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

![Graph](image)

**Fig. 3** Evolution of small signal gain

The inversion parameter, \( \mu \), is related to the measured spontaneous noise spectral density, \( p_{sp} \), through

\[
\mu = p_{sp} k_b T (G - 1)
\]

where \( G \) is the gain.

For \( G = 13 \, \text{dB} \) \( (P_{pump} = 20 \, \text{mW}) \) at 1532 nm wavelength, we find \( \mu = 1.68 \). The noise figure \( F \) for spontaneous-signal beat noise limited operation is given by

\[
F = 2G(G - 1)/G + 1
\]

yielding an expected noise figure of about 5.8 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 \( ^{2}I_{11/2} \) absorption band was the evident upconversion emission at 540, 668, 850, 980 and 1130 nm. An inspection of the ASE bandwidth was the evident upconversion of the 41i,,2 absorption band which was the evident upconversion yielding an expected noise figure of about 5 dB. This value is comparable with the excellent noise figure associated with silica-based fibre amplifiers.

**References**


**NONINTERACTIVE OBLIVIOUS TRANSFER**

**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, 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, \( m_1 \) and \( m_2 \), 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, exchanging secrets, and sending certified mail. Bellare and Micali 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. There is a prime, $P$, and two generators, $x$ and $y$, which are public values. Each user randomly selects a number $s \in [0, P - 1]$ and calculates one of the two values

$$y_0 = x^s \mod P$$

or

$$y_1 = y^s \mod P$$

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

$$K_{A,B} = y_B^s \mod P$$

where $y_B$ 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

$$K_{B,A} = y_A^s \mod P$$

where $y_A$ is Alice's secret key.

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 $x$ and $y$ which are public values. Each user will randomly select two numbers, $x_0$ and $x_1$, in $[0, P - 1]$ and calculates three values

$$y_0 = x_0^s \mod P$$

$$y_1 = x_1^s \mod P$$

and

$$y_2 = y^s \mod P$$

The public key in receiving mode is $(y_0, y_1, y_2)$ (i.e., with $s = 0$ or 1). The public key in transmitting mode is $y_3$ the secret keys in receiving and transmitting modes and selection bit are $y_0, y_1$ 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, $y_A$, and $y_{B,1}$, and computes

$$K_{A,B,1} = y_A^s \mod P$$

and

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

where $y_{B,1}$ is Alice's secret key used in transmitting mode. Then Alice transmits $C_0 = m_0 \oplus K_{A,B,1}$ and $C_1 = m_1 \oplus K_{B,A,1}$ to Bob. Once Bob receives $(C_0, C_1)$, Bob needs to access Alice's public key in transmitting mode, $y_{A,1}$, and computes

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

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

ON COMPUTING THE DISCRETE WIGNER-VILLE DISTRIBUTION

Indexing terms: Signal processing, Fourier transforms

The Wigner-Ville distribution is an important tool in non-stationary 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. A new efficient method for computing the discrete Wigner-Ville distribution based on the real and periodic properties of the DWVD is 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.

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

$$W(t, f) = \int_{-\infty}^{\infty} s(t + \frac{\tau}{2})s^*(t - \frac{\tau}{2})e^{-j2\pi ft} d\tau$$

where $s(t)$ 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

ELECTRONICS LETTERS 10th May 1990 Vol. 26 No. 10