Global Journals LaTeX JournalKaleidoscope™

Artificial Intelligence formulated this projection for compatibility purposes from the original article published at Global Journals. However, this technology is currently in beta. *Therefore, kindly ignore odd layouts, missed formulae, text, tables, or figures.*

Design and Implementation of Data Scrambler & Descrambler System using VHDL

Naina Randive[1]

[1] Sant Gadge Baba Amaravati University

Received: 10 December 2014 Accepted: 5 January 2015 Published: 15 January 2015

Abstract

Multimedia data security is very important for multimedia commerce on the internet and real time data multicast. An striking solution for encrypting data with adequate message security at low cost is the use of Scrambler/Descrambler. Scramblers are necessary components of physical layer system standards besides interleaved coding and modulation. Scramblers are well used in modern VLSI design especially those are used in data communication system either to secure data or re-code periodic sequence of binary bits stream. However, it is necessary to have a descrambler block on the receiving side while using scrambling data in the transmitting end to have the actual input sequence on the receiving end. Scrambling and De-scrambling is an algorithm that converts an input string into a seemingly random string of the same length to avoid simultaneous bits in the long format of data. Scramblers have accomplish of uses in today's data communication protocols. On the other hand, those methods that are theoretical proposed are not feasible in the modern digital design due to many reasons such as slower data rate, increasing information, circuit hazards, uncountable hold-up etc. Therefore it is requisite for the modern digital design to have modified architecture to meet the required goal. We will recommend here modified scrambler design which is perfectly suitable for any industrial design.

Index terms— scrambler, descrambler, VHDL, and FPGA.

Abstract-Multimedia data security is very important for multimedia commerce on the internet and real time data multicast. An striking solution for encrypting data with adequate message security at low cost is the use of Scrambler/Descrambler. Scramblers are necessary components of physical layer system standards besides interleaved coding and modulation. Scramblers are well used in modern VLSI design especially those are used in data communication system either to secure data or re-code periodic sequence of binary bits stream. However, it is necessary to have a descrambler block on the receiving side while using scrambling data in the transmitting end to have the actual input sequence on the receiving end. Scrambling and De-scrambling is an algorithm that converts an input string into a seemingly random string of the same length to avoid simultaneous bits in the long format of data. Scramblers have accomplish of uses in today's data communication protocols. On the other hand, those methods that are theoretical proposed are not feasible in the modern digital design due to many reasons such as slower data rate, increasing information, circuit hazards, uncountable hold-up etc. Therefore it is requisite for the modern digital design to have modified architecture to meet the required goal. We will recommend here modified scrambler design which is perfectly suitable for any industrial design.

Keywords: scrambler, descrambler, VHDL, and FPGA.

1 I. INTRODUCTION

n telecommunications, a scrambler is a device that transposes or inverts signals or otherwise encodes a message at the transmitter to make the message unintelligible at a receiver not equipped with an appropriately set descrambling device. while encryption usually refers to operations carried out in the digital domain, scrambling typically refers to operations carried out in the analog domain. Scrambling is consummate by the addition of components to the original signal or the changing of some important component of the original signal in order to make extraction of the original signal complex .To improve the degree of data security in a conventional Scrambler the number of stages of the shift register needs to be enhanced. This conversely increases error propagation. A uncomplicated method for ensuring security is to encrypt the data. The pseudonoise (PN) key generation is of paramount importance Author ? ?: Dept. of Electronics and Telecommunications Dept. of Electronics and Telecommunications P.R. Pote (Patil) college of Engineering and, Management, Amravati, India. e-mails: naina0689@gmail.com, gauri.borkhade@gmail.com for any secure communication system. PN sequences base on Linear Feedback Shift Registers (LFSR) and non linear combination based implementations are simplest to give moderate level of security. Chaos base encryption techniques have proved fruitful, but complexity of such systems is important. The complex system generated is used to scramble incoming plain text. At the receiving end, the same code be generated and successfully used to decrypt the transmitted data. The ease of the circuit along with the complexity of the generated codes makes the circuit striking for secure message communication applications.

2 II. PROPOSED WORK

The entire operation is proposed using Modelsim and Xilinx blocks goes through three phases. Descrambler is performed in order XOR the 8bit crypt word (D0-D7) character with the 8-bit output of the LFSR. An output of the LFSR is XOR with crypto word of the data to be processed. The LFSR and data register are then consecutively advanced and the output processing is repeated for D1 through D7.

3 c) Overview of Scrambler and Descrambler

In the transmitter, a pseudorandom cipher sequence is added (modulo 2) to the data (or control) sequence to produce a scrambled data (or control) sequence.

In the receiver, the same pseudorandom cipher sequence is subtracted (modulo 2) from the scrambled data (or control) sequence to recover the transmitted data (or control) sequence, as illustrated in figure. A new modified scheme for complex PN-code based data scrambler and descrambler has been presented. A scrambler & descrambler accepts information in intelligible form and through intellectual transformation assure data quality with fastest rate without any error or dropping occurrence. We used our proposed and modified design in our present universal serial bus architecture. Moreover, this current design is very efficient, more securable, high speed, low power and lower area used & it has lots of scope to improved.

4 V. ACKNOWLEDGMENT

I have taken efforts in this project. Though it would not have been possible without the kind support and help of many individuals and organizations. I would like to make bigger my sincere thanks to all of them. I am highly indebted to Prof .G. P. Borkhade for their guidance and constant supervision as well as for providing necessary information regarding the project & also for their support in completing the project.

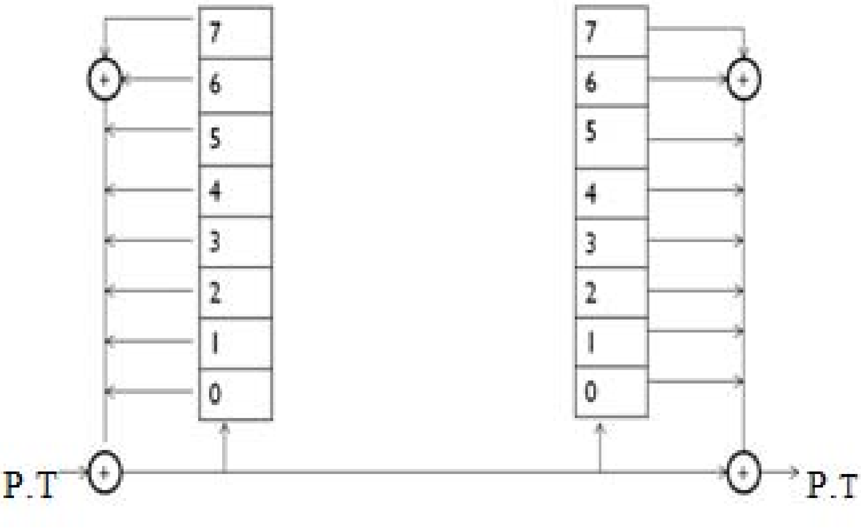
I would like to convey my pleasure towards my guide & member of Electronics and Telecommunication Engineering for their kind co-operation and encouragement which help me in completion of this project.

I would like to express my special gratitude and thanks to institute persons for giving me such attention and time. My thanks and appreciations also go to my colleague in developing the project and people who have willingly helped me out with their abilities. [1] [2]

[1] © 2015 Global Journals Inc. (US)

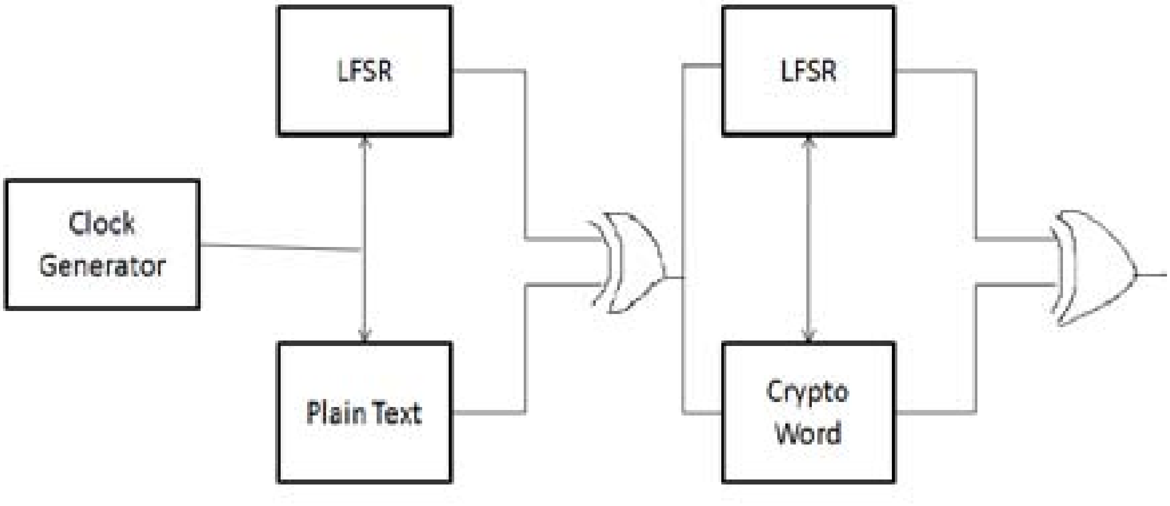
[2] © 2015 Global Journals Inc. (US) 1

Figure 1:



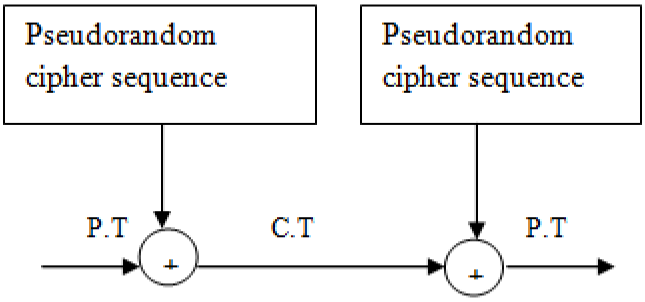
1

Figure 2: 1 .



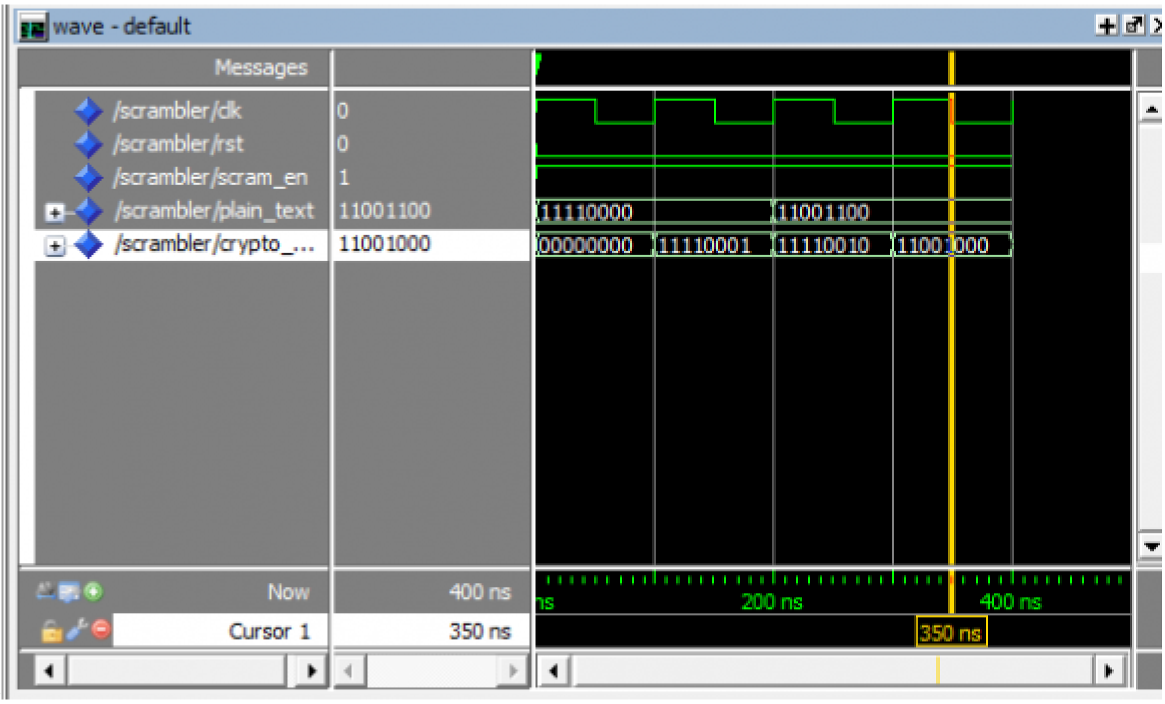
12

Figure 3: Figure 1 :Figure 2 :



34

Figure 4: Figure 3 :Figure 4 :



```
/scrambler/clk          0
/scrambler/rst          0
/scrambler/scram_en     1
/scrambler/plain_text   11001100    11110000                    11001100
/scrambler/crypto_...   11001000    00000000  11110001  11110010  11001000

Now                     400 ns      ns        200 ns              400 ns
Cursor 1                350 ns                               350 ns
```

5

Figure 5: Figure 5 :

6178

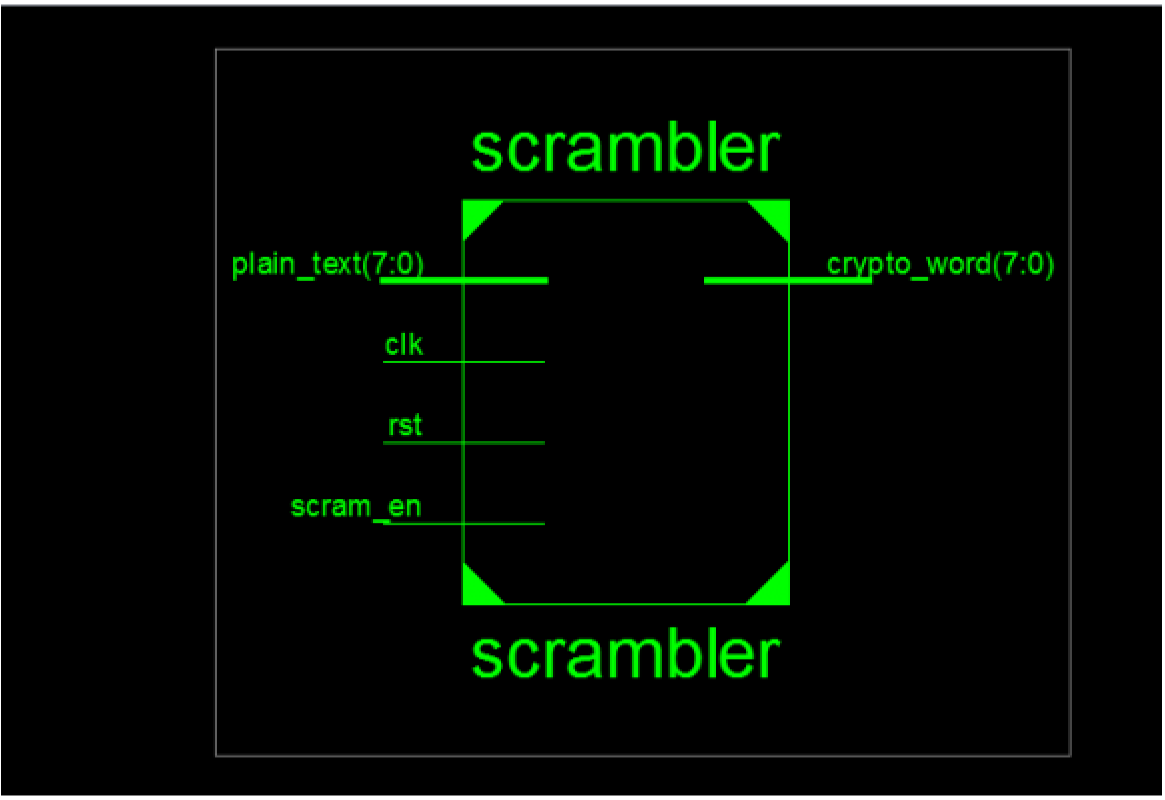


Figure 6: Figure 6 : 1 34Figure 7 :Figure 8 :

9

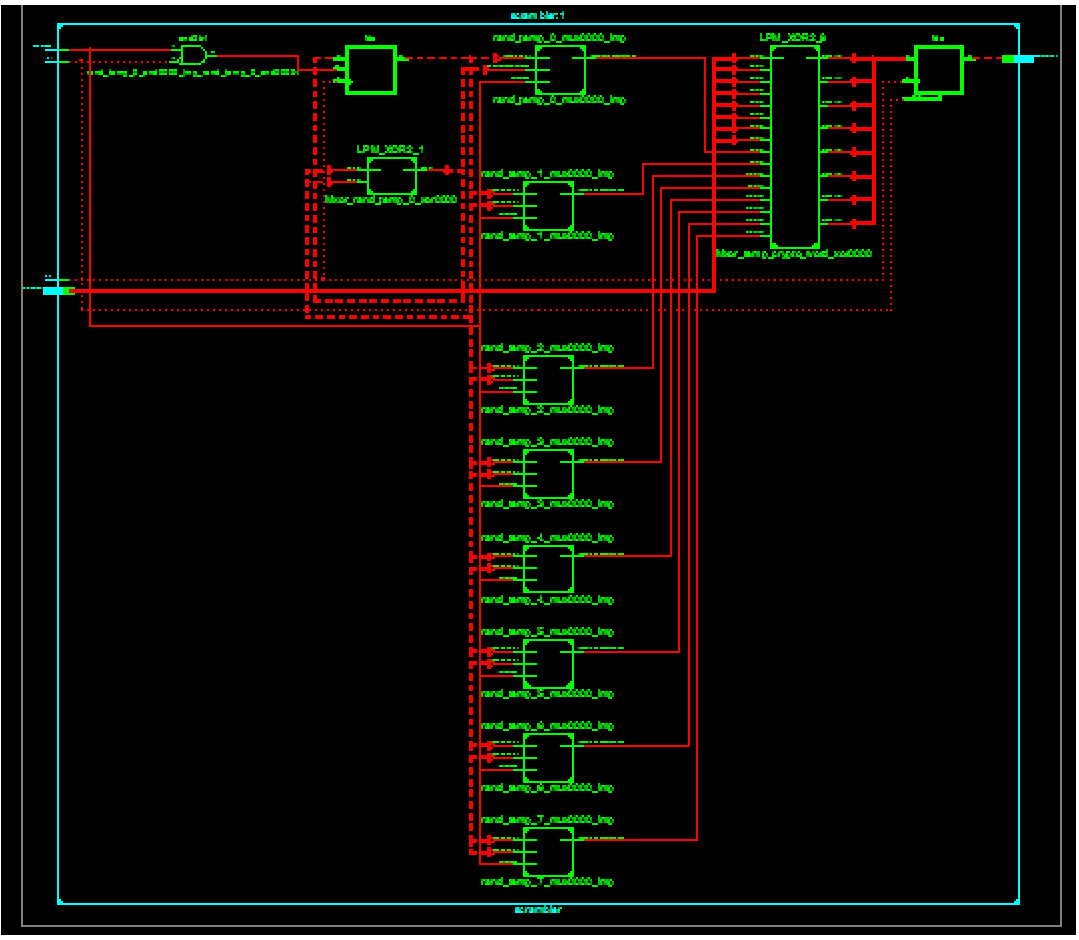
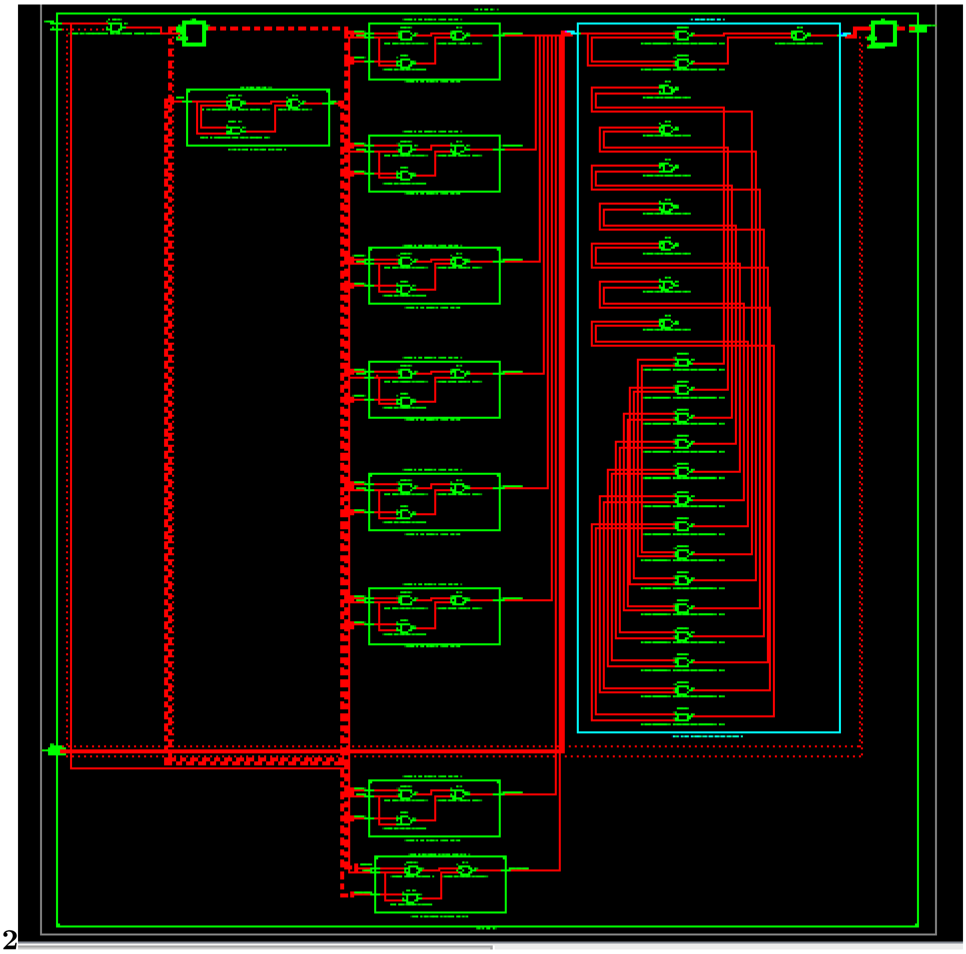


Figure 7: Figure 9 :



1012

Figure 8: Figure 10 :Figure 12 :

14151617

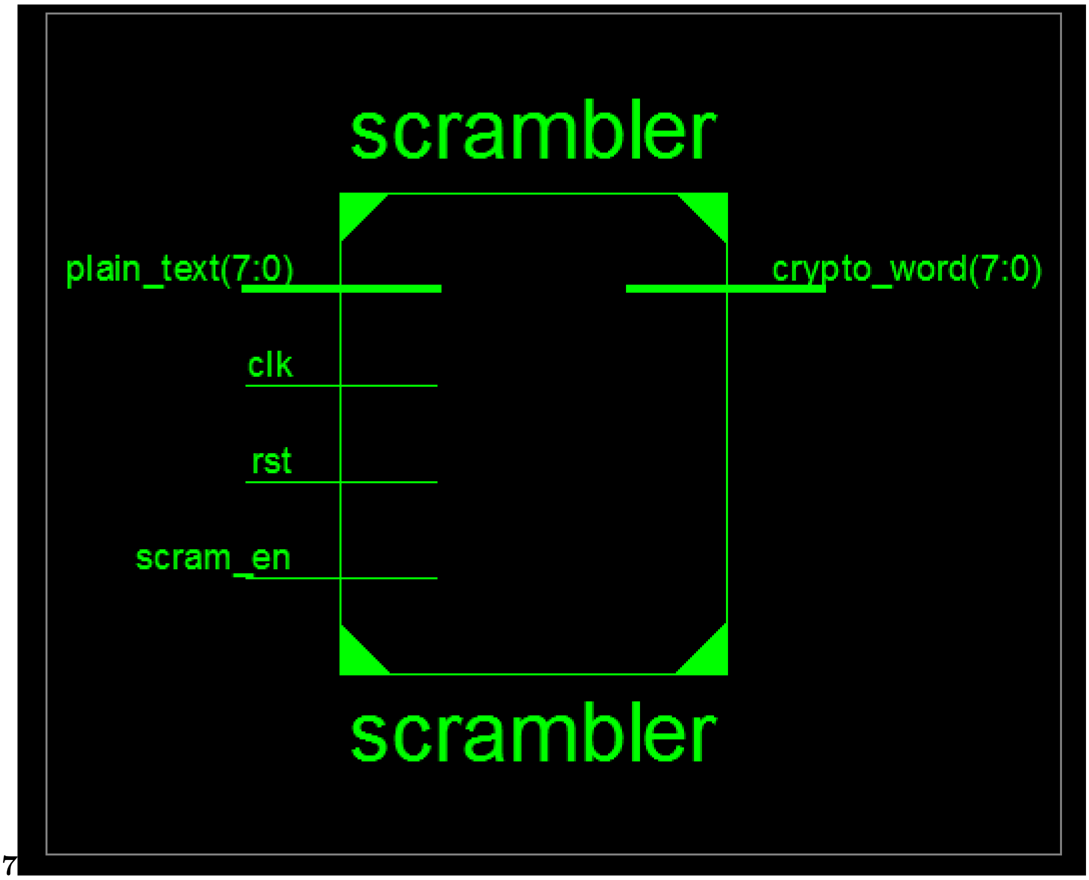
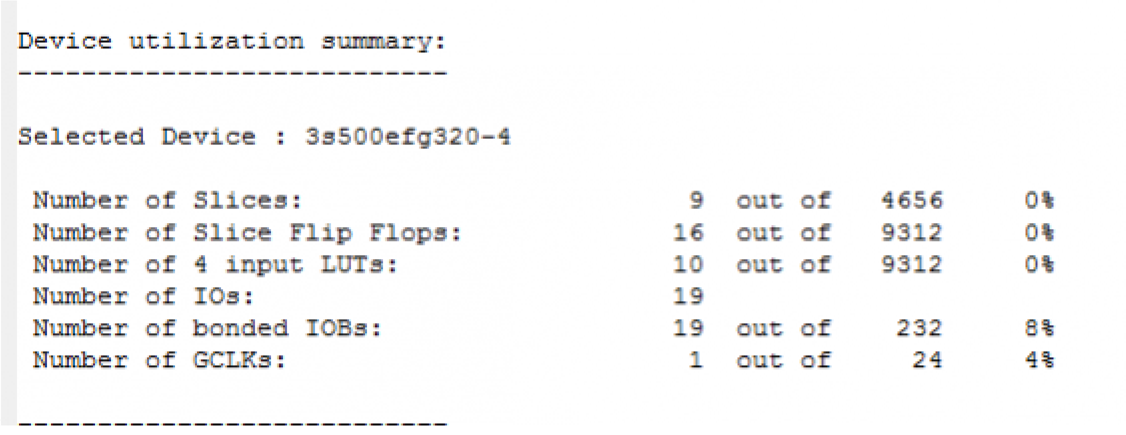


Figure 9: Figure 14 :Figure 15 :Figure 16 :Figure 17 :

18



```
Device utilization summary:
---------------------------

Selected Device : 3s500efg320-4

 Number of Slices:                        9  out of   4656     0%
 Number of Slice Flip Flops:             16  out of   9312     0%
 Number of 4 input LUTs:                 10  out of   9312     0%
 Number of IOs:                          19
 Number of bonded IOBs:                  19  out of    232     8%
 Number of GCLKs:                         1  out of     24     4%

---------------------------
```

Figure 10: Figure 18 :

191

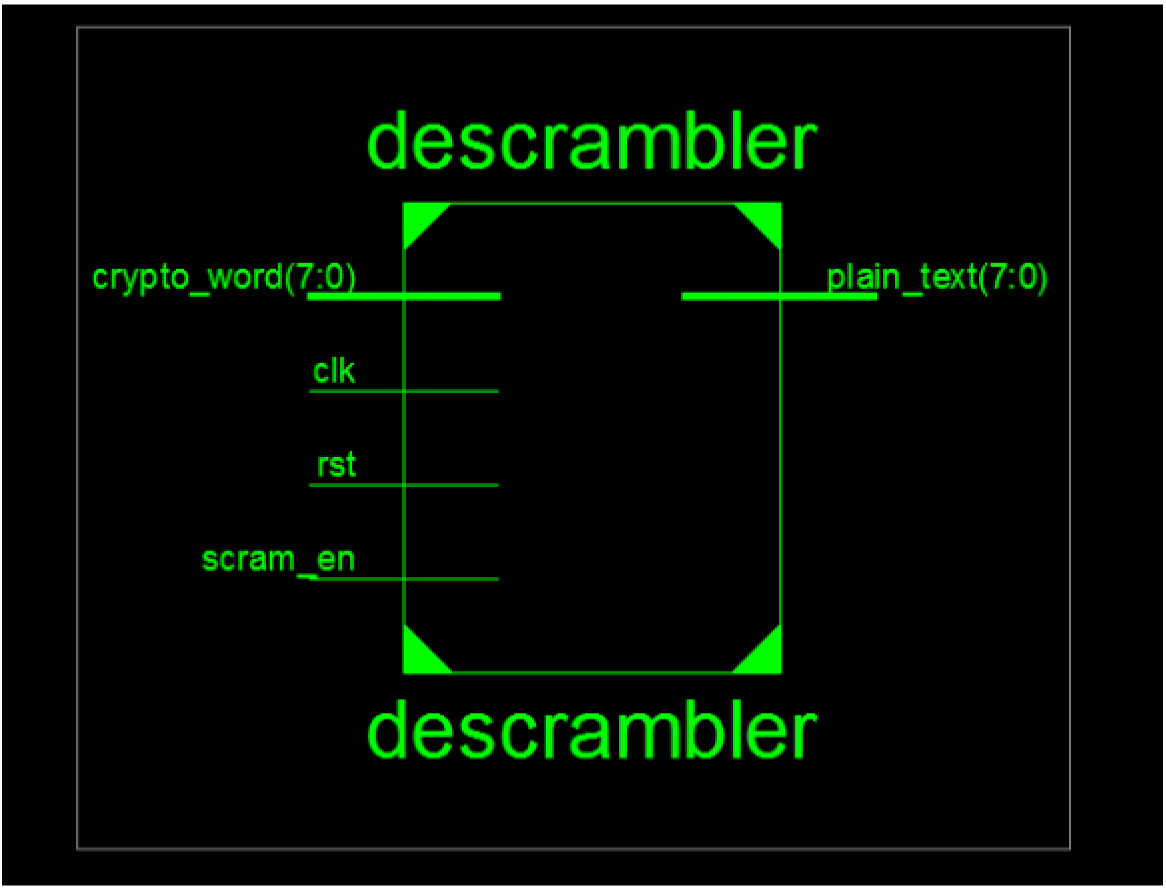
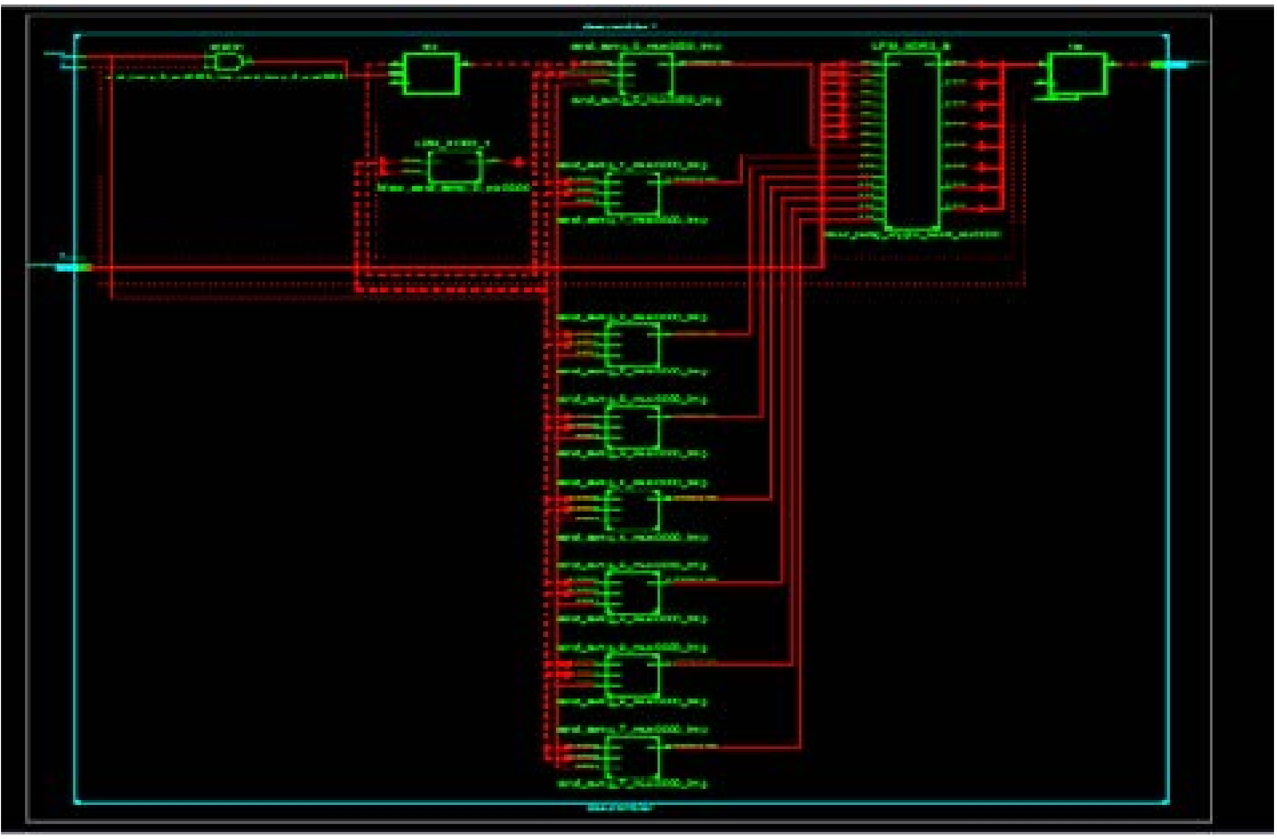


Figure 11: Figure 19 : 1 36



23

Figure 12: Figure 23 :

[Liu et al. (2013)] *A Study of Reconstruction of Linear Scrambler using Dual Words of Channel Encoder*, Xiao-Bei Liu , Soo Ngee Koh , Chee-Cheon Chui , Xin-Wen Wu . March 2013.

[Davinder Pal and Sharma ()] *Data scrambler of ultrawide band communication system*, Davinder Pal , Sharma . 2013.

[Kumar and Kumar (2014)] *Design and implementation of Logical Scrambler Architecture for OTN Protocol*, Hethan Kumar , Praveen Kumar , Y G , Dr . April 2014. 3.

[Sharma and Singh ()] 'DSP based implementation of scrambler for 56Kbps modem'. D P Sharma , J Singh . *Signal Processing -An International Journal* 2010. 4 p. .

[Indurtial Modified Digital scrambler and descrambler system Rajib Imranand Monirul Islam ()] 'Indurtial Modified Digital scrambler and descrambler system'. *Rajib Imranand Monirul Islam* 2013.

[Sharma and Singh ()] *Simulation and spectral analysis of the scrambler for 56Kbps modem. The Journal of Signal Processing Systems*, D P Sharma , J Singh . 2012. 67 p. .

[Bhat et al. ()] *VHDL modeling and simulation of data scrambler and descrambler for secure data communication*, G M Bhat , M Mustafa , Shabir Ahmad , Javaid Ahmad . 2009.