Appl. Phys. B 73, 855–859 (2001)
DOI: 10.1007/s003400100723

Applied Physics B
Lasers and Optics

S. LORENZ[1,✉]
CH. SILBERHORN[1]
N. KOROLKOVA[1]
R.S. WINDELER[2]
G. LEUCHS[1]

Squeezed light from microstructured fibres: towards free-space quantum cryptography

[1] Zentrum für moderne Optik, Universität Erlangen-Nürnberg, Staudtstr. 7/B2, 91058 Erlangen, Germany
[2] Bell Laboratories, Lucent Technologies, 700 Mountain Avenue, Murray Hill, NJ 07974, USA

Received: 9 July 2001
Published online: 23 November 2001 •

ABSTRACT Amplitude-squeezed pulsed light has been produced using a microstructured silica fibre. By spectrally filtering after the non-linear propagation in the fibre a squeezing value of -1.7 dB has been measured. A quantum key distribution scheme based on squeezed light from such microstructured fibres is proposed.

PACS 03.67.Dd; 42.50.Lc; 42.65.-k

1 Introduction

Over the past years quantum effects have been demonstrated in systems described by continuous variables. Entanglement was produced using non-degenerate parametric amplification [1–3], the Kerr effect in a silica fibre [4] and four-wave mixing in a fibre-optic parametric oscillator [5]. One way to produce the entanglement is by interference of two squeezed-light beams. We introduce a new tool to generate non-classical light in the near infrared, which shows great potential as compared to a device using standard silica fibres.

2 Quantum effects in microstructured fibres

The microstructured fibre evolved from experiments with photonic band gap materials. It consists of pure silica, with a bulk core and a cladding which has a regular pattern of holes, oriented in the longitudinal direction [6]. Due to these holes, the cladding has a lower effective refractive index than the solid silica core. This refractive-index difference causes total internal reflection at the core–cladding interface. The guiding effect thus is the same as in standard silica fibres.

However, the light mode is not completely confined in the core; there is a small part of the mode which propagates in the cladding. Its relative proportion depends on the wavelength. The effective refractive index of the cladding therefore depends on the penetration depth, and thus on the wavelength of the propagating field.

✉ E-mail: stefan.lorenz@physik.uni-erlangen.de

2.1 *Pulse propagation*

Pulse propagation in fibers can be described by the so-called non-linear Schrödinger equation (NLSE)

$$\mathrm{i}\frac{\partial A}{\partial z} - \frac{\beta_2}{2}\frac{\partial^2 A}{\partial T^2} + \gamma|A|^2 A = 0, \tag{1}$$

which describes the propagation of ps and sub-ps pulses [7], neglecting higher-order dispersion and higher-order non-linearity. In the case of a negative group velocity dispersion β_2 the fibre non-linearity γ allows for the formation of a stable pulse, called a soliton [8, 9]. Due to the stability of the soliton against dispersive broadening, the pulse's peak power remains virtually constant over a long interaction length. Thus, even the low non-linearity of silica can lead to significant quantum effects.

2.2 *Spectral filtering*

A stable soliton solution of the classical equation (1) is a pulse with a special envelope (hyperbolic-secant) and a particular peak amplitude. When quantising the field the corresponding solutions of the quantised version of (1) are no longer stable, owing to the amplitude and phase uncertainties. Thus the non-linear Kerr effect induces new spectral sidebands in the pulse by self-phase modulation, depending on the amplitude of the propagating field, even for solitons. This interaction between different spectral components of the pulse leads to amplitude noise correlations. They can be exploited to reduce the overall noise in the pulse. This technique is known as squeezing by spectral filtering and has been used for ps pulses [10] and for sub-ps pulses [11]. Numerical simulations [12] as well as experimental tests [13] have shown the high degree of correlation. Our goal is to investigate whether the correlations also exist in the new microstructured fibre, where solitons can propagate at a centre wavelength shorter than 800 nm. In this interesting wavelength regime, only non-soliton photon-number squeezing has been shown [14, 15] so far.

2.2.1 Experimental setup. The experimental configuration is shown in Fig. 1. The 130-fs pulses of a commercial Ti:sapphire laser system (Spectra Tsunami, repetition rate

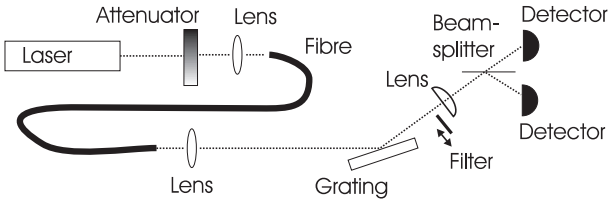

FIGURE 1 Experimental setup

82 MHz) were launched into a 1-m piece of microstructured fibre (Lucent) through a telescope and an aspheric lens. The output beam was collimated through another aspheric lens and reflected by a blazed, gold-plated grating (Jobin Yvon, 600 lines/mm). The fibre end was imaged to the filter plane, where a knife edge acted as a high-pass filter. The filtered beam was then focused by a cylindrical lens through a 50 : 50 beam splitter onto two photodetectors which served as a balanced detection system (photodiode: Osram BPW34, silicon PIN). The balanced detection enabled us to measure amplitude fluctuations with reference to the shot-noise level. The sum and difference AC photocurrents of the two detectors were recorded by two electronic spectrum analysers (HP 8590) at 23 MHz with a bandwidth of 300 kHz, a video bandwidth of 30 Hz and averaged over 30 measurement cycles.

2.2.2 Results. Figure 2 shows typical input and output spectra of the fibre, as well as autocorrelation traces. The nonlinearity of the microstructured fibre is about 20 times larger than that of standard telecommunication fibres and the soliton energy is 9 pJ. For the measurement reported here a slightly higher pulse energy was used. This explains the pulse narrowing shown in Fig. 2. The pulse energy and the resulting average power are still ten times below saturation, in contrast to previous experiments [14]. In the experiment reported here, the detector signal was only slightly above the electronic noise, so that the sum as well as the difference photocurrents have been corrected for electronic noise of the detection system. Note that the ratio between the optical signal or noise and the electronic noise will be an order of magnitude higher when using heterodyne detection with local oscillator pulses as discussed below.

To check that the measured difference photocurrent corresponded to the shot noise, the beam was attenuated with several neutral density filters. The variance of the photocurrent difference exhibited a linear behaviour with respect to the beam power as expected for Poissonian statistics.

A typical measurement is shown in Fig. 3. For a filter cut-off frequency between 9.5 and 10.25, the sum AC photocurrent drops below the difference photocurrent, which represents the shot-noise level. The maximum squeezing obtained is -1.7 dB.

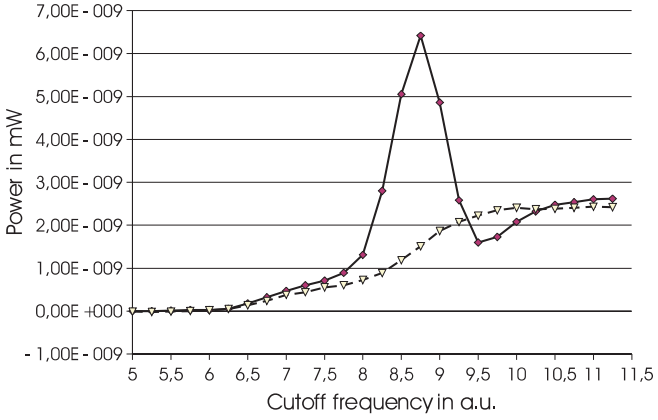

FIGURE 3 Typical measurement curve at a pulse energy of 15.8 pJ. The AC noise powers of sum (*solid line*) and difference (*dashed line*) photocurrents over the filter high-pass cut-off are given in arbitrary units

2.3 *Non-linear fibre Sagnac interferometer*

A squeezing source that uses spectral filtering has some inherent technical difficulties. The spectral dispersion at the grating is very lossy, and the collimation of the filtered beam is tedious. There is also a fundamental limit for squeezing using spectral filtering [16]. We therefore aim at another scheme of squeezed-light production, which has proven to be useful before in a standard silica fibre [17]. The asymmetric non-linear fibre Sagnac interferometer is known as a stable source for squeezed bright-light pulses. The input

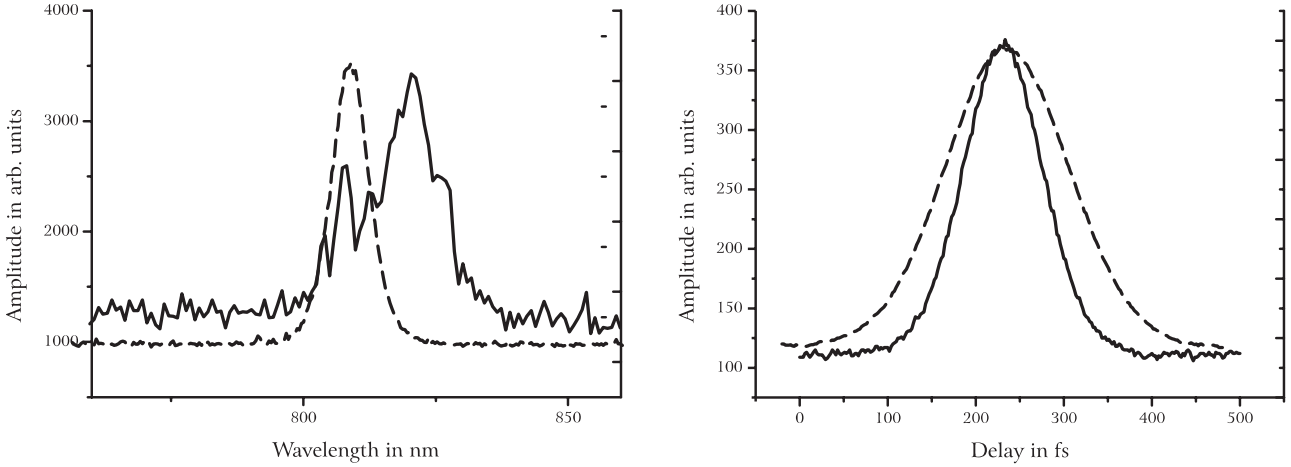

FIGURE 2 *Left*: input and output spectra at an output power of 1.16 mW corresponding to a pulse energy of 14.1 pJ. *Right*: corresponding autocorrelation traces. The *dashed curves* show the input pulse, the *solid curves* the output pulse after the fibre

pulse is split into a bright and a dark pulse, which counter-propagate in the same fibre in the interferometer. They interfere at the output, and for certain input energies they generate a bright amplitude squeezed output pulse. Due to the insufficient polarisation-maintaining properties of the fibre used, the double NOLM (non-linear optical loop mirror) principle [4] cannot be used. Thus, we plan to build two independent NOLMs to produce two independently amplitude-squeezed pulses.

3 Possible entangled states

With two amplitude-squeezed beams, one can realise an entangled quantum state. In the past there have been problems in defining entanglement in the case of continuous-variable systems. If one defines entanglement as the non-separability of a state, necessary and sufficient conditions for entanglement of discrete-variable systems have been found by Peres [18] and Horodecki [19, 20]. Their criterion has been expanded by Duan et al. [21] and Simon [22] for the case of continuous-variable systems.

If it comes to practical quantum communication, however, one might be interested in the correlations between the two subsystems (A and B) of an entangled system. These are the correlations which help to infer the value of a variable measured at subsystem A if the variable is already known at subsystem B. This quantum-mechanical property of an entangled pair was pointed out by Einstein et al. [23] and later by Reid [24] for optical fields. It is the basic building block of the proposed cryptography system.

3.1 *Amplitude and phase entanglement*

The entanglement scheme applied with a quantum cryptographic application in mind uses uncertainty correlations produced by the superposition of two amplitude-squeezed beams at a beam splitter [25]. This results in amplitude 'noise' anti-correlations and phase 'noise' correlations of the two output beams. The amplitude correlations have been measured directly, and the phase correlations indirectly for a NOLM made of a non-polarisation-preserving telecommunication fibre [4].

3.1.1 Optical heterodyne detection. The noise of a single beam can be measured by balanced optical heterodyne detection, using a strong local oscillator, a beam splitter and a pair of balanced photodetectors. By variations of the phase of the local oscillator, amplitude and phase noise of the signal beam can be measured. Up to now, an optical heterodyne measurement has not been realised for intense beams, as the strong local oscillator would lead to saturation effects in the photodetectors. A NOLM using microstructured fibres would operate at a lower signal power, so that optical heterodyne detection may be used.

3.2 *Polarisation entanglement*

An alternative to amplitude- and phase-correlated beams is polarisation entanglement with intense beams [26]. In contrast to dichotomic polarisation systems, not the polarisations themselves, but the variances of the Stokes' parameters, are correlated. The detection of these correlations is possible by use of passive, linear elements only, without the need for a local oscillator.

4 Quantum cryptography

Quantum cryptography uses quantum effects to establish a random bit key, only known to two parties (Alice and Bob). The presence of an eavesdropper (Eve) can be detected during the key generation.

4.1 *Free-space quantum cryptography*

There are two applications which require free-space transmission rather than fibre-based communication. The first is short-distance communication up to several kilometres [27, 28], mainly in urban areas, where a fibre-based connection is too expensive to deploy. The second is secure satellite communication, where a fibre link is not possible.

For both applications a system operating at a wavelength of 800 nm has several advantages over a system operating at 1.5 μm. The beam divergence is considerably lower, allowing for smaller transmitter and receiver optics. The shorter wavelength also allows for the use of silicon photodetectors, which are cheaper, have lower dark-noise levels and are standard industry products. In addition, the atmospheric transmission has several transparency windows at 800 nm, while there is considerable absorption at 1.5 μm.

4.2 *A quantum key distribution scheme*

The quantum key distribution (QKD) scheme we intend to use is described in [29, 30]. It depends on the correlations that exist between amplitude and phase noise of an entangled pair of bright pulses. The bit value generated depends on the type of measurement Bob and Alice perform: for example '1' for amplitude and '0' for phase measurement. Alice keeps one pulse of the pair and sends the other to Bob over the quantum channel. They both now measure randomly and independently amplitude or phase of their pulses, and Bob sends the results – but not the type – of his measurement back to Alice. If Alice can spot correlations between her measurement and Bob's, she knows that they both have performed the same type of measurement. She tells Bob that his measurement was correlated, and they each assign the appropriate bit values to these measurement slots. If Alice detects a reduced degree of correlation, she knows that the quantum channel has been manipulated.

We propose the implementation of the quantum key distribution system where the squeezed-light sources are built on the basis of NOLMs made of microstructured fibre. The scheme is secure against beam-splitting attacks, provided the correlations are strong enough. The speed of key generation is limited by the pulse-repetition rate of the system, as well as by the correlation-measurement time. From the correlation measurements already conducted we estimate the maximum achievable raw bit rate to be 10% of the pulse-repetition rate. A repetition rate of up to 100 GHz is conceivable.

4.2.1 QKD for amplitude and phase correlations. The proposed setup is shown in Fig. 4. Two independent NOLMs produce two amplitude-squeezed light pulses, which are used to generate an entangled pulse pair. The first pulse stays at Alice's site and either its phase or its amplitude fluctuations are measured. The second pulse is transmitted to Bob, along with the local oscillator. Bob also measures either amplitude or phase fluctuations and transmits his photocurrents back to Alice. She checks the photocurrents for correlations and marks the measurements where she and Bob measured the same variable. From the type of measurement Alice and Bob generate a string of shared random bits.

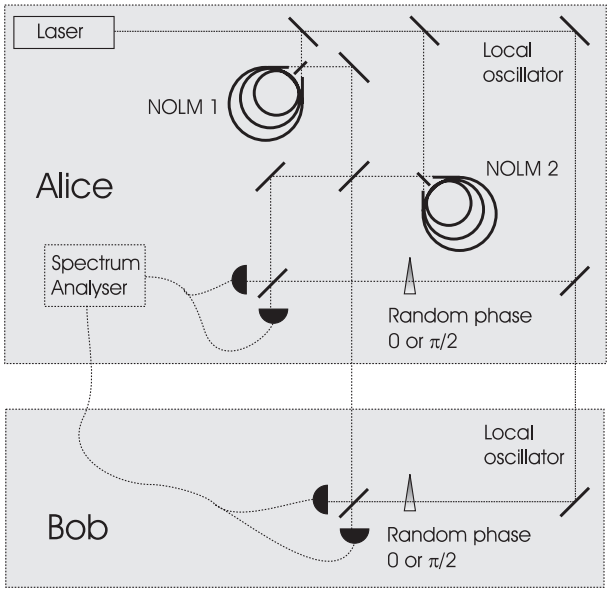

FIGURE 4 Proposed setup for the QKD system

4.2.2 QKD for polarisation correlations. To implement a QKD scheme using polarisation correlations as mentioned above, one would need four NOLMs, or two with a polarisation-maintaining fibre. The greater effort one has to put into the generation of the entangled pulses is compensated by the substantially reduced complexity of the detection apparatus. There is no need to transmit a local oscillator to Bob, so that his receiving station is a simple linear device with no need for interferometric stability. We plan to update the amplitude/phase setup to a polarisation setup in a second step.

5 Conclusions

The potential of the microstructured fibre for the production of non-classical bright light has been shown. An amplitude squeezing of 1.7 dB below shot noise was achieved using spectral filtering. We hope to improve this value by optimising system parameters such as the fibre length. A next goal is the implementation of the microstructured fibre in two asymmetric fibre Sagnac interferometers, to produce an EPR (Einstein Podolski Rosen)-entangled beam pair at 810 nm. With the operation of the fibre-based system in this new wavelength regime, free-space quantum cryptography with continuous variables will become viable.

ACKNOWLEDGEMENTS The authors wish to thank Florence Gadaud, Oliver Glöckl, Michael Langer and Christoph Marquardt for their support. This work was supported by the German ministry of education and science (BMBF) under VDI-AZ 0155/00.

REFERENCES

1 Z.Y. Ou, S.F. Pereira, H.J. Kimble, K.C. Peng: Realization of the einstein-podolsky-rosen paradox for continuous variables. Phys. Rev. Lett. **68**, 3663 (1992)
2 A. Furusawa, J.L. Sorensen, S.L. Braunstein, C.A. Fuchs, H.J. Kimble, E.S. Polzik: Unconditional quantum teleportation. Science **282**, 706 (1998)
3 Y. Zhang, H. Wang, X. Li, J. Jing, C. Xie, K. Peng: Experimental generation of bright two-mode quadrature squeezed light from a narrow-band nondegenerate optical parametric amplifier. Phys. Rev. A **62**, 023913 (2000)
4 Ch. Silberhorn, P.K. Lam, O. Weiß, F. König, N. Korolkova, G. Leuchs: Generation of continuous variable einstein-podolsky-rosen entanglement via the kerr nonlinearity in an optical fibre. Phys. Rev. Lett. **86**, 4267 (2001)
5 J.E. Sharping, M. Fiorentino, P. Kumar: Observation of twin-beam-type quantum correlation in optical fiber. Opt. Lett. **26**, 367 (2001)
6 J.K. Ranka, R.S. Windeler, A.J. Stentz: Visible continuum generation in air-silica microstructure optical fibers with anomalous dispersion at 800nm. Opt. Lett. **25**, 25 (2000)
7 G.P. Agrawal: *Nonlinear fiber optics*. *Optics and Photonics* (Academic, San Diego 1995)
8 A. Hasegawa, F. Tappert: Transmission of stationary nonlinear optical pulses in dispersive dielectric fibers. i. anomalous dispersion. Appl. Phys. Lett. **23**, 142 (1973)
9 L.F. Mollenauer, R.H. Stolen, J.P. Gordon: Experimental observation of picosecond pulse narrowing and solitons in optical fibers. Phys. Rev. Lett. **45**, 1095 (1980)
10 S.R. Friberg, S. Machida, M.J. Werner, A. Levanon, T. Mukai: Observation of optical soliton photon-number squeezing. Phys. Rev. Lett. **77**, 3775 (1996)
11 S. Spälter, M. Burk, U. Strößner, M. Böhm, A. Sizmann, G. Leuchs: Photon number squeezing of spectrally filtered sub-picosecond optical solitons. Europhys. Lett. **38**, 335 (1997)
12 D. Levandovsky, M. Vasilyev, P. Kumar: Perturbation theory of quantum solitons: continuum evolution and optimum squeezing by spectral filtering. Opt. Lett. **24**, 43 (1999)
13 S. Spälter, N. Korolkova, F. König, A. Sizmann, G. Leuchs: Observation of multimode quantum correlations in fiber optical solitons. Phys. Rev. Lett. **81**, 786 (1998)
14 F. König, S. Spälter, I.L. Shumay, A. Sizmann, Th. Fauster, G. Leuchs: Fiber-optic photon-number squeezing in the normal group-velocity dispersion regime. J. Mod. Opt. **45**, 2425 (1998)
15 D. Krylov, K. Bergman, Y. Lai: Photon-number squeezing in the normal-dispersion regime. Opt. Lett. **24**, 774 (1999)
16 A. Mecozzi, P. Kumar: Linearized quantum-fluctuation theory of spectrally filtered optical solitons. Opt. Lett. **22**, 1232 (1997)
17 S. Schmitt, J. Ficker, M. Wolff, F. König, A. Sizmann, G. Leuchs: Photon-number squeezed solitons from an asymmetric fiber-optic sagnac interferometer. Phys. Rev. Lett. **81**, 2446 (1998)
18 A. Peres: Separability criterion for density matrices. Phys. Rev. Lett. **77**, 1413 (1996)
19 M. Horodecki, P. Horodecki, R. Horodecki: Separability of mixed states: necessary and sufficient conditions. Phys. Lett. A **223**, 1 (1996)
20 P. Horodecki: Separability criterion and inseparable mixed states with positive partial transposition. Phys. Lett. A **232**, 333 (1997)
21 L.M. Duan, G. Giedke, J.I. Cirac, P. Zoller: Inseperability criterion for continuous variable systems. Phys. Rev. Lett. **84**, 2722 (2000)
22 R. Simon: Peres-horodecki separability criterion for continuous variable systems. Phys. Rev. Lett. **84**, 2726 (2000)
23 A. Einstein, B. Podolsky, N. Rosen: Can quantum-mechanical description of physical reality be considered complete? Phys. Rev. **47**, 777 (1935)
24 M.D. Reid: Quantum cryptography with a predetermined key, using continuous-variable einstein-podolsky-rosen correlations. Phys. Rev. A **62**, 062308 (2000)

25 G. Leuchs, T.C. Ralph, Ch. Silberhorn, N. Korolkova: Scheme for the generation of entangled solitons for quantum communication. J. Mod. Opt. **46**, 1927 (1999)
26 N. Korolkova, G. Leuchs, R. Loudon, T.C. Ralph, Ch. Silberhorn: Polarization squeezing and continuous variable polarization entanglement. Phys. Rev. (2001), submited
27 W.T. Buttler, R.J. Hughes, P.G. Kwiat, S.K. Lamoreaux, G.G. Luther, G.L. Morgan, J.E. Nordholt, C.G. Peterson, C.M. Simmons: Practical free-space quantum key distribution over 1 km Phys. Rev. Lett. **81**, 3283 (1998)
28 J.G. Rarity, P. Gorman, P.R. Tapster: Free space quantum cryptography and satellite secure key distribution. In: Dig. QUICK Conf., Cargese, Corsica, 2001, p. WeM2
29 Ch. Silberhorn, N. Korolkova, G. Leuchs: Quantum cryptography with bright entangled beams. In: Dig. Conf. IQEC'2000, Nice, 2000, p. 8
30 Ch. Silberhorn, N. Korolkova, G. Leuchs: Quantum key distribution with continuous variables. Tech. Rept, Lehrstuhl für Optik – Annu. Rept 2000, 2001