ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 12, December 2014

A review on implementation of data scrambler & descrambler system using VHDL

Naina K.Randive[1], Professor G. P. Borkhade[2]

Department of Electronics and Telecommunication Engineering,

P. R. Pote (Patil) College of Engineering and Management, Amravati, India [1,2]

Abstract: Multimedia data security is very important for multimedia commerce on the internet and real time data multicast. An attractive solution for encrypting data with adequate message security at low cost is the use of Scrambler/Descrambler. Scramblers are essential components of physical layer system standards besides interleaved coding and modulation. Scramblers are successfully 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/ De-scrambling are 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 many uses in today's data communication protocols. However, those methods that are theoretical proposed are not feasible in the modern digital design due to many reasons such as slower data rate, dropping information, circuit hazards, uncountable delays etc. Therefore it is required for the modern digital design to have modified architecture to meet the required goal. We will propose here modified scrambler design which is perfectly suitable for any industrial design. Besides, we showed simulation result, detailed analysis and usage in digital design.

Keywords: Scrambler, Descrambler, VHDL, and FPGA.

I. INTRODUCTION

In 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. Whereas encryption usually refers to operations carried out in the digital domain, scrambling usually refers to operations carried out in the analog domain. Scrambling is accomplished 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 difficult.

To enhance the degree of data security in a conventional Scrambler the number of stages of the shift register needs to be increased. This, however, increases error propagation. A simple method for ensuring security is to encrypt the data. The pseudo-noise (PN) key generation is of paramount importance for any secure communication system. PN sequences based on Linear Feedback Shift Registers (LFSR) and non linear combination based implementations are simplest to give moderate level of security. Chaos based encryption techniques have proved fruitful, but complexity of such systems is high. The complex code generated is used to scramble incoming plain text. At the receiving end, the same code is generated and successfully used to decrypt the transmitted data.

The simplicity of the circuit along with the complexity of the generated codes makes the circuit attractive for secure message communication applications.

II. LITERATURE REVIEW

[1] Rajib Imran and Monirul Islam Embedded[1] In this paper consist of Scrambling/ De-scrambling are 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. The scrambling function can be implemented with one or many Linear Feedback Shift Registers (LFSRs). A linear feedback shift register (LFSR) is a delay line which feeds back a logical combination of its stages to the input. On the Transmit side, scrambling is applied to characters prior to the encoding. On the Receive side, de-scrambling is applied to characters after decoding. A scrambler accepts information in intelligible form and through intellectual transformation assure data quality with fastest rate without any error or dropping occurrence.

[2] Xiao-Bei Liu, Soo Ngee Koh, Chee-Cheon Chui, and Xin-Wen Wu [2]. This paper consist of the reconstruction of the feedback polynomial as well as the initial state of a linear feedback shift register (LFSR) in a synchronous scrambler placed after a channel encoder is studied. The study is first based on the assumption that the channel is noiseless and then extended to the noisy channel condition. The dual words, which are orthogonal to the codewords generated by the channel encoder, are used in the reconstruction algorithm. The number of bits required by the new algorithm is compared with another recently proposed.

[3] G.M. Bhat, M. Mustafa, Shabir Ahmad and Javaid Ahmad [3]. This paper is about VHDL modelling and simulation of a typical data scrambler and descrambler for

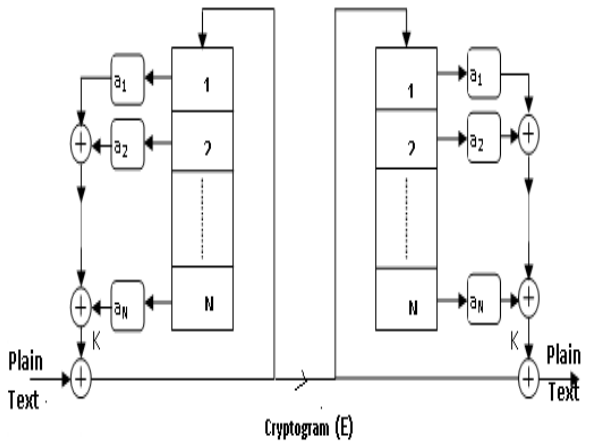
ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 12, December 2014

secure data communication has been presented. The encoder and decoder has been implemented using VHDL approach which allows the reconfigurability of the proposed system such that the key can be changed as per the security requirements. The power consumption and space requirement is very less compared to conventional discrete I.C. design which is pre-requisite for any system designer.

III. PROPOSED WORK

Fig. 1. Conventional data scrambler/ de-scrambler



An encrypting data with adequate message security at low cost is the use of Scrambler/ Descrambler. In a conventional scrambler the encrypted data is used for generation of key as shown in Fig 1. To improve the degree of data security in a conventional Scrambler the number of stages of the shift register needs to be increased. This, however increases error propagation.
In the customized scrambler reported in the literature with the Modified logic for Pseudo random key generation, selection of the outputs of the shift register for the key generation is controlled by means of a pseudo random sequence generator. In this case, an increase in the number of stages of the PN sequence generator results into a significant increase in message security. Though an increase in hardware is necessary for enhancing the security level of a scrambler using conventional integrated circuit implementation. The proposed scheme implements the scrambler and descrambler using Hardware Description Language (VHDL).An important lead of VHDL implementation is that there is perfect synchronization between transmitter and receiver.

ACKNOWLEDGMENT

I have taken efforts in this project. However, it would not have been possible without the kind support and help of many individuals and organizations. I would like to extend 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 express my gratitude 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.

REFERENCES

[1] Rajib Imran and Monirul Islam Embedded, FPGA based, VLSI and ASIC Designs, June 2013,e-ISSN: 2321-6980 "Industrial Modified Digital scrambler & Descrambler system".
[2] Xiao-Bei Liu, Soo Ngee Koh, Chee-Cheon Chui, and Xin-Wen Wu, "A Study of Reconstruction of Linear Scrambler using Dual Words of Channel Encoder" IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 8, NO. 3, MARCH 2013.
[3] G.M. Bhat, M. Mustafa, Shabir Ahmad and Javaid Ahmad, Vol.2 No. 10 (Oct 2009) "VHDL Modelling and Simulation Of Data Scrambler and Descrambler For Secure Data Communication".
[4] Hethan Kumar, M Praveen Kumar Y G, Dr. M volume 3 Issue 4,April 2014, "Design and implementation of Logical Scrambler Architecture for OTN Protocol"
[5] Ghulam M .Bhatt, Muhammad Mustafa,Shabir A. Parah, Javaid Ahmad ,2010," Field programmable gate array (FPGA) implementation of novel complex PN-code generator based data scrambler and descrambler".