Available online at www.sciencedirect.com
SCIENCE DIRECT®
Optics Communications 234 (2004) 203–210
OPTICS COMMUNICATIONS
www.elsevier.com/locate/optcom

Tunable electro-optic polarization modulator for quantum key distribution applications

Nikita Yu. Gordeev [1], Karen J. Gordon *, Gerald S. Buller

School of Engineering and Physical Sciences, Heriot–Watt University, Riccarton, Edinburgh EH14 4AS, UK

Received 27 November 2003; received in revised form 4 February 2004; accepted 13 February 2004

Abstract

A tunable polarization retarder based on a bulk buried heterostructure semiconductor waveguide has been demonstrated for the specific application of quantum key distribution. Simplicity of construction, low drive voltage, wide spectral range of operation and potentially high frequency response make it ideal for polarization modulation at the transmitter (Alice) and receiver (Bob) in at least two quantum key distribution protocols. The modulator performance was analyzed in a test quantum key distribution system.

PACS: 42.79.H; 03.67.D

Keywords: Polarization modulator; Quantum cryptography; Quantum key distribution; Optoelectronic device

1. Introduction

Optical modulators based on compound semiconductor structures are commonly used in optical communication applications. These devices are amplitude or phase modulators employing a number of different effects, e.g., the linear electro-optic (LEO), quadratic electro-optic (QEO), band-gap shift, free carrier plasma, Franz–Keldysh, Stark and so on (see examples in [1]). Polarization modulators are generally less widely used, although polarization modulation transmission schemes have been proposed for long-haul telecommunication [2].

The electro-optic effect is caused by the difference in the change of the refractive index of the crystal in the directions of the ordinary and extraordinary rays due to the application of an electric field [1, p. 458]. The electro-optic effect includes both the LEO and QEO effects. The linear electro-optic effect (or Pockels effect) occurs when the electrically induced birefringence is proportional to the applied electric field. The LEO effect is well known as being exhibited in zincblende-type crystals GaAs, InP, and related compounds [3]. One important feature of LEO is that the phase

* Corresponding author. Tel.: +44-131-451-3048; fax: +44-131-451-3136.
E-mail address: k.j.gordon@hw.ac.uk (K.J. Gordon).
[1] On leave from AF Ioffe Physico-Technical Institute, St. Petersburg, Russia.

0030-4018/$ - see front matter © 2004 Elsevier B.V. All rights reserved.
doi:10.1016/j.optcom.2004.02.036

shift between TM and TE modes – the electro-optic retardation – depends on the applied electric field. For example, if linearly polarized input light with its plane of polarization inclined at 45° to each of principal dielectric axes is incident on the crystal, then by varying the applied electric field the output polarization state can be changed to circular polarized or linear polarized light (oriented 90° with respect to the input polarization) [1]. Such a waveguide modulator is a transverse electro-optic modulator. So-called longitudinal electro-optic modulators [1, p. 462] based on bulk semiconductor have also been used as tunable waveplates [4], although they have the disadvantage of requiring a high operating voltage (of typically >1 kV). This, and their bulky size, makes the use of such a device in a fiber based optical system less attractive. Widely used quantum well (QW) modulators mostly employ non-linear electro-optic effects. However, generally in III–V QW structures there is anisotropy and a consequent built-in birefringence [1, p. 466].

Although the LEO effect in semiconductor waveguides is well known [5], to the best of our knowledge, there are no reports of its use as a tunable polarization retarder in the application of quantum key distribution. The expanding field of quantum information processing, particularly quantum key distribution, extensively uses polarization modulation in its protocols [6,7], typically by use of two or more separately modulated lasers [8], or by use of $LiNbO_3$ crystals [9,10]. This paper describes an investigation of an electro-optic polarization modulator based on bulk III–V semiconductor waveguide microstructures, which offers a potentially less complex, and less expensive solution, as well as having the potential for higher speed modulation useful for future advanced quantum key distribution systems.

2. Experimental and discussion

2.1. Waveguide fabrication

The prototype modulator was created from an existing AlGaAs/GaAs heterostructure, originally designed as a laser structure. The heterostructure was grown by liquid phase epitaxy (LPE) and was composed of a bulk AlGaAs active region (0.3 μm) surrounded by cladding layers (2.0 μm each) forming the waveguide. The overlap integral of electric field and propagating light at zero external bias was reduced by the creation of a p–n junction in the upper cladding layer at a distance of 0.4 μm from the waveguide. The prototype modulator was fabricated in a rudimentary geometry similar to that used for a gain-guiding semiconductor laser (i.e., a metal contact on the substrate side, a metal stripe of 8 μm width acting as a contact on epilayer side, with a cavity length of ~1 mm). The device was selected so that the peak of the spontaneous emission occurred at a wavelength of 765 nm, in order that the waveguide was transparent at the operating wavelength of 850 nm. To inhibit the effects of Fabry–Perot oscillations and reduce the insertion loss, both waveguide facets were antireflection coated to $\sim 1 \times 10^{-3}$ reflectance at the operating wavelength of 850 nm. The coated sample was mounted on a copper heatsink.

2.2. Waveguide microstructure as tunable waveplate

Initially the modulator was investigated under constant reverse bias voltage. It is important to notice that the dielectric breakdown voltage was >−20 V. The polarization state of the transmitted light through the waveguide was analyzed using a linear polarizer and optical power-meter. In Fig. 1, a simulation of the voltage dependence of passing light polarization is shown. In this example, the plane of polarization of the incident light is inclined at 45° with respect to the plane of the p–n junction, so that light is launched into both TE and TM modes. Under zero bias, the transmitted light maintains its incident polarization state. However, when a non-zero reversed-biased voltage is applied, the transmitted light polarization is changed significantly. Under the applied voltage of ≈−3.5 V the transmitted polarization becomes right circular. Increasing the applied voltage to −7 V makes the output polarization linear, but the polarization is rotated by an angle of 90° with respect to the input polarization. An applied voltage of ~−10.5 V makes the output polarization left circular, and so on. Thus the waveguide

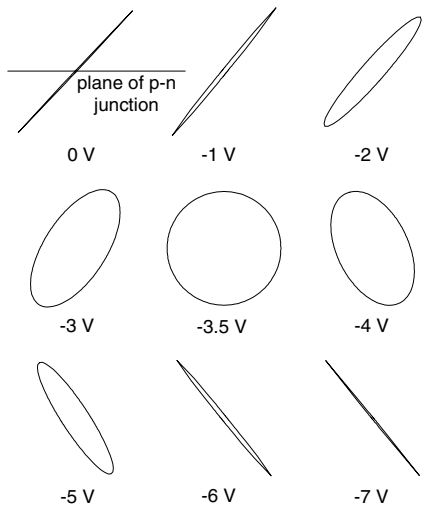

Fig. 1. Reversed-biased voltage dependence of polarization state of light transmitted through the waveguide.

can operate as a tunable electro-optic waveplate, and by applying the appropriate voltage one can use it as $\lambda/4$, $\lambda/2$ or a $3\lambda/4$ waveplate (Table 1).

2.3. Evaluation of polarization modulator used in a two-state quantum key distribution protocol

The B92 protocol is a commonly used quantum key distribution protocol, and one implementation of this protocol is the employment of a pair of non-orthogonal single photon polarization states [6,11]. In this application of the B92 protocol, Alice (the transmitter) encodes the photons with two non-orthogonal linear polarization states (for example, circular and linear polarized photons), whilst Bob (the receiver) independently (and randomly) makes a measurement of either state. Both Alice and Bob can use the proposed device as a tunable zero-half waveplate to both encode and analyze the photon stream. To investigate the possibility of using the modulator in an application of the B92 protocol, a test transmission set-up was constructed, as shown in Fig. 2. This experimental set-up was not a complete implementation of a B92-protocol quantum key distribution system, as it only employed two *orthogonal* polarization states in order to test the practicality of encoding two polarization states using this modulator. However, such a test system can be used to examine the potential of using the modulator in a QKD system based on B92 or BB84 protocols using polarization encoding [11,12]. A similar approach was used by Townsend [9] to examine an optical fiber-based QKD system operated in the first telecommunication window. The use of such short wavelengths (~850 nm) in standard telecommunications fiber will lead to high optical absorption and subsequently reduced transmission ranges. However, the mature technology afforded

Table 1
Comparison of output and input states of waveguide modulator

Input polarization state	Reverse bias voltage (V)	Output polarization state
$\theta°$ (with respect to plane of p–n junction)	0	$\theta°$
	X	Right elliptical
	Y	$-\theta°$ (change of $2\theta°$)
	Z	Left elliptical
45° (with respect to plane of p–n junction)	0	45°
	X	Right circular
	Y	−45° (change of 90°)
	Z	Left circular

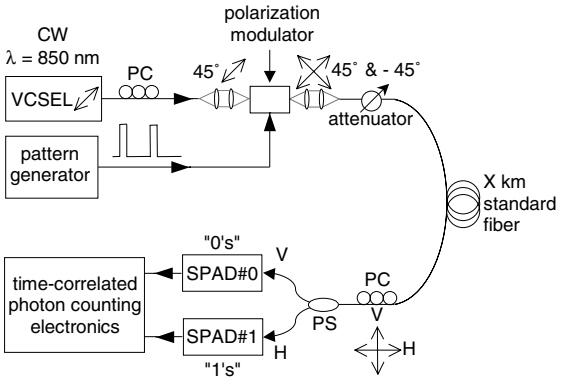

Fig. 2. Experimental arrangement for the investigation of the electro-optic polarization modulator. PC: polarization controller, PS: polarization splitter, SPAD: single photon avalanche diode, VCSEL: vertical-cavity surface-emitting laser, V: vertical polarization state = 0, H: horizontal polarization state = 1.

by the Si-based single-photon detectors operational at such wavelengths can lead to vastly increased bit rates [13,14]. This is due to the relative lack of the deleterious effects of after pulsing that are evident in detectors operational at longer wavelengths [15,16]. A highly attenuated vertical-cavity surface-emitting laser (VCSEL) with an emission wavelength of 850 nm was used as a continuous wave light source in these test measurements. The VCSEL source was driven at a constant current consistent with single spatial mode operation. The waveguide was modulated by a non-return to zero (NRZ) pulsed voltage signal produced by a pattern generator, where the upper voltage level was selected in order for the waveguide to operate as a half-waveplate. For simplicity the zero-voltage will be denoted "0" and non-zero denoted as "1". The incident light had a plane of polarization inclined at 45° to the plane of p–n junction. Hence, when a "0" is applied to the modulator, the optical output from the modulator had a linear polarization of 45°, and correspondingly a "1" gave a linear polarization of −45°. A polarization controller was introduced to give an additional 45° of polarization rotation; hence, a polarizing beam splitter (PBS) could be used to discriminate between the two orthogonal polarization states of the photons of light. At the PBS, the incoming optical signals were routed to the two single-photon detectors according to their polarization states. The encoded photons were detected using single photon avalanche diode (SPAD) detectors, and registered by an acquisition card located in a personal computer. The incoming optical signals with vertical polarization (0°) were directed to SPAD#0 while the optical signals with horizontal polarization (90°) were directed to SPAD#1. An example result is shown in Fig. 3, where counts from both SPADs are shown as a function of time for the case when waveguide is repetitively modulated by the sequence "100101". Fig. 3 shows the histogram developed over many repeats (i.e., $>10^7$) of this test bit sequence, since photon counting statistics and available hardware restrict the actual collection of data to less than one event per transmitted sequence. It is important to notice that the SPADs do not have identical detection efficiency and hence there is a difference in the maximum count levels measured by each SPAD.

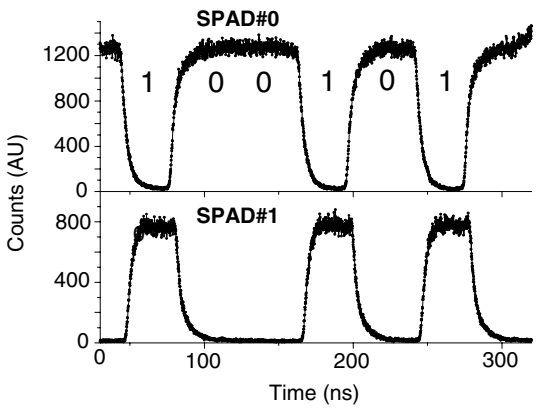

Fig. 3. Photon counts histogram measured using SPAD#0 (vertical polarization) and SPAD#1 (horizontal polarization), for a modulating frequency of 25 MHz.

2.4. Quantum bit error rate, frequency response and propagation losses

The quantum bit error rate (QBER) is the ratio of spurious bits to the total amount of detected bits [6]. In our case QBER for SPAD#0 is:

$$\mathrm{QBER}_{\#0} = \frac{p_{\#1}}{p_{\#1} + p_{\#0}}, \tag{1}$$

where $p_{\#1}$ is the probability of getting a false detection in SPAD#1, $p_{\#0}$ is the probability of detecting a photon in the correct port (i.e., a signal count in SPAD#0). The QBER for port #1 is calculated in a similar manner. To measure QBER, the intensity of light launched into the fiber was reduced to the level of an average of 0.1 photons per bit – similar to that used in experimental QKD systems using weak coherent sources [10,17]. Since the laser was pumped by constant direct current held just below the lasing threshold, the bit length was determined by the modulating signal applied to the waveguide. QBER for different lengths of optical fiber was measured at a modulating frequency of 50 MHz as shown in Fig. 4. The different fiber lengths were mostly simulated by the addition of known attenuation, assuming the losses in optical fiber of 2.2 dB/km. For comparison

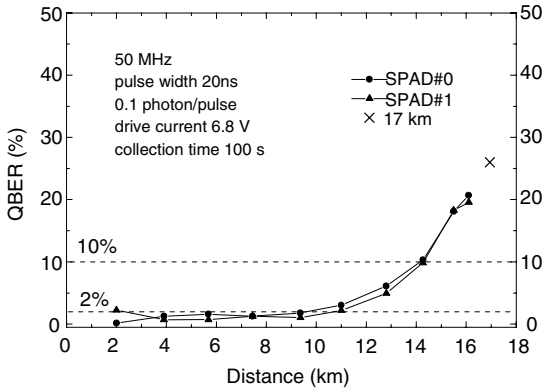

Fig. 4. Quantum bit error rate versus distance for two SPADs. Value of QBER obtained for a 17 km length of standard telecommunications fiber is marked by cross (×), the other points were measured using additional attenuation to simulate the effects of transmission loss. These measurements were taken at 50 MHz modulation frequency, with a corresponding pulse width of pulse width 20 ns, and a mean photon number of 0.1 photons per pulse.

and verification of these results, an actual fiber length of 17 km was also examined under the same conditions as shown in Fig. 4. The QBER was calculated for both detectors and appears very similar. The QBER increases at longer distances because the dark count probability is constant whilst the probability of detection of a "signal" photon diminishes with increased transmission length (i.e., optical absorption) in the fiber. The QBER for both detectors is less than 10% for distances as high as 14 km – a QBER of 10% being widely regarded as close to the maximum acceptable level for secure transmission of the encryption key when such an average number of photons per bit period are emitted from Alice.

The capacitance and series resistance of the waveguide device limits the maximum modulation frequency. The frequency response of the device was investigated, although the prototype device was not optimized for high modulation frequency.

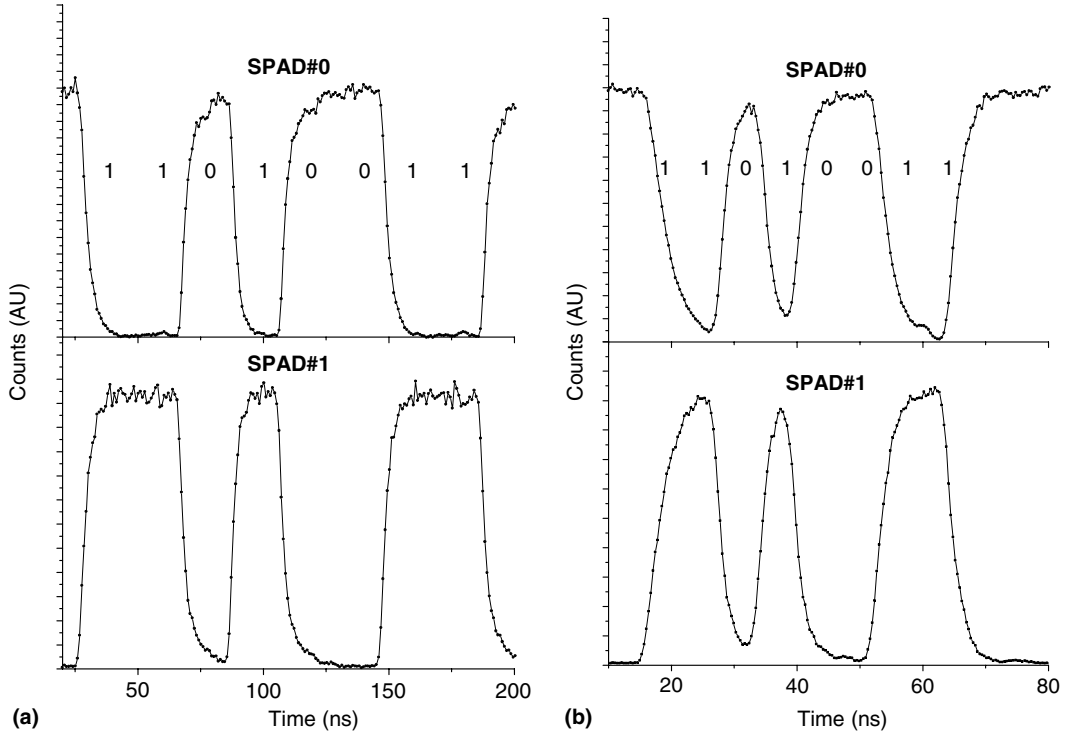

Fig. 5. (a) Photon count histogram for a modulation frequency of 50 MHz; (b) photon count histogram for a modulation frequency of 165 MHz.

Figs. 5(a) and (b) show photon count histograms at the two different modulation frequencies of 50 and 165 MHz (which was the upper limit of driving pattern generator used). Even at the higher frequency, the ratio of the maximum counts to the minimum counts is more than a factor of 10. We believe that by using more appropriate sample waveguide geometry and electronic packaging, the frequency response can be significantly improved.

For effective operation, especially at the receiver (see later), the modulator should keep additional transmission losses as small as possible. From the experiment, we estimated the upper limit of propagation losses as 1.3 dB/mm. The length of the modulator used in these experiments was 1 mm. Again, this value could be reduced by improving the non-optimal waveguide geometry used in these demonstration experiments.

2.5. Polarization modulator in the BB84 protocol of quantum key distribution

BB84 is four-state protocol, one implementation of which involves Alice (transmitter) and Bob (receiver) employing two linear and two circular polarization states of single photons [6,12]. Alice must encode photons in one of the four following polarization states: vertical linear, horizontal linear, right circular, and left circular. Bob must be able to analyze the incident photons in either of the two non-orthogonal basis sets – linear or circular. According to Table 1, the modulator allows Alice to produce photons in each of these four states. Similarly, Bob can also employ the waveguide device as a tunable quarter waveplate in order to chose either the linear or circular measurement basis set. It is important to notice that a pattern generator providing a sequence of pulses with four voltage levels is essential to drive the polarization modulator in a true four-state protocol QKD system. However, these experiments demonstrate the feasibility of using the modulator at both Alice and Bob.

To evaluate the modulator we inserted a fiber-based quarter waveplate in front of the PBS modified the experimental set-up shown in Fig. 2. The modulating voltage was chosen to convert the input 45° linear polarization into right circular or left circular polarization so that the modulator worked as a $\lambda/4$ or $3\lambda/4$ waveplate. The quarter waveplate converts circularly polarized light passed through the fiber into linearly polarized light, in order for right circular polarization to be registered in SPAD#0 and left circular polarization in SPAD#1, respectively. The corresponding time response is presented in Fig. 6.

A complementary experiment was performed to evaluate the modulator performance at Bob. Using the fiber based quarter waveplate described above, circularly polarized light was launched into the modulator. Again, it worked as a $\lambda/4$ or $3\lambda/4$ waveplate modulated circularly polarized light into linearly polarized 0° or 90°, respectively, as shown in Fig. 7.

These experiments demonstrate the potential of utilizing two modulators in a polarization-encoded implementation of the BB84 protocol.

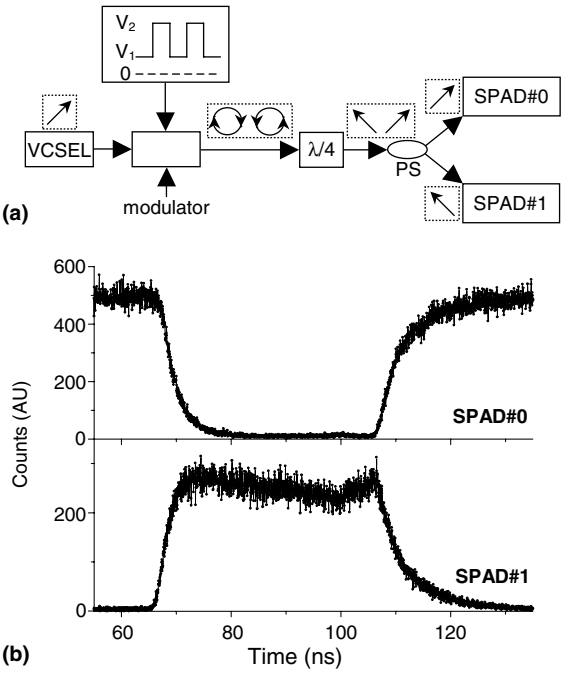

Fig. 6. (a) The device modulates linear polarized light into left or right circular polarized light at transmitter (Alice). PS: polarization splitter. (b) Experimental results for SPAD#0 and SPAD#1.

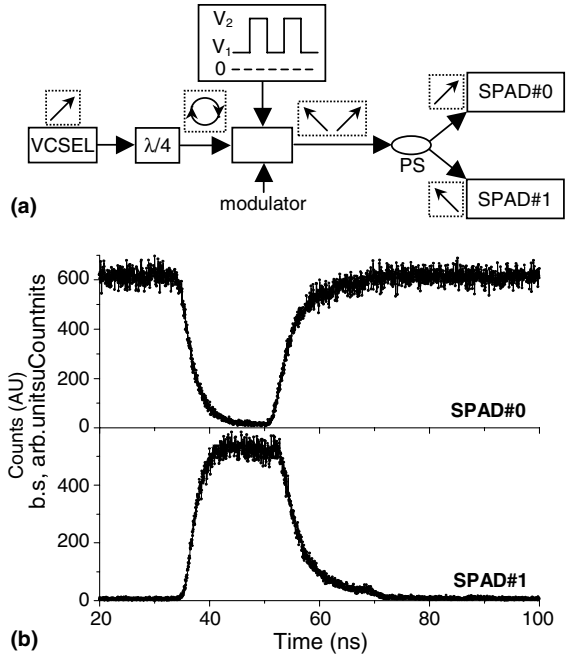

Fig. 7. (a) The device modulates left or right circularly polarized light into linear polarized light at Bob's receiver. PS: polarization splitter. (b) Experimental results for SPAD#0 and SPAD#1.

3. Conclusions

A polarization modulator has been demonstrated which is suitable for use in polarization-encoding implementations of both the B92 and BB84 quantum key distribution protocols. The simplicity of construction and ease of use makes this device a practical and inexpensive solution to the problem of polarization modulation in QKD schemes, at both the transmitter and receivers. The device was demonstrated at a clock rate of 165 MHz, however modulation rates of GHz are potentially achievable with additional routine device microfabrication steps. The prototype AlGaAs/GaAs modulator was suitable for use at wavelengths of around 850 nm, however the same approach could be used to construct similar modulators from other material systems for QKD demonstrators operating at wavelengths of 1.3 and 1.55 μm. As quantum key distribution system demonstrations move to higher clock rates, the modulation method used for polarization encoding will become an increasingly important issue. Recent experiments from this group [18] have shown gigahertz clock rates that utilize modulation by separate laser sources, however the use of multiple weak sources can compromise security via spectral interrogation by an eavesdropper. The modulator used in these experiments can be adapted for high frequency polarization modulation of the output from a single weak coherent source.

Acknowledgements

This work was supported by the UK Engineering and Physical Sciences Research Council project GR/N12466, and the European Commission's Framework Five EQUIS project (IST-1999-11594). The authors acknowledge many useful discussions with Professor Paul Townsend, University College Cork, Ireland.

References

[1] P.K. Bhattacharya, Semiconductor Optoelectronic Devices, second ed., Prentice-Hall Int., Englewood Cliffs NJ, 1997.
[2] A. Carena, V. Curri, R. Gaudino, N. Greco, P. Poggolini, S. Benedetto, in: Proceedings of the European Conference Optical Communications (ECOC 98), Madrid, Spain, 20–24 September, 1998, p. 429.
[3] S.S. Lee, R.V. Ramaswamy, IEEE J. Quant. Electron. 27 (1991) 726.
[4] Y. Bitou, T. Minemoto, Appl. Opt. 37 (1998) 4347.
[5] K. Wakita, Semiconductor Optical Modulators, Kluwer Academic Publishers, Dordrecht, 1998.
[6] P.D. Townsend, Opt. Fiber Technol. 4 (1998) 345.
[7] R.J. Hughes, G.L. Morgan, C.G. Peterson, J. Mod. Opt. 47 (2000) 533.
[8] R.J. Hughes, J.E. Nordholt, D. Derkacs, C.G. Peterson, New. J. Phys. 4 (2002) 43.1.
[9] P.D. Townsend, IEEE Photon. Tech. Lett. 10 (1998) 1048.
[10] J.G. Rarity, P.R. Tapster, P.M. Gorman, J. Mod. Opt. 48 (2001) 1887.
[11] C.H. Bennett, Phys. Rev. Lett. 68 (1992) 3121.
[12] C.H. Bennett, G. Brassard, in: Proceedings of the IEEE International Conference of Computers, Systems and Signal Processing, Bangalore, India, 1984, p. 175.

[13] S. Cova, A. Lacaita, G. Ripamonti, IEEE Electron Device Lett. 12 (1991) 685.
[14] H. Dautet, P. Deschamps, B. Dion, A.D. MacGregor, D. MacSween, R.J. McIntyre, C. Trottier, P.P. Webb, Appl. Opt. 32 (1993) 3894.
[15] F. Zappa, A.L. Lacaita, S.D. Cova, P. Lovati, Opt. Eng. 35 (1996) 938.
[16] P.A. Hiskett, G.S. Buller, A.Y. Loudon, J.M. Smith, I. Gontijo, A.C. Walker, P.D. Townsend, M.J. Robertson, Appl. Opt. 39 (2000) 6818.
[17] P.A. Hiskett, G. Bonfrate, G.S. Buller, P.D. Townsend, J. Mod. Opt. 48 (2001) 1957.
[18] K.J. Gordon, V. Fernandez, P.D. Townsend, G.S. Buller, IEEE J. Quant. Electron. (2004) (submitted).