tuations on the signal path. However, since the response time of the algorithm running on the microcomputer is currently limited to one second, deliberately bending the fibre caused

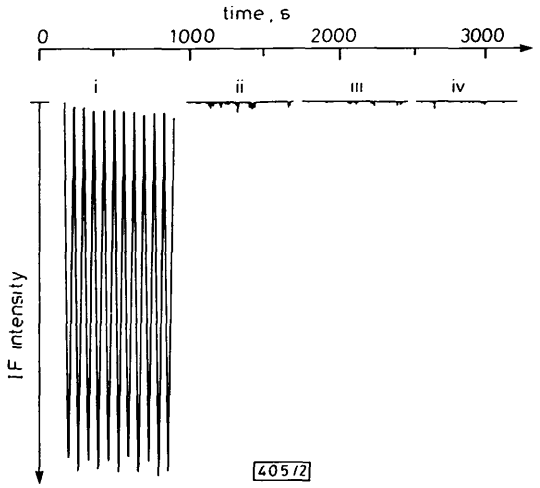


Fig. 2 *Fluctuations in IF level*
(i) Controller switched off
(ii)–(iv) Controller switched on and input state of polarisation rotating about three orthogonal circles on the Poincaré sphere

significant loss of data. It is envisaged that a hardware implementation of the algorithm should be able to track polarisation fluctuations at several hundred Hz, which would be sufficient for all reported variations.[7]

The controller introduces large absolute phase shifts, which may be a problem in some applications, particularly if a high speed control algorithm is used. At the expense of additional splice loss, this can be partially compensated by replacing each of the four PM fibre coils by two coils, wound on separate piezoelectric cylinders and spliced together with a 90° rotation between their principal axes. If the cylinders are then driven in antiphase, the crossing of the fast and slow axes of the PM fibre will make the differential phase shift additive, whilst the absolute phase shifts will cancel. This approach was not required for our application, but preliminary experiments indicated that absolute phase shifts could easily be reduced by a factor of 20.

Conclusions: A rugged all-fibre polarisation controller with a 1·5 dB loss has been produced, and its performance has been extensively verified. It is capable of endless control between two arbitrary time-varying polarisation states, and has been successfully used in a 565 Mbit/s coherent optical transmission system over the installed fibre, with no observed sensitivity penalty. There is potential for increasing the speed of response, with a hardware implementation of the control algorithm, and also for reducing the insertion loss.

Acknowledgments: The authors thank Mark Rutherford for technical assistance, and the Director of Research and Technology, British Telecom Research Laboratories for permission to publish this letter.

G. R. WALKER
N. G. WALKER
British Telecom Research Laboratories
Martlesham Heath
Ipswich IP5 7RE, United Kingdom

8th September 1988

References

1 OKASHI, T.: 'Polarisation-state control schemes for heterodyne or homodyne optical fibre communications', *IEEE J. Lightwave Tech.*, 1985, **LT-3**, pp. 1232–1237
2 CREANER, M. J., STEELE, R. C., WALKER, G. R., and WALKER, N. G.: '565 Mbit/s optical PSK transmission system with endless polarisation control', *Electron. Lett.*, 1988, **24**, (5), pp. 270–271
3 TATAM, R. P., PANNELL, C. N., JONES, J. D. C., and JACKSON, D. A.: 'Full polarisation state control utilising linearly biefringent monomode optical fibre', *IEEE J. Lightwave Tech.*, 1987, **LT-5**, pp. 980–985
4 WALKER, N. G., and WALKER, G. R.: 'Endless polarisation control using four fibre squeezers', *Electron. Lett.*, 1987, **23**, pp. 290–292
5 RASHLEIGH, S. C.: 'Polarimetric sensors: exploiting the axial stress in high birefringence fibres'. First International Conference on Optical Fibre Sensors, IEE, London, 1983, pp. 210–213
6 EICKHOFF, W.: 'Temperature sensing by mode-mode interference in birefringent optical fibres', *Opt. Lett.*, 1981, **6**, pp. 204–206
7 NAMIHIRA, Y., HORIUCHI, Y., RYU, S., MOCHIZUKI, K., and WAKABAYASHI, H.: 'Dynamic polarisation fluctuation characteristics of optical fibre submarine cables under various environmental conditions', *IEEE J. Lightwave Tech.*, 1988, **6**, pp. 728–738

FIELD DEMONSTRATION OF 565 Mbit/s DPSK COHERENT TRANSMISSION SYSTEM OVER 176 km OF INSTALLED FIBRE

Indexing terms: Lasers and laser applications, Optical communications, Optical fibres, Optical transmission

We report the results of a 565 Mbit/s coherent system field trial over 176 km of installed SM fibre. Fully automated endless polarisation control was employed using a novel method and error free operation was achieved with BER readings of better than 10^{-13}.

Introduction: To date many coherent systems have been developed and tested in laboratory environments. However, at present a large technological gap needs to be bridged in order to develop a coherent optical transmission system capable of operating in a field environment. Here we report the results of the first coherent system field demonstration to be performed over conventional installed single mode fibre. The 565 Mbit/s DPSK heterodyne system features miniaturised long external cavity (LEC) lasers, automated endless polarisation control and a laser amplifier as a power booster at the transmitter. Error free operation was achieved with BER readings of better than 10^{-13}.

System description: The system arrangement is shown in Fig. 1. Packaged external cavity lasers tuned to 1·534 μm and

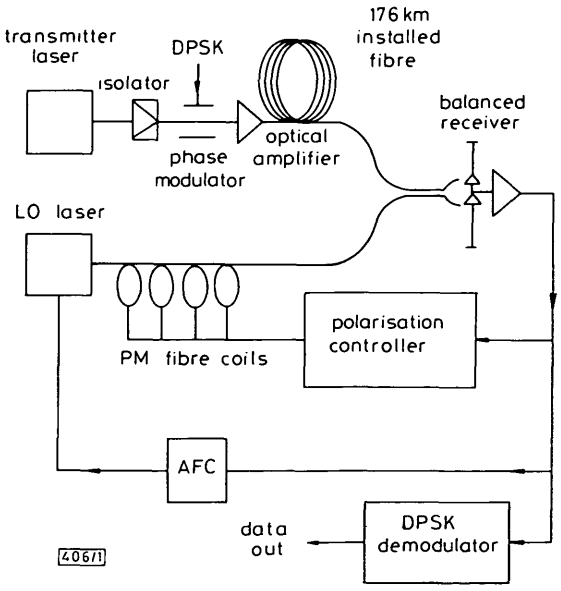


Fig. 1 *DPSK coherent system diagram*

temperature stabilised to better than 0·1°C were used for both the transmitter and local oscillator. These lasers are continuously tunable over 50 GHz and step tunable over 50 nm with a linewidth of less than 100 kHz and a launch power >0 dBm.[1] The transmitter laser was DPSK modulated at

565 Mbit/s using a $LiNbO_3$ phase modulator. A fibre coupled optical isolator[2] was used to prevent reflection induced line-broadening and the combined loss of ~10 dB through the isolator and phase modulator resulted in a net launch power of −10 dBm. The polarisation control system, with a loss of 3·3 dB, was inserted in the local oscillator arm and comprised four lengths of PM fibre wound on piezoelectric cylinders.[3] The fibre sections were spliced together with their principle axes mutually oriented at 45°. Stretching of the fibres via the cylinders modifies the net birefringence, giving polarisation rotations about successively orthogonal axes on the Poincaré sphere, while applying very low strain to the fibre. The control algorithm to achieve endless polarisation control has been previously described.[4]

A dual detector balanced receiver was used with a 3 dB bandwidth of 3 GHz and a noise current spectral density of 13·4 pA $Hz^{0.5}$. This was designed for a high return loss (>50 dB) thereby eliminating the need for optical isolation of the local oscillator laser. The 3·3 dB loss in the polarisation controller resulted in a local oscillator power at the receiver of −3 dBm. Automatic frequency control of the local oscillator laser via piezoelectric movement of the grating stabilised the intermediate frequency to 847 ± 10 MHz. A delay line demodulator with IF and baseband filtering was used to recover the data. The entire transmission system (optics and electronics) was assembled into a standard 19 inch rack unit (Fig. 3) which was easily dismantled and reassembled after transport to the test site.

Transmission system results: The transmission path comprised conventional single-mode fibre in an 18-fibre cable, installed in the British Telecom network between Cambridge, St. Neots and Bedford (Fig. 2). Two routes, *A* and *B*, were configured by splicing the available fibres in the cable to form loops measuring 108 km and 176 km, respectively. The initial experiment was performed over the 108 km route and the power budget is shown in Table 1. A 2^7 PRBS was transmitted at 565 Mbit/s and error free operation was achieved, indicating a BER level of below 10^{-13}. The measured receiver sensitivity was −47·6 dBm (276 photons/bit) at 10^{-9} BER, yielding a system margin of 8 dB.

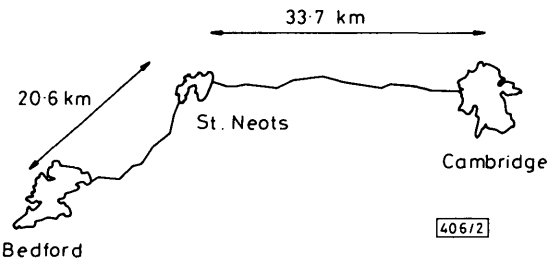


Fig. 2 *Installed cable route map*

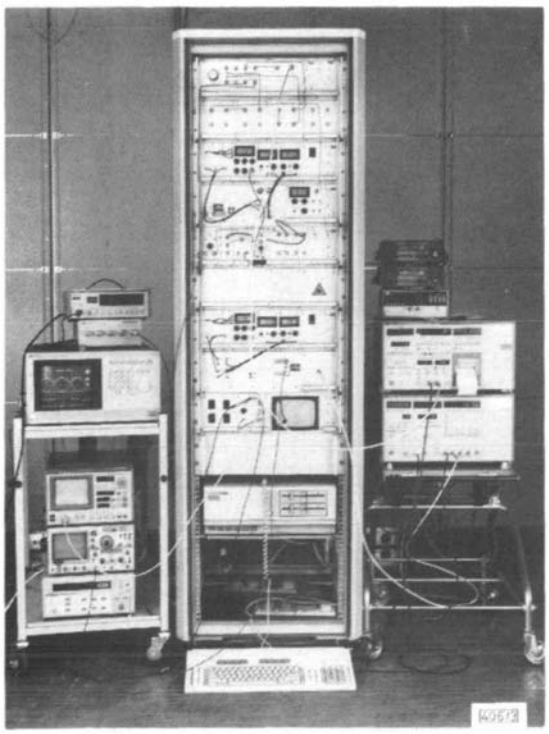


Fig. 3 *19 inch rack layout*

Table 1 Power budgets for routes *A* and *B*

	Route A (without laser amplifier)	Route B (with laser amplifier)
Transmitter laser launch power	0 dBm	0 dB.
Isolator loss	−3 dB	−3 dB
Phase modulator loss	−7 dB	−7 dB
Laser amplifier gain (route *B* only)		+11 dB
Total effective launch power	−10 dBm	+1 dBm
Route loss	−29·6 dB	−49 dB
Received signal power	−39·6 dBm	−48 dBm
Receiver sensitivity	−47·6 dBm	−47·6 dBm
Route margin	8 dB	−0·4 dB

To facilitate transmission over the 176 km route, a laser amplifier was used as a power amplifier at the transmitter, boosting the effective launch power to > +1 dBm. This gave a total power budget of 48·6 dB. Transmission over the 176 km route with a route loss of 49 dB yielded a BER of 5×10^{-9}. To demonstrate that no error floor was introduced by the laser amplifier a 150 km route was configured and this yielded BER values of below 10^{-13}. It should be noted that the average fibre loss on the 176 km route was 0·28 dB/km. Values as low as 0·22 dB/km have been achieved on both undersea and terrestrial cables, which would realise a reach in excess of 220 km.

Discussion: The receiver sensitivity of −47·6 dBm (10^{-9} BER) is 10·4 dB from the theoretical quantum limit. Thermal noise in the receiver accounts for 3·6 dB, the quantum efficiency of the *pin* diodes accounts for 2 dB and the baseband filter for 1·7 dB. The remaining 3·1 dB may be ascribed to residual AM modulation from the phase modulator, IF gain fluctuations and nonoptimal electrical components.

Introduction of the laser amplifier as a simple power booster at the transmitter caused no additional penalty, and increased the transmission span from 108 km to 176 km.

The response time of the polarisation controller was limited by the computer to approximately 1 s, but this was adequate for the typically slow polarisation fluctuations over installed fibre. No observable penalty was introduced in transferring the system from a laboratory environment to a field environment.

Conclusions: A 565 Mbit/s DPSK coherent system field demonstration was performed over 176 km conventional installed single mode fibre. The key features of the system are miniaturised long external cavity lasers, automated endless polarisation control, a laser power amplifier at the transmitter and error free operation consistent with a BER of below 10^{-13}. The measured receiver sensitivity was −47·6 dBm at 10^{-9} BER.

We have demonstrated that the laser sources and other components can be assembled into transportable units which are sufficiently rugged to maintain an error floor of below 10^{-13} BER in a field environment and we have proved the ability of the polarisation controller to cope with typical polarisation changes on installed fibre. Introduction of the laser amplifier as a simple power booster at the transmitter increased the transmission span from 108 km to 176 km.

Acknowledgment: The authors wish to thank the Director of Research and Technology, British Telecom Research Laboratories, for permission to publish this paper.

M. J. CREANER
R. C. STEELE
I. MARSHALL
G. R. WALKER
N. G. WALKER
J. MELLIS
S. AL CHALABI
I. STURGESS
M. RUTHERFORD
J. DAVIDSON
M. BRAIN

British Telecom Research Laboratories
Martlesham Heath
Ipswich IP5 7RE, United Kingdom

8th September 1988

References

1 MELLIS, J., AL CHALABI, S., *et al.*: 'Miniature packaged external cavity laser with 50 GHz continuous electrical tuning range', *Electron. Lett.*, 1988, **24**, (16), pp. 988–989
2 MELLIS, J., AL CHALABI, S., and BARKER, L.: 'Characteristics of fibre coupled optical isolator at 1·5 μm', *ibid.*, 1988, **24**, (5), pp. 290–291
3 WALKER, G. R., and WALKER, N. G.: 'Rugged all-fibre endless polarisation controller', *ibid.*, 1988, **24**, (22), pp. 1353–1354 (this issue)
4 WALKER, N. G., and WALKER, G. R.: 'Endless polarisation control using four fibre squeezers', *ibid.*, 1987, **23**, (5), pp. 290–292

NEW NONINTERACTIVE IDENTITY-BASED KEY DISTRIBUTION SYSTEM

Indexing terms: Information theory, Identity-based cryptosystems, Key distribution systems, Common keys

The paper presents a new identity-based key distribution system (IDKDS), in which the common keys can be shared without auxiliary communications. The proposed IDKDS can be regarded as an identity-based version of Diffie and Hellman's key distribution system, and is a generalisation of the identity-based cryptosystem (IDC) developed by the authors. The paper also analyses the security of the IDKDS and shows that the IDKDS is practically secure.

Introduction: The identity-based key distribution system (IDKDS) provides a powerful tool for sharing common keys in large-scale telecommunications networks. Blom's scheme[1] and Matsumoto and Imai's scheme[2] are known as the IDKDS without any auxiliary communications, which is a desirable property for common key distribution. (We refer to such schemes as noninteractive IDKDSs throughout this letter.)

This letter presents a new noninteractive IDKDS applying the same idea to a identity-based cryptosystem.[3] (The noninteractive IDKDS developed in this letter can be regarded as an identity-based version of Diffie and Hellman's key distribution system,[4] and the related work can be found in Reference 5.) The proposed IDKDS has the threshold number of entities for the security of the trusted centre's secret; however, it is one of the most robust noninteractive IDKDSs proposed so far. Furthermore, we show a practical modification in the light of the secure common key cryptosystem.

Protocol for key distribution: Here we present the protocol for key distribution of the proposed noninteractive IDKDS. The protocol comprises two phases, i.e. the first phase is the preliminaries of the trusted centre and each entity, and the second phase is the procedure for the key distribution between two arbitrary entities.

First phase (preliminaries):
(1) The trusted centre chooses a large prime p and an arbitrary generator g of the multiplicative group of Z_p. The trusted centre also randomly chooses an n-dimensional vector $\boldsymbol{a} = (a_1, a_2, \ldots, a_n)$ over Z_{p-1} and defines $\boldsymbol{h} = (h_1, h_2, \ldots, h_n)$ over Z_p as $h_i = g_i^a \pmod p$ $(1 \leq i \leq n)$. The trusted centre makes public p, $\boldsymbol{h}$ and the one-way function $f(.)$ to all entities, while keeping g and $\boldsymbol{a}$ secret.

(2) Entity 'i' registers its identity (denoted ID_i) with the trusted centre in the form of the binary vector $\boldsymbol{ID}_i = (x_{i1}, x_{i2}, \ldots, x_{ik})$, where $k < n$ and $x_{ij} \in \{0, 1\}$ $(1 \leq j \leq k)$.

(3) For entity 'i', the trusted centre defines an extended ID (denoted EID_i) in the form of binary vector $\boldsymbol{EID}_i$ by $\boldsymbol{EID}_i = f(\boldsymbol{ID}_i) = (y_{i1}, y_{i2}, \ldots, y_{in})$, where $y_{ij} \in \{0, 1\}$ $(1 \leq j \leq n)$. The trusted centre evaluates entity i's secret s_i by

$$s_i = \sum_{1 \leq j \leq n} a_j y_{ij} \pmod p = \boldsymbol{EID}_i \,.\, \boldsymbol{a} \pmod p \tag{1}$$

and issues it to entity 'i' through a highly secure channel.

Second phase (key distribution): Without loss of generality, we show the protocol of key distribution between entity 1 and entity 2. The procedure is basically the same as with Diffie and Hellman's scheme.[4]

(1) Entity 1 generates entity 2's extended ID by $\boldsymbol{EID}_i = f(\boldsymbol{ID}_i) = (y_{21}, y_{22}, \ldots, y_{2n})$ and evaluates z_2 by

$$z_2 = \prod_{1 \leq i \leq n} (h_i)^{y_{2i}} \pmod p \tag{2}$$

Note that $z_2 = g^{s_2} \pmod p$. Furthermore, entity 1 computes $K_{12} = (z_2)^{s_1} \pmod p$. Here it can easily be shown that $K_{12} = g^{s_1 s_2} \pmod p$.

(2) Entity 2 performs a similar procedure with entity 1, and can then generate $K_{21} = g^{s_2 s_1} \pmod p$.

Thus entity 1 and entity 2 succeed in sharing a common key K $(= K_{12} = K_{21})$ without auxiliary communications.

Security:
(*a*) *Trusted centre's secret:* The security of the trusted centre's secret $\boldsymbol{a}$ is completely the same as with the case of the IDC in Reference 3. Each entity 'i' has its own secret s_i, which is a partial sum of the trusted centre's secret, in the following form:

$$s_i = \sum_{1 \leq j \leq n} a_j y_{ij} \pmod p = \boldsymbol{EID}_i \,.\, \boldsymbol{a} \pmod p \tag{3}$$

Hence, if n entities' $\boldsymbol{EID}_j$ $(1 \leq j \leq n)$ are linearly independent over Z_{p-1}, then the trusted centre's secret will be derived by them. (For notational simplicity, we assume that n entities are numbered as 1, 2, ..., n.) Thus the threshold number of entities' conspiracy to find $\boldsymbol{a}$ is n.

(*b*) *Each entity's secret:* The security of each entity's secret s_i is somewhat different from the case of the IDC in Reference 3. The one possible attack to find some entity k's secret s_k is that t $(<n)$ entities try to produce entity k's $\boldsymbol{EID}_k$ by the linear combination of their $\boldsymbol{EID}_i$ $(1 \leq i \leq t)$ over Z_{p-1}. (For notational simplicity, we assume that t entities are numbered as 1, 2, ..., t. This attack is completely the same as with the case of the IDC in Reference 3.) We define the probability Pr (t) that t entities succeed in finding the other entity's secret by the above attack. Then we have Pr $(t) \leq 2^{t-n}$; so, for example, for $n = 500$, Pr $(450) \leq 2^{-50} = 10^{-15}$, Pr $(400) \leq 2^{-100} = 10^{-30}$ etc. However, the strict formulation for this problem is whether it is possible for t $(<n)$ entities to find a common key K_{ij} of entities i and j $(i, j \geq t)$.* Note that K_{ij} is given by

$$K_{ij} = g^{s_i s_j} \pmod p$$
$$= g^{(\boldsymbol{EID}_i \,.\, \boldsymbol{a})(\boldsymbol{EID}_j \,.\, \boldsymbol{a}) \,(\mathrm{mod}\, p-1)} \pmod p \tag{4}$$

This is not a problem of linear algebra; hence the tight threshold for this problem is not clear at present and further analysis of it will be required.

* SHAMIR, A.: private communication, June 1988