is done by removing some of the parity bits after encoding with the Convolutional encoder. Puncturing reduces the complexity of the encoder and increases the flexibility of the system. Generally predefined codes are used for puncturing at the encoder and de-puncturing is done at the decoder.

3.2.3 Interleaver

Interleaving is a technique for making the encoding schemes more robust to counter the burst errors. Interleaving will perform the reordering of data in such a way that consecutive bytes of data are distributed over a larger sequence of data to reduce the effect of burst errors.This method thus equips the transmitter to correct errors which can appear in groups, which is generally not correctable by the encoders. Interleaver will spread the transmitted data over time resulting in significant improvements in finding and correcting errors at the error correction decoders. Interleaver can be implemented in the form of matrix interleaver.

3.2.4 QAM Modulation

Quadrature amplitude modulation (QAM) is a modulation technique which can be used for both analog signal and digital bit streams. In this modulation technique the two carrier waves used are out of phase by 90 degrees and thus the name quadrature. It performs Amplitude Shift Keying(ASK) for both the carrier waves and sum these waves thus the final waveform is a combination of phase shift keying(PSK) and Amplitude Shift Keying(ASK).QAM is used as the modulation technique for most of the telecommunication systems.

This dissertation work aims in developing a 16-QAM for both the transmitters. The 16 QAM consists of a square lattice of message points where there are four message sequences at four quadrants of the square lattice. In general a 16 QAM will transmit 16 independent signals over the same channel bandwidth. Generally the output of the 16QAM will be 16 real bits and 16 imaginary bits.

3.3 Receiver section:

3.3.1 De-Modulator

The demodulator will perform the inverse operation of the modulator by removing the carrier bits which were modulated by the data bits and will give an output consisting of only the spatially spread data bits which are to be de interleaved.

3.3.2 De-interleaver

The de-interleaver will perform the reverse operation of the interleaver .The de-interleaver has been realized by using matrix de-interleaving.

3.3.3 De-puncturing

The de-puncturing unit will perform the reverse operation of the puncturing and it is generally used with the Viterbi decoder.

3.3.4 Viterbi Decoder

The Viterbi decoder module implemented in the dissertation work is shown in the fig.3. The decoder receives 3-bit data input which is convolutional encoded along with control inputs like clk, reset and enable. After performing viterbi algorithm on code words, the decoder gives a single bit output. In this dissertation work the viterbi decoder consists of five modules such as a serial to parallel duplicator, that duplicates the same code word thrice followed by a clock pulses, followed by a Branch metric unit(BMU) that calculates the branch metric between any two paths. The next module is an Add Compare and select unit followed by a survivor memory management unit that gives the final decoded output.[15]

3.4 Decryption

Decryption is the reverse, moving from unintelligible cipher text to the plain text. This is the reverse operation of encryption algorithm. The Fig.4 shows the decryption block diagram. The receiver receives the encrypted data where this data is cipher text which is Xor'd with subkey (k) where subkey generation is done using PN sequence generated by LFSR and the original data is retained which is of 8-bit.

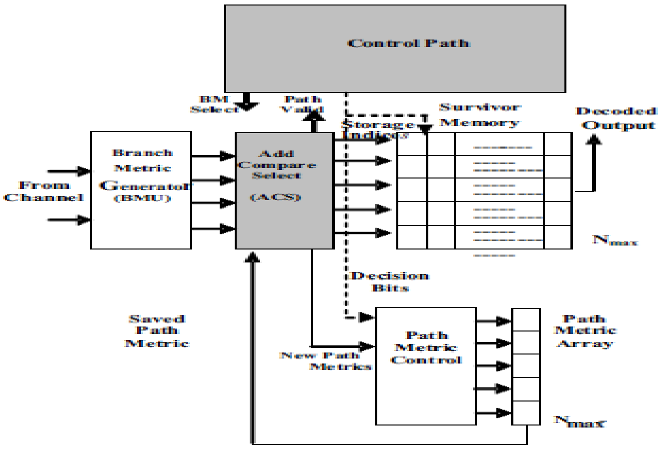


Fig.3 Adaptive Viterbi Decoder architecture.[15]

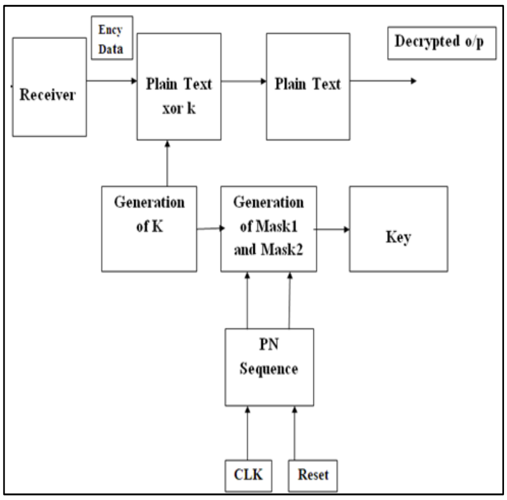


Fig.4. Block diagram of Decryption module

IV. Results

Once the system is designed it has to be verified using appropriate tools which supports for the design. Here as we are executing in Xilinx 14.7 and simulated using modelsim 6.3f and Implemented on Artix-7 XC7A100T-3CSG324. The executed system provides detailed description of result with their input and outputs. The design has been done using Verilog code, which stands as one of high descriptive language in VLSI.

The Simulation of SISO Encryption-Decryption module is as shown in the figure 5. Initially rst=1, then rst=0, valid=1, ShiftEn=0, Fillsel=0, DataIn_m1=0, DataIn_m2=0, data_in=11111110 and key_in=1111111011111110.Then the output will generated after 32 clock cycles in decryption. The same value data_out=1111110 will be generated.

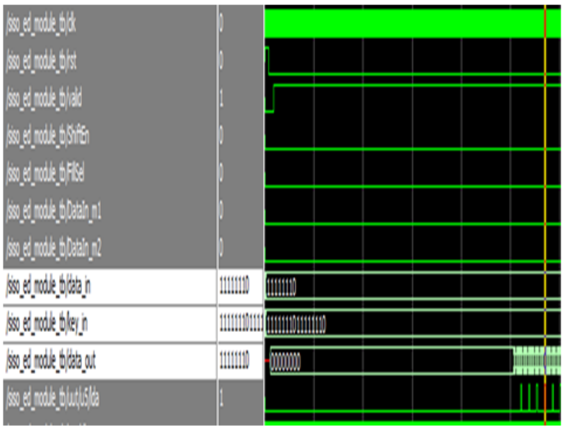

/siso_ed_module_tb/clk 0
/siso_ed_module_tb/rst 0
/siso_ed_module_tb/valid 1
/siso_ed_module_tb/ShiftEn 0
/siso_ed_module_tb/FillSel 0
/siso_ed_module_tb/DataIn_m1 0
/siso_ed_module_tb/DataIn_m2 0
/siso_ed_module_tb/data_in 1111110 1111110
/siso_ed_module_tb/key_in 11111101111 111111011111110
/siso_ed_module_tb/data_out 1111110 00000000
/siso_ed_module_tb/uut/u5/lda 1

Fig 5: Simulation of SISO Encryption-Decryption Top Module

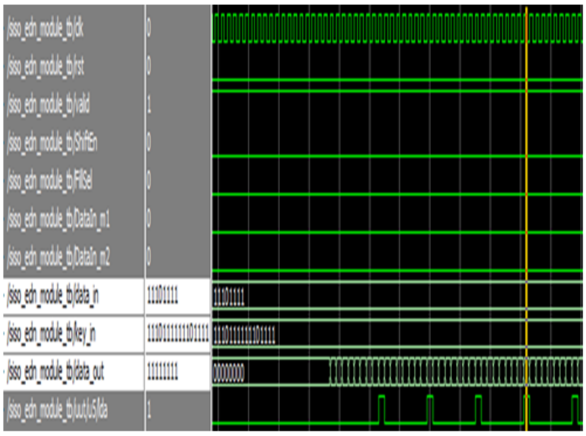

/siso_edn_module_tb/clk 0
/siso_edn_module_tb/rst 0
/siso_edn_module_tb/valid 1
/siso_edn_module_tb/ShiftEn 0
/siso_edn_module_tb/FillSel 0
/siso_edn_module_tb/DataIn_m1 0
/siso_edn_module_tb/DataIn_m2 0
/siso_edn_module_tb/data_in 11101111 11101111
/siso_edn_module_tb/key_in 1110111111101111 1110111111101111
/siso_edn_module_tb/data_out 11111111 00000000
/siso_edn_module_tb/uut/u5/lda 1

Fig.6: Simulation of SISO Encryption-Decryption Top Module with Noise

The Simulation of SISO Encryption-Decryption module with noise is as shown in the Fig 6. The initially rst=1, then rst=0, valid=1, ShiftEn=0, Fillsel=0, DataIn_m1=0, DataIn_m2=0, data_in=11101111 and key_in=1110111111101111.Then the output will generated after 32 clock cycles in decryption. The data_out=11111111 will be generated.

Fig.7 shows the RTL Schematic of SISO Encryption-Decryption Top module. For comparison purpose we have chosen 2x2 MIMO systems with respect to Alimohammad and Fard [7]. They have Chosen vertex E and we have chosen Virtex-4 for comparison purpose.There is an improvement in encoder, interleaver and deinterleaver modules with respect to maximum frequency and the less slice consumption in encoder and overall MIMO system. This proves that area is improved w.r.t to [7].

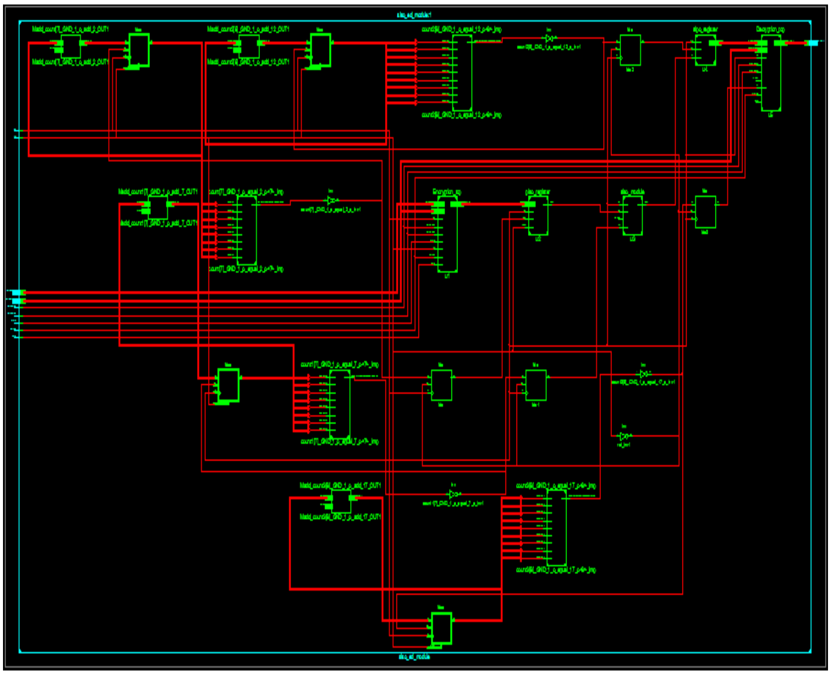


Fig.7. RTL View of SISO Encryption-Decryption Top Module

V. Conclusion

The obtained results are compared with the Alimohammad and Fard [7] for area constraints and is been concluded that we achieved optimized area than [7]. The designed system is implemented in high end applications, which demands high security.

References

[1] Figueiras, João, and Simone Frattasi. Mobile positioning and tracking: from *conventional to cooperative techniques*. John Wiley & Sons, 2011.

[2] Turner, Richard H., and Roger F. Woods. Highly efficient, limited range multipliers for LUT-based FPGA architectures. *Very Large Scale Integration (VLSI) Systems, IEEE Transactions* on 12.10 (2004): 1113-1118.

[3] Leroux, Camille, et al. "Towards Gb/s turbo decoding of product code onto an FPGA device. Circuits and Systems, 2007. ISCAS 2007. *IEEE International Symposium* on. IEEE, 2007.

[4] Bölcskei, Helmut. "MIMO-OFDM wireless systems: basics, perspectives, and challenges. Wireless Communications, IEEE 13.4 (2006): 31-37.

[5] Vejdaniamiri, Mehdi. Signal Processing Techniques for Power Efficiency and Signal Quality Enhancement of SISO and MIMO Radio Systems. Diss. University of Calgary, 2014.

[6] King, R. E., and P. N. Paraskevopoulos. "Parametric identification of discrete-time SISO systems." International Journal of Control 30.6 (1979): 1023-1029.

[7] Alimohammad, Amirhossein, and Saeed Fouladi Fard. FPGA-based bit error rate performance measurement of wireless systems. Very Large Scale Integration (VLSI) Systems, IEEE Transactions on 22.7 (2014): 1583-1592.

[8] Numan, M.W, Islam, M.T., Misran.N., An efficient FPGA-based hardware implementation of SISO wireless systems. *Communication Systems Networks and Digital Signal Processing conference* , ISBN: 978-1-4244-8858-2, pages: 152-156 Conference date:21-23 July 2010.

[9] Padmini.K, Leelavathi.G " Design and Implementation of Efficient Embedded Cryptography algorithm using FPGA" in International Journal of Advanced Computer technology, volume 2 Number 4, ISSN:2319 – 7900.

[10] Yu Heejung, Kyon Ghee song, KwhanghuynRyn Design and FPGA implementation of SISO -OFDM based WLAN system,*Vehicular technology conference VTC-2006 spring* IEEE 63, volume 3, pages 1333-1338, publication year: 2006.

[11] Paulraj.A.J, Gore.D.A, Nabar.R.U, Bolcskei.H, An overview of SISO communications-a key to gigabit wireless, *Proceedings of the IEEE, ISSN:0018-9219,* volume:92, pages: 198-218,publication:08 November 2004.

[12] Murphy.P, Lou.F, Sabharwal.A, Frantz.J.P , An FPGA based rapid prototyping platform for SISO system, *Signal Systems and Computer Conference 2004*, Record of the 37 Asilomar conference , volume 1, pages:900-904, publication: 2003.

[13] Chan H,Perrig A, Song D.Rnadom key predistribution schemes for sensor networks, *In:Proe.of IEEE 2003Symposium on Research in Security and Privacy*. Berkeley,CA:IEEE Computer Society, 2003, PP.197-213.

[14] Jolly G.A Low-energy key management protocols for wireless sensor networks, *ISCC, Eighth IEEE Symposiumon Computers and Communications, 2003*.

[15] Siddeeq Y.Ameen, Mohammed H.Al-Jammas & Ahmed S.Aleneezi FPGA Implementation of modified Architecture for Adaptive Viterbi Decoder. 978-1-4577-0069-9/11/$26.00© 2011 IEEE.

[16] W. Fumy and P. Landrock, Principles of key management,*IEEE Journal of Selected Areas in Communications*, vol. 11,pp. 785-793, June 1993.

[17] L. Eschenauer and V. D. Gligor, A Key Management Scheme for Distributed Sensor Networks, in 9th ACM Conference on Computer and Communications Security— CCS 2002, November 2002.