Power-penalty-free all-optical decryption using stimulated Brillouin scattering in optical fiber

2013 Laser Phys. Lett. 10 045102

(http://iopscience.iop.org/1612-202X/10/4/045102)

IOP PUBLISHING LASER PHYSICS LETTERS
Laser Phys. Lett. **10** (2013) 045102 (5pp) doi:10.1088/1612-2011/10/4/045102

LETTER

Power-penalty-free all-optical decryption using stimulated Brillouin scattering in optical fiber

L L Yi, T Zhang, Z X Li, Y Zhang, Y Dong and W S Hu

State Key Lab of Advanced Optical Communication Systems and Networks, Department of Electronic Engineering, Shanghai Jiao Tong University, Shanghai 200240, People's Republic of China

E-mail: lilinyi@sjtu.edu.cn

Received 22 May 2012, in final form 2 September 2012
Accepted for publication 3 September 2012
Published 14 February 2013
Online at stacks.iop.org/LPL/10/045102

Abstract
We propose to all-optically encrypt and decrypt high-speed optical signals using the stimulated Brillouin scattering (SBS) effect in optical fiber for the first time. The spectral-shaped SBS gain or loss distorts the broadband optical signal so as to realize optical encryption. A corresponding SBS loss or gain with the same spectral shape and amplitude recovers the distorted signal to implement optical decryption. We experimentally demonstrate the SBS encryption/decryption process on 10.86 Gb s^{-1} non-return-to-zero-on-off-keying (NRZ-OOK) data using phase-modulated Brillouin pumps to generate a spectral-shaped SBS gain/loss encryption key, and no power penalty is observed for the best decryption case. The proposed all-optical encryption/decryption method is completely compatible with existing fiber-optic communication systems.

(Some figures may appear in colour only in the online journal)

1. Introduction

Physical-layer encryption and decryption using optical approaches is a robust security method with the properties of high speed and difficulty in eavesdropping, where the signal is covered by noise or completely distorted and can therefore not be properly recognized without correct decryption. Chaos communication [1–4] is a major physical-layer optical encryption method. Chaos encryption needs to generate a chaotic carrier from the transmitter through all-optical feedback [2] or electro-optic feedback [3] to cover the optical signal, while the same feedback scheme is required before the receiver to synchronize the chaotic carrier and therefore recover the optical signal. Chaos communication has been demonstrated in the real world with a data rate up to several Gb s^{-1} [4], but a higher data rate is limited by the relaxing oscillation frequency of the laser. Optical code-division-multiplexing access (OCDMA) is an optical multi-address access technique, which can also provide a sort of security by broadening the narrow-width pulse using specific gratings and overlapping with other users [5–7]. OCDM requires a picosecond pulse laser as the source to implement signal encoding and decoding. Therefore the common feature of chaotic communication and OCDMA requires special transmitters and receivers to encrypt and decrypt the optical signal. From the practical viewpoint, it is desirable to directly encrypt/decrypt the optical signal based on a traditional transmitter and receiver, thus being compatible with existing fiber-optic communication systems.

In this letter, for the first time, we propose to use the stimulated Brillouin scattering (SBS) effect in optical fiber to encrypt and decrypt high-speed optical signals based on traditional transceivers. Part of the frequency components of the signal are amplitude- and phase-distorted by a SBS

gain/loss to implement encryption and then completely recovered by using a corresponding SBS loss/gain. The encryption keys could be the SBS gain/loss amplitude and the spectral shape. We experimentally demonstrate the encryption and decryption performance of a 10.86 Gb s^{-1} non-return-to-zero-on-off-keying (NRZ-OOK) signal using phase-modulated Brillouin pumps to generate a spectral-shaped SBS gain/loss encryption key. After encryption, the eye diagram of the signal is totally distorted and the bit-error-rate (BER) cannot be measured. The distorted eye diagram is recovered by using a corresponding spectral-shaped SBS loss/gain as the decryption key. No power penalty is observed for the best decryption case. Moreover, the power and phase modulation frequency of the Brillouin pump can be slowly varied to achieve an average encryption result, therefore the eavesdropper cannot recognize the encryption keys from either the frequency-domain or time-domain of the encrypted signal, thus enhancing the security. The proposed SBS encryption method is completely compatible with existing fiber-optic communication systems.

2. Principle

The stimulated Brillouin scattering process can be considered as the interaction between a pump light with frequency of ν_0 and a counter-propagated probe light with frequency of $\nu_0 - \nu_B$ in the transmitting medium, where ν_B is the Brillouin frequency shift of the medium. The power is transferred from the pump to the probe light, therefore the pump experiences SBS absorption and the probe experiences SBS amplification. The amplification or absorption bandwidth is determined by the properties of the transmitting medium, which is around 30–50 MHz for single-mode fiber (SMF). The SBS process is widely used in temperature/strain sensors [8, 9], slow light [10, 11] and Brillouin fiber lasers [12, 13].

In this letter, we use the SBS process for the encryption and decryption of high-speed optical signals. If two lasers with frequencies of $\nu_0 - \nu_B$ and $\nu_0 + \nu_B$ are used as Brillouin pumps, the SBS amplification and absorption will happen at the same frequency of ν_0. By controlling the power of the two Brillouin pumps, the SBS gain can completely compensate the SBS loss and the corresponding phase variation is also counterbalanced. If a broadband signal is amplified/absorbed by a SBS gain/loss, both the amplitude and phase of the carrier and the low-frequency components of the signal will be changed, resulting in a distorted eye diagram. The signal can be recovered by using a corresponding SBS loss/gain to compensate the amplitude and phase variation. The signal distortion and recovery process can be treated as encryption and decryption respectively, and the SBS gain/loss amplitude and spectral shape could be the encryption keys. The SBS gain spectral shape is the convolution of the pump spectrum and the natural SBS gain spectrum [14], therefore it can be configured by controlling the Brillouin pump spectrum. We have demonstrated control of the SBS gain spectral shape to both broadband Gaussian shape and super-Gaussian shape by directly modulating the Brillouin pump laser using current noise [15]. After experiencing the spectral-shaped

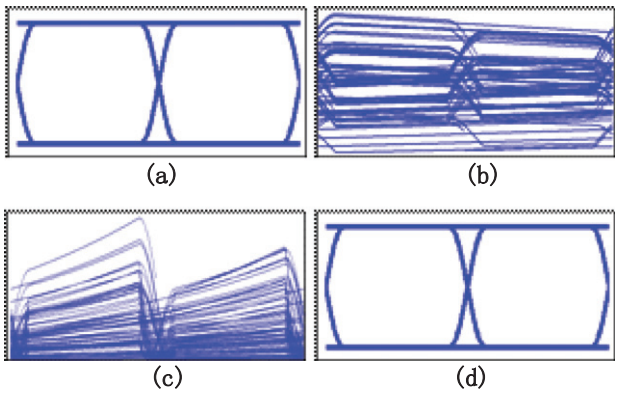

Figure 1. (a) The eye diagram of a 10 Gb s^{-1} NRZ-OOK signal, (b) the encrypted 10 Gb s^{-1} signal by a 500 MHz-spaced 3-line SBS gain, (c) the encrypted 10 Gb s^{-1} signal by a 500 MHz-spaced 3-line SBS loss, (d) the decrypted 10 Gb s^{-1} signal.

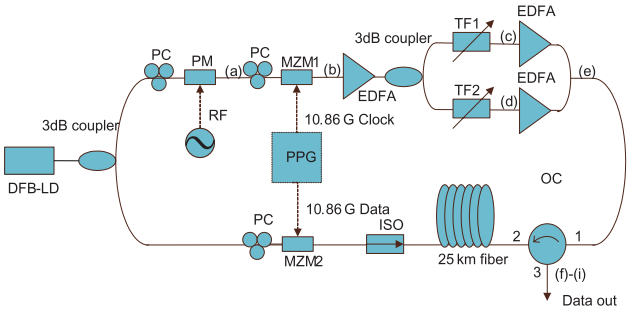

Figure 2. The experimental setup of the proposed SBS based security method.

SBS gain/loss and transmitting a distance z, the signal electrical field can be written as

$$E_s(z, \nu) = E_s(0, \nu)e^{(S_p \otimes (g(\nu)+\alpha(\nu)))I_p z} = E_s(0, \nu) \quad (1)$$

where S_p represents the pump spectrum, $g(\nu)$ and $\alpha(\nu)$ are the natural SBS gain and loss spectrum, I_p is the Brillouin pump amplitude. $E_s(0, \nu)$, $E_s(0, \nu)e^{(S_p \otimes g(\nu))I_p z}$, $E_s(0, \nu)e^{(S_p \otimes \alpha(\nu))I_p z}$, $E_s(z, \nu)$ represent the original signal, the encrypted signal by spectral-shaped SBS gain and loss, and the decrypted signal respectively. If the encryption and decryption Brillouin pumps have the same pump spectral shape and power, the decrypted signal is equal to the original signal. S_p and I_p can be considered as the encryption keys and they can be dynamically varied to enhance the security. By defining S_p as a 500 MHz-speed 3-line SBS gain/loss spectra and using it as the encryption/decryption key, the corresponding eye diagrams of a 10 Gb s^{-1} NRZ-OOK signal are shown in figure 1.

3. Experimental results and discussions

We shape the Brillouin pump spectrum using external phase modulation to configure the SBS encryption and decryption keys. In the proof-of-concept experiment, we use a single distributed-feedback laser diode (DFB-LD) with a central wavelength of 1549.66 nm as a common source for both the

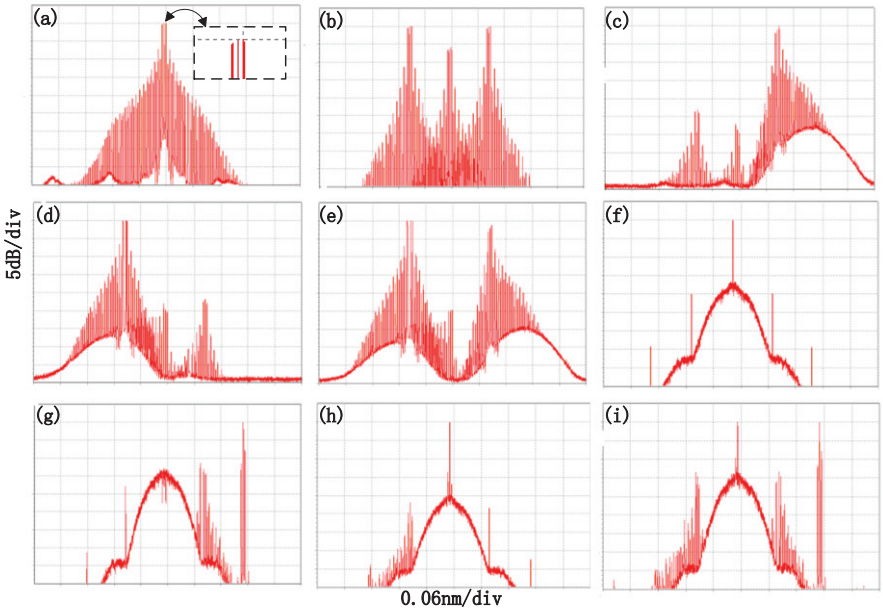

Figure 3. The measured optical spectra at the corresponding points marked at figure 2.

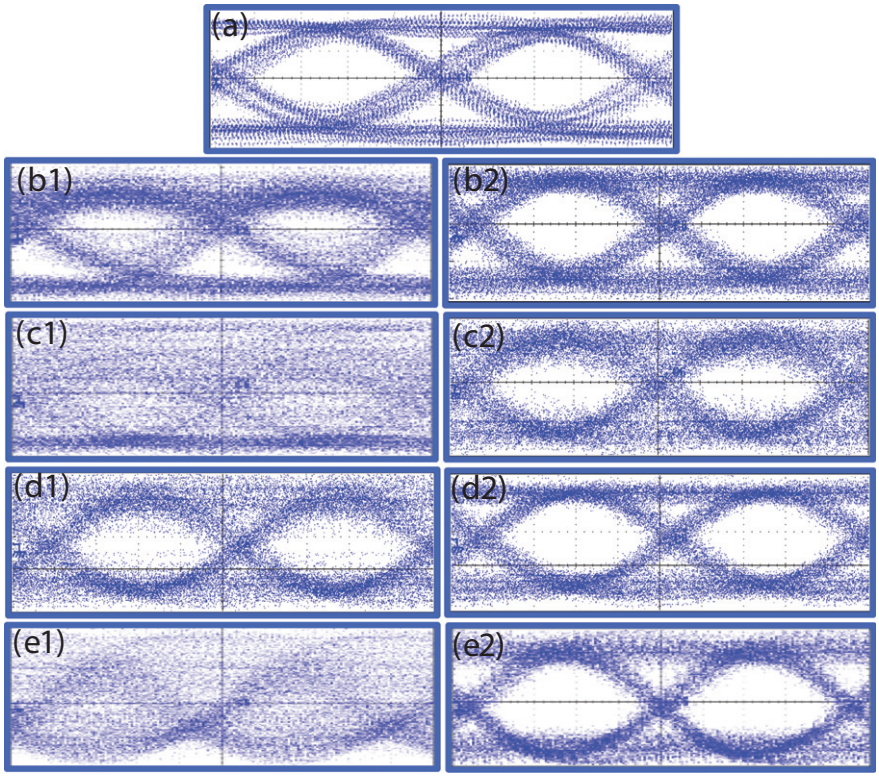

Figure 4. The eye diagrams of the original signal (a), the encrypted signals by 2 dB SBS gain (b1), 4 dB SBS gain (c1), 5 dB SBS loss (d1), 10 dB SBS loss (e1) and the decrypted signals by 2 dB SBS loss (b2), 4 dB SBS loss (c2), 5 dB SBS gain (d2), 10 dB SBS gain (e2).

signal and the Brillouin pumps. The experimental setup is shown as figure 2. The output of the DFB-LD is divided into two parts by a 3 dB coupler. In the upper path, the light is first modulated by a phase modulator (PM) using a 500 MHz radio frequency (RF) to generate an optical frequency comb (OFC) as the spectra-shaped Brillouin pump. Then the OFC Brillouin pump is modulated by a Mach–Zehnder modulator (MZM1) at the Brillouin frequency (10.86 GHz) of the SMF using the well-known optical carrier-suppressing (OCS) double-sidebands technique by tuning the bias voltage at the nulling point of the MZM [16]. To separate the left and right sidebands, the OCS-modulated Brillouin pump is divided by another 3 dB coupler and then selected by two tunable filters (TFs). The separated left and right sidebands serve as the two

Brillouin pumps. Two erbium-doped fiber amplifiers (EDFAs) follow the TFs to tune the Brillouin pump's power and thereby control the SBS amplification or absorption amplitude. The amplified Brillouin pumps are combined by another 3 dB optical coupler and then launched into the SMF through an optical circulator (OC). In the lower path, the light is modulated by MZM2 with 10.86 Gb s^{-1} pseudo-random bit sequence (PRBS) NRZ data from a pulse pattern generator (PPG). The broadband signal is launched into a 25 km long SMF through an optical isolator (ISO). Polarization controllers (PC) are used to control the polarization state of the light. The broadband signal is exported from port 3 of the OC.

Figures 3(a)–(e) show the optical spectra at corresponding points marked on figure 2. Figures 3(f)–(h) represent the optical spectra of the original 10.86 Gb s^{-1} NRZ-OOK signal, and the signals distorted by SBS loss and SBS gain, respectively. When the pump powers are properly controlled, the SBS gain and loss can be compensated and therefore the distorted signal can be recovered as shown in figure 3(i). The Rayleigh backscattering of the Brillouin pumps and the SBS gain spectra of the right sideband Brillouin pump can be suppressed by a narrow-band optical filter to prevent the optical spectra from being recognized.

Figures 4 and 5 show the eye diagrams and the BER measurement results of the original, encrypted and decrypted signals in different SBS gain/loss amplitude cases. Note that the defined SBS gain and loss are experienced by the carrier. With a 2 dB SBS gain, even though the eye is distorted, the BER is still detectable and therefore the encryption is not ideal. With a 4 dB SBS gain, the eye becomes severely distorted and the BER is not measurable due to data out of synchronization, and therefore not shown in figure 5, realizing a complete encryption. But the sensitivity of the corresponding decrypted signal becomes worse, as shown in figure 5(a), due to higher SBS amplification and absorption noise. With a SBS gain higher than 5 dB, error-free operation of the decrypted signal cannot be achieved.

Apart from the SBS amplification encryption method, the signal can also be encrypted by the SBS loss. Figures 4(d1) and (d2) show the distorted eye diagram from a 5 dB SBS loss and the recovered eye diagram from the corresponding SBS gain. The sensitivities for the distorted and recovered signal are −13.5 dBm and −16 dBm, respectively. Therefore the signal cannot be encrypted by low SBS loss, which is similar to the SBS gain encryption case. However, the signal can be totally encrypted by a 10 dB SBS loss, as shown in figure 4(e1). Again, the BER cannot be measured due to data out of synchronization. With a corresponding 10 dB SBS gain, the encrypted signal can be fully recovered with a sensitivity of −16 dBm, as shown in figure 5(b). No power penalty is observed compared with the original signal, therefore perfect encryption and decryption performance are achieved. For the encryption with a SBS loss higher than 10 dB, the corresponding decryption performance becomes worse. Note that the decryption performance using SBS loss encryption is better than that of the gain encryption case. This is because the signal always works in the gain/loss saturation region for the gain encryption case, resulting in higher amplification/absorption noise.

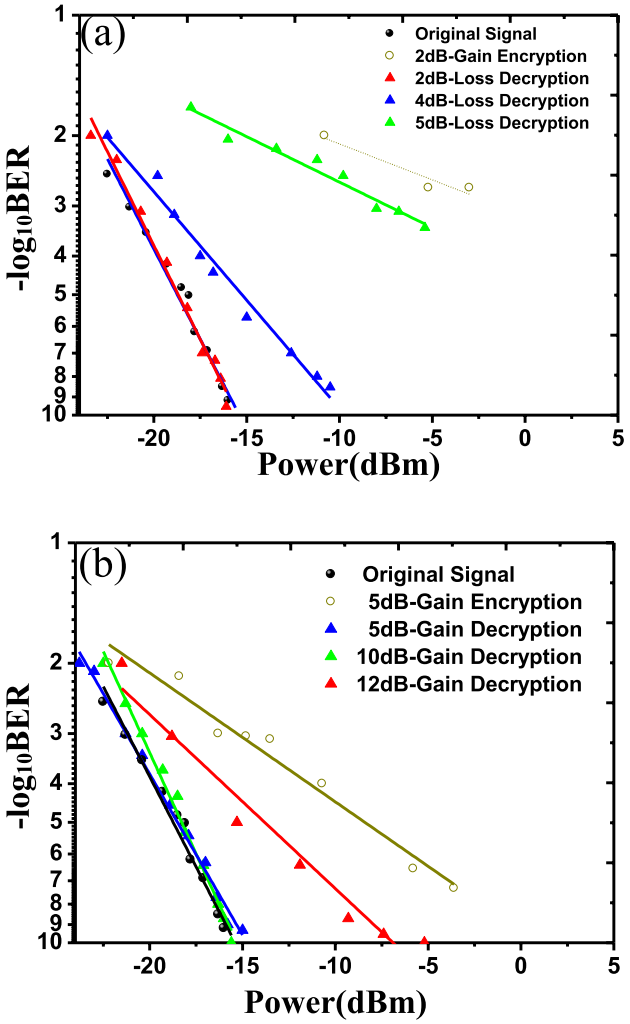

Figure 5. BER measurement results with SBS gain encryption (a) and SBS loss encryption (b).

We can vary the frequency spacing by tuning the phase modulation frequency of the Brillouin pumps so as to change the encryption key. Figures 6(a) and (b) show the encrypted/decrypted optical signals from 2.45 GHz frequency-spaced OFC Brillouin pumps. If the frequency spacing of the encrypted and decrypted Brillouin OFC pumps does not match, the signal distortion due to SBS amplification and absorption will be superposed, resulting in an even worse eye diagram, as shown in figure 6(c).

If the frequency spacing of the OFC Brillouin pumps is dynamically modulated using a slowly varied waveform (such as in the ∼ms level), the security level could be significantly enhanced, since the eavesdroppers can only see the average result and cannot recognize the encryption key from either the frequency-domain or time-domain of the encrypted signal. Only legal users who know the encryption keys can decrypt the signals. A synchronized slowly varied waveform has to be used for correct decryption, but the synchronization is not difficult since it operates only at a very low speed. One can

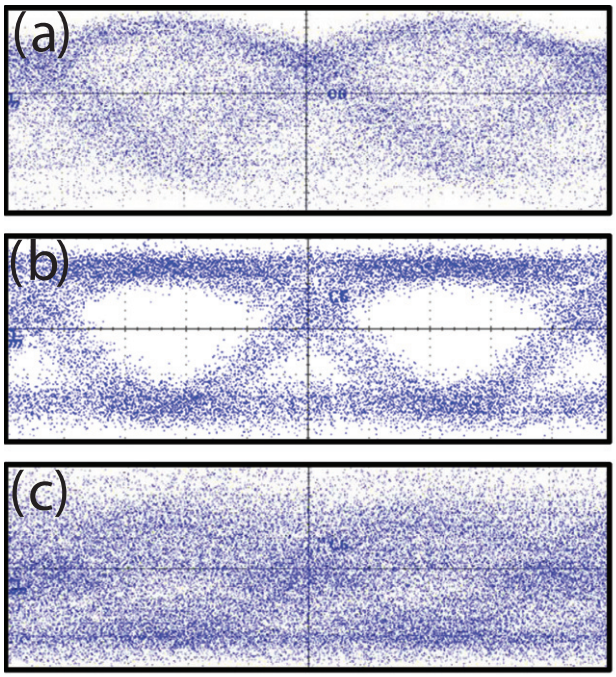

Figure 6. The encryption/decryption eye diagrams with 2.45 GHz frequency-spaced OFC Brillouin pumps, and the eye diagram with the mismatched Brillouin pumps.

also dynamically tune the Brillouin pump power to enhance the security for the same reasons as explained above.

4. Conclusion

In conclusion, we have experimentally demonstrated the encryption and decryption performance of 10.86 Gb s^{-1} NRZ-OOK data using phase-modulated Brillouin pumps to generate spectral-shaped SBS gain/loss encryption keys. For a 10 dB SBS loss encryption, no power penalty is observed for the decrypted signal. The security level could be enhanced by varying the power or frequency spacing of the OFC Brillouin pumps using a slowly varied waveform. The proposed SBS encryption/decryption proposal is completely compatible with existing fiber-optic communication systems.

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] Van Wiggeren G D and Roy R 1998 *Science* **279** 1198
[2] Paul J, Lee M W and Shore K A 2005 *IEEE Photon. Technol. Lett.* **17** 920
[3] Lin F Y and Liu J M 2002 *Appl. Phys. Lett.* **81** 3128
[4] Argyris A, Syvridis D, Larger L, Annovazzi-Lodi V, Colet P, Fisher I, Garcia-Ojalvo J, Mirasso C R, Pesquera L and Shore K A 2005 *Nature* **438** 343
[5] Jiang Z, Seo D, Yang S, Leaird D E, Roussev R V, Langrock C, Fejer M M and Weiner A M 2005 *IEEE Photon. Technol. Lett.* **17** 705
[6] Fok M P and Prucnal P R 2009 *Opt. Lett.* **34** 1315
[7] Gao Z, Dai B, Wang X, Kataoka N and Wada N 2011 *Opt. Lett.* **36** 1623
[8] Zou L, Bao X, Wan Y and Chen L 2005 *Opt. Lett.* **30** 370
[9] Song K Y, Kishi M, He Z and Hotate K 2011 *Opt. Lett.* **36** 2062
[10] Thevenaz L 2008 *Nature Photon.* **2** 474
[11] Zhu Z, Gauthier D J and Boyd R W 2007 *Science* **14** 1748
[12] Shahi S, Harun S W and Ahmad H 2009 *Laser Phys. Lett.* **6** 454
[13] Shirazi M R, Shahabuddin N S, Aziz S N, Thambiratnam K, Harun S W and Ahmad H 2008 *Laser Phys. Lett.* **5** 361
[14] Herraez M G, Song K Y and Thevenaz L 2007 *Opt. Express* **14** 1395
[15] Yi L, Jaouen Y, Hu W, Su Y and Bigo S 2007 *Opt. Express* **15** 16972
[16] Yu J, Jia Z, Yi L, Su Y, Chang G K and Wang T 2006 *IEEE Photon. Technol. Lett.* **18** 265