A Review on All Optical Encryption and Decryption methods

Vipul Agarwal[1] and Vijayshri Chaurasia[2]
[1,2]Electronics and Communication Department,
[1]Aisect University, Bhopal, India.
[2]MANIT, Bhopal, India.

***Abstract*:** In present times, the protection of Optical signal data is becoming very important as large amount of internet data is transferred through Optical fibres. The data can be easily protected by encrypting data before transmission. There many different techniques for optical signal encryption. In this paper, we survey on existing methods used in optical signal encryption.

***Keywords*—** Fibre Bragg Grating, pseudo noise, Mach–Zehnder interferometer, OR logic gate.

I. INTRODUCTION

Data security is most important in today's world. Lot of methods have been proposed to encrypt data signals to make it more secure and robust. In recent years the field of information security has grown and evolved significantly. The vast outspread of internet and advance in digital techniques have made it possible to copy and edit images, audio, video and other types of multimedia data. As a result digital information may be exposed to variety of vulnerabilities, including loss, misuse, duplication and unauthorized modification of information. Optical techniques have shown great potential for information security applications. By 2018 it is expected that internet users will be doubled as compared to number of users at present .This means that amount of data carried by the optical fibres will also be doubled. The Hackers worldwide are trying to hack /steal the data for their personal benefit. They try to steal personal information like internet banking passwords, credit card details .Due to these threats it is very important to encrypt data before transmitting it to optical fibres. Data encryption will not only protect data it will also bring confidence to users to use internet without any worry. With the increase applications of optical communication, the security is becoming an important issue for the researchers in the field of all optical communication. To ensure secure high speed optical communication networks, the all optical encryption decryption is of prime importance. Physical layer of optical network is vulnerable to eavesdropping and demands high level of information security. Various encryption schemes have been proposed that require opto electronic conversion. Electronic encryption however becomes difficult at bit rates exceeding 5 Gb/s due to speed limitations of electronic optical interfaces. Encryption Decryption Scheme is difficult to implement on high speed data transmission (more than 10 Gb/s) as bit error rate increases to unacceptable level.

Hence a need exists for high speed low latency optical encryption and Decryption system which do not require opto electronic conversion and bit error rate of decrypted signal remains to be of acceptable level. This chapter focuses mainly on the different kinds of optical encryption and decryption techniques used till now. A brief comparison is made between different optical encryption techniques and conclusion is drawn based on advantages and disadvantages of these techniques. In this paper we have reviewed various optical encryption techniques that are existing. This study extends to the performance parameters used in encryption process and analysing their security issues.

II. LITERATURE SURVEY

In 2002, J. Ohtsubo [1] demonstrated Chaos based encryption scheme in which message was added to the chaotic signal generated by the oscillator, then transmitted to the receiver. The variations of the message amplitude were hidden by the chaotic fluctuations of the carrier signal intensity. They demonstrated that masking technique requires two conditions: the first one is that the spectrum of the message needs to be completely overlapped by the spectrum of the generated chaos. The second condition relates to the efficiency of the masking. The message amplitude, m(t), must be sufficiently small relative to the chaotic fluctuations c(t) of the chaotic carrier. Message and noise were then intermingled. Significant noise levels reduce the communication quality very rapidly. Consequently, this type of encoding is seldom used for communication because of the noise problem.

Wang et al.[2] proposed a new optical encryption scheme in 2003. In the proposed system, the security performance was increased by adding the encryption key which is a tuning signal of TFBGs. The broadband light pulses modulated by an electro-optic modulator (EOM) were reflected by periodically controlled TFBGs array in an encoder, and the pulses were split into a series of lower power pulses in the time domain. The authors investigated that to recover the original signal in a decoder, one must know not only the inverted sequence of TFBGs but also the tuning signal of each TFBG used in the encoder. Transmission experiment was performed with the data rate of 155 Mb/s through the optical fibre length of 50 km. Bit error rate of decrypted signal was 10^{-10}.

In 2005 Fred F Frochlich, Craig H Price, Terry M Turpin and Janeen [3] A Cooke proposed all optical encryption system. The complexity of their encryption system remains relatively constant as data rate increases. Diagram of all optical encryption system is shown in Fig. 1. Beginning at the upper left in the figure, the dashed box represents an optical communications signal as either a single optical wavelength or as a WDM set of wavelengths to be transmitted. The optical signal is passed to an optical spectrum analyzer/combiner where the optical spectrum of the signal is spatially dispersed across the elements of an array of reflective phase modulators. As each spectral component is reflected off its corresponding phase modulator element, a different static phase offset is imparted onto each spectral component as determined by the phase settings of the elements, which are set by the array phase controller using settings prescribed by the encryption key. The reflected ensemble of spectral components then re-enters the bidirectional spectrum analyzer/combiner and is recombined into a contiguous spectrum signal which exits as the encrypted optical signal. The signal can be considered to be encrypted at this point because the phase distortion on the signal is so severe that its temporal waveform becomes noise-like.

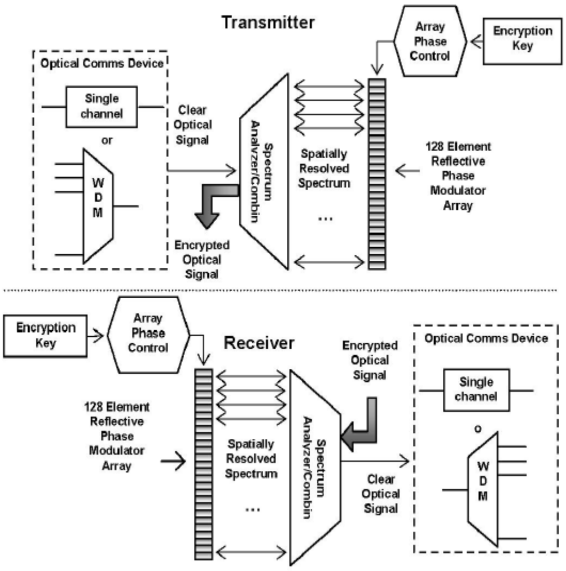

Figure-1 : Diagram of all optical encryption system

At the receiver the process is reversed. The encrypted optical signal is input to the spectrum analyzer/combiner, the spectrum is dispersed across the reflective phase modulator array, the conjugates of the encryptor phase settings are applied to the spectral components, and the phase-restored components are recombined to form the original temporal waveform optical signal.

In 2006 Jose M Castro, Ivan B Djordjevic and David Geraghty [4] proposed and optical encryption based on super structured Bragg gratings. The encryption process is performed in two steps: encoding and masking .During the encoding process, data is transformed into optical noise like pattern by the use of pseudorandom SSBG since amplitude and phase are changed pseudorandomly. In masking process the encoded signal is combined with a quasi –orthogonal noise generated by another set of PR-SSBG. The resultant signal to be transmitted is a noise like sequence in which the structure of bits in frequency and temporal domain is lost for an eavesdropper. In the receiver side there is a set of conjugate PR-SSBG to decode the information bits. The sizes of the set and pseudo noise components determine the degree of security. The advantage of this scheme is that there is no need to synchronize noisy lasers .The security can be further enhanced by increasing number of gratings and by adding tunability to the PR-SSBGs. The drawback of this encryption technique is that it reduces bit rate considerably & use of quasi –orthogonal noise introduces the moderate power penalty for unauthorised users,

In Jan 2007 Valerio Annovazzi-Lodi, Sabina Merlo & Mauro Benedetti [5] proposed message encryption by phase modulation, using chaotic optical carrier. They used chaotic laser [master laser (ML)] at the transmitter side to hide the information to be transmitted (the message); another laser [slave laser (SL)], at the receiver allows message recovery. The extraction of the hidden message from chaos is based on synchronization between ML and SL, i.e., on the generation of the same chaotic waveform at both ends of the channel. Synchronization can be only obtained under suitable conditions, by injecting part of the ML output into the SL, and relies on two lasers being closely matched, which ensures security. The cryptographic key consists in the set of parameters of the two matched lasers. The arrangement for the phase modulation experiment is shown in Fig. 2, and consists of a typical master/slave configuration. A LiTaO crystal is included in the master cavity and is used as a phase modulator to insert the message; the crystal in the slave cavity only keeps symmetry, as required for efficient synchronization.

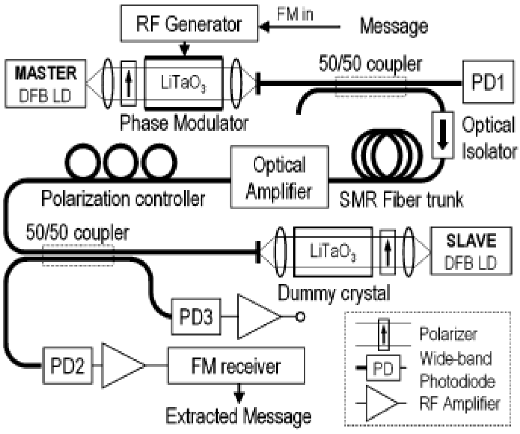

Figure-2 : Encryption setup of Chaotic optical carrier

Master/slave synchronization was obtained by adjusting the injection current (50% above threshold), the alignment, and the temperature of both lasers, as well as the injection level. The two external cavities were also carefully matched. The regimes of the two lasers were compared by observing the outputs of photodiodes PD1 and PD2 by an RF spectrum analyzer. The synchronization level was checked by observing the spectrum of the difference of ML (at PD3) and SL (at PD2) outputs. Transmission experiments were performed by modulating the input voltage of the master LiTaO crystal, giving rise to a 100-MHz carrier, modulated on its turn by a 1-kHz message. At the slave output, the carrier was fed to an FM receiver to get the message. The limitation of encryption method is that only analog signal can be encrypted, however most optical signals are digital.

In 2007 Chang Wan Son, Seok Lee, Gill Sang Geun and Tae Hoon Yoon [6] successfully demonstrated optical encryption and decryption system using cross gain modulation (XGM) technology of semiconductor optical amplifiers. They used SOA based logic gates to encrypt optical signal as it is simple to implement & can be used for ultrafast bitrates, also it is insensitive to the polarization of input signals. The operation principle of all optical XOR gate using SOAs are shown in Fig 3. Boolean AB is obtained by using signal B as a probe beam and signal A as a pump beam in SOA-1. Boolean AB is obtained by using signal A as a probe beam and signal B as a pump beam in SOA-2. XOR logic is acquired by adding Boolean A'B + AB' From SOA 1 & SOA 2.

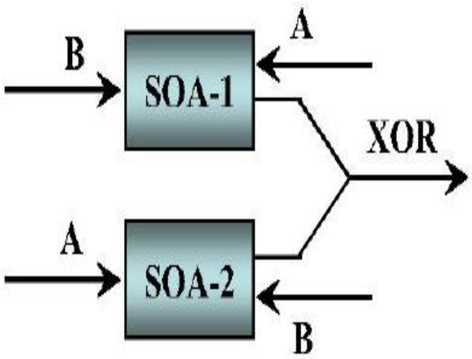

Figure-3 : Operation principle of all optical XOR using SOAs

The brief scheme of experimental setup for all optical encryption and decryption system using XOR logic gate is shown in Fig. 4. In encryption part, Boolean Pi Ki' is obtained by using signal Pi as a probe beam and signal Ki as a pump beam in SOA-1. Boolean Pi' Ki is obtained by using signal Ki as a probe beam and signal Pi as a pump beam in SOA-2. XOR logic is acquired by adding Boolean Pi Ki' and Pi' Ki from SOA-1 and SOA-2. In decryption part, Ci and Ki signal is used as probe and pump beam and Pi signal is obtained by the optical XOR logic operation

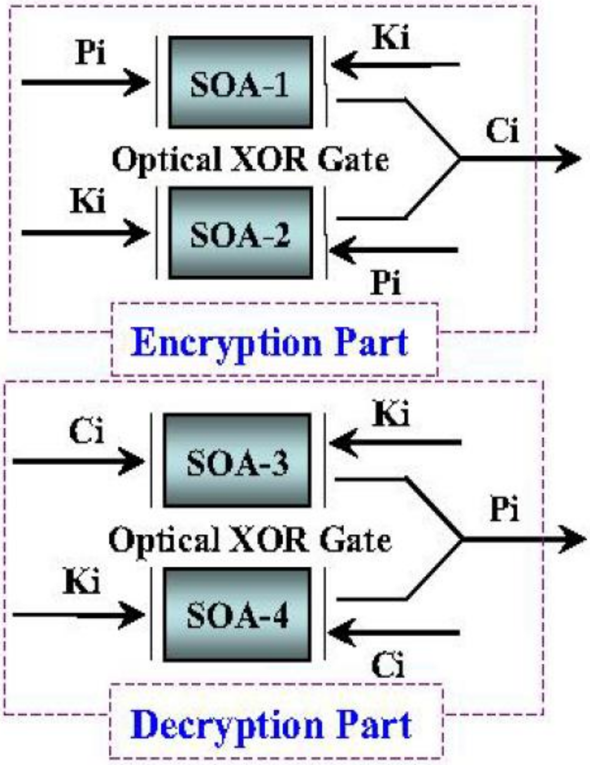

Figure -4 : Experimental setup

In 2009, Mable P. Fok and Paul R. Prucnal experimentally demonstrated a compact and low latency fibre based approach for optical steganography. Optical steganography aims at transmitting data secretly through a stealth channel which is hidden under public fibre optic communications, while all others are unaware of its existence. The principle of optical steganography is stretching an optical pulse extensively so that the stretched waveform is weak enough to hide under the system noise. The amplitude of the signal is hidden under the noise floor of the network. The signal can be restored at the receiver by destretching an optical pulse. A chirped fibre Bragg grating (CFBG) was used to temporally spread the stealth channel pulses. The amplitude of the signal is hidden under the noise floor of the network. The signal can be restored at the receiver by using another CFBG providing the same but opposite dispersion. Due to presence of stealth channel, the public channel shows only a 1 dB power penalty.

In 2009, WANG [7] et al. Proposed an encryption- decryption technique at 2.5 Gb/s which uses a cross- phase modulation (XPM)-based XOR logic gate. Encryption of signal was realized by employing an XOR based on an XPM between an O-band (1310 nm) and a C- band (1550 nm) light wave. The drawbacks of this encryption scheme are that it is complicated and requires precise synchronization of every bit. Also, the amplified spontaneous emission (ASE) noise accumulated from the cascaded SOAs puts a limit to practical applications of the system. As per authors, this scheme to work at 10 Gb/s it is necessary to overcome pattering effects imposed by the slow recovery time of the SOA.

In 2012, Yi et al. [8] proposed a novel optical encryption/decryption method by using the stimulated Brillouin scattering (SBS) effect in optical fibre. At the transmitter side, the SBS gain or loss with configurable shape distorts both the amplitude and phase of the broadband signal so as to implement the encryption process. At the receiver side, the corresponding SBS loss or gain with the same amplitude and spectral shape is used to recover the distorted signal for decryption. The encryption keys are the SBS gain amplitude, bandwidth and the spectral shape, which are controlled by the users. Complete encryption and error-free decryption was demonstrated at 10.86 Gb/s. with BER 2X10^{-5}.

Wu et.al, in 2013 proposed a method to encrypt the modulated ASE noise in a two dimensional key space. The expansion to two dimensions increases the key space in a geometrical progression. The first dimension was taken as optical delay. The second dimension was dispersion. Extra dispersion was deliberately added at the transmitter of the stealth channel. The BER measurements at 2 Gb/s of the stealth channel showed that the BER reaches a minimum of 10^{-4} when both the dispersion and optical delay are matched which is very less. Forward error correction with Reed-Solomon codes is required to improve bit error rate. The BER increases dramatically when one of the matching conditions is not satisfied.

Wu et al. [10] proposed and experimentally demonstrated an optical encryption method based on interference cancellation in 2014. The digital signals were combined with stronger analog interference noise. The authors explained that signal can only be recovered by matching the interference noise and the cancellation noise. Both the phase and amplitude of the noise can be controlled and used as key distribution parameters between the transmitter and the receiver. Through eye diagram it was showed that clear eye opening can only be obtained when the matching conditions are satisfied. The data rate of the transmitted data was 12 Gb/s with BER 9X10-5.

III. CONCLUSION

In this paper we have reviewed recently proposed optical encryption algorithms. All these algorithms have its own merits and demerits..Froehlich showed it will take 6.5*10^{81} years for eavesdropper to guess 75% of the correct settings of phase array, however a finite delay is introduced in signal transmission due to this method. J.M Castro encryption method proposed a method in which a the signal is masked by the quasi-orthogonal noise, due to which observation and grating synthesis becomes extremely difficult. It was demonstrated by simulation that the use of the quasi-orthogonal noise introduces the moderate power penalty for authorized users. Chan Wan Son proposed encryption and decryption technique using cross gain modulation of SOA’s. However in this technique transmission speed was limited to 10 Gbps. Wu et al proposed encryption method based on interference cancellation . The data rate of the transmitted data was 12 Gb/s with BER 9X10-5.

REFRENCES

[1] J. Ohtsubo, “Chaos synchronization and chaotic signal masking in semiconductor lasers with optical feedback,” IEEE J. Quantum Electron., vol. 38, no. 9, pp. 1141–1154, Sep. 2002.

[2] Young-Seok Wang, Sang-Chul Moon “Optical encryption communication system using a

periodically controlled tunable fiber Bragg grating array" IEEE J. Quantum Electron., vol. 40, no. 10, pp. 746–750, 2003.
[3] Froehlich, F.F., Price, C.H., Turpin, T.M., Cooke, J.A.: All-optical encryption for links at 10 Gbps and above. IEEE MILCOM **4**, 2158–2164 (2005).

[4] J. M. Castro, I. B. Djordjevic, and D. F. Geraghty, "Novel super structured Bragg gratings for optical encryption," IEEE J. Lightw. Technol., vol. 24, iss. 4, pp. 1875 – 1885, April 2006.

[5]Valerio Annovazzi-Lodi,Sabina Merlo & Mauro Benedetti, "Message encryption by phase modulation of a Chaotic Optical Carrier",IEEE Photonics Technology Letters, vol 19,1041-1135-2007

[6]Chan Wan Son,Seok Lee,Sang Geun ,Tal Hoon, "Realization of 10 Gbps optical encryption using cross gain modulation," IEEE 10.11.09/COINACOFT.2008.

[7] 2009 WANG Ya-Ping , WU Chong-Qing, WANG Zhi, "An Encryption-Decryption Method Using XOR Gate Based on the XPM between O-Band and C-Band Light Waves," CHIN. PHYS. LETT Vol. 26, No. 7 (2009) 074219.

[8] Lilin Yi, TaoZhang, ZhengxuanLi, "Secure optical communication using stimulated Brillouin scattering", Optics Communications 290(2013)146–151, 2012.

[9] Ben Wu, Zhenxing Wang and Bhavin J. Shastri, "Two Dimensional Encrypted Optical Steganography Based on Amplified Spontaneous Emission Noise," CLEO:2013 Technical Digest, 978-1-55752-973-2/13,OSA, 2013.

[10] Ben Wu, Matthew P. Chang, Zhenxing Wang, Bhavin J. Shastri, and Paul R. Prucnal "Optical Encryption Based on Cancellation of Analog Noise", CLEO:2014.