It is apparent that by varying the number of blocks one can easily design a new balanced code (for example, the encoding table for (8,4,2) code has only four rows and two columns, etc).

Trellis design procedure: We consider a trellis for the designed code as a set of eight similar subtrellises each one corresponding to each of the eight rows given by Table 1. We start with the design of the first sub-trellis:

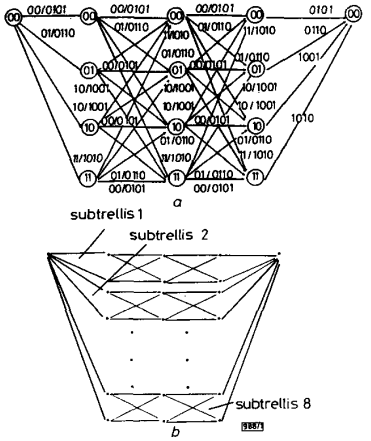

Fig. 1 *Trellis diagrams for (16,6,4) (first subtrellis) and (16,9,4) codes*

(i) If $x_0 = x_1 = x_2 = 0$ (the first row in Table 1), the trellis diagram for the (16,6,4) balanced code can be design using the technique introduced in [4] and is shown in Fig. 1*a*. This subtrellis has N_c = 5 columns and N_s = 4 states. The trellis branches at depth p correspond to a pth column of Table 1 and are labelled as $\mathbf{X}_p/\mathbf{Y}_p$, where $\mathbf{X}_p$ are 2-tuple binary vectors of information digits and $\mathbf{Y}_p$ are 4-tuple binary vectors encoded according to function f_1.

(ii) If $x_0 = x_1 = 0$ and $x_2 = 1$ (the second row in Table 1) the trellis diagram for the (16,7,4) balanced code can be derived easily by inverting the labelling at the final depth $p = 4$ in the second subtrellis.

(iii) The remaining six subtrellises will have a similar structure with branch labels at depth p modified according to the pth column of Table 1 and function f_2. The overall trellis diagram for the (16,9,4) code is shown in Fig. 1*b* (it is apparent that a combination of the first four subtrellises represents the trellis diagram of the (16,8,4) balanced code [2]).

As follows from this Figure, the trellis diagram of the nonlinear (16,9,4) balanced code has 32 states and five columns; there are 2^9 distinct paths through this trellis diagram and each path corresponds to a unique codeword.

The designed trellis possesses a useful feature which allows us to reduce the complexity of the Viterbi decoder: in every subtrellis, the trellis branches starting from different states have similar labelling (see Fig. 1*a*). This allows us to reduce the number of calculations by a factor of ~4 without degradation of the maximum-likelihood performance.

Computer simulation results: The simulation tests were carried out under additive white Gaussian noise channel conditions for the binary unipolar signalling scheme. In Fig. 2 the probability of bit error rate (BER) is plotted as a function of E_b/N_0, where E_b is the energy per information bit and N_0 is equal to the noise variance. As expected, trellis decoding provides about 2dB coding gain over conventional hard decision decoding.

Conclusion: A low-complexity encoding and trellis decoding technique for nonlinear balanced ECCs is presented. The technique is illustrated by the design of a (16,9,4) nonlinear balanced code together with its trellis diagram. A regular structure of the designed trellis allows achievement of maximum-likelihood performance with reduced decoding complexity.

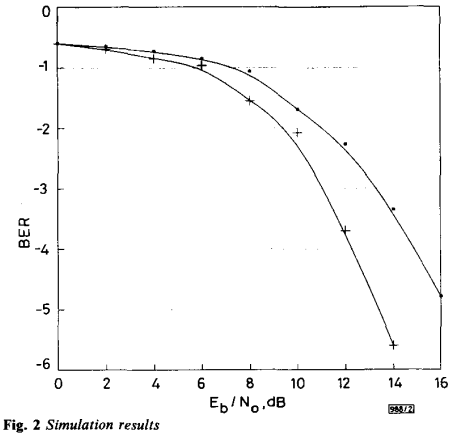

Fig. 2 *Simulation results*

—■— hard decision decoding
—+— trellis decoding

18 January 1995
Electronics Letters Online No: 19950337

G. Markarian and B. Honary (*Communications Research Centre, Lancaster University, Lancaster LA1 4YR, United Kingdom*)

M. Blaum (*IBM Research Division, Almaden Research Center, San Jose, CA 95120-6099, USA*)

References

1 SCHOUHAMMER IMMINK.: 'Coding techniques for optical and magnetic recording channels' (Prentice Hall, New York, 1990)
2 FERREIRA, H.: 'Low bounds on the minimum Hamming distance achievable with runlength constrained or dc-free block codes and the synthesis of a (16,8) D_{min} = 4 dc-free block code', *IEEE Trans.*, 1984, **MAG-20**, pp. 881–883
3 BLAUM, M., LITSYN, S., BUSKENS, V., and VAN TILBORG, H.: 'Error correcting codes with bounded digital running sum', *IEEE Trans.*, 1993, **IT-39**, pp. 216–226
4 MARKARIAN, G., and HONARY, B.: 'Trellis decoding technique for block RLL/ECC', *IEE Proc. Commun.*, 1994, **141**, (5), pp. 297–302
5 BLAUM, M.: 'A (16, 9, 6, 5, 4) error correcting DC-free block code', *IEEE Trans.*, 1988, **IT-34**, pp. 138–141
6 WOLF, J.K.: 'Efficient maximum likelihood decoding of linear block codes using a trellis', *IEEE Trans.*, 1978, **IT-24**, (1), pp. 76–80
7 FORNEY, G.D. Jr.: 'Coset codes - Part 2: Binary lattices and related codes', *IEEE Trans.*, 1988, **IT-34**, (5), pp. 1123–1151
8 MARKARIAN, G., HONARY, B., and BLAUM, M.: 'Trellis decoding for the (16, 9, 5, 4) balanced code'. IBM Research Report RJ 9790 (84853), April 1994, San Jose, USA

Modified key agreement protocol based on the digital signature standard

L. Harn

Indexing terms: Cryptography, Information theory

Arazi proposed a scheme to integrate a key exchange protocol into the DSS (digital signature standard) to authenticate two public keys exchanged between two users and then one corresponding secret session key can be shared by two parties based on the Diffie-Hellman public-key distribution scheme. Later, Nyberg and Rueppel pointed out a weakness in the Arazi protocol: if one secret session key is compromised then the others will be disclosed as well. The Letter proposes a modified key agreement protocol based on the DSS.

Introductron: Diffie and Hellman [1] proposed the well known public-key distribution scheme based on the discrete logarithm problem in 1976 to enable two parties to establish a common secret session key based on their exchanged public keys. However, their scheme did not provide an authentication mechanism for the exchanged public keys. In 1985, ElGamal [2] proposed a digital signature scheme based on the discrete logarithm problem. The ElGamal signature scheme can provide an authenticated mechanism for distributing the public keys.

In 1993, Arazi [3] proposed a scheme to integrate a key exchange protocol into the DSS (digital signature standard) [4] to authenticate the public keys. Later, Nyberg and Rueppel [5] pointed out a weakness in the Arazi protocol: if one secret session key is compromised then the others will be disclosed as well. This Letter proposes a modified key agreement protocol based on the DSS. Instead of distributing a single public key in each communication session, we propose to distribute multiple public keys in each session.

There is some public information that should be agreed to by all users:

p = a large prime modulus, where $2^{511} < p < 2^{512}$
q = a prime divisor of p–1, where $2^{159} < q < 2^{160}$
α, where $\alpha = h^{(p-1)/q} \bmod p$, h is a random integer with $1 \leq h \leq p-1$ such that $h^{(p-1)/q} \bmod p > 1$
x_i = a secret key for user i, where $2^{159} < x_i < 2^{160}$
y_i = a corresponding public key for user i, where $y_i = \alpha^{x_i} \bmod p$
H = the secure hash function (SHA) proposed by the NIST.

$\{p, q, \alpha, y_i\}$ are public values and $\{x_i\}$ is each user's secret key.

Modified key agreement protocol: We assume that user A wants to share three secret session keys with user B. Then:

(i) User A randomly selects two secret integers, v_1 and $v_2 \in [1, q-1]$ and computes

$$m_{A1} = \alpha^{v_1} \bmod p$$
$$m_{A2} = \alpha^{v_2} \bmod p$$
$$r_A = (m_{A1} m_{A2} \bmod p) \bmod q$$
$$s_A = (v_1 + v_2)^{-1}[H(m_{A1}, m_{A2}) + x_A r_A] \bmod q$$

and sends (m_{A1}, m_{A2}, s_A) to B.

(ii) User B randomly selects two secret integers, w_1 and $w_2 \in [1, q-1]$ and computes

$$m_{B1} = \alpha^{w_1} \bmod p$$
$$m_{B2} = \alpha^{w_2} \bmod p$$
$$r_B = (m_{B1} m_{B2} \bmod p) \bmod q$$
$$s_B = (w_1 + w_2)^{-1}[H(m_{B1}, m_{B2}) + x_B r_B] \bmod q$$

and sends (m_{B1}, m_{B2}, s_B) to A.

(iii) User A computes

$$r_B = (m_{B1} m_{B2} \bmod p) \bmod q$$

verifies the DSS-signature (r_B, s_B) of the message (m_{B1}, m_{B2}), then computes the shared secret keys as

$$K_{AB1} = m_{B1}^{v_1} \bmod p$$
$$K_{AB2} = m_{B2}^{v_2} \bmod p$$
$$K_{AB3} = m_{B1}^{v_2} \bmod p$$

(iv) User B computes

$$r_A = (m_{A1} m_{A2} \bmod p) \bmod q$$

verifies the DSS-signature (r_A, s_A) of the message (m_{A1}, m_{A2}), then computes the shared secret keys as:

$$K_{AB1} = m_{A1}^{w_1} \bmod p$$
$$K_{AB2} = m_{A2}^{w_2} \bmod p$$
$$K_{AB3} = m_{A2}^{w_1} \bmod p$$

Security: We follow the known-key attack proposed by Nyberg and Rueppel [5] to examine the security of the modified scheme. We have

$$K_{AB1} = \alpha^{v_1 w_1} \bmod p$$
$$K_{AB2} = \alpha^{v_2 w_2} \bmod p$$
$$K_{AB3} = \alpha^{v_2 w_1} \bmod p$$

where

$$v_1 + v_2 = s_A^{-1}[H(m_{A1}, m_{A2}) + x_A r_A] \bmod q$$
$$w_1 + w_2 = s_B^{-1}[H(m_{B1}, m_{B2}) + x_B r_B] \bmod q$$

Hence, by multiplying the above two equations, we obtain

$$\begin{aligned} v_1 w_1 + v_1 w_2 + v_2 w_1 + v_2 w_2 &= s_A^{-1} s_B^{-1}[H(m_{A1}, m_{A2}) H(m_{B1}, m_{B2}) \\ &+ H(m_{A1}, m_{A2}) x_B r_B + H(m_{B1}, m_{B2}) x_A r_A \\ &+ x_A r_A x_B r_B] \bmod q \end{aligned}$$

From the above equation, we obtain

$$\begin{aligned} (K_{AB1} K_{AB2} K_{AB3} \alpha^{v_1 w_2})^{s_A s_B} &= \alpha^{H(m_{A1}, m_{A2}) H(m_{B1}, m_{B2})} \times \\ & y_B^{H(m_{A1}, m_{A2})(r_B)} y_A^{H(m_{B1}, m_{B2})(r_A)} \times \\ & (\alpha^{x_A x_B})^{(r_A r_B)} \bmod p \end{aligned}$$

Under known-key attack, since $\alpha^{v_1 w_2}$ has never been used as the secret session key, all quantities in this equation except two values, $\alpha^{v_1 w_2}$ and $\alpha^{x_A x_B}$, are publicly known or sent between the parties. Thus, the proposed known-key attack cannot work successfully in our modified scheme.

Conclusion: We have proposed a key agreement protocol based on the DSS. This protocol allows us to exchange n pairs of public keys between two users and to establish n^2–1 secret session keys.

14 February 1995
Electronics Letters Online No: 19950298

L. Harn (*Computer Science Telecommunications Program, University of Missouri, Kansas City, MO 64110, USA*)

References

1 DIFFIE, W., and HELLMAN, M.E.: 'New directions in cryptography', *IEEE Trans.*, 1976, **IT-22**, (6), pp. 644–654
2 ELGAMAL, T.: 'A public key cryptosystem and signature scheme based on discrete logarithms', *IEEE Trans.*, 1985, **IT-31**, (4), pp. 469–472
3 ARAZI, A.: 'Integrating a key cryptosystem into the digital signature standard', *Electron. Lett.*, 1993, **29**, (11), pp. 966–967
4 'The digital signature standard', *Commun. ACM*, 1992, **35**, (7), pp. 36–40
5 NYBERG, K., and RUEPPEL, R.A.: 'Weaknesses in some recent key agreement protocols', *Electron. Lett.*, 1994, **30**, (1), pp. 26–27

Integration process for photonic integrated circuits using plasma damage induced layer intermixing

B.S. Ooi, A.C. Bryce and J.H. Marsh

Indexing terms: Ion beam effects, Semiconductor junction lasers, Integrated circuits, Plasma techniques

A new quantum-well intermixing process in GaAs/AlGaAs structures, based on ion bombardment damage, has been developed. Bandgap tuned lasers and extended cavity lasers have been fabricated. Results show that the quality of the material is still high after intermixing. Losses as low as 18dB cm^{-1} have been measured in the passive waveguides of the extended-cavity lasers.

Introduction: Damage induced by reactive ion bombardment of a semiconductor from a glow discharge system primarily comprises point defects. Point defects generated in this manner have been found to enhance group Ga-Al interdiffusion, and hence blue-shift the bandgap energy by intermixing GaAs/AlGaAs quantum wells (QWs) during an annealing step [1].

A high-RF-power, and hence high-damage, H_2 plasma process was used here to create point defects on the surface of semiconductor samples, followed by annealing to diffuse the point defects down into the QW region. In this study, bandgap tuned oxide