Optics Communications 290 (2013) 146–151

Contents lists available at SciVerse ScienceDirect

Optics Communications

journal homepage: www.elsevier.com/locate/optcom

Secure optical communication using stimulated Brillouin scattering in optical fiber

Lilin Yi [a,*], Tao Zhang [a], Zhengxuan Li [a], Junhe Zhou [b], Yi Dong [a], Weisheng Hu [a]

[a] State Key Laboratory of Advanced Optical Communication Systems and Networks, Shanghai Jiao Tong University, Shanghai, China
[b] Department of Electronics Science and Engineering, Tongji University, China

ARTICLE INFO

Article history:
Received 11 June 2012
Received in revised form
6 August 2012
Accepted 9 October 2012
Available online 2 November 2012

Keywords:
Secure
Optical communication
Encryption
Decryption
Stimulated Brillouin scattering

ABSTRACT

We propose to encrypt/decrypt high-speed optical signal using stimulated Brillouin scattering (SBS) effect in optical fiber for the first time. The broadened SBS gain or loss distorts the amplitude and phase of the optical signal so as to realize all-optical encryption. The corresponding SBS loss or gain with the same bandwidth and amplitude recovers the distorted signal to implement optical decryption. The encryption/decryption keys could be the SBS gain amplitude, bandwidth, central wavelength and the spectral shape, which are configurable and can be flexibly controlled by the users. The operation principle of the SBS based encryption and decryption is explained in detail. Complete encryption and error-free decryption for a 10.86-Gb/s on-off-keying signal has been experimentally demonstrated using broadband SBS amplification and absorption. The immunity of the proposed encryption method to the eavesdropper's attack is also analyzed. The SBS based secure optical communication is compatible with the current optical communication systems.

1. Introduction

With the rapid growth of the Internet data flow, secure transmission for the mass important data becomes indispensable, therefore data encryption is necessary. Traditional encryption is based on the software algorithm and the security relies on the computation complexity. Optical encryption which is also called as "hardware" security has attracted much attention recently, where the security is determined by the physical property of the transmitted signal [1]. Chaotic communication is a well-known secure communication way, where a chaotic carrier is generated through laser oscillation by all-optical [2] or electro-optic [3] means, and then the message is embedded in the chaotic carrier to realize data encryption. The noise-like message is recovered from the chaos by chaotic synchronization in receivers, which exactly matches with the transmitters. Chaotic communication has been demonstrated in real world with a data rate up to several Gb/s [4], but a higher data rate is limited by the relaxing oscillation frequency of the laser. Besides, the security is determined by the laser itself rather than the users. Optical steganography transmission was recently proposed as a method of secure transmission over a public optical communication network [5–7], where the optical stealth channel is temporally spread by using dispersion components and then phase-coded using phase masks into a noise-like signal, therefore concealed underneath existing public channels to realize signal security. The security is determined by the dispersion value and the phase mask, which is configurable by the users. But for high-speed data security, an ultra-narrow pulse laser has to be used as the laser source. Therefore both of the encryption methods mentioned above need to use special laser sources, which are not completely compatible with the traditional optical communication systems.

In this paper, we propose a novel optical encryption/decryption method by using the stimulated Brillouin scattering (SBS) effect in optical fiber. 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 could be the SBS gain amplitude, bandwidth and the spectral shape, which are controlled by the users. We explain the principle in detail and experimentally demonstrate the SBS encryption and decryption process for a 10.86-Gb/s non-return-to-zero on-off-keying (NRZ-OOK) data for proof-of-concept. The signal is successfully encrypted and decrypted by using SBS gain and loss with a 200-MHz bandwidth and different amplitudes. The exact match between the encryption and decryption keys is necessary for the correct signal decryption. The current optical communication system can be upgraded to a secure communication system by directly adding SBS encryption and decryption modules without changing the terminal transceivers.

* Corresponding author.
E-mail address: lilinyi@sjtu.edu.cn (L. Yi).

0030-4018/$ - see front matter © 2012 Elsevier B.V. All rights reserved.
http://dx.doi.org/10.1016/j.optcom.2012.10.017

2. Theory and operation principle

The effect of stimulated Brillouin scattering (SBS) is normally described as the interaction of two counter-propagated waves, namely pump wave and Stokes wave. If the frequency difference of the pump and Stokes wave equals to the Brillouin frequency shift (v_B) of the medium, an acoustic wave is generated, which scatters the photons and transfers the energy from the pump to the Stokes wave, therefore the pump wave is absorbed and the Stokes power is amplified. The SBS process can also be treated as a narrowband amplification or absorption process with the bandwidth of ~30 MHz in silica optical fiber.

Assuming the pump and Stokes waves meet the relationship of $v_p = v_s + v_B$, the coupled equation of the SBS process can be expressed as follows:

$$\frac{dA_p}{dz} = -\frac{g_B}{2A_{eff}}\frac{|A_s|^2}{1-2j\left(\frac{\Delta v}{\Delta v_B}\right)}A_p - \frac{\alpha}{2}A_p \tag{1}$$

$$\frac{dA_s}{dz} = \frac{g_B}{2A_{eff}}\frac{|A_p|^2}{1+2j\left(\frac{\Delta v}{\Delta v_B}\right)}A_s + \frac{\alpha}{2}A_s \tag{2}$$

$$\Delta v = v_s - (v_p - v_B) \tag{3}$$

where A_p, A_s, α, A_{eff}, v_s, v_p and Δv_B represent the pump electrical field, the Stokes signal electrical filed, Brillouin gain coefficient, attenuation coefficient, mode effective area, the Stokes signal frequency, the pump frequency and the Brillouin gain bandwidth respectively. The complex gain $g(v)$experienced by the Stokes signal can be written as:

$$g(v) = \frac{g_B}{1+2j\left(\frac{\Delta v}{\Delta v_B}\right)} \tag{4}$$

The real part of the complex gain represents the amplitude gain and the imaginary part represents the induced phase variation. The real and imaginary parts meet the Kramers-Kronig relationship. Meanwhile the pump wave will experience absorption and the complex loss $\alpha(v)$ can be written as:

$$\alpha(v) = -\frac{g_B}{1-2j\left(\frac{\Delta v}{\Delta v_B}\right)} \tag{5}$$

Similar to the SBS gain case, the real/imaginary part of the complex loss represents the amplitude loss and the induced phase variation. The whole process is shown in Fig. 1(a).

If there are three frequencies at v_{p1}, v_s, and v_{p2} interacted one another in the fiber with the frequency relationship as $v_{p1} - v_{p2} = 2v_B$, the signal at frequency of v_s will experience both the SBS gain from pump 1 and SBS loss from pump 2, which can be expressed as:

$$g(v) = \frac{g_B}{1+2j\left(\frac{\Delta v}{\Delta v_B}\right)} \tag{6}$$

$$\Delta v = v_s - (v_{p1} - v_B) \tag{7}$$

$$\alpha(v) = -\frac{g_B}{1-2j\left(\frac{\Delta v'}{\Delta v_B}\right)} \tag{8}$$

$$\Delta v' = v_{p2} - (v_s - v_B) \tag{9}$$

Considering $v_{p1} - v_{p2} = 2v_B$, we can achieve $\Delta v' = -\Delta v$, therefore Eq. (8) can be rewritten as:

$$\alpha(v) = -\frac{g_B}{1+2j\left(\frac{\Delta v}{\Delta v_B}\right)} = -g(v) \tag{10}$$

Therefore after experiencing both SBS gain and loss and transmitting z distance in the optical fiber, the Stokes signal electrical field can be written as:

$$E_s(z,v) = E_s(0,v)e^{(g(v)+\alpha(v))I_p z} = E_s(0,v) \tag{11}$$

which means with the same Brillouin pump power and after transmitting the same distance, the signal can be recovered to the original case. Fig. 1(b) shows that the SBS gain can completely compensate the SBS loss and the corresponding phase variations are also counterbalanced.

Fig. 1 only shows the narrowband SBS gain and loss case. Actually the SBS gain or loss spectra can be expressed as the convolution of the pump spectra and the natural Brillouin gain/loss spectra [8].Therefore both the SBS gain and loss spectra can be broadened and the spectral shape can be controlled through shaping the Brillouin pump spectrum using direct noise modulation [9] or external phase modulation [10]. If two Brillouin pumps with $2v_B$ frequency spacing have the same spectral shape and power, the Stokes signal electrical field after experiencing broadband SBS gain/loss and transmitting z distance can be written as:

$$E_s(z,v) = E_s(0,v)e^{(S_p \otimes (g(v)+\alpha(v)))I_p z} = E_s(0,v) \tag{12}$$

where S_p represents the pump spectrum. Therefore it can be concluded that the broadband SBS gain/loss and the corresponding phase variation can also be counterbalanced.

If a broadband signal at frequency v_s with 10-Gb/s data rate is firstly amplified by the SBS gain with a broadened 400-MHz bandwidth, both the carrier and the low frequency components of the broadband signal are amplified, therefore the signal is totally distorted and we cannot obtain any useful information from the closed eye diagram. After being attenuated by a SBS loss with the same amplitude, bandwidth and spectral shape as the SBS gain, the distorted signal is completely recovered. If the SBS loss does

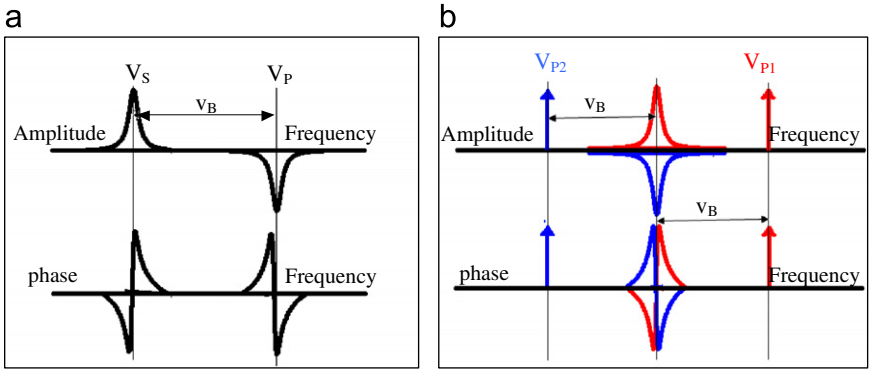

Fig. 1. The operation principle of the proposed SBS encryption and decryption methods.

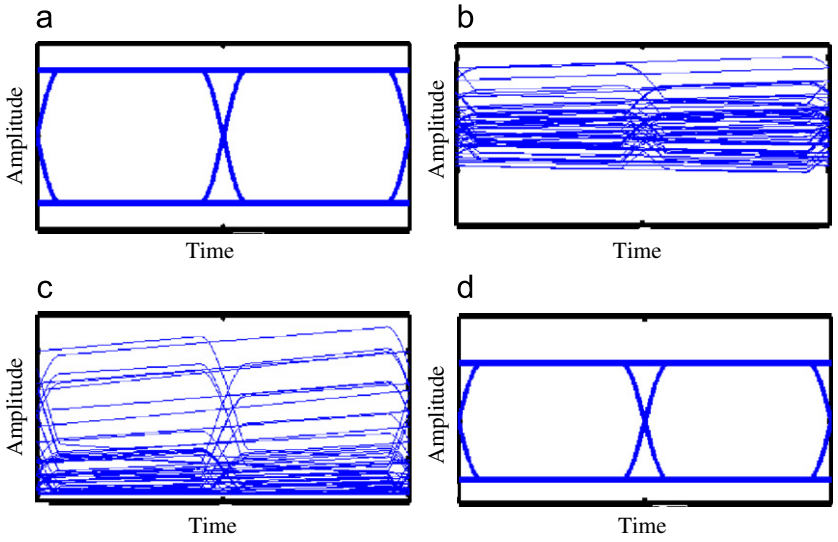

Fig. 2. (a) The eye-diagram of a 10-Gb/s NRZ-OOK signal, (b) The encrypted 10-Gb/s signal by a 400-MHz broadband SBS gain, (c) The undecrypted 10-Gb/s signal by a 400-MHz broadband SBS gain and a 200-MHz broadband SBS loss and (d) The correctly decrypted 10-Gb/s signal.

not match with the SBS gain, the distorted signal cannot be recovered. Fig. 2 shows the entire process from signal distortion to recovery.

We can make use of the above phenomenon to encrypt and decrypt the broadband signal. The SBS amplification is treated as the encryption process and the matched SBS absorption is the decryption process. The encryption/decryption key could be the SBS gain amplitude, central frequency, bandwidth and spectral shape. Only when the encryption and decryption keys match, the distorted signal could be recovered. The encryption keys are configurable and flexibly controlled by the users. The encrypted signal bandwidth could be as high as several tens of Gb/s and is not limited by the laser oscillation frequency as in chaotic communication systems. Furthermore the SBS encryption/decryption method is compatible with the traditional optical communication systems by directly adding the SBS encryption and decryption modules, without changing the transceivers at the communication terminals.

3. Experimental results and discussion

We make an experiment to evaluate the SBS encryption/decryption proposal as a proof-of-concept. The experimental setup is shown in Fig. 3. A distributed feedback laser diode (DFB-LD) with a central wavelength of 1549.21 m serves as both the Brillouin pump and signal. The power of the laser is boosted to 16 dBm by an erbium-doped fiber amplifier (EDFA1) then divided into two parts by a 3-dB coupler. In the lower path, the light is modulated by a Mach-Zehnder modulator (MZM1) with a 10.86-Gb/s Pseudo-random bit sequence (PRBS) non-return-to-zero (NRZ) data from a pulse pattern generator (PPG). The broadband signal is launched into a 25-km long single-mode fiber (SMF) with a Brillouin frequency of 10.86 GHz through an optical isolator (ISO). In the upper path, the light is modulated by MZM2 at the Brillouin frequency of the SMF using the optical carrier-suppressing double sidebands (OCS-DS) technique [11]. EDFA2 is used to compensate the strong loss of the OCS-DS signal, which is then divided into two parts by a 3-dB optical coupler. Two tunable optical filters (TOFs) are employed to select the upper sideband and the lower sideband, serving as the two Brillouin pumps. EDFA3 and EDFA4 are used to control the Brillouin pump powers. The amplified Brillouin pumps are combined by another 3-dB optical coupler and then sent to the SMF through an optical circulator (OC). Polarization controllers (PCs) are used to control the polarization state of the light. The broadband signal is exported from port 3 of the OC. Turning off both EDFA3 and EDFA4, the original signal is observed. SBS amplification is achieved by turning on EDFA3. The signal is simultaneously amplified and attenuated by SBS gain and loss through turning on both EDFA3 and EDFA4. We dither the DFB-LD using a current white noise so as to broaden the SBS gain bandwidth to $\sim$200 MHz as shown in the inset of Fig. 3. The 10.86-Gb/s signal is distorted by the 200-MHz SBS gain therefore implementing the encryption process. The distorted signal can be recovered using a 200-MHz SBS loss with the same amplitude and spectral shape to realize the decryption process. Fig. 3(a–e) shows the optical spectra at the corresponding points of the experimental setup. Fig. 3(f–h) represents the signal is attenuated by SBS loss, amplified by SBS gain, and simultaneously experiences SBS gain and loss.

The eye diagrams of the encrypted and decrypted signals in different cases are shown in Fig. 4 to verify the SBS based encryption and decryption process. The corresponding bit error rate (BER) curves are shown in Fig. 5 to evaluate the performance of the encryption and decryption. For 1-dB broadband SBS loss and 1-dB broadband SBS gain, the eye diagrams are a little distorted but we can still detect the open eyes. The best BERs for loss and gain cases are 2×10^{-5} and 3×10^{-4} respectively. The worse BER performance of the SBS gain case is due to the stronger noise than in the attenuation case. The eye is clearly open when the signal simultaneously experiences the SBS gain and loss with the same 1-dB amplitude and 200-MHz bandwidth. The sensitivity is -17 dBm, corresponding to $\sim$1 dB power penalty compared with the back-to-back (BtB) case. When the SBS loss is increased to 2 dB, the eye distortion becomes severe and the best BER is only 3×10^{-3}. For the 2-dB SBS gain case, the signal is totally distorted and the BER cannot be measured due to data out of synchronization, therefore realize the complete encryption. In the same manner, the eye diagram can be recovered when the SBS gain and loss match each other, implementing the decryption process. The power penalty is increased to $\sim$4 dB due to the cumulative SBS gain and loss noise. With the further increase of the SBS gain and loss, the eye diagrams are completely closed, and the eavesdroppers cannot achieve any useful information from the noise-like signals by direct detection. With a 4-dB SBS gain

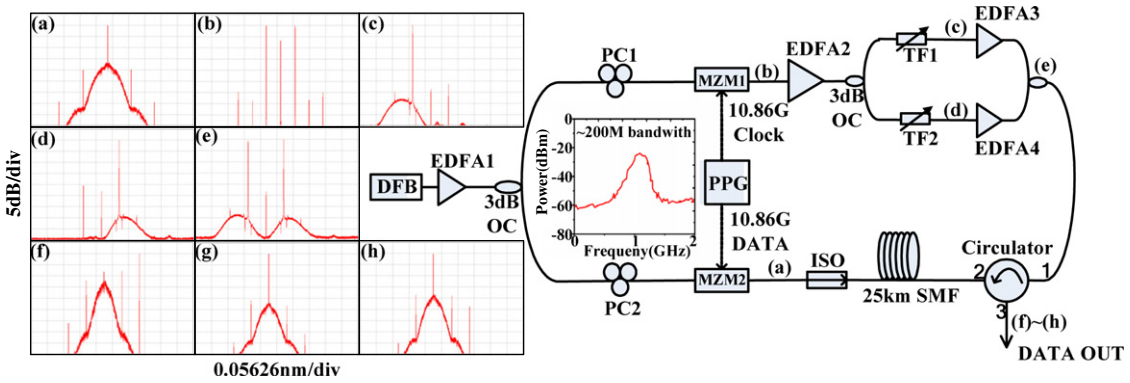

Fig. 3. The experimental setup and the measured optical spectra at the marked points.

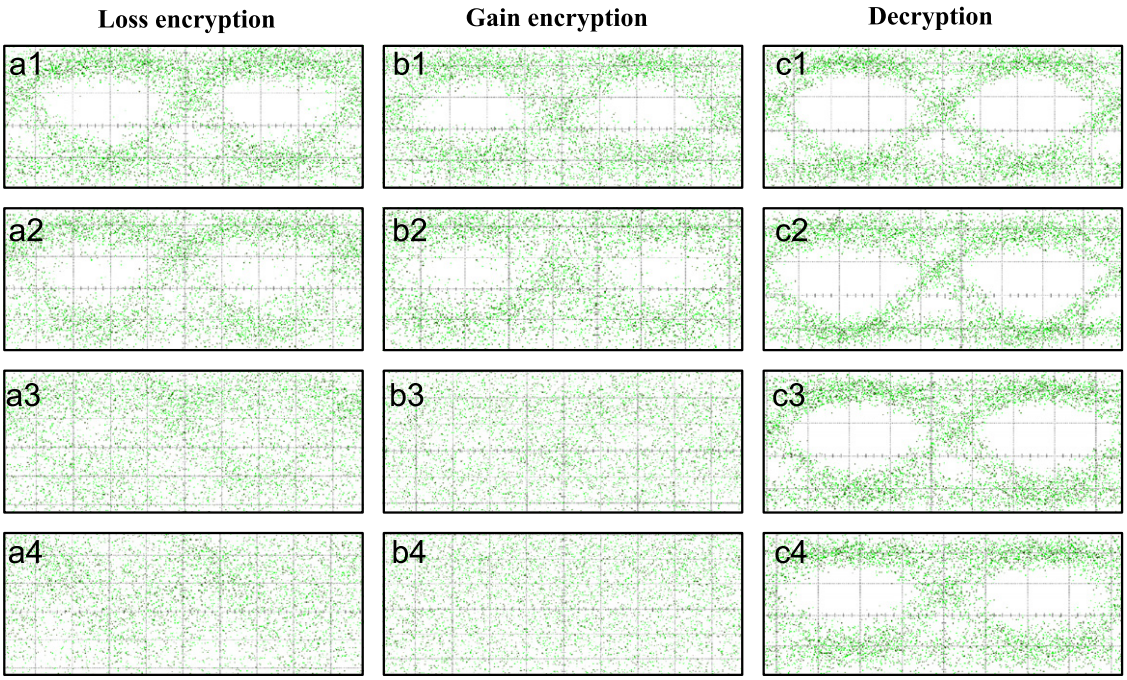

Fig. 4. The eye diagrams of the encrypted 10.86-Gb/s NRZ-OOK signal by 200-MHz Gaussian-shape SBS gain/loss, and the decrypted single by matched SBS gain and loss. (a1) 1-dB SBS loss, (b1) 1-dB SBS gain, (c1) 1-dB SBS gain and 1-dB SBS loss, (a2) 2-dB SBS loss, (b1) 2-dB SBS gain, (c1) 2-dB SBS gain and 2-dB SBS loss, (a3) 3-dB SBS loss, (b3) 3-dB SBS gain, (c3) 3-dB SBS gain and 3-dB SBS loss, (a4) 4-dB SBS loss, (b4) 4-dB SBS gain, (c4) 4-dB SBS gain and 4-dB SBS loss.

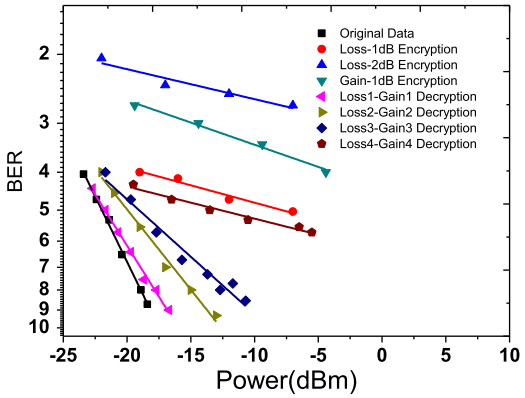

Fig. 5. BER measurement results of the original, encrypted and decrypted signals.

and a 4-dB SBS loss of the same bandwidth, the closed eye can still be recovered, but the cumulative SBS noise degrades the decrypted signal and error-free operation cannot be achieved. By employing the forward-feedback correction (FEC) technique, the BER can be corrected to 1×10^{-9}; therefore successful decryption can still be realized.

From the measurement results of both eye diagrams and BERs, it can be concluded that the exact match between the encryption key and the decryption key can successfully realize signal recovery. We further measure the eye diagrams for the mismatch of the encryption/decryption keys as shown in Fig. 6. For the amplitude mismatch (1-dB loss vs. 2-dB gain), central frequency mismatch (50-MHz frequency difference) and bandwidth mismatch (200 MHz loss vs. 400 MHz gain), the eyes are still closed and cannot be recovered, which proves that the eavesdroppers cannot recover the encrypted signal if they are using the wrong decryption keys, showing the robustness of the proposed SBS based encryption method. Note that the central frequency mismatch and bandwidth mismatch are realized by modulating one of the Brillouin pumps using external phase modulator.

Furthermore, we analyze the difficulty of the eavesdroppers in recognizing the encryption keys. Since the encryption keys are included in the Brillouin pump spectrum and the eavesdroppers

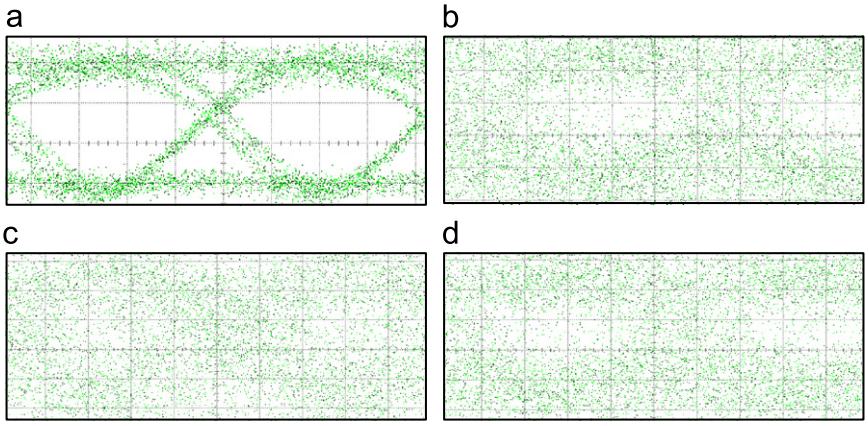

Fig. 6. The measured eye diagrams of the original 10.86-Gb/s NRZ-OOK signal (a), the distorted signal by a 1-dB SBS loss and a 2-dB SBS gain (b), the distorted signal by a 50-MHz frequency drift between the SBS loss and gain (c) and the distorted signal by a 200-MHz broadband SBS loss and a 400-MHz broadband SBS gain.

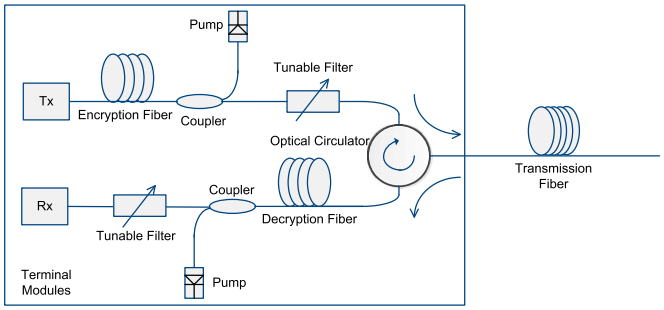

Fig. 7. The schematic of practical encryption and decryption terminal modules.

are possible to monitor the residual Brillouin pump in the transmission fiber using bidirectional tapping, we have to prevent the Brillouin pump power from leaking into the transmission fiber to avoid this kind of attack. Fig. 3 just shows the proof-of-concept experimental setup, where the signal encryption and decryption are implemented in the transmission fiber, however in the practical applications, the encryption and decryption fibers are installed inside the terminal modules to avoid the temperature and strain variation and facilitate the Brillouin and signal frequency matching as shown in Fig. 7. The encryption and decryption fibers could be specialty fibers with low Brillouin threshold and high Brillouin gain coefficient such as chalcogenide fiber to reduce the Brillouin pump power requirement therefore weaken the residual Brillouin pump power. For the encryption case, the Rayleigh backscattering of the Brillouin pump will launch into the transmission fiber together with the signal. We can use a narrowband tunable optical filter to suppress the weak Rayleigh backscattering power of the Brillouin pump. For the decryption case, the residual forward Brillouin pump power is blocked by the optical circulator. Therefore we can know that the eavesdroppers cannot achieve the Brillouin pump spectrum in the transmission fiber even using bidirectional tapping.

We suppose the eavesdroppers try to achieve the encryption keys from the signal itself. They can monitor the encrypted signals by detecting the eye diagrams, optical spectra and electrical spectrum using oscilloscope, optical spectrum analyzer (OSA) and electrical spectrum analyzer (ESA) respectively. From the completely distorted eye diagrams, it is impossible to know the encryption keys. From the optical spectrum, since the gain or loss amplitude is only 2–3 dB, the effect on the optical spectrum is negligible only if a very high resolution OSA is used. The electrical spectrum measurement effect is similar with the high resolution OSA case and the spectra in the range of 0–500 MHz are shown in Fig. 8 for the original data, the encrypted data by a 2-dB SBS gain with 200-MHz bandwidth and the decrypted signal. From Fig. 8(b), a minor amplitude increase of the low frequency components is detected, but is not obvious. If a phase-modulated signal is used, coherent detection has to be adopted to detect the electrical spectrum, which further increases the difficulty of recognizing the encryption keys.

The encryption keys include 4 independent parameters: gain amplitude, spectral position, spectral width, and spectral shape. The former 2 parameters can be controlled by tuning the Brillouin pump power and wavelength, and the latter two can be manipulated by controlling the Brillouin pump spectrum. By directly driving the Brillouin pump laser diode using an arbitrary waveform generator, the pump spectral width and shape can be controlled by the amplitude and waveform function of the driven current [12,13]. White noise modulation of the pump laser diode can generate Gaussian-shape spectrum, saturated amplified white noise modulation of the pump generates nearly square-shaped spectrum and square wave modulation of the pump generates two peaks at the pump spectral edge. Other user-defined waveform modulations of the pump can generate versatile pump spectral shape therefore flexibly controlling the gain spectral shape. Furthermore, by using multiple pumps with different spectral shape or externally modulating the spectral-shaped pump using a radio frequency, the diversity of the pump spectral shape can be further increased. The mismatch between the encryption pump spectrum and the decryption pump spectrum will result in frequency and phase distortion of the signal, therefore causes failure in the signal recovery. Since each of the 4 encryption parameters can be tuned independently, there are numerous combinations of the encryption keys. Among them, the spectral shape is the most flexible one. By dynamically tuning the encryption keys, the eavesdroppers can only detect the averaged signal spectrum therefore it is impossible to know the exact keys from the detected signal spectrum and any steady-state spectrum compensation will lead to severe distortion of the signal therefore cannot recover the encrypted signal. In this case, synchronization is required for the correct decryption, but the tuning speed of the encryption keys can be set in $\sim$ms level to reduce the synchronization difficulty for the legal users.

Note that, the proposed SBS based encryption method is based on frequency amplitude and phase distortion, which can be combined with other encryption methods to further improve the data security. The SBS based encryption method is easy to implement

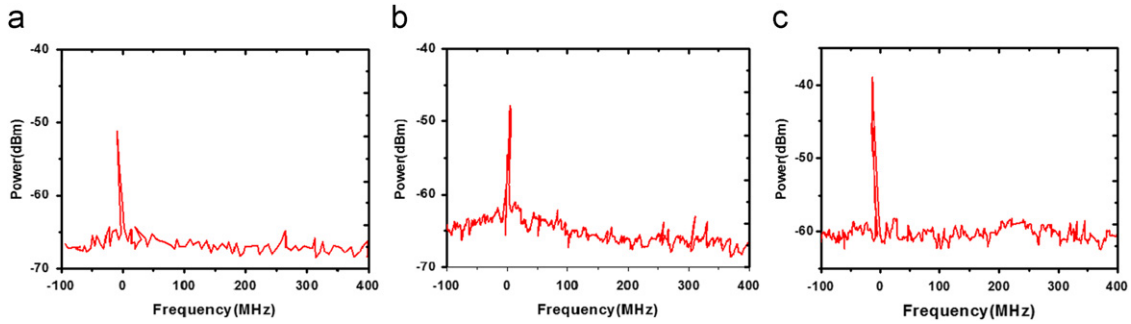

Fig. 8. The electrical spectra of the original signal, the encrypted by SBS gain and decrypted signals.

and is completely compatible with the existing fiber-optic communication systems without changing the terminal transceivers.

4. Conclusion

We propose to use SBS process in optical fiber to encrypt and decrypt high-speed optical signals for the first time. The encryption/decryption keys could be SBS gain amplitude, central frequency, bandwidth and spectral shape. The operation principle is explained in detail and a proof-of-concept experiment is made to verify this proposal. A 10.86-Gb/s NRZ data is successfully encrypted and decrypted using a 3-dB SBS gain and loss with 200-MHz bandwidth. The encryption/decryption performance is analyzed and the improvement methods are proposed for the further work. The SBS encryption and decryption processes are completely compatible with the traditional communication systems without updating the transceivers in the terminals.

Acknowledgments

This work was supported by 973 Program (2012CB315602 and 2010CB328204–5), Nature Science Foundation China (61007041, 61090393, 61132004 and 60825103), 863 Program, Program of Shanghai Subject Chief Scientist (09XD1402200), Program of Shanghai Chen Guang Scholar (11CG11) and Program of Excellent PhD in China (201155).

References

[1] O. Buskila, A. Eyal, M. Shtaif, Optics Express 16 (2008) 3383.
[2] J. Paul, M.W. Lee, K.A. Shore, IEEE Photonics Technology Letters 17 (2005) 920.
[3] J.P. Goedgebuer, P. Levy, P. Larger, L. Chen, W.T. Rhodes, IEEE Journal of Quantum Electronics 38 (2002) 1178.
[4] A. Argyris, D. Syvridis, L. Larger, V. Annovazzi-Lodi, P. Colet, I. Fisher, J. Garcia-Ojalvo, C.R. Mirasso, L. Pesquera, K.A. Shore, Nature 438 (2005) 343.
[5] B. Wu, E.E. Narimanov, Optics Express 14 (2006) 3738.
[6] Z. Wang, M.P. Fok, L. Xu, J. Chang, P.R. Prucnal, Optics Express 18 (2010) 6079.
[7] X. Hong, D. Wang, L. Xu, S. He, Optics Express 18 (2010) 12415.
[8] M.G. Herraez, K.Y. Song, L. Thevenaz, Optics Express 14 (2007) 1395.
[9] Z. Zhu, Andrew M.C. Dawes, Daniel J. Gauthier, L. Zhang, Alan E. Willner, Journal of Lightwave Technology 25 (2007) 201.
[10] L. Yi, L. Zhan, W. Hu, Y. Xia, IEEE Photonics Technology Letters 19 (2007) 619.
[11] J. Yu, Z. Jia, L. Yi, Y. Su, G.K. Chang, T. Wang, IEEE Photonics Technology Letters 18 (2006) 265.
[12] L. Yi, Y. Jaouen, W. Hu, Y. Su, S. Bigo, Optics Express 15 (2007) 16972.
[13] L. Thevenaz, Nature Photonics 2 (2008) 474.