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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 10, October 2015

Logical Data Scrambler for High Speed Application

Dhiraj S. Bhojane, Dr. A. S. Joshi

Student, Dept. of Electronics & Telecommunication, SIPNA C.O.E.T, Amravati, India

Professor. Dept. of Electronics & Telecommunication, SIPNA C.O.E.T, Amravati, India

Sant Gadge Baba Amravati University

ABSTRACT: Nowadays, the requirements of high speed applications are increasing day by day. So, to achieve such type of data transfer rate in OTN (optical transfer network) protocol a proposed architecture has been designed. This architecture is called as logical scrambler architecture which is specifically designed for OTN protocol & specifications of their logical resources. The logical scrambling architecture can be designed using serial scrambling architecture, in which registers are connected in parallel to achieve high data transfer rate in OTN. ITU-T defines an Optical Transport Network (OTN) as a set of Optical Network Elements (ONE) connected by optical fiber links, able to provide functionality of transport, multiplexing, switching, management, supervision and survivability of optical channels carrying client signals.OTN is a system which is designed support for optical networking using wavelength-division multiplexing (WDM) unlike its predecessor SONET/SDH. The whole design has been simulated using modelsim software and analysed on ALTERA FPGA using quartus II software to achieve the higher throughput for different data bit system using with and without pipelining concept.

.

KEYWORDS: Optical transfer networks, optical network elements, wavelength division multiplexing, ITU-T, SONET/SDH

I. INTRODUCTION

In telecommunications, a scrambler is a logical device that transposes or inverts signals or otherwise encodes a message at the transmitter which makes the message string unintelligible at a receiver not equipped with an appropriately set descrambling device. While encryption system usually refers in digital domain to carry out operations and scrambling typically refers to operations carried out in the analogue domain. Scrambling is consummate by the addition of components to the original signal or some important content of the original message signal is being changed to make extraction of the original message signal complex .The level of data security in a conventional Scrambler can be improved by enhancing the number of stages of shift registers. This conversely increases error propagation. An uncomplicated method for ensuring security is to encrypt the data. For any secure communication system the pseudo-noise (PN) key generation is very important parameter. The Pseudo-Noise (PN) sequences based on LFSR (Linear Feedback Shift Registers) and non linear sequence based implementations are simplest to get medium level of security. Chaos base encryption techniques have proven fruitful, still complexity of such systems is important. To scramble incoming plain text the complex system generated code is used. At the receiving end also, same code be generated and successfully used to decrypt the transmitted data. The easiness of the circuit along with the complexity of the generated codes makes the circuit striking for secure message communication application.

The OTN (optical transfer networks) are standards for data transmission over fiber optic links. Due to long sequences of consecutive bits from incoming message streams, the clock signals speeds become low and lead to wait in clock signal. This downturn the transfer rate of data in OTN system. Hence complexity increase in OTN system and leads to over utilization of logic resources. Hence there is a need of clock recovery at the receiver, which in turn requires a guaranteed less number of transitions in the succeeding serial data stream. The mechanism to achieve this

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 10, October 2015

transition frequency is known as scrambling. And this uses PRBS (pseudorandom bit sequence) circuit to perform scrambling. The basic building of architecture to achieve this scrambling uses logical scrambler architecture which is called as serial scrambler architecture. This work presents the satisfactory solution by implementing logical scrambler architecture. By using basic architecture of serial scrambler, logical scrambler architecture can be implemented in which registers are connected in parallel manner.There are many applications of scrambler. In security systems scrambler is used for encryption of data, to remove non-linearity of common carrier systems which causes inter-channel interference and to remove systematic anxiety caused by self-retiming circuits in base-band Pulse Code Modulation (PCM) systems. In data communication systems, scrambler main purpose is to add redundancy in the transmitted data stream so that timing information can be retrieved from received data at the receiver i.e. to aid the synchronization between two modems. The present study is based on the implementation of the scrambler used for synchronization purpose.[10]

II. RELATED WORK

In modern VLSI design scramblers are successfully used in data communication system either to secure data or re-code periodic sequence of binary bits stream. The authors have discussed the digital design, simulation, and FPGA implementation. They have shown the digital architecture used to implement the system.

Xiao-Bei Liu, Soo NgeeKohet.al[1]Presents a Study on Regeneration of Linear Scrambler Using Dual Words of Channel Encoder. In this paper, the initial state of a linear feedback shift register (LFSR) as well as the feedback polynomial is reconstructed in a synchronous scrambler placed after a channel encoder is studied. Finally, the weight of the dual word plays a key part in the reconstruction, as it is very easy to found low weight dual words and in noisy condition, low weight dual words lead to fewer bits required for the reconstruction. Therefore, one might consider using error correcting codes which do not have low weight dual words.

Xiao-BeiLiu ; Sch. of Electr. & Electron. Eng.et.al[2]proposed a design and implementation of Investigation on Scrambler reconstruction with Minimum a Priori Knowledge. The algorithm proposed in this paper is very promising in reconstruction of the linear feedback shift register (LFSR) in a synchronous type of scrambler, as it does not need any a priori knowledge of the input bits, except the source bias.

ZhigangChen ; Xin Hu ; XiaoenJu ; Shin, K.G,et.al[3] presents a paper on LISA that is Location information Scrambler for privacy protection on smart phones. They have proposed a novel approach of a protection of a user's location privacy based on unobservability, preventing the attackers from relating any particular POI's(points of interest) to the user's current location. They have design, implement, and evaluate a privacy-protection system, called the LISA(Location Information Scrambler) which protects the privacy of user's location by adjusting the location noise and hence, the association of users location with any POI is uncertain, while conserving resources (especially battery energy) on mobile devices.

Liu, X.-B. ; Sch. Of Electr. & Electron. Eng. Et.al[4]have presented a paper on Primitive polynomials for robust LFSR based scramblers and stream ciphers.

Guilherme Guindani Frederico Ferlini Jeferson Oliveira Ney Calazans Daniel Pigatto Fernando Moraes [5]presented a complete solution for an OTN framer using FPGA devices. The OTN framer receives a 10 Gbps stream originated from optical fiber link, extracts payload information from it, and transmits that payload data at 10 Gbps. Such type of a working prototype was implemented in Virtex-4 and Virtex-5 devices.

III. PROPOSED WORK OR METHODOLOGY

The general structure of scrambler/descrambler system uses programmable length shift registers and modulo-2 adders in its design architecture. Depending on the size of the data to be transmitted the number of registers and its lengths varies. To make it simple let's take a simple design as shown in figure. It consists of two registers of definite length in addition to two modulo-2 adders [1].

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 10, October 2015

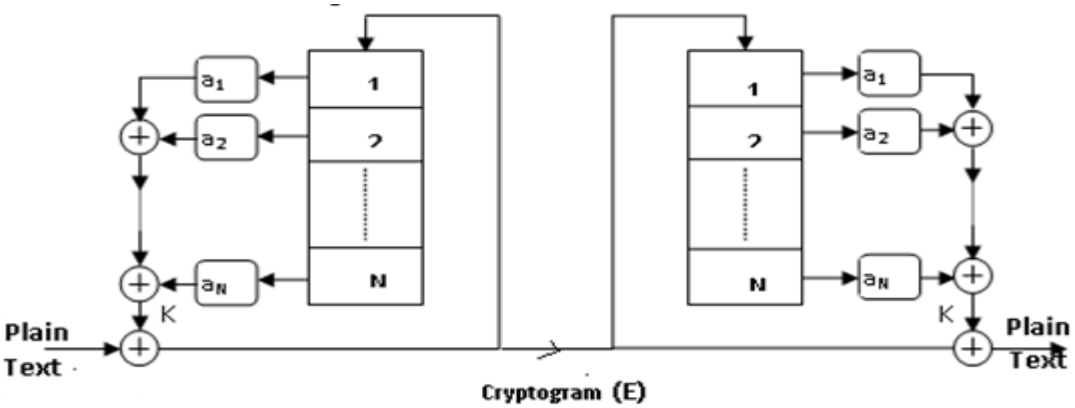


Fig I. Conventional data Scrambler/Descrambler

There are various ways to implement scrambler but all rely on the same basic building blocks of linear feedback shift registers and mod-2-addition functions. Many researchers have discussed the general theory about implementation of scramblers [2-4], [6-7]. In general, the data enters serially in LFSR (linear feedback shift register), where at each stage in LFSR the register delays the signal by one time unit as shown in Fig. (2). The delayed output signal is then fed back and mod-2-addition is performed with the input signal.

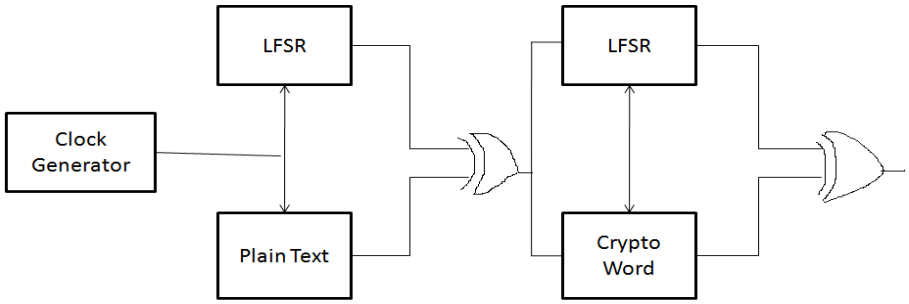


Fig II:Block diagram of scrambler And descrambler

Block diagram of scrambler & descrambler shown in Figure. Scrambler is performed in sequence X-OR the 8-bit plain text message D0-D7 character with the 8-bit D0-D7 output of the LFSR. An o/p of the LFSR is XOR with plain text of the data to be processed. The data register and LFSR are then successively advanced and the output processing is repeated for D1 through D7.Descrambling is performed in order XOR the 8-bit crypto word (D0-D7) character with the 8-bit (D0-D7) output of the LFSR. An o/p of the LFSR is X-ORed with crypto word of the data to be processed. The data register and LFSR are then consecutively advanced and the output processing is repeated for D1 through D7. [4]

To increase the throughput of the system we have implemented it using pipelining architecture concept. A pipeline is a technique which has already been design for computers to raise their instruction throughput. The basic instruction cycle is separated up into a series called a pipeline.

Rather than processing each and every instruction in sequential manner, each instruction is split up into a sequence of steps so various steps can be executed in parallel (i.e at the same time) and concurrently by distinct circuitry. By performing multiple operations concurrently in pipelining, instruction throughput get increases, but does not reduce instruction latency (the time to accomplish a single instruction from start to finish) as it still must go through all steps. [13]

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

International Journal of Innovative Research in Computer and Communication Engineering

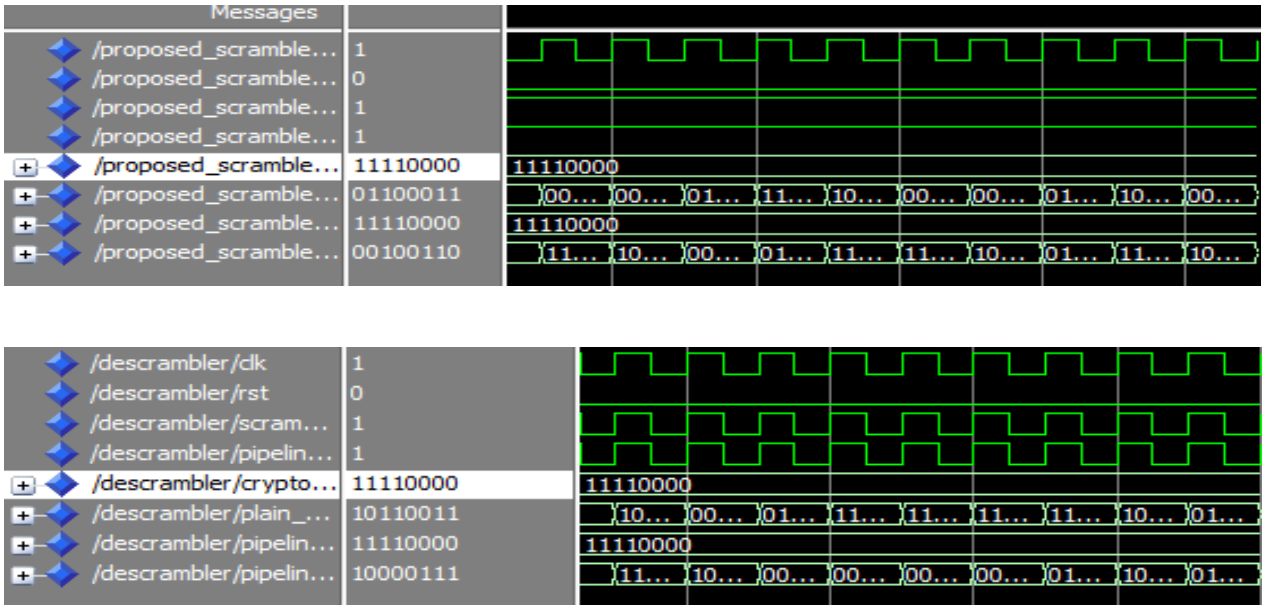
(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 10, October 2015

IV. RESULT AND DISCUSSION

In this paper, we have presented the test environment and the provisional results of our design modules. Our objectives of this project are to design and implement the Scrambler and Descrambler algorithm to improve speed performance and throughput, reduction area. The design is implemented in VHDL, simulated using modelsim and synthesized by alteraquartus II.

Simulation result for 8 bit scrambler and descrambler:



Here, above fig. shows the 8 bit scrambler and descrambler system simulation result which has been achieved on modelsim simulation software also we have synthesized the design based on various parameters mentioned below with and without pipelined concept for different data type system.

For 8 bit scrambler and descrambler, we have synthesized the code based on with and without pipeline as shown below

Table I: 8 Bit scrambler

Sr. No.	Parameters	Without Pipelining	With Pipelining
1	Area	16LE	17LE
2	Time	10.442 ns	7.533ns
3	Frequency	0.095 GHz	0.13 GHz
4	Power	68.91mW	69.01 mW
5	Throughput	0.76Gbps	1.06 Gbps

With ref. to above table, we have synthesized and analyse our design on altera quartus II design software where we have analyse the design in comparative format for Area, Time, Frequency, Power and Throughput. From this tabular result you can see that by using pipelining concept how our results get improved.

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 10, October 2015

From this above discussion we can understand that by implementing such type of scrambling and descrambling device, the throughput of the system in OTN protocol get increases and along with that we get additionally a data security.

V. CONCLUSION AND FUTURE WORK

Scrambler block is a very easy but efficient and extremely important block in the data communication protocol. A scrambler admits information in intelligible form and through intellectual transformation assures data quality with fastest rate without any error or dropping occurrence.A new modified scheme for complex Pseudo Noise-code based data scrambler and descrambler has been presented. Moreover, this current design is very efficient, more securable, high speed, lower area used & it has lots of space to further improve.An efficient scheme for data scrambling and descrambling for secure data transmission using VHDL has been proposed. It has been found that the proposed scheme is capable of giving a range of applications in Spread Spectrum Modulation, CDMA (Code Division Multiple Access) and Global Positioning Systems and OTN protocol. The proposed system can be synthesized and implemented on any of the existing FPGA systems as per the degree of optimization required.

One could work on selection of a different bit size and by implementing pipelining which would make the algorithm is more secure, and a larger input block to increase the throughput. The extra increase in area can however be tolerated. So such an algorithm with high level of security and high throughput can have ideal applications such as in multimedia communications. Furthermore study of optimization approaches for the implementations supporting multiple bit lengths according to applications and modes of operation have tremendous scope for future work. In future high data transfer rate is possible by removing the more critical paths among the high speed circuit.

REFERENCES

1. Xiao-Bei Liu, Soo NgeeKoh, Chee-Cheon Chui, and Xin-Wen Wu, Member, IEEE "A Study on Reconstruction of Linear Scrambler Using Dual Words of Channel Encoder" VOL. 8, NO. 3, MARCH 2013
2. Xiao-Bei Liu ; Sch. of Electr. & Electron. Eng., Nanyang Technol. Univ., Singapore, Singapore ; Soo Ngee Koh ; Xin-Wen Wu ; Chee-Cheon Chui" Investigation on Scrambler Reconstruction with Minimum A Priori Knowledge" published in Global Telecommunications Conference (globecom 2011), 2011 IEEE Date of Conference: 5-9 Dec. 2011 houston, TX, USA. ISSN 1930-529X pp 1-5
3. Zhigang Chen ; Xin Hu ; Xiaoen Ju ; Shin, K.G." LISA: Location information scrambler for privacy protection on smartphones" Published in: Communications and Network Security (CNS), 2013 IEEE Date of Conference: 14-16 Oct. 2013 , national harbor ,MD pp 296-304 DOI:1109/CNS.2013.6682719
4. Liu, X.-B. ; Sch. of Electr. & Electron. Eng., Nanyang Technol. Univ., Singapore, Singapore ; Koh, S.N. ; Wu, X.-W. ; Chui, C.-C. "Primitive polynomials for robust linear feedback shift registers-based scramblers and stream ciphers" Published in: Information Security, IET (Volume:6 , Issue: 3) Date of Publication: Sept. 2012 pp:183 – 189 ISSN : 1751-8709.
5. Guilherme Guindani Frederico Ferlini Jeferson Oliveira Ney Calazans Daniel Pigatto Fernando Moraes "A 10 Gbps OTN framer implementation targeting FPGA devices", Dec.2009.
6. Xiao-Bei Liu, Soo NgeeKoh, Xin-Wen Wu, Member, IEEE, and Chee-Cheon Chui "Reconstructing a Linear Scrambler With Improved detection Capability and in the Presence of Noise" VOL. 7, NO. 1, FEBRUARY 2012
7. Chethan Kumar M, Praveen Kumar Y G, Dr. M. Z. Kurian ,"Design and Implementation of Logical Scrambler Architecture for OTN Protocol", Volume VI, Issue II, May 14
8. Win C. H., Chen C. N., Wang Y. J., Hsiau J.Y., Jou s. J., "Parallel Scrambler for HighSpeed Applications", Jul. 2006.
9. Arley Salvador, Valentino Corso "100 Gbit/s Scrambler Architectures for OTN Protocol:FPGA Implementation and Result Comparison", Aug.2012
10. ITU-T "G.870: Terms and definitions for optical transport networks (OTN)". Available at: http://www.itu.int/rec/TREC- G.870-200803-I/en, Apr. 2009.
11. Sawyer N. "SONET and OTN Scramblers/Descramblers", Application Note XAPP 651, Nov. 2002.
12. David Marple and Larry Cooke, "Programming Antifuses in CrossPoint's FPGA," Proc. CICC 94, May 1994, pp. 185-188.
13. Designing high performance digital circuits using wave pipelining : Algorithms and practical experiences by Dereck C. wong, Member, IEEE, Giovanni De Micheli , senior Member,IEEE and Michael .J Flynn . Fellow, IEEE.