A Survey on Logical Data Scrambler for High Speed Application

Dhiraj S. Bhojane **Dr. A. S. Joshi**

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 scrambler architecture can be designed using serial scrambler architecture, in which parallel connection of registers are used 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 fiber optic links which provides transporting, switching, multiplexing, supervision, management and survivability of optical channels carrying client signals. OTN was designed to provide support for optical networking using wavelength-division multiplexing (WDM) unlike its predecessor SONET/SDH. The whole design will be simulated using modelsim software and analyzed on ALTERA FPGA using quartus II software**.

Key Words: **Optical Transfer Network, Logical Scrambler, Optical Network Element, Wavelength Division Multiplexing.**

I INTRODUCTION

The optical transfer networks (OTN) are standards for data transmission over fiber optic links. Due to long sequences of consecutive digits from incoming data streams, the clock signals become low and lead to delay in clk signal which decrease the data transfer rate in OTN system. Hence complexity increase in OTN system and leads to over consumption of logic resources. Hence there is a need to recover a clock at the receiver, which in turn requires a minimum number of transitions in the incoming serial data stream. To achieve this transition density a scrambling technique is used. And this uses pseudorandom bit sequence (PRBS) circuit to perform scrambling. The basic architecture to achieve this scrambling uses serial scrambler architecture. This work presents the suitable solution by implementing logical scrambler architecture. The logical scrambler architecture can be implemented using basic architecture of serial scrambler in which registers are connected in parallel.[6] ITU-T OTN Definition described in the ITU-T Recommendation G.709 (2003), it adds administration, maintenance, operation and provisioning (OAM&P) functionality to optical carriers in a multi-wavelength system such as DWDM (dense wavelength division multiplexing).

OTN was designed in such a way that it specifies a digital wrapper in which a method is used for encapsulating an existing data frame, regardless of the native protocol, to create an ODU i.e optical data unit, similar to that used in SDH/SONET. OTN provide the network management functionality of SDH and *SONET* but on a wavelength basis. A digital wrapper is flexible in terms of frame size and allows multiple existing frames of data to be wrapped together into a single entity that can be more efficiently managed through a lesser amount of overhead in a multi-wavelength system.

II RELATED WORK

Xiao-Bei Liu, Soo Ngee Koh, Chee-Cheon Chui et.al [1] presents a study on Reconstruction of linear scrambler using dual words of channel encoder. In this paper, 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 codeword's 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 algorithm and results show that the number of bits required to do the reconstruction can be significantly reduced.

Xiao-Bei Liu, Soo Ngee Koh, Xin-Wen Wu, Chee-Cheon Chui [2] proposed a design and implementation of investigation on scrambler reconstruction with minimum a priori knowledge. The existing algorithm for reconstruction of the feedback polynomial in a linear scrambler relies on the assumption that the input sequence is produced by a biased memory less source and the source bias is known and used for reconstruction. In this paper, the problem of reconstruction of the feedback polynomial in a linear scrambler without knowledge of the source bias is studied. An algorithm is proposed to reconstruct the scrambler without knowledge of the source bias and factors which affect the performance of this algorithm are discussed. A scheme which reduces the number of bits used in the reconstruction without affecting the detection capability of the reconstruction algorithm is also proposed in this paper.

Zhigang Chen, Xin Hu, Xiaoen Ju, Shin, K.G. et.al [3] presents a paper on LISA that is location information scrambler for privacy protection on smart phones. As use of location-based services (LBSs) is becoming increasingly prevalent, mobile users are more and more enticed to reveal their locations, which may be exploited by attackers to infer the points of interest (POIs) the users visit and then their privacy information. They proposed a novel approach to the protection of a user's location privacy based on unobservability, preventing the attackers from relating any particular POI to the user's current location. They design, implement, and evaluate a privacy-protection system, called the Location Information Scrambler (LISA) which protects the user's location privacy by adjusting the location noise and hence, the uncertainty of associating his location with any POI, while conserving

resources (especially battery energy) on mobile devices. By protecting location privacy locally on each mobile user's device, LISA eliminates the reliance on the trusted third-party servers required by most existing approaches. Therefore, it not only avoids the vulnerability of a single point of failure, but also facilitates the deployment of LBSs. Their evaluation of LISA using real-world users' traces demonstrates its efficacy and efficiency.

Liu, X.-B., Soo Ngee Koh, Wu chee cheon, X.-W.Chui, C.-C. et.al [4] have proposed a paper on Primitive polynomials for robust linear feedback shift registers-based scramblers and stream ciphers. It is well known that in order to build linear scramblers and stream ciphers that are robust against correlation-based reconstruction, primitive polynomials which do not have sparse multiples of moderate degrees must be used. In this paper, the existence and density of such good primitive polynomials` are studied. Two theoretical lower bounds on the degree d of the primitive polynomial are derived. When d is larger than the first lower bound, there exists at least one primitive polynomial of degree d which does not have any sparse multiple of moderate degree and when d is larger than the second lower bound, it is almost guaranteed that a randomly chosen primitive polynomial of degree d does not have any sparse multiples of moderate degree. To make the lower bound tight, the distribution of the minimum degrees of sparse multiples of primitive polynomials is investigated in this paper. From comparison, it can be seen that the lower bounds obtained in this paper are much better than the previous results reported in the literature

III PROPOSED WORK

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 transporting, switching, management, multiplexing, supervision and durability of optical channels carrying client signals. ONE may Re-time, Re-Amplify, Re-shape (3R) but it does not have to be 3R— it can be purely photonic. OTN was designed to provide support for optical networking using wavelength-division multiplexing (WDM).

OTN protocol is preferably used for high speed data transmission over a fiber optic link and such type of speed is achieved by using serial data scrambler with its PRBS. Fig.1 [11] below shows the basic building block diagram of serial data scrambler. In digital transmission systems, there are always scramblers to scramble the transmission data. In general, multiples of base rate signals are multiplexed and then scrambled before transmission which is descrambled and demultiplexed after reception. Scrambling used to be done serially.

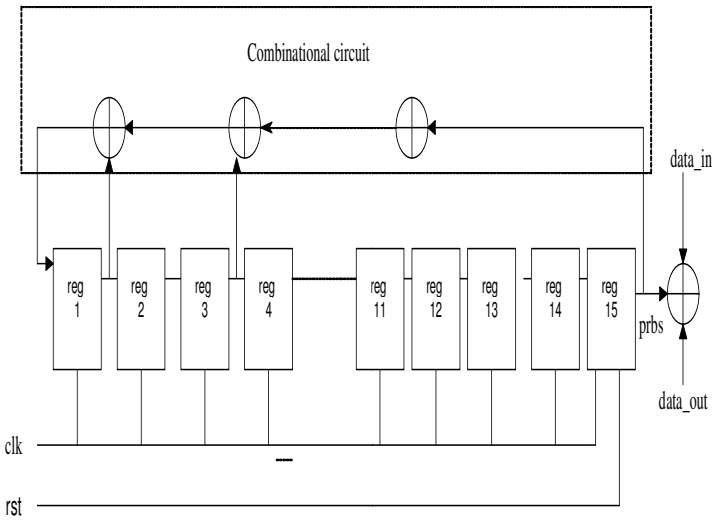

Figure.1 serial scrambler block diagram

The above serial scrambler diagram shown in fig 1, generates a continuous stream of output bits which is same as the bit rate of transmitted one.

The scramblers scramble the input data string by applying a PRBS i.e mod-2 addition. Sometimes a pre-existing PRBS stored in ROM is used, but more often it is generated by using linear feedback shift register (LFSR).A synchronizing word is used for synchronous operation in between transmitting & receiving LFSR. A synchronous word is set in the data string through equal intervals in each frame. A receiver searches for a few synchronous -words in adjacent frames and hence determines the place when its LFSR must be reloaded with a pre-defined initial state.

Fig.2 illustrates a generalize block diagram of a logical scrambler. This logical scrambler architecture is implemented using register set which are feedback through a combinational circuit [8][9].The pseudorandom signal generated by the circuit feed the output bus called ***prbs***[(L-1)..0], where L represents the number of output bits. The simple example for this type of generator is shown in Fig. 1, where the output of the PRBS has only one bit.

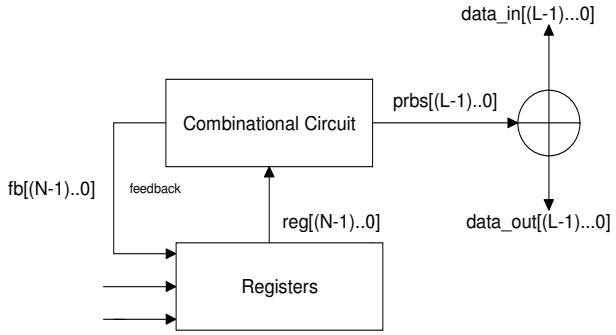

Fig.2. Logical scrambler block diagram

In this serial scrambler, the initialization block forces the reset of all registers that keep a high logic level in their outputs. As can be seen from the above fig., for each clock cycle the register data are shifted to the right and the LSB (least

significant bit) is calculated from the combined output of the register *reg*(0),*reg*(2), *reg*(11) and *reg*(15). This process continues until 2^{16} -1 values are generated, and the sequence is then restarted. If an operating frequency of FPGA board is at 150 MHz then the pseudorandom bit sequence generator produces a single bit for each cycle, hence, the data rate is 150 Mbit/s.[9]

To fulfill our project requirements we choose the FPGA platform, because it has various advantages & applications from which we can develop our logical data scrambler which is very important part stated in this project. This logical scrambler can be implemented on FPGA platform by using VHDL code. The VHDL code of logical scrambler will be synthesize on altera FPGA platform & after synthesis, we are going to analyse various performance parameters like device utilization summary, timing summary that is prapogation delay of a circuit & power consumed by the design.

CONCLUSIONS

The architecture of logical data scrambler can be designed to achieve higher data rate in OTN protocol. By achieving this high performance rate the problem get resolved in OTN system due to large series of continuous digits from incoming data string, the clock signals get low and lead to hold in clock signal. The above architecture will be implemented using VHDL and this proposed methodology will be design and verify using FPGA platform. This proposed design will be analyze for area, speed and power platform. The whole design will be simulated using modelsim software and analyzed on ALTERA FPGA using quartus II software.

REFERENCES

[1] Xiao-Bei Liu, Soo Ngee Koh, Chee-Cheon Chui, and Xin-Wen Wu, Member, IEEE "A study on reconstruction of linear scrambler using dual words of channel encoder" IEEE transactions on information forensics and security vol. 8, no. 3, march 2013 pp 542-552

[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] Xiao-Bei Liu, Soo Ngee Koh, Xin-Wen Wu, Member, IEEE, and Chee-Cheon Chui "Reconstructing a linear scrambler with improved detection capability and in the presence of noise" Published in: Information Security, IET (Volume:6 , Issue: 3) Date of Publication: Sept. 2012 pp208 – 218 ISSN : 1556-6013

[6]. Chethan Kumar M, Praveen Kumar Y G, Dr. M. Z. Kurian ,"design and implementation of logical scrambler architecture for OTN protocol", volume III, issue IV, Apr 14

[7]. Win C. H., Chen C. N., Wang Y. J., Hsiau J.Y., Jou s. J., "parallel scrambler for highSpeed applications", Jul. 2006.

[8]. Guilherme Guindani Frederico Ferlini Jeferson Oliveira Ney Calazans Daniel Pigatto Fernando Moraes "A 10 Gbps OTN framer implementation targeting FPGA devices", Dec.2009.

[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.