WDM Systems Confidentiality: A Survey

Anita Antwiwaa, Anil Kumar and A. K Jaiswal

Abstract-The evolution of novel telecommunication technologies has boosted the appetite of already data hungry customers to increase their search for information to satisfy their hunger. This has called for some group of people to illegally access information which does not belongs to them. This has caused a lot of losses to the telecommunication companies and thereby putting innocent customers at risk. Fiber communication which is termed as secured has its own vulnerabilities. The internet during its development did not keep strong security in mind. Over 150000 computers were victims to the so called code red attack in only 14 hours period on the 9/11/2001 attack. Moreover, 86000 computers were affected in the NIMDA attack. There is therefore a need to provide security mechanism for the physical layer of an optical network. Eavesdropping, interception, jamming, physical infra-structure attack, among others are some of the attacks that affects the optical network. The way an optical network is implemented determines the type of threat which can affect the network. However, threats are generalized into four. If an unauthorized person tries to listen to the conversation which intend puts the confidentiality of the communication at risk, then the attack is known as confidentiality attack. An unauthorized person might also try to impersonate and communicate as an authorized user and this is also known as authentication attack. The unauthorized user manipulate or alters the communication which puts the integrity of the communication at risk and this is termed as integrity attack. Finally, there is a situation whereby the unauthorized user observes the communication and analyze the traffic as well and this is known as Privacy attack. This work will review the confidentiality issues of WDM optical systems and propose some future security required for optical network.

Keywords- Attacks, Cipher-text, Confidentiality, Data, Security, Soliton, WDM.

I. INTRODUCTION

The demand for data by hungry users has increased in the recent times. In order to respond to the higher demand of data traffic, there is a need for an optical high speed signal which can withstand all perturbations in the event of data transmission.

Anita Antwiwaa is a PhD. Student in ECE Department, SHIATS Allahabad, India aantwiwaa@anuc.edu.gh +917897324709

Anil Kumar is an Associate Prof. in ECE Department, SHIATS Allahabad, India; anil.kumar@shiats.edu.in

K. Jaiswal is a Prof. in ECE Department, SHIATS Allahabad, India; head_ece@shiats.edu.in

This can be achieve using solitons which are essentially stable pulse which travels through the optical medium without change in their shape. This transmission can be achieved by employing the services of the wavelength division multiplexing which will combine multiple wavelength of signals together for transmission. Transmission of soliton in the WDM domain has a lot of security vulnerabilities which cannot be detected using (optical time domain reflectometer) OTDR. The various optical monitoring devices limitations are represented in table 1 [1].

This work is sectioned into five. Section II will focused on the overview of a WDM system. Section III will survey the WDM security and confidentiality mechanisms. Section IV and V will focused on the future optical security required and conclusion respectively.

II. WDM SYSTEM OVERVIEW

The main aim of a WDM system is to transmit multiple number of signals having different wavelengths parallel on a single optical fiber. This adds flexibility to the complex communication systems by injecting different information channel at different location and extracting at different points by the kind help of add/drop multiplexers present in [2], [3], [4]. Figure 1 represents a WDM system with add/drop multiplexer and demultiplexer and an Erbium doped fiber amplifier (EDFA).

Table 1 Limitations of various optical monitoring devices

OPTICAL MONITORING DEVICE	LIMITATION
1. OTDR	No continuous monitoring. No intrusion detection. No characterization or optical fault detection. Ineffective at detecting dynamic or transient disturbances.
2. Optical power level attenuation monitoring	No intrusion shutdown. No fault characterization.
3. Vibration sensing technology	No intrusion shutdown. 6dB optical insertion loss.

Table 2: DWDM capabilities (adapted from [5])

	Single-fiber	Fiber pair DWDM
Maximum number of wavelength spacing	20 (C-band)	32ch (C-band) @ 100GHz 40ch (C-band) @100GHz 80ch (C-band) @ 50GHz
Wavelength spacing	200GHz	100GHz or 50GHz
Capacity per wavelength	100Mb/s-10Gb/s	100Mb/s-40Gb/s
Maximum number of traffic channels per wavelength (electrical multiplexing)		
Modularity (wavelengths)	Add/drop filter architecture with 4ch add/drop 2ch add/drop 1ch add/drop	100GHz: 8ch MDU architecture using odd and even 100GHz channels via Optical Interleaver. 50GHz: 40ch MDU and 8ch MDU architecture using odd and even 50GHz channels via Optical Interleaver. 1ch and 4ch add-drop filter also available.
Maximum distance	Up to ~130km without amplifiers	Up to to ~100km without amplifiers Up to to ~150km without intermediate line amplifiers Up to to ~1500km with intermediate line amplifiers

WDM systems allow telecommunication companies expand their system capacity adding more fibers to the existing ones. The combination of WDM and optical amplifiers aids in accommodating several innovative technologies in the optical network without having to renovate the network backbone. WDM employs the services of dense wavelength division multiplexing (DWDM) system which utilizes the C-band with operating frequencies

between 1530nm-1560nm window. This system effectively uses the capabilities of EDFA which operates well between 1525-1565nm C-band or 1570-1610nm L-band.

Most system uses 40 channels at 100Ghz spacing or 80 channels with 50Ghz spacing in the C-band.Table 2 represents the capabilities of DWDM system.

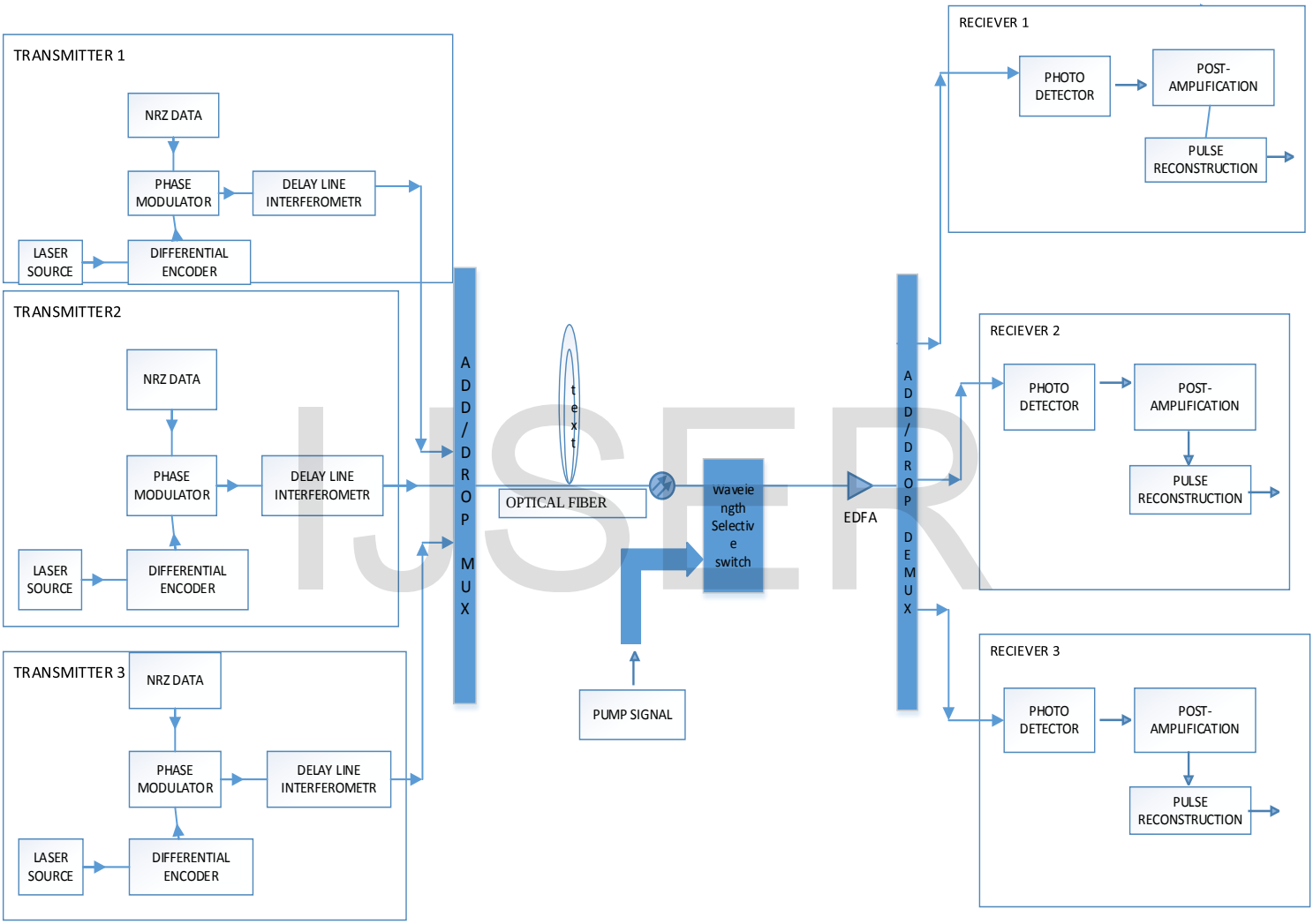

Fig.1 WDM system diagram.

If an unauthorized person tries to listen to the conversation which intend puts the confidentiality of the communication at risk, then the attack is known as confidentiality attack. An unauthorized person might also try to impersonate and communicate as an authorized user and this is also known as authentication attack. The unauthorized user manipulate or alters the communication which puts the integrity of the communication at risk and this is termed as integrity attack. Finally, if the unauthorized user observes the

communication and analyze the traffic as well and this is known as Privacy attack.

An optical fiber network can physically be tapped into by an eavesdropper or the attacker can impersonate a legitimate user by listening to the residual crosstalk for the neighboring channel as given in [12] and [13]. It is easy to tap a fiber without protection. The attacker has to place a second fiber closer to the exposed fiber for small amount of light to escape through that fiber. Tapping the optical signal will cause signal power reduction which can easily be detected using OTDR therefore for the activities of the eavesdropper to be unnoticeable, its operation should be a low signal to noise ratio. Fibers are mostly in bundles therefore peeling of the protection is somehow practically impossible therefore the best way to access a fiber network is to make use of the residual crosstalk by impersonating an actual user. The issue of confidentiality can be enhanced by using an encryption, so that if the eavesdropper gets hold of a small portion of the light signal, extracting the raw data will be difficult without the knowledge of the encryption key given in [10].

A. QUANTUM CRYPTOGRAPY METHOD

This method uses a quantum key distribution to share a secrete key between the sender and the receiver so that an eavesdropper will not be able to access or know the content of the information sent. This method preserves the secrecy of the conversation taking place between two parties.

Example of the encryption methods is the quantum cryptograph which uses the quantum key distribution. Figure 2 represents how a quantum key is generated between two users [14].

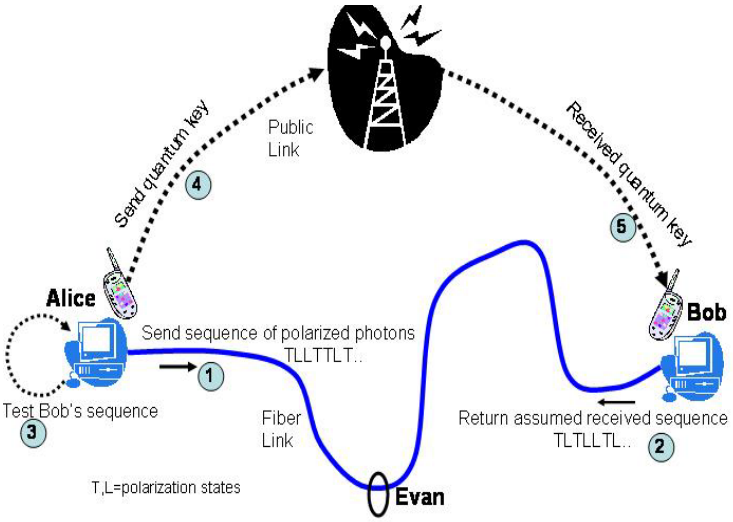

Fig 2: The quantum key distribution. T and L between two users Alice and Bob only.

The procedure for the quantum key generation is as follows:

1. Alice sends a sequence of binary bits through a random polarization filter which is related to a subset of polarization state associated with logic '1' and logic '0' and it is only known by Alice.
2. Bob then passes the sequence of polarized photons through his independently randomly varying polarized filter without knowing the associate logic value and polarization state.
3. The received randomly polarized photons either get rejected or passes through Bob's random polarization state filter.

4. If Bob's filter generates sequence which has some common bits as the one Alice sent but not the same, both Alice and Bob at this point does not know the common bits generated.
5. Bob then communicate over the unsecure channel with Alice and tells her the polarization sequence which he used while receiving Alice's polarized photon. He will not reveal the polarized sequence generated.
6. Base on Bob's response, Alice passes the sequences through Bob's Polarization sequence. Alice compares the initial bit string with the one generated from the experiment and she identifies the bits that are common in the two bit strings in [14].

Another type of quantum key distribution is represented in figure 3. The diagram make use of an optical encryption system at the transmitter and a decryption at the receiver. The key and the data has been placed at a trusted and a secured area out of reached by the eavesdropper. A different coding scheme like OCDMA is used to precode the signal. The signal and the key are lunched into the optical encryption block consisting of an optical XOR gate. The receiver then optically decode and decrypt the signal using the Key as described by authors in [15], [16], [17] and [18].

Another type of quantum cryptography was presented in [14] known as the Photon entanglement where by two orthogonal states of a photon is passed through a strongly polarized birefringent crystal that creates two strongly orthogonal Polarized states. These two states are combined to propagate together in an entangled states. If one part of the entangled state is tapped by the eavesdropper, it will affect the properties of the entangled photon which will be received thereby making it somehow secure.

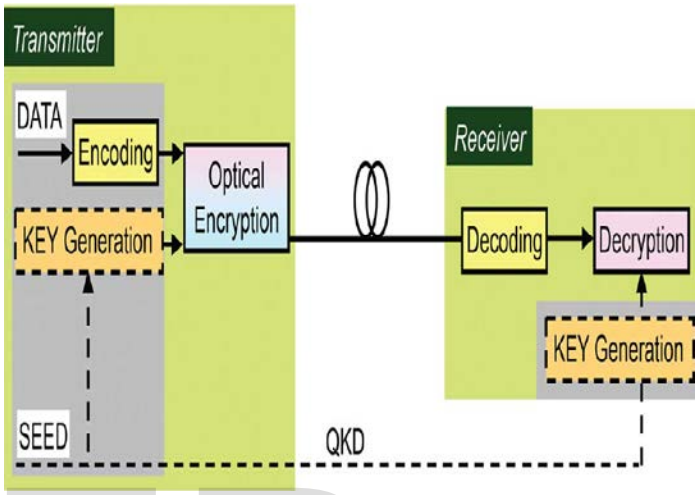

Fig 3: All optical encryption using quantum key distribution.

B. BIT AND BLOCK CIPHERING METHOD

Bit ciphering establishes a direct relationship between the optical codes and the bits. The code space equates the number of encoding/decoding (E/D) ports in a 1-D coding while the code space is exponentially larger in an n-D code. Enlarging the code cardinality enhances the system security.

In block ciphering, the transmitted data is divided into m bits and encoded with an alphabet of $M = 2^m$ determinations which corresponds with the optical code and the bit sequence. The laser pulse are splitted among N-input ports of the encoder to generate a codeword of 2^N, a block length of n= N bits and

$2^N!$ for all possible correspondence between optical codes and bit sequences using n-D codes. Each bit is also assigned a different n-D code as shown in figure 4. In order to enhance the system confidentiality the bit sequence is encrypted with two or more multi-dimensional selected code.

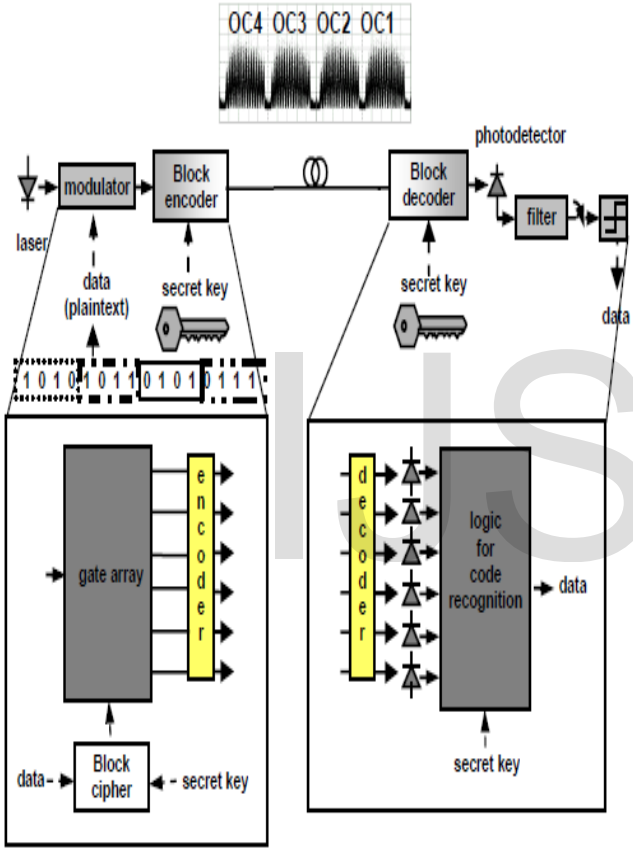

Fig 4: Block ciphering method

C. ONE TIME PAD METHOD

This technique requires the use of a pre-shared one-time key which is of the same size as the

plain text. In this method a random secret key is paired with the plaintext by encrypting each bit character of the plain text with the corresponding bit character from the pad using a modular addition. For the key to be impossible to be decrypted by an eavesdropper, it should be of the same length as the plain text, never used in part or full and must be kept completely secrete.

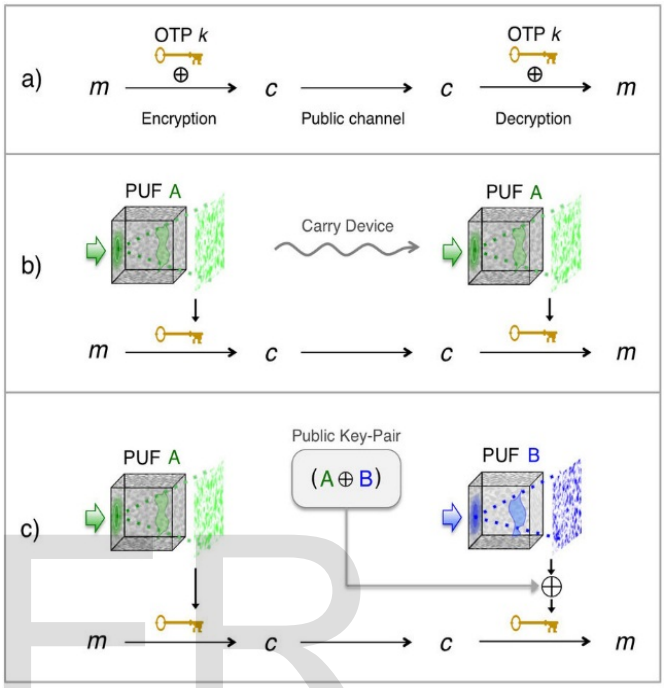

Fig 5: one-time pad application

Authors in [19] described an encrypted communication principle that forms a secure link between two parties without electronically saving the keys but kept the random cryptographic bits safe within a unique mesoscopic randomness of two volumetric scattering material. Figure 5 describes the model designed by in [19]. In diagram (a) an ideally encrypted cipher text was created by using a theoretically perfect OTP mixed binary message m with random digital key k. In diagram (b) the key is stored within a volumetric scatterer's random structure (PUF A). The key be accessed with specifically shaped optical probes but if there is a truly unique and unclonable

volumetric scattering structure then the only way to share the key is via physical transportation which is not practical. Finally, (c) provides unique keys from PUF A and A which is an outcome of a digital XOR which forms an encrypted OTP cipher text itself. This provides a secure communication between them.

IV. FUTURE OPTICAL SECURITY REQUIRED

Security has been a major concern for all telecommunication companies therefore there is a need of devising means of increasing the security of an optical network. Some of the ways of increasing the network security of fiber optics are listed in table 3.

Table 3: Desired future security elements

CATEGORY	DESIRED SECURITY ELEMENT
1. Monitoring	Continuous Real-time Monitoring. Capabilities of differentiating and characterizing optical anomalies. Automatic intrusion detection and shutdown. Automatic re-routing to redundant paths.
2. Coding	Advance multi-level coding
3. Encryption	Multiple encryption and decryption application. Advance encryption format.eg AES 256 bits

V. CONCLUSION

A compromised security of a network is like sleeping in a crime zone with an open door at night. Users are hungry for information, therefore there is a need for proper encryption and decryption methods in order to secure a communication network.

This work reviewed the WDM system and surveyed the various confidentiality methods. A future security required for optical system was proposed. This was categorized into three namely monitoring, coding and encryption. A secured network protects the confidentiality of the users.

REFERENCES

[1] Opterna and iDefense, "Threats to fiber-optic Infrastructures", Ablackhat briefing 1-2 October, 2003, pp32.

[2] Bujari S.S., "A survey on simulation of MEMS optical switch for WDM applications", *World Journal of Science and Technology, VOL. 2, NO. 10, pp 39-43,* 2012.

[3] E. GerdKeiser,"A Review of WDM Technology and Applications", *Optical Fiber Technology, VOL. 5, pp 3-39,* 1999.

[4] J. M. Senior & S. D. Cusworth, "Devices for wavelength multiplexing and demultiplexing", *Optoelectronics, IEE Proceedings, VOL. 136, NO. 3, pp 183- 202,* 1989.

[5] WDM the transmodeway :https://www.infinera.com/wpcontent/uploads/2015/09/WDM-

TheTransmodeWay_A.pdf/22-11-2016/12:37

[6] M. M´edard, D. Marquis, R. A. Barry and S. G. Finn, "Security Issues in All-Optical Networks", IEEE Network Magazine, vol. 11, no. 3, pp.42–48, May 1997.

[7] T. Wu and A. K. Somani, "Cross-Talk Attack Monitoring and Localizationin All-Optical Networks," IEEE/ACM Transactions on Networking 13, pp. 1390-1401 (2005).

[8] M. M´edard, D. Marquis, S. R. Chinn, "Attack Detection Methods for All-Optical Networks", in in Proc. of Network and Distributed Systems Security Symposium, Session 3, paper 2, San Diego, California, 1998.

[9] J. K. Patel, S. U. Kim, D. H. Su, S. Subramaniam and H.-A. Choi, "A Framework for Managing Faults and Attacks in WDM Optical Networks," Proc. of the DARPA Information Survivability Conference and Exposition, Anaheim, California 2001.

[10] Fok, M.P., Wang, Z., Deng, Y. &Prucnal, P.R. (2011). Optical Layer Security in Fiber-Optic Networks. *IEEE Transactions on Information Forensics and Security*, Vol. 6, No. 3, (September 2011), pp. (725-736), ISSN 1556-6013

[11] Médard, M., Marquis, D., Barry, R.A. & Finn, S.G. (1997). Security Issues in All-Optical Networks. *IEEE Network*, Vol. 11, No. 3, (May/June 1997), pp. (42-48), ISSN 0890-8044.

[12] K. Shaneman and S. Gray, "Optical network security: Technical analysis of fiber tapping mechanisms and methods for detection & prevention," in *Proc. IEEE Military Communications Conf. (MILCOM)*, 2004, vol. 2, pp. 711–716.

[13] M. Furdek, N. Skorin-Kapov, M. Bosiljevac, and Z. Sipus, "Analysis of crosstalk in optical couplers and associated vulnerabilities," in *Proc.33rd Int. Convention (MIPRO)*, May 2010, pp. 461–466.

[14] C. Gabriella, M. Gianluca, Naaya W. and K. kenichi, "Physical layer security: All optical Cryptography in access network", ICTON 2008, pp. 127-130, 2008.

[15] M. P. Fok and P. R. Prucnal, "All-optical XOR gate with optical feedback using highly Ge-doped nonlinear fiber and a TOAD," *Appl. Opt.*, submitted for publication.

[16] M. P. Fok and P. R. Prucnal, "All-optical encryption based on interleaved waveband switching modulation for optical network security," *Opt. Lett.*, vol. 34, pp. 1315–1317, Apr. 2009.

[17] M. P. Fok and P. R. Prucnal, "Low-latency nonlinear fiber-based approach for data encryption and anti-jamming in optical network," presented at the 2008 IEEE/LEOS AnnualMeeting, Newport Beach, U.S., Nov. 2008, Paper ThG 3.

[18] Z. Wang, A. Chowdhury, and P. R. Prucnal, "Optical CDMA code wavelength conversion using PPLN to improve transmission security," *IEEE*

Photon. Technol. Lett., vol. 21, no. 6, pp. 383–385, Mar. 15, 2009.

[19] R. Horstmeyer, B. Judkewitz and C. Yang, " Physical key-Protected one-time pad", scientific reports 3, article no. 3543(2013), doi:10.1038/srep 03543, Dec. 18,2013.