In eqn. 10, unlike eqn. 1, there is no noise added to **As**. However, we can apply the free energy method to a sequence of problems of the form (**As** + **n**) mod 2 = **z** with increasing inverse temperature β, such that the noise-free task is the limiting case, β = ∞.

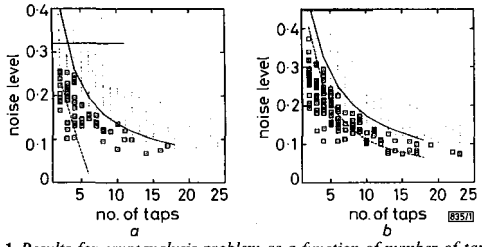

Fig. 1 *Results for cryptanalysis problem as a function of number of taps and noise level*

a $k = 100$, $N = 1000$
b $k = 50$, $N = 5000$

Experimental results: Test data were created for specified k and N using random taps in the LFSR and random observation noise with fixed uniform probability. The parameter β was initially set to 0.25. For each value of β, the optimisation was run until the decrease in free energy was below a specified tolerance (0.001). β was increased by factors of 1.4 until either the most probable vector under $Q(\mathbf{s}; \theta)$ satisfied eqn. 10, or until a maximum value of β = 4 was passed.

Results are shown in Fig. 1. Each dot represents an experiment. A box represents a successful decoding. On each graph a horizontal line shows an information theoretic noise bound above which one does not expect to be able to infer **s**, and two curved lines, from Tables 3 and 5 of [1], show (lower line) the limit up to which Meier and Staffelbach's 'algorithm B appeared to be very successful in most experiments' and (upper line) the theoretical bound beyond which their approach is definitely not feasible.

Conclusion: This Letter has derived an algorithm with a well defined objective function for inference problems in modulo 2 arithmetic. In application to a cryptanalysis problem, this algorithm is similar to algorithm of B Meier and Staffelbach [1] and thus answers their question of whether a derivation could be provided. But it is not identical: the details of the mapping from $[0, 1]^N \rightarrow [0, 1]^N$ are different, and there is no analogue of their multiple 'rounds' in which the data vector $\mathbf{a}_1$ is changed. The new algorithm appears to give superior performance and frequently succeeds at parameter values right up to the upper theoretical limits derived by Meier and Staffelbach.

Acknowledgments: I thank R. Anderson, R. Neal and R. Sewell for helpful discussions.

3 January 1995
Electronics Letters Online No: 19950331

D.J.C. MacKay (*Cavendish Laboratory, Madingley Road, Cambridge CB3 0HE, United Kingdom*)

References

1 MEIER, W., and STAFFELBACH, O.: 'Fast correlation attacks on certain stream ciphers', *J. Cryptol.*, 1989, **1**, pp. 159–176
2 ANDERSON, R.J.: 'Searching for the optimum correlation attack' *in* PRENEEL, B. (Ed.): Proc. 1994 K.U. Leuwen Workshop on Cryptographic Algorithms, Lecture Notes in Computer Science (Springer-Verlag, 1995)
3 HOPFIELD, J.J., and TANK, D.W.: 'Neural computation of decisions in optimization problems', *Biol. Cybern.*, 1985, **52**, pp. 1–25
4 FEYNMAN, D.E.: 'Statistical mechanics' (W.A. Benjamin, Inc., 1972)
5 VAN DEN BOUT, D.E., and MILLER, T.K.: 'Improving the performance of the Hopfield-Tank neural network through normalization and annealing', *Biol. Cybern.*, 1989, **62**, pp. 129–139
6 MACKAY, D.J.C.: 'A free energy minimization framework for interference problems in modulo 2 arithmetic'. Proc. 1994 K.U.Leuven Workshop on Cryptographic Algorithms, 1995

Maximum-likelihood trellis decoding technique for balanced codes

G. Markarian, B. Honary and M. Blaum

Indexing terms: Error correction codes, Decoding

A low-complexity encoding and maximum-likelihood trellis decoding (MLTD) technique for nonlinear balanced codes is presented. The technique is illustrated by the design of a (16,9,4) balanced code.

Introduction: Over recent years much progress has been achieved in designing DC-free balanced error control codes (ECCs), which find applications in magnetic recording and metallic and optical cable systems [1 – 3]. However, the constructed codes do not have simple encoding and maximum-likelihood decoding procedures. Recently [4], a technique that allows low-complexity encoding and MLTD of DC-free ECCs has been proposed. Although this technique is very efficient in terms of creating trellis decoders for linear DC-free error control codes, it cannot be applied for the trellis design of nonlinear ECCs which provide the highest possible minimum Hamming distance d_{min} for a given information rate.

In this Letter we propose a simple procedure which allows the design of nonlinear balanced ECCs together with their MLTDs. The procedure is illustrated by the design of a practically important (16,9,4) code [5]: this means that the length of the code $n = 16$, its dimension $k = 9$, $d_{min} = 4$ and each code word has a weight of 8. It is apparent that, because the code is nonlinear, known trellis design procedures [4, 6, 7] cannot be applied.

Code construction: To illustrate the encoding procedure we describe how to encode the 9 bit input vector $\mathbf{X} = (x_0, x_1, ..., x_8)$ into the 16 bit output balanced vector $\mathbf{Y} = (y_0, ..., y_{15})$. We denote by ⊕ the exclusive-OR operation, by ∧ the AND operation, and by $\bar{a}$ the complement of a. Let the functions f_1 and f_2 be defined as follows:

$$f_1(a_1, a_2) = (a_1, \overline{a_1}, a_2, \overline{a_2})$$
$$f_2(a_1, a_2) = (a_1 \wedge a_2, a_1 \wedge \overline{a_2}, \overline{a_1} \wedge a_2, \overline{a_1} \wedge \overline{a_2})$$

and

$$p_0 = x_3 \oplus x_5 \oplus x_7 \qquad p_1 = x_4 \oplus x_6 \oplus x_8$$

The desired balanced codeword we consider as a concatenation of four 4 bit blocks, each one encoded according to function f_1 or f_2. The encoding procedure is given by Table 1.

Table 1: Encoding procedure for (16, 9, 4) code

$x_0x_1x_2$	$y_0y_1y_2y_3$	$y_4y_5y_6y_7$	$y_8y_9y_{10}y_{11}$	$y_{12}y_{13}y_{14}y_{15}$
000	$f_1(x_3,x_4)$	$f_1(x_5,x_6)$	$f_1(x_7,x_8)$	$f_1(p_0,p_1)$
001	$f_1(x_3,x_4)$	$f_1(x_5,x_6)$	$f_1(x_7,x_8)$	$\overline{f_1(p_0,p_1)}$
010	$f_2(x_3,x_4)$	$f_2(x_5,x_6)$	$\overline{f_2(x_7,x_8)}$	$f_2(p_0,p_1)$
011	$f_2(x_3,x_4)$	$\overline{f_2(x_5,x_6)}$	$f_2(x_7,x_8)$	$\overline{f_2(p_0,p_1)}$
100	$f_2(x_3,x_4)$	$\overline{f_2(x_5,x_6)}$	$\overline{f_2(x_7,x_8)}$	$f_2(p_0,p_1)$
101	$\overline{f_2(x_3,x_4)}$	$f_2(x_5,x_6)$	$f_2(x_7,x_8)$	$\overline{f_2(p_0,p_1)}$
110	$\overline{f_2(x_3,x_4)}$	$f_2(x_5,x_6)$	$\overline{f_2(x_7,x_8)}$	$f_2(p_0,p_1)$
111	$\overline{f_2(x_3,x_4)}$	$\overline{f_2(x_5,x_6)}$	$f_2(x_7,x_8)$	$f_2(p_0,p_1)$

Example: Assume that we want to encode the vector $\mathbf{X}$ = (000101010). First we find that $p_0 = 1$ and $p_1 = 0$. Therefore, according to Table 1, the encoded vector is given as $\mathbf{Y}$ = (1001100110011001). Similarly:

(010101010) ↔ (0100010010111011)
(011101010) ↔ (0100101101001011)
(100101010) ↔ (0100101110110100)

Theorem: The code described above is a (16,9,4) balanced code.

Proof: This follows from the construction (for proof, the reader is referred to [8]).

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:

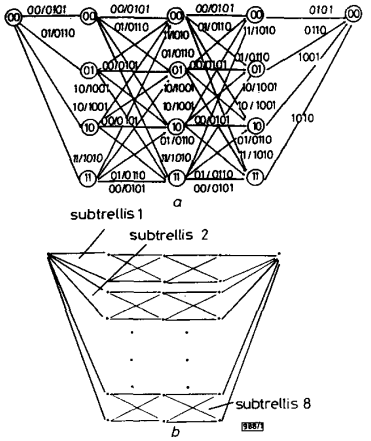

Fig. 1 *Trellis diagrams for (16,6,4) (first subtrellis) and (16,9,4) codes*

(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.

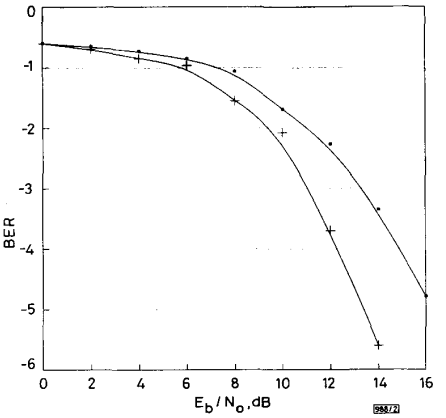

Fig. 2 *Simulation results*

—■— 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.