power. Because the corresponding measured remnant pump power was 16 mW, improvements in the gain figure are likely with optimisation of the fibre length.

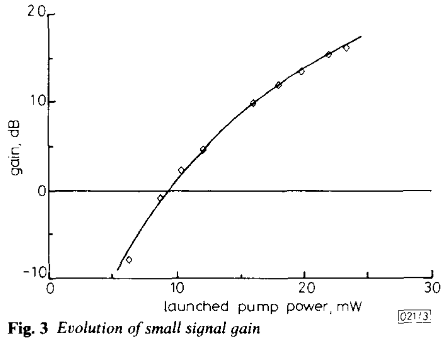

Fig. 3 *Evolution of small signal gain*

The inversion parameter, μ, is related to the measured spontaneous noise spectral density, ρ_{sp}, through[5]

$$\mu = \rho_{sp}\lambda/2hc(G - 1) \tag{1}$$

where G is the gain.

For $G = 13$ dB ($P_{pump} = 20$ mW) at 1532 nm wavelength, we find $\mu = 1{\cdot}68$. The noise figure F for spontaneous-signal beat noise limited operation is given by[10]

$$F = 2\mu(G - 1)/G \tag{2}$$

yielding an expected noise figure of about 5 dB. This value is comparable with the excellent noise figure associated with silica-based fibre amplifiers.

A further observation associated with direct pumping into the ${}^4I_{13/2}$ absorption band was the evident upconversion emission at 540, 668, 850, 980 and 1130 nm. An inspection of the energy-levels of Er^{3+} reveals that the ion must become at least three times more energetic to enable these transitions to be observed. This loss of energy from the upper lasing level is undesirable, but it does not appear to affect reasonable amplifier performance at 1530 nm.

More detailed investigations into up-conversion processes will be the subject of future publications.

Conclusions: Erbium-doped ZBLANP fibre is an alternative host glass for fibre amplifiers in the 1520–1570 nm wavelength region. When pumped using a semiconductor laser at 1482 nm, the gain coefficient (nonoptimised) was 15 dB/25 mW and the ASE bandwidth was 45 nm. The noise factor was estimated to be about 5 dB. Upconversion emission was also observed, indicating that this parasitic phenomenon may limit the ultimate performance of amplifiers using this fibre material.

Acknowledgments: The authors thank Steve Carter and John Williams for making the ZBLAN fibre, David Rogers for the photoluminescence measurements, John Regnault and colleagues in the Devices Division for the pump laser, Ian Wilkinson for the fibre multiplexer, and Mike Brierley and Tim Whitley for useful discussions.

C. A. MILLAR
P. W. FRANCE
23rd March 1990

British Telecom Research laboratories
Optical Physics and Materials Divisions
Martlesham Heath, Ipswich, Suffolk, United Kingdom

References

1 BRYANT, E. G., CARTER, S. F., ELLIS, A. D., STALLARD, W. A., WRIGHT, J. V., and WYATT, R.: 'Unrepeatered 2·4 Gb/s transmission experiment over 250 km of step-index fibre using erbium power amplifier', *Electron. Lett.*, 1990, **26**, (8), pp. 528–530

2 EDAGAWA, N., *et al.*: '904 km, 1·2 Gb/s non-regenerative transmission experiment using 12 erbium doped fibre amplifier'. Proc. 15th ECOC, 1989, 3, **PDA-8**, p. 33

3 GILES, C. R., DESURVIRE, E., ZYSKIND, J. L., and SIMPSON, J. R.: 'Noise performance of erbium doped fibre amplifier pumped at 1·49 μm, and application to signal preamplification at 1·8 Gb/s', *IEEE Photonics Tech Letts.*, 1989, **1**, (11), p. 367

4 AINSLIE, B. J., CRAIG, S. P., DAVEY, S., and WAKEFIELD, B.: 'Fabrication, assessment and optical properties of high concentration erbium and neodymium doped silica based fibres', *Mats. Letts.*, 1988, **6**, p. 139

5 WHITLEY, T. J., CREANER, M. J., STEELE, R. C., BRAIN, M. C., and MILLAR, C. A.: 'Laser diode pumped erbium doped fibre amplifier in a 565 Mb/s DPSK coherent transmission experiment', *IEEE Photonics Tech. Letts.*, 1989, **11**, (12), p. 425

6 CREANER, M. J., *et al.*: 'Field demonstration of coherent transmission system with diode pumped erbium fibre amplifiers', accepted for publication in *Electron. Lett.*, 1990

7 BRIERLEY, M. C., and HUNT, M. H.: 'Efficient semiconductor laser-pumped fluoride fibre lasers'. SPIE Proceedings, 1990, vol. 1171, 15 . Proc. Conf on Fibre Lasers and Amplifiers, Boston, USA, Sept. 1989

8 MILLAR, C. A., BRIERLEY, M. C., and FRANCE, P. W.: 'Optical amplification in an erbium doped ZBLAN fibre between 1480 nm and 1600 nm'. Proc. 14th ECOC, IEE Publications, Part 1, p. 66, Brighton, UK, 1988

9 PEDERSEN, J. E., BRIERLEY, M. C., CARTER, S., and FRANCE, P. W.: 'Amplification in the 1300 nm telecommunications window in a neodymium doped fluoride fibre', *Electron. Lett.*, 1990, **26**, (5), p. 329

10 OLSHANSKY, R.: 'Noise fibure for erbium doped optical fibre amplifiers', *Electron. Lett.*, 1988, **24**, (12), p. 1363

NONINTERACTIVE OBLIVIOUS TRANSFER

Indexing term: Codes

Two new approaches to implement oblivious transfer and 1–2 oblivious transfer without interaction, based on the well-known Diffie–Hellman public-key distribution algorithm are proposed.

Introduction: We define two protocols discussed in this letter. A fundamental oblivious transfer protocol is an unusual protocol in which Alice transfers a secret message, m, to Bob in such a way that

* With probability 1/2, Bob receives the message, and with probability 1/2, Bob learns nothing about the message.

* At the end of this protocol, Alice does not know whether or not Bob received the message.

With a slight modification of the fundamental oblivious transfer, Alice can use the 1–2 oblivious transfer protocol to transfer two secret messages, m_0 and m_1, to Bob in such a way that

* Bob has a selection bit, s, to decide which message to receive.

* Bob can only learn one of the messages and does not learn anything about the other message.

* Alice learns nothing about the value of s.

The oblivious transfer protocol is a powerful in the design of cryptographic applications, such as coin flipping by telephone,[1] exchanging secrets,[2] and sending certified mail.[3] Bellare and Micali[4] have shown how to implement noninteractive 1–2 oblivious transfer protocol through the use of a public file and how to extend the application to the noninteractive zero knowledge proofs. We propose two new approaches to implement the fundamental oblivious transfer and 1–2 oblivious transfer. In comparing with Reference 4 our new method requires less on-line processing time and the transmitted information required is only half that for their method.

Noninteractive fundamental oblivious transfer protocol: Our method is based on the well known Diffie–Hellman public-key distribution scheme.[5] There is a prime, P, and two generators, α and β, which are public values. Each user randomly selects a number $x \in [0, P - 1]$ and calculates one of the two values

$$y_0 = \alpha^x \bmod P$$

or

$$y_1 = \beta^x \bmod P$$

That users public key is y_0 or y_1, and the secret key is x.

When Alice wants to transfer a message, m, to Bob, Alice needs to access Bob's public key, y_B, and computes

$$K_{A,B} = y_B^{x_A} \bmod P$$

where x_A is Alice's secret key. Then Alice transmits $C = m \oplus K_{A,B}$ to Bob.

Bob receives C. Bob needs to access Alice's public key, y_A, and computes

$$K_{B,A} = y_A^{x_B} \bmod P$$

where x_B is Alice's secret key. If Bob and Alice used the same generator (either α or β) to calculate their public keys, then $K_{A,B} = K_{B,A}$, therefore $m = C \oplus K_{B,A}$. Otherwise, $K_{A,B} \neq K_{B,A}$, and it is impossible for Bob to learn m.

Security discussion: The security of this scheme is the same as for the Diffie–Hellman public-key distribution scheme, which was based on the difficulty of computing discrete logarithms. Although the public keys are available in the public file, it is impossible for anyone else except the secret key holder to learn the secret key, x. Since there the probability is 1/2 that Alice and Bob will use the same generator to calculate their public keys, Bob has probability of 1/2 of learning the message. On the other hand, since both persons involved in this protocol have their own control, one will not dominate the other.

Noninteractive 1–2 oblivious transfer protocol: There is a prime P and two generators α and β which are public values. Each user will randomly select two numbers, x_0 and $x_1 \in [0, P - 1]$ and calculate three values

$$y_0 = \alpha^{x_0} \bmod P$$

$$y_1 = \beta^{x_0} \bmod P$$

and

$$y_2 = \alpha^{x_1} \bmod P$$

The public key in receiving mode is (y_s, y_{1-s}) (i.e., with $s = 0$ or 1). The public key in transmitting mode is y_2 the secret keys in receiving and transmitting modes and selection bit are x_0, x_1 and s, respectively.

When Alice wants to transfer one of two secret messages, m_0 and m_1, to Bob, Alice must access Bob's public keys in receiving mode, $y_{B,s}$ and $y_{B,1-s}$, and computes

$$K_{A,B,s} = y_{B,s}^{x_{A,1}} \bmod P$$

and

$$K_{A,B,1-s} = y_{B,1-s}^{x_{A,1}} \bmod P$$

where $x_{A,1}$ is Alice's secret key used in transmitting mode. Then Alice transmits $C_0 = m_0 \oplus K_{A,B,s}$ and $C_1 = m_1 \oplus K_{A,B,1-s}$ to Bob.

Once Bob receives (C_0, C_1), Bob needs to access Alice's public key in transmitting mode, $y_{A,2}$, and computes

$$K_{B,A} = y_{A,2}^{x_{B,0}} \bmod P$$

where $x_{B,0}$ is Bob's secret key used in the receiving mode. If $s = 0$, then $K_{B,A} = K_{A,B,s}$, and $m_0 = C_0 \oplus K_{B,A}$. Otherwise, $s = 1$, then $K_{B,A} = K_{A,B,1-s}$, and $m_1 = C_1 \oplus K_{B,A}$.

Security and some discussion: The security of the algorithm is based on a similar approach previously proposed. The security is the same as the Diffie–Hellman cryptosystem. Since the two messages are encrypted by two keys, based on two different generators, α and β, and there is only one common secret key, $K_{B,A}$, which is based on the generator, α, can be shared between these two users. Either m_0 or m_1 can be decrypted by the receiver. In comparing to their method,[4] instead of transmitting a four-tuple ciphertext each time, our method only needs to transmit a two-tuple ciphertext. We propose a time–memory trade-off technique to reduce the on-line processing time.

L. HARN
H. Y. LIN

Computer Science Telecommunications Program
University of Missouri–Kansas City
4747 Troost, Kansas City, MO 64110, USA

26th February 1990

References

1 BLUM, M.: 'Three applications of the oblivious transfer: 1. Coin flipping by telephone, 2. How to excahnge secrets, 3. How to send certified electronic mail', Dept. EECS, University of California, Berkeley, Calif., 1981

2 RABIN, M. O.: 'Exchange of secrets'. Dept. of Applied Physics, Harvard University, Cambridge, Mass, 1981

3 BLUM, M., and RABIN, M. O.: 'How to send certified electronic mail'. Dept. EECS, University of California, Berkeley, Calif., 1981

4 BELLARE, M., and MICALI, S.: 'Non-interactive oblivious transfer and applications'. Presented at Crypto'89, Santa Barbara, California, U.S.A., to appear in Advances in Cryptology. Proc. of Crypto'89 (Lecture Notes in Computer Science), Springer-Verlag, August 1989

5 DIFFIE, W., and HELLMAN, M.: 'New directions in cryptography', *IEEE Trans.*, 1976, **IT-22**, (6), pp. 644–654

ON COMPUTING THE DISCRETE WIGNER–VILLE DISTRIBUTION

Indexing terms: Signal processing, Fourier transforms

The Wigner–Ville distribution is an important tool in nonstationary signal analysis. Many algorithms to compute the discrete Wigner–Ville distribution (DWVD) have been proposed. New efficient methods for computing the discrete Wigner–Ville distribution are presented. Observing that the DWVD is real and periodic, it is possible to express it as the DFT of a complex conjugate sequence of reduced length. Comparison to other algorithms are also made.

Introduction: The Wigner–Ville distribution is an important tool in nonstationary signal analysis. Many algorithms for use in computing the discrete Wigner–Ville distribution (DWVD) have been proposed.[1–4] New efficient methods for computing the discrete Wigner–Ville distribution based on the real and periodic properties of the DWVD are presented. It is found that the DWVD can be expressed as the DFT of a complex conjugate sequence of reduced length. This in turn can be computed using efficient real-valued fast Fourier transform algorithms.[5]

The Wigner–Ville distribution of a real signal $s(t)$ is defined as

$$W(t, f) = \int_{-\infty}^{\infty} z\left(t + \frac{\tau}{2}\right) z^*\left(t - \frac{\tau}{2}\right) e^{-j2\pi f\tau}\, d\tau \tag{1}$$

where $z(t)$ is the analytic signal associated with the real signal $s(t)$. As can be seen from eqn. 1, evaluating the WVD is a noncausal operation. In practice, this limitation is overcome