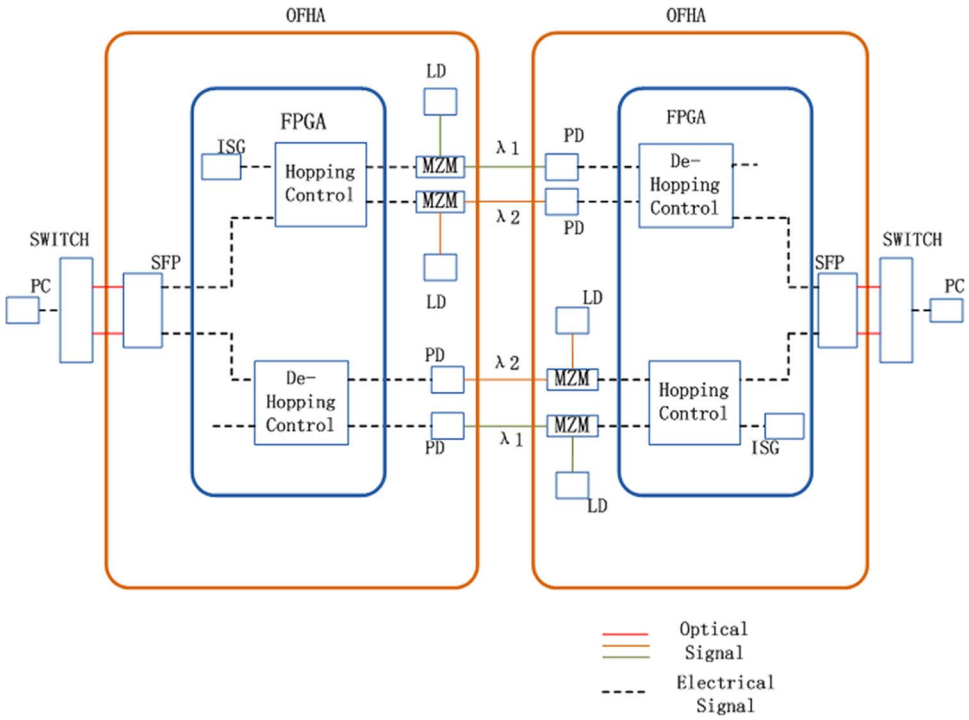
IEEE Photonics Journal
An IEEE Photonics Society Publication

Open Access

A Novel Optical Frequency-Hopping Scheme for Secure WDM Optical Communications

Volume 7, Number 3, June 2015

Sun Long Wang
Wei Chen
Ning Hua Zhu, Member, IEEE
Jian Guo Liu
Wen Ting Wang
Jin Jin Guo



DOI: 10.1109/JPHOT.2015.2429635
1943-0655 © 2015 IEEE

A Novel Optical Frequency-Hopping Scheme for Secure WDM Optical Communications

Sun Long Wang, Wei Chen, Ning Hua Zhu, *Member, IEEE*, Jian Guo Liu, Wen Ting Wang, and Jin Jin Guo

State Key Laboratory on Integrated Optoelectronics, Institute of Semiconductors, Chinese Academy of Sciences, Beijing 100083, China

DOI: 10.1109/JPHOT.2015.2429635
1943-0655 © 2015 IEEE. Translations and content mining are permitted for academic research only. Personal use is also permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.

Manuscript received March 24, 2015; revised April 29, 2015; accepted April 30, 2015. Date of publication May 6, 2015; date of current version May 15, 2015. This work was supported by the National Natural Science Foundation of China under Grant 61405187. Corresponding author: W. Chen (e-mail: wchen@semi.ac.cn).

Abstract: A novel optical frequency-hopping scheme in wavelength-division multiplexing (WDM) systems is proposed to achieve secure communications with high capacity. Frequency hopping is realized by the hopping of digital signals among different channels. In the proposed system, the signal from any source is separated into small segments in the time domain, and the segments are carried by more than one different-wavelength optical carrier. All the optical waves in the proposed WDM system are modulated by signals from two or more sources at different times. The signal from a certain source is also interference to signals from other sources. Hopping, synchronization, de-hopping, and routing are all digitally implemented in field-programmable gate array chips. The system is reconfigurable by software to adapt to different rates. Slow frequency hopping, fast frequency hopping, and intermediate frequency hopping are all available. A demonstration system is designed to support transmission speed from 0 to 10 Gb/s, and a video communication based on it is built to demonstrate the 1-Gb/s optical frequency-hopping system.

Index Terms: Optical frequency hopping, wavelength division multiplexing, secure communication.

1. Introduction

Wavelength division multiplexing (WDM) technology which is proposed to increase the capacity and bandwidth of optical communication has been employed in many applications such as WDM radio over fiber (WDM-RoF) and WDM passive optical network (WDM-PON) [1], [2]. By transmitting simultaneously multiple high speed signals on the different-wavelength optical carriers, the tremendous bandwidth of optical fibers is exploited [3], [4]. However, with hundreds of gigabits per second being transmitted in a single fiber over long distance, the security of transmission has become an indispensable issue [5]. The signals in the fibers can be eavesdropped by fiber tapping which is based on fiber optical techniques such as bending, splitting, evanescent coupling, etc. [6]. Therefore, it is necessary to encrypt the data being transmitted. Traditional solutions are to encrypt the communicating data by software before transmission. In these ways security relies on the computation complexity and the basic structures of data stream in

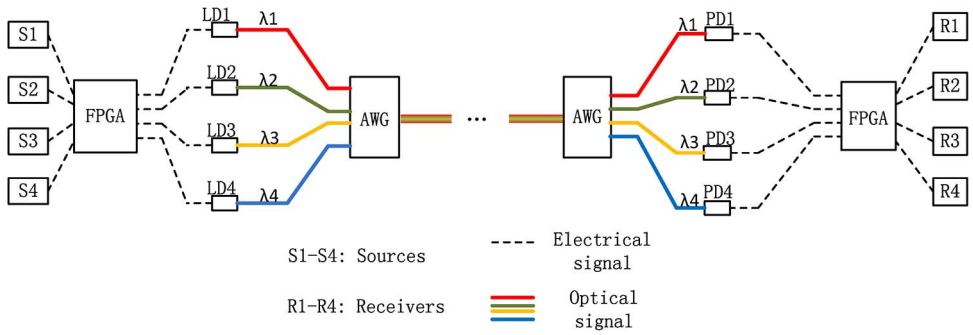


Fig. 1. Architectural principle of the frequency-hopping WDM optical communication system. LD1–LD4 are unique wavelength lasers with modulators. AWG is short for Arrayed Waveguide Grating. PD1–PD4 are Photoelectric Detectors. FPGA is short for Field Programmable Gate Array.

the transmission fibers are not destroyed [7], [8]. The eavesdropper can get enough frame information and recover the original structures with the help of the fast developing cryptanalysis techniques [8]. Recently, hardware-based encryption on the physical layer has attracted much attention. One typical example is the chaotic optical communication where signals are embedded in chaotic carriers. Nevertheless, chaotic synchronization is difficult in long-distance fiber communications [4].

Optical frequency hopping is another hardware-based encryption technique to protect optical signals from being eavesdropped effectively. In an optical frequency hopping system, the carrier of a certain signal is hopping among N frequencies rapidly and randomly, stopping the eavesdroppers from obtaining coherent data. In the wireless communication area, frequency hopping is carried out in a frequency synthesizer, which is to generate microwaves with different frequency in electrical circuits. In the optical communications, however, the frequency shifting is not so easy because changing the wavelength of a laser needs a period of time which is not very short. For the tunable lasers, a tuning time of < 100 ns is very difficult to realize [9], [10]. Others ways are using passive optical components such as Bragging gratings to select certain wavelengths [11], [12], but tuning the optical components is slow and not flexible. In addition, during frequency switching, there is a transient state that may be captured and that will decrease the security of the system [13]. As another spread spectrum technology, optical code division multiple access (OCDMA) technology has been widely discussed for security transmission for its noise-like waveforms of optical signals. However, it has been proven by investigations that the signal can be eavesdropped using energy detectors [14].

In this paper, we have proposed a novel “passive hopping” scheme in WDM systems, which means to make the signals hop among different carriers rapidly while the carriers are kept stable. The effect is the same as optical frequency hopping. The signals in a FPGA chip are able to shift from one channel to another at a high rate, and the tuning time or transient state can be neglected. Hopping rate higher than bit rate is possible. The system security is improved because any signal from a certain source is also interference to other signals in the WDM system. We have also built an experimental demonstration system to verify the feasibility of this scheme. In the proposed scheme, frequency hopping with high rates which is generally discussed in the wireless communications is realized in the optical systems. And the scheme has firstly introduced frequency hopping among multiple optical carriers in WDM systems for signal encryption on the physical layer to enhance the security of communication.

2. Principle

The general architecture of the WDM system is a $N \times N$ network with N wavelengths [15]. Fig. 1 shows a 4×4 frequency hopping WDM optical communication system with four wavelengths. The signal from any source is hopping among the four channels according to a noise-like sequence such as pseudorandom sequences [16] and is equal to the carrier for a certain

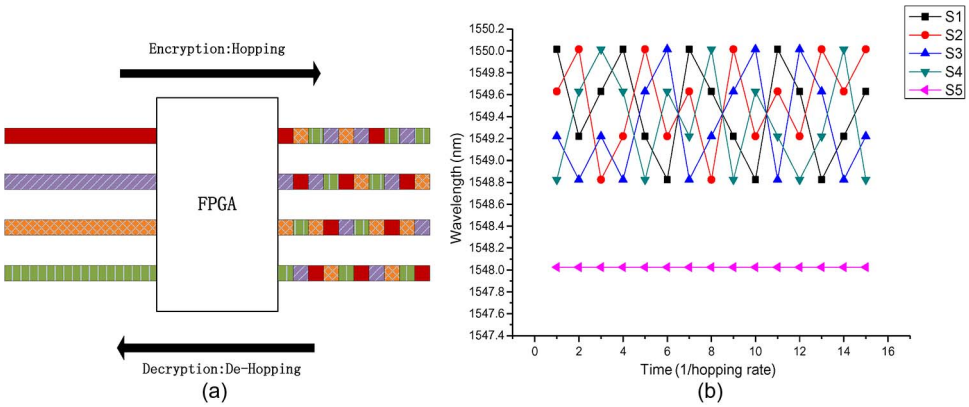


Fig. 2. Process of frequency hopping. (a) Signal being processed in the FPGA chip. (b) Wavelengths of the carriers for $S1-S5$ changes with time.

signal hopping among four wavelengths. The noise-like sequence is the key for data encryption. On the receiver side, the same key is necessary to select the distributed segments from the four channels and recover them into a complete signal. The FPGA chip is the core for encryption, where the signals are separated into segments and distributed into multiple channels. It is also the center for decryption and routing, where reconstructing the segments together as effective signals and sending them to the correct receivers are finished. In the transmission fiber, there are four optical waves carrying signal segments from the four sources. The signal from one source also plays a role as an interference signal to the signals from other sources. Therefore, the eavesdropper cannot obtain the effective and complete signal.

2.1. Hopping Process

The hopping and de-hopping process are both finished in a FPGA chip, as shown in Fig. 2(a). On the transmitter side, the signals from $S1-S4$ are separated into small segments in the FPGA chip. The segments are mixed together, forming four new signals. The de-hopping process on the receiver side is just the inverse process. For a 4×4 network with four wavelengths, there are 24 possibilities for each hopping, and for a $N \times N$ network with N wavelengths, the possibilities is $N!$. With the value of N increases, the uncertainty of hopping pattern increases, and so does the security of the system. The total possibility in a transmission can be expressed as

$$P = N! \times A \times \frac{R_h}{R_b} \tag{1}$$

where N is the number of wavelengths, A is the communication amount in the form of bits, R_h is the hopping rate and R_b is the bit rate. From (1), we can see that in a certain communication system with a unique bit rate, the possibility increases with the number of wavelengths and the hopping rate. Therefore, the system security can be enhanced by adding wavelengths or raising the hopping rate.

For each signal, the optical carrier is changing with time, as showed in Fig. 2(b). $S1-S4$ are the four signals in a 4×4 network, the wavelengths of their carriers are changing among four values, and $S5$ is a signal in a normal optical communication system, carried by a single optical carrier with a stable wavelength.

2.2. Synchronization and Routing

Synchronization between the transmitter and the receiver is the first and also the most important step for signal decryption. It mainly contains two aspects for the receiver: using the same pseudorandom sequence as the transmitter and capturing the first bit of the hopped signals. To realize synchronization, a “Header” is inserted to the beginning of the hopped signals, as shown

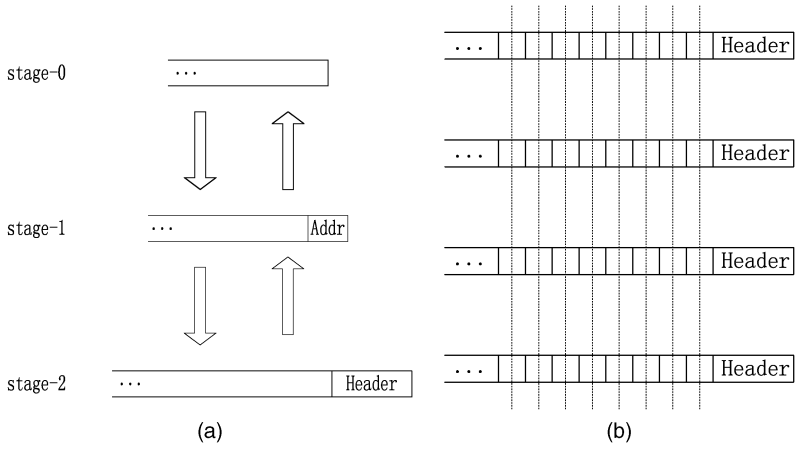


Fig. 3. (a) Changes of signal from one source in the FPGA chip. (b) Signal synchronization according to the header.

in Fig. 3(a). In traditional WDM communications, wavelength is regarded as the routing information [15]. In the proposed frequency hopping system, however, wavelengths are used for encryption. Therefore, an "Addr" is added to the beginning of the signal before hopping, as shown in Fig. 3(a).

As illustrated in Fig. 3(a), the communicating signal experiences three stages in the FPGA chip. In stage-0, it is a pure signal from the source. Then, in stage-1, a certain data segment which contains the information of destination address will be added to the head of the signal. Finally, after the process of frequency hopping, another segment will be added to the start of the four channels, as shown in Fig. 3(a). The Header contains the information of the pseudorandom sequence and a certain sequence for the receiver to distinguish. On the transmitter side, the signal turns from stage-0 to stage-2 and on the receiver side, from stage-2 to stage-0.

During communication, the receiver FPGA chip keeps searching until the Header arrived. The segment following the Header must be the first hopping segment. The phase of the four signals can be locked because all hopping segments are of equal length, as shown in Fig. 3(b). The correct pseudorandom sequence will be selected for de-hopping according to the information in the Header. After de-hopping, the four signals are transmitted to the correct destination receivers according to the information in the Addr.

There is a buffer module in the FPGA chip to align the signals in different channels. Channel delay less than 1 ms will not affect the synchronization. The delay caused by the chromatic dispersion of the transmission fiber can be expressed as

$$\Delta t = D \times \Delta\lambda \times L \tag{2}$$

where Δt is the delay time, D is the dispersion coefficient of optical fiber, $\Delta\lambda$ is the difference of wavelength and L is the transmission distance. If the value of D is 17 $\mathrm{ps}/(\mathrm{nm} * \mathrm{km})$, the wavelength difference is 1.6 nm and the transmission distance is 1000 km, we can get that the delay time is 27.2 ns. Therefore, the channel delay caused by the chromatic dispersion of the transmission fiber doesn't affect the synchronization.

2.3. Hopping Rate

According to the relative value of hopping rate to signal bit rate, there are three kinds of frequency hopping systems: slow frequency hopping (SFH), fast frequency hopping (FFH), and intermediate frequency hopping (IFH) [17]. In a slow frequency hopping system, the hopping rate is lower than the signal bit rate. During the time between two hops, more than one bits are transmitted at the same frequency. In a fast frequency hopping system, the frequency hopping rate is higher than the signal bit rate which means the signal on a certain frequency carrier lasts

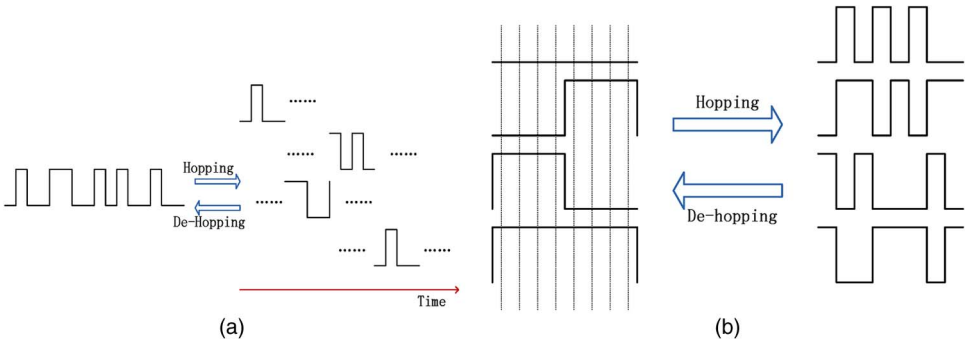


Fig. 4. Electrical waveforms before and after hopping. (a) Hopping rate lower than bit rate. (b) Hopping rate higher than bit rate.

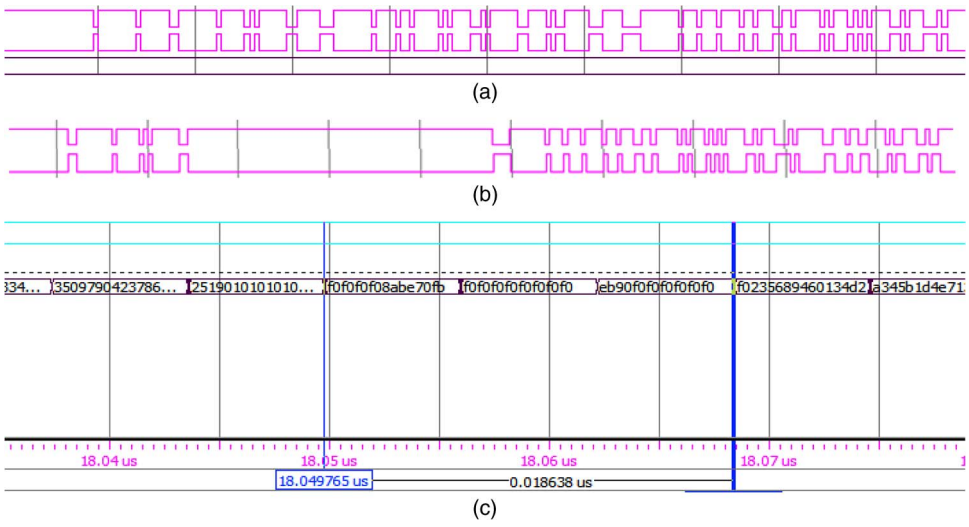


Fig. 5. FPGA simulation waveforms of (a) original digital signals, (b) digital signals after encryption, and (c) header of the signal after encryption.

shorter than a bit period time. In this case, one bit is transmitted at two or more frequencies. In the intermediate frequency hopping system, the hopping rate is equal to bit rate.

Fig. 4(a) shows a slow frequency hopping waveform. The signal changes channels every four bits. The bit rate is four times the hopping rate. Fast frequency hopping is also possible in the proposed system. In Fig. 4(b), the hopping rate is four times the bit rate. To achieve fast frequency hopping, the sampling rate in the FPGA chip must be higher than the bit rate. For example, by setting sampling rate at 10 Gb/s, a fast frequency hopping system is achieved for the 2.5 Gb/s communication. As we can see in Fig. 4, the uncertainty of communication or the security of the system increases with the hopping rate. However, the requirement for the property of the FPGA chip also increases.

3. Simulation and Experimental Results

In the proposed frequency hopping system, the FPGA chip is the control center for both data encryption and decryption, mainly containing hopping channelize, synchronization, de-hopping channelize, and routing. We selected a Kintex 7 FPGA from Xilinx Inc. to build a demonstration system.

Fig. 5 is three waveforms of the simulation results with a bit rate of 10.3125 Gb/s. Fig. 5(a) is one of the channels of the original signals, and Fig. 5(b) is one of the channels of the encrypted

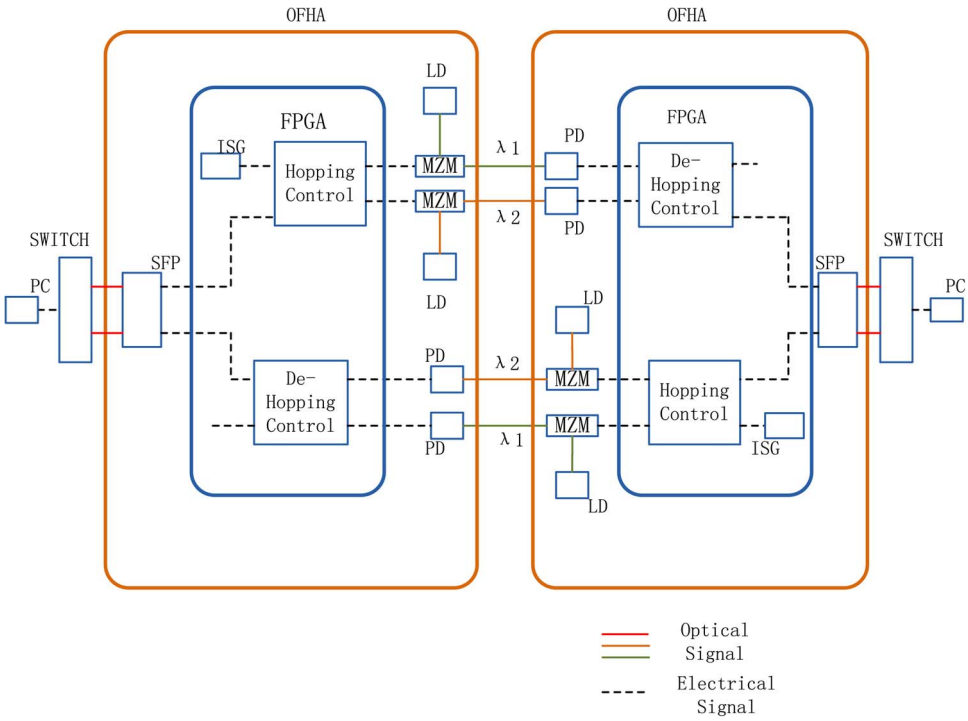
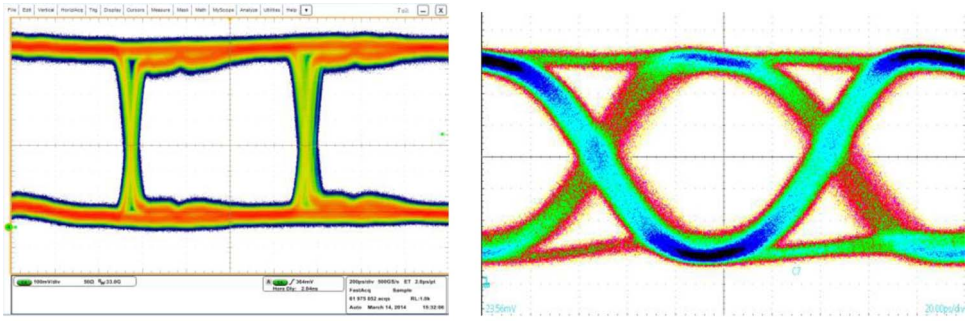


Fig. 6. Principle of the experimental demonstration system. PC: Personal Computer; SFP: Small Form-factor Pluggable; ISG: Interference Signal Generator; FPGA: Field Programmable Gate Array; MZM: Mach-Zehnder Modulator; PD: Photo-Detector; LD: Laser Diode; OFHA: Optical Frequency Hopping Apparatus.

signals, and both of them are in the forms of differential signal pairs. Fig. 5(c) shows the Header inserted into the encrypted data which is a sequence of 192 bits with a last time of about 0.018638 us. The header contains the information for synchronous detection and decryption key.

The principle of the experimental demonstration system is illustrated in Fig. 6. It is a 2 $\times$ 2 frequency hopping WDM system with two wavelengths. Two personal computers (PCs) and two interference signal generators (ISGs) make up the four sources. The ISG is a module in the FPGA chip which sends out interference signals as an electrical transmitter does. Two optical switches are used to achieve photo-to-electric and electric-to-photo conversions between the PCs and the optical frequency hopping apparatuses (OFHAs). The OFHA is a specially designed apparatus to realize optical frequency hopping which is mainly made up of a small form-factor pluggable (SFP) optical module, a FPGA chip, two laser diodes (LDs), two photo-detectors (PDs), and two Mach-Zehnder modulators. On the transmitter side, the signal from PC and ISG are mixed together and distributed into two new channels according to a pseudorandom sequence in the Hopping Control module. Two optical waves from two LDs with wavelengths of λ1 and λ2, respectively, are modulated by the two channels of encrypted signals in the two MZMs. On the receiver side, two PDs demodulate the two received optical signals and transmit the electrical signals to the FPGA chip. In the De-Hopping Control module, the two encrypted signals are detected and locked on the basis of the header and then decrypted into two original signals according to the same pseudorandom sequence as the one in the Hopping Control module. The two SFP modules are used to achieve photo-to-electric and electric-to-photo conversions between the switches and the FPGA chips.

The proposed OFHA is designed to support optical communication systems with speed from 0 to about 10 Gb/s. Adjusting the bit rate of the OFHA can be done by changing the FPGA design which is finished in software. Fig. 7(a) is the eye diagram of a 1 Gb/s frequency hopping optical WDM communication system which is obtained by using a external photo-detector (PD)



(a) (b)

Fig. 7. Eye diagrams of (a) 1.25 Gb/s optical signal and (b) 10.3125 Gb/s optical signal.

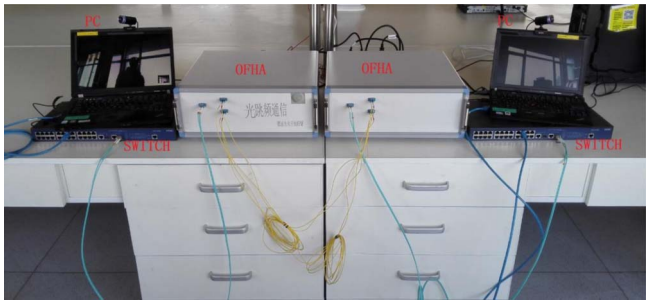


Fig. 8. Experimental demonstration system.

with a bandwidth of 18 GHz and a real-time oscilloscope with a bandwidth of 33 GHz. Fig. 7(b) is the eye diagram of the 10 Gb/s system achieved by using a 18 GHz PD and a 70 GHz sampling oscilloscope. The eye diagrams have verified the bandwidth capacity of the OFHA. It is necessary to explain that most optical communication systems employ the 8B/10B or 64B/66B encoder technique and the result is that the real bit rate in an optical signal is higher than the net system bit rate. For the 1 Gb/s systems, the optical signal bit rate after 8B/10B encoding is 1.25 Gb/s. In the 10 Gb/s systems, the optical signal bit rate after 64B/66B encoding is 10.3125 Gb/s.

Fig. 8 is the 1 Gb/s demonstration system with two PCs, two OFHAs, and two 1 Gb/s optical switches. The signal transmission between the two PCs is demonstrated by a video communication. The signal in each direction of the two is transmitted in two fibers and there are totally four fibers between the two OFHAs. Interruption of any fiber will stop the video communication.

4. Conclusion

We have proposed, analyzed and experimentally demonstrated a novel optical frequency hopping scheme in WDM systems to achieve secure communications. Frequency hopping is realized by the signal hopping among different channels. In the proposed system, the signal from any source is separated into small segments in the time domain and the segments are carried by more than one different-wavelength optical carriers. All the optical waves in the proposed WDM system are modulated by signals from two or more sources at different time. Hopping control, synchronizations, de-hopping control and routing are all implemented digitally in FPGA chips. The system is reconfigurable by software to adapt to different bit rates and hopping rates. SFH, FFH and IFH are all possible. The demonstration system is designed to support transmission speed from 0 to 10 Gb/s and that has been verified by the signal eye diagrams. A video communication has been built to demonstrate the 1 Gb/s optical frequency hopping system. In the proposed system, signals are encrypted and decrypted on the physical layer, and it is protocol-transparent.

References

[1] C. Zhang *et al.*, "A full-duplex WDM-RoF system based on tunable optical frequency comb generator," *Opt. Commun.*, vol. 334, pp. 65–70, Jun. 2015.

[2] S.-G. Mun, E.-G. Lee, J. H. Lee, S. S. Lee, and J. C. Lee, "Wavelength initialization employing wavelength recognition scheme in WDM-PON based on tunable lasers," *Opt. Fiber Technol.*, vol. 21, pp. 141–145, Jan. 2015.

[3] M. Guy, B. Villeneuve, M. Svilans, and N. Cyr, "Optical frequency control for DWDM networks using sum-frequency generation in multilayer waveguides," *IEEE Photon. Technol. Lett.*, vol. 6, no. 3, pp. 453–456, Mar. 1994.

[4] Q. Zhao and H. Yin, "Performance analysis of dense wavelength division multiplexing secure communications with multiple chaotic optical channels," *Opt. Commun.*, vol. 285, no. 5, pp. 693–698, Mar. 2012.

[5] K. Ghoumid *et al.*, "Tunable filter based on cavity electro-optic modulation for DWDM applications," *Opt. Commun.*, vol. 334, pp. 332–335, Jan. 2015.

[6] S. Keith and G. Stuart, "Optical network security: Technical analysis of fiber tapping mechanism and methods for detection and prevention," in *Proc. IEEE Mil. Commun. Conf.*, 2004, pp. 711–716.

[7] L. Yi *et al.*, "Secure optical communication using stimulated Brillouin scattering in optical fiber," *Opt. Commun.*, vol. 290, pp. 146–151, Mar. 2013.

[8] S. Su, J. Zhou, Z. Huang, Y. Zhang, and Z. Zuo, "A secure transmission scheme on link level for optical fiber communication systems," *Optik*, vol. 125, no. 19, pp. 5647–5650, Oct. 2014.

[9] N. Zhu *et al.*, "The improved wavelength coded optical time domain reflectometry based on the optical switch," *Opt. Exp.*, vol. 22, no. 12, pp. 15 111–15 117, Jun. 2014.

[10] J. Buus and E. J. Murphy, "Tunable lasers in optical networks," *J. Lightw. Technol.*, vol. 24, no. 1, pp. 5–11, Jan. 2006.

[11] H. Fathallah, L. A. Rusch, and S. LaRochelle, "Passive optical fast frequency-hop CDMA communications system," *J. Lightw. Technol.*, vol. 17, no. 3, pp. 397–405, Mar. 1999.

[12] D. Benhaddou, G. Chaudhry, and R. J. Runser, "Design and scalability analysis of a fast-frequency-hopping optical CDMA switch architecture," *J. Opt. Netw.*, vol. 3, no. 9, pp. 694–706, Sep. 2004.

[13] Y. Yuan, Z. Huang, and X. Wang, "Detection of frequency-hopping radio frequency-switch transients," *Electron. Lett.*, vol. 50, no. 13, pp. 956–957, Jun. 2014.

[14] D. E. Leaird, Z. Jiang, and A. M. Weiner, "Experimental investigation of security issues in OCDMA: A code-switching scheme," *Electron. Lett.*, vol. 41, no. 14, pp. 817–819, Jul. 2005.

[15] C. A. Brackett, "Dense wavelength division multiplexing networks: Principles and applications," *IEEE J. Sel. Areas Commun.*, vol. 8, no. 6, pp. 948–964, Aug. 1990.

[16] X. Chen, F. Harris, and E. Venosa, "Polyphase channelizers for fully digital frequency hopping systems," *Analog Integr. Circuits Signal Process.*, vol. 73, no. 2, pp. 517–530, Nov. 2012.

[17] A. Yahya, O. Sidek, and J. Mohamad-Saleh, "Design and develop wireless system using frequency hopping spread spectrum," *Eng. Lett.*, vol. 13, no. 3, pp. 260–267, Nov. 2006.