4-25-2011

# Optical encryption as a function of polarization in optical fiber communications

Syed H. Murshid

Hari Priya Muralikrishnan

Jayachandran Tamilarasan

Abhijit Chakravarty

John H. Caulfield

# Optical encryption as a function of polarization in optical fiber communications

Syed H. Murshid[1], Hari Priya Muralikrishnan[1], Jayachandran Tamilarasan[1], Abhijit Chakravarty[1] and H. John Caulfield[2, 3]
[1]Optronics Laboratory,
Department of Electrical and Computer Engineering,
Florida Institute of Technology, 150 W. University Blvd., Melbourne, Fl 32901
[2]Department of Physics, Alabama A&M University, AL 35762
[3]Diversified Research Corp., TN 37047

## ABSTRACT

An optical encryption technique based on polarization property of light is proposed. Many techniques using polarization beam splitters to encrypt the signal have been proposed earlier. They are based on splitting and interference of two light signals, namely message and noise. Only by placing suitable mirrors and a second beam splitter in a suitable position, the two signals are reconstructed at the output. In this paper we report the fiber optic version of a polarization based encryption technique that also has the potential to double the data carrying capacity of the fiber. Using polarization dependent couplers in the fiber optic cables, we are able to achieve encryption of the light signal. Theoretical analysis and simulated results are also presented.

**Keywords:** Encryption, Polarization, Couplers, Fiber Optic communication

## INTRODUCTION

Security and authentication of data in fiber optic communication systems has always been one of the important areas of research. Encryption and decryption usually involves a special key, known only to the user, to encode the data[1]. However there has been significant interest in securing data through physical layer encryption and Matoba et al [2,3] have shown an interesting method of encryption by employing double random phase encryption where the signal is masked and converted into a noise like data. Similarly Javidi et al [4,5] have shown that a signal can be encrypted using a polarization encoded mask. Spatial domain multiplexing [6-10] is another recent technique that can be used for physical layer encryption through spatial mode hopping of optical channels of the same wave length inside optical fibers. Sylman et al [11] have recently demonstrated an entanglement based method for optical encryption and decryption, where an intelligent message is allowed to mix with noise and travel in free space.

Along with frequency, polarization is a property of light that largely remains unchanged while propagating significant distances through the atmosphere. Consequently there have been many successful endeavors in the past to exploit the horizontal and vertical polarizations of coherent light beams to push the bandwidth of single mode optical fibers. Therefore it is natural and straightforward to send two polarization states through multimode fibers and reconstitute the phase relationship at the remote receiver location before detection.

In this manuscript, we present an extension of polarization based encryption technique shown by Sylman et al, to optical fibers. It does not involve any encryption or decryption keys. Instead, it uses polarization property of light to allow secure data communication over an optical fiber. A simple approach has been adopted in this method to physically encrypt light signals using unique polarization keys before sending it over a fiber. Two light signals of different polarizations are mixed using couplers for encryption. Matching couplers and polarizers can be used at the decryption side to split the signals and reconstruct the original data. Figure 1 shows the block diagram of this system. Simulation results using Optisystem [12] show that only by proper alignment of the second polarizer, the original signal can be reconstructed. As a result the security of the signal can be greatly increased.

Enabling Photonics Technologies for Defense, Security, and Aerospace Applications VII, edited by Michael J. Hayduk, Peter J. Delfyett, Jr., Proc. of SPIE Vol. 8054, 80540M · © 2011 SPIE · CCC code: 0277-786X/11/$18 · doi: 10.1117/12.884426

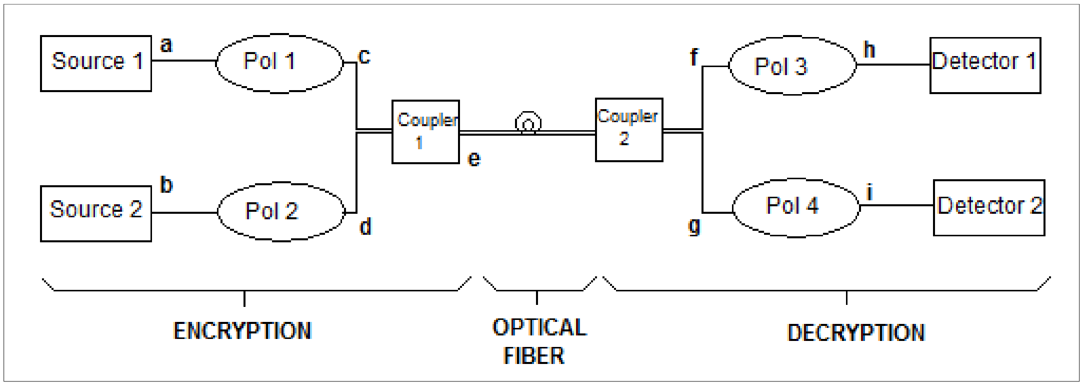


**Fig 1: Block Diagram of the system showing Encryption and Decryption**

# 1. ENCRYPTION

The Encryption model of this technique is designed using linear polarizers and directional couplers. The polarizers are used to linearly polarize the light beam at a given angle 'θ'. Combination of two or more linear polarizers can be used for better confinement of light to a particular angle. Figure 1 shows that two light signals, source 1 and source 2 are linearly polarized and then combined using a 2x2 coupler. By properly adjusting the coupling coefficients of the couplers, maximum output at the first output branch can be obtained. This signal is then sent over a fiber of desired length. We attenuate the output from the second branch of the coupler to minimize reflections; hence this branch can be ignored.

# 2. DECRYPTION

At the receiver side the signal is split from the fiber by using a 2x2 coupler with a 3dB split ratio. To decrypt the signals linear polarizers of suitable angle are used. The angle $\theta_3$ of polarizer 3, which is used to achieve decryption of the signal, depends on parameters including $\theta_1$, $\theta_2$ and length of the fiber.

# 3. SYSTEM ANALYSIS

Jones vectors and Jones matrices [13] can be used for the analysis of the polarization based optical fiber encryption and decryption system.

## 3.1 Encryption

Sylman et al [11] have shown the analysis of an optical interferometer based system [14] for optical entanglement in free space by taking two signals; a message input and a noise input

$$\text{Input 1}=\begin{bmatrix} a_1 \\ a_2 \end{bmatrix}, \text{Input 2}=\begin{bmatrix} b_1 \\ b_2 \end{bmatrix}$$

The two signals are mixed after passing through the beam splitter and are analyzed [15]:

$$\text{Output 1 from first polarization beam splitter} = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}\begin{bmatrix} a_1 \\ a_2 \end{bmatrix} + \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} b_1 \\ b_2 \end{bmatrix} = \begin{bmatrix} a_1 \\ b_2 \end{bmatrix} \quad (1)$$

$$\text{Output 2 from first polarization beam splitter} = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} a_1 \\ a_2 \end{bmatrix} + \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}\begin{bmatrix} b_1 \\ b_2 \end{bmatrix} = \begin{bmatrix} b_1 \\ a_2 \end{bmatrix} \quad (2)$$

For our application in fiber optic communications we apply the boundary conditions of the optical fiber and utilize the Jones matrix given by the Optisystem software. The Jones Matrices of the coupler and linear polarizer are as follows

$$\text{Coupler: } C = \alpha_1 \begin{bmatrix} \sqrt{1-c_1} & j\sqrt{c_1} \\ j\sqrt{c_1} & \sqrt{1-c_1} \end{bmatrix},$$

$$\text{Linear polarizer: } P = \begin{bmatrix} cos^2\theta & \cos(\theta)\sin(\theta) \\ \cos(\theta)\sin(\theta) & sin^2\theta \end{bmatrix}$$

### 3.2 Decryption

Decryption of the original signals is done using appropriate polarization beam splitter at the output as follows:

$$\text{Reconstruction of input 1} = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} a_1 \\ b_2 \end{bmatrix} + \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} b_1 \\ a_2 \end{bmatrix} = \begin{bmatrix} a_1 \\ a_2 \end{bmatrix} \qquad (3)$$

$$\text{Reconstruction of input 2} = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} a_1 \\ b_2 \end{bmatrix} + \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} b_1 \\ a_2 \end{bmatrix} = \begin{bmatrix} b_1 \\ b_2 \end{bmatrix} \qquad (4)$$

The fiber optic version of the model shows that only specific values of the linear polarizers can provide the desired decryption of the signals.

## 4. SIMULATED RESULTS

The simulation setup of the polarization based encryption and decryption system is shown in figure 2. The input signal is shown in figure 3 and the corresponding output is shown in figure 4.

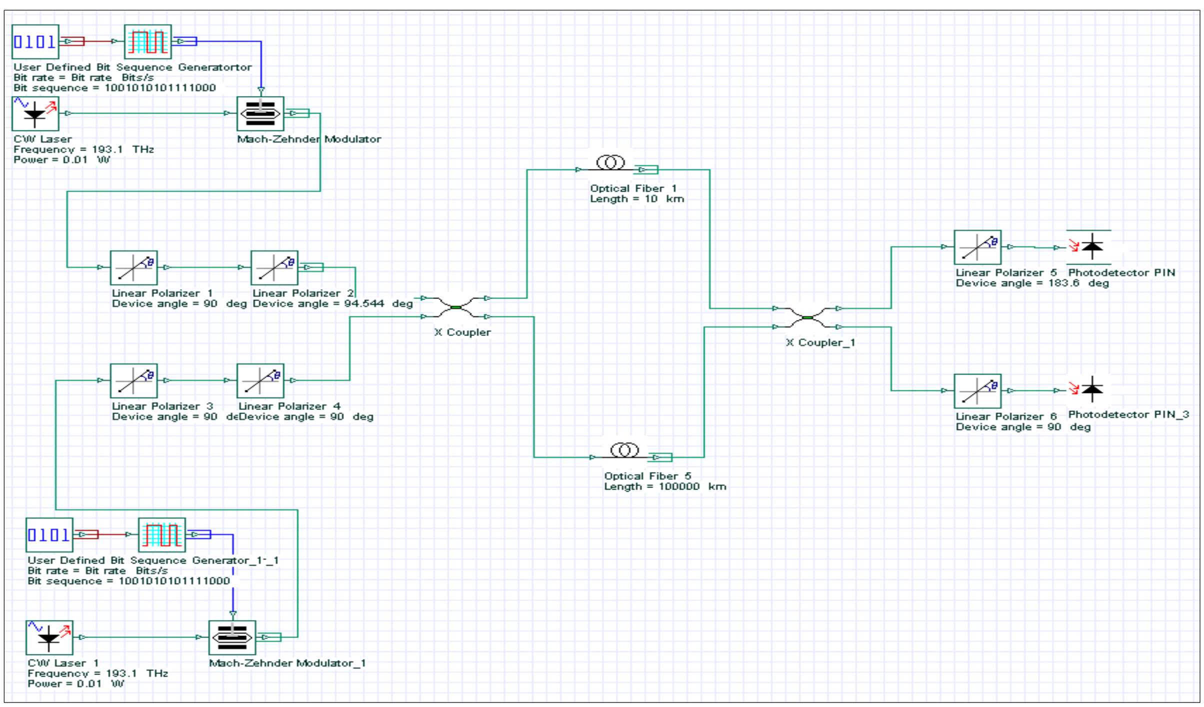


**Figure 2: Simulation setup of the system, Encryption and Decryption**

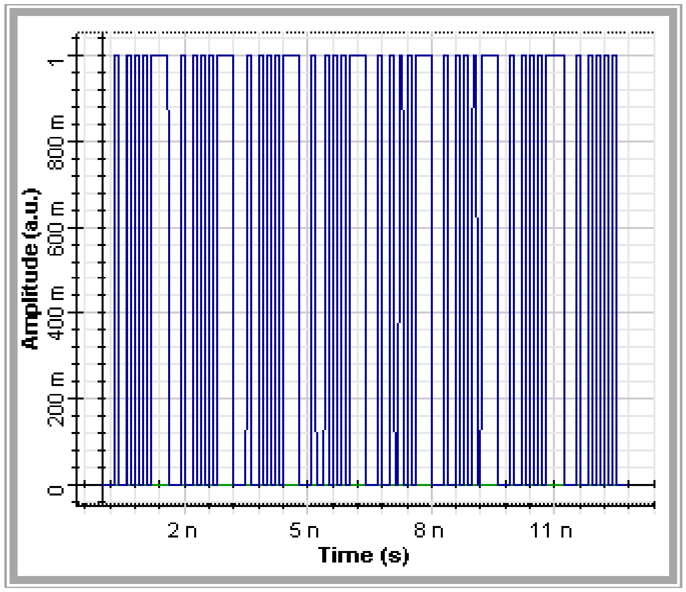


**Figure 3: Graph showing input signal 1**

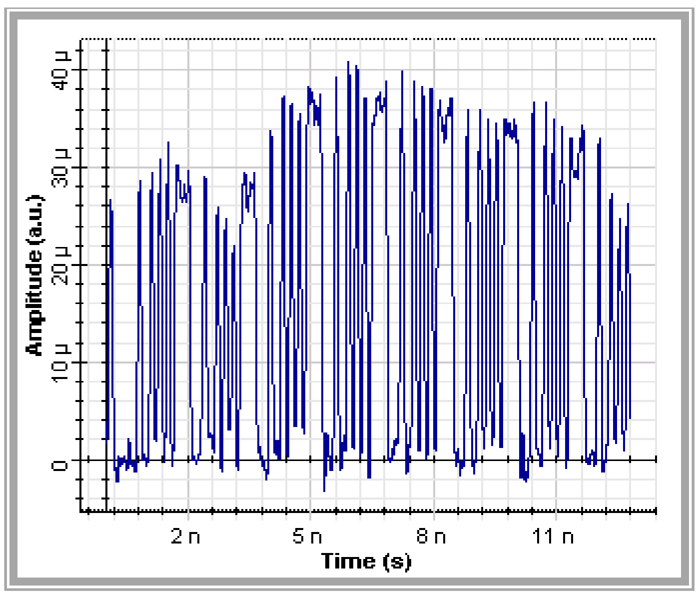


**Figure 4: Graph showing output signal 1 after decryption**

The table 1 shows the typical polarization values that can be used for successful encryption and decryption of signals in optical fibers. It also shows that only for a small range of values of $\theta_3$ the original signal is reconstructed with a Bit Error Ratio (BER) of $10^{-9}$. For all other values of $\theta_{3,}$ the BER was of the order of $10^{-5}$ or worse, thus proving that a message can only be successfully decrypted by employing proper output polarizer at the detector end of the system. The range of the angle values is currently being investigated and the model [16,17] is being refined. We plan to experimentally verify these results in the near future. Table 2 shows that two independent messages of differing polarizations $\theta_1$ and $\theta_2$ can be mixed together to encrypt them and decryption can only be achieved by using polarizers of specific range of angles given by $\theta_3$ and $\theta_{4.}$ As a result the two messages are not only encrypted but the bandwidth of the channel can also be effectively doubled.

**Table 1: The linear polarizers' example angle values that produce correct encryption and decryption for input 1**

| $\theta_1$ (i) | $\theta_1$ (ii) | $\theta_2$ (i) | $\theta_2$ (ii) | $\theta_3$ | $\theta_4$ |
|---|---|---|---|---|---|
| $90^o$ | $94.544^o$ | $90^o$ | $90^o$ | $183.6\text{-}183.7^o$ | $90^o$ |

**Table 2: Range of polarization angles that provide encryption/decryption of both inputs thus doubling bandwidth**

| $\theta_1$ | $\theta_2$ | $\theta_3$ | $\theta_4$ |
|---|---|---|---|
| 85 | 93 | 171-178 | 172-177 |

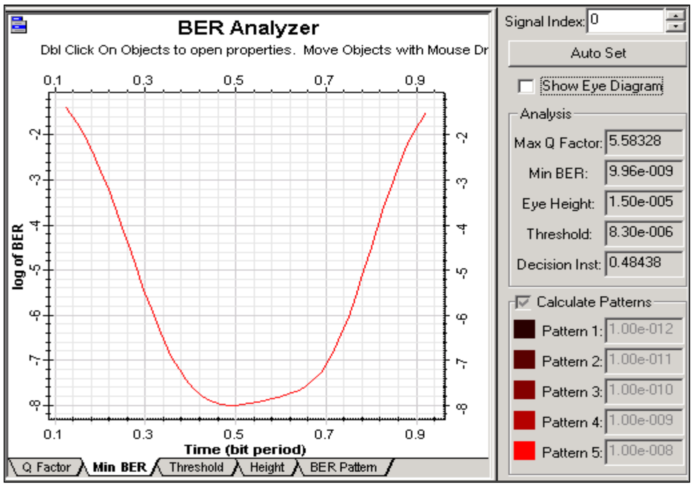


**Figure 5: Graph showing BER of $10^{-9}$ of the output signal for the mentioned angle values**

## 5. CONCLUSION

We have presented a technique for encrypting a light signal to be sent over a fiber link as a function of polarization. Simulated results and analysis of such systems have been presented. The result show that this system can be used for physical layer security and encryption of signals in optical fiber without using encryption and decryption keys. Furthermore the bandwidth of the system can also be doubled by using this technique. Currently we are designing experiment to implement this method in hardware with the help of appropriate polarizers and polarization dependant couplers.

## 6. REFERENCES


[1] W. Diffie and M. Hellman, "New Directions in Cryptography," IEEE Transactions on Information Theory 22, 644–654 (1976).

[2] O. Matoba, T. Nomura, E. Pe´rez-Cabre´, M. S. Milla´n, and B. Javidi, "Optical Techniques for Information Security," Proc. IEEE 97, 1128-1148 (2009).

[3]O. Matoba and B. Javidi, "Secure holographic memory by double random polarization encryption," Appl. Opt. **43**, 2915–2919, (2004).

[4] B. Javidi and T. Nomura, "Polarization encoding for optical security systems," Opt. Eng. **9**, 2439–2443, (2000).

[5] O. Matoba and B. Javidi, "Encrypted optical storage with wavelength-key and random phase codes," Appl. Opt. **38**,

[6] S. Murshid, B. Grossman, and P. Narakorn, Spatial domain multiplexing: a new dimension in fiber optic multiplexing, Journal of Optics and Laser Technology, 40(8), 10301036, November (2008).

[7] S. H. Murshid and J. Iqbal, Concentric octagonal CMOS photodiodes for direct detection of spatially multiplexed optical fiber channels, presented at Frontiers in Optics (FiO) 2008/Laser Science XXIV (LS) Conf. FiO/LS, OSA

Technical Digest (CD) (Optical Society of America), paper FTuU6, October 2008 Rochester, New York, Laurin Publishing, Pittsfield, MA (2008).
[8] S. Murshid, A. Chakravarty, and R. Biswas, Spatially multiplexed beam combining and beam separator modules for optical communication bandwidth enhancement, 8th IASTED Intl. Conf. Wireless Opt. Communi., WOC 621133 (2008).
[9] S. Murshid and A. Chakravarty, Experimental results from copropagating analog channels of same wavelength over 600-meter-long standard step index multimode fiber SPIE Journal of Optical Engineering, Opt. Eng. 47, 105002, October (2008).
[10] S. Murshid, A. Chakravarty, and R. Biswas, Attenuation and Modal Dispersion Models for Spatially Multiplexed Co-Propagating Helical Optical Channels in Step Index Fibers. Journal of Optics and Laser Technology, available online 6 August 2010, pp430-436, 43 (2011).
[11] David Sylman, Zeev Zalevsky, and H. John Caulfield Entanglement based Optical Transient Encryption, Optics Communications 2010, Volume 283, Issue 23, p. 4551-4557.
[12] www.optiwave.com
[13] Jan Bechtle, Gert F. Trommer, S-matrix representation of polarization dependent fiber optic couplers for the simulation of optical networks, Workshop on Fibres and Optical Passive Components, 2005. Proceedings of 2005 IEEE/LEOS, 192 – 197, 2005.
[14] TRATNIK, Jurij, BATAGELJ, Boštjan. “Fiber interferometric communications using Mach-Zehnder interferometer topology”. V: Eurocon 2009 : proceedings. Piscataway: IEEE, cop. 2009, str. 1725-1730.
6785–6790, (1999).
[15] E. Hecht, Optics, 4th ed., Pearson Education, Singapore, (2006).
[16] Anthony VanderLugt, Optical Signal Processing,, 2nd ed, WILEY Series in pure and applied optics, USA (2005)
[17] S.O.Kasap, Optoelectronics and Photonics Principles and Practices, 1st ed, Prentice Hall USA (2001)