References

1 DIMARIA, D. J., and KERR, D. R.: 'Interface effects and high conductivity in oxides grown from polycrystalline silicon', *Appl. Phys. Lett.*, 1975, **27**, pp. 505–507

2 ANDERSON, R. M., and KERR, D. R.: 'Evidence for surface asperity mechanism of conductivity in oxide grown on polycrystalline silicon', *J. Appl. Phys.*, 1977, **48**, pp. 4834–4836

3 CHEN, C. F., and WU, C. Y.: 'Superior characteristics of nitrided thermal oxide grown on polycrystalline silicon', *Appl. Phys. Lett.*, 1986, **48**, pp. 165–167

4 ALVI, N. S., LEE, S. K., and KWONG, D. L.: 'Thin polyoxide films grown by rapid thermal processing', *IEEE Electron Dev. Lett.*, 1987, **EDL-8**, (5)

5 MAURY, A., KIM, S. C., MANOCHA, A., OH, K. H., KOSTELNICK, D., and SHIVE, S.: 'Application of rapid thermal oxidation to the development of high dielectric strength polyoxides'. IEDM tech. dig., 1986, pp. 676–679

COMMENT

BLOCKING METHOD FOR RSA CRYPTOSYSTEM WITHOUT EXPANDING CIPHER LENGTH

A recently proposed RSA blocking method is shown to be insecure and of very limited value.

Blocking method: A recent paper[1] described a 'blocking method' for using the RSA cryptosystem[2] which has the advantage that ciphertext produced using this technique is no longer than the corresponding plaintext (unlike normal uses of RSA). It operates as follows.

Suppose N, the RSA modulus, has an n-bit binary representation. Define the one-to-one function F_e, mapping integers from the closed interval $[0, 2^n - 1]$ onto itself as follows:

$$F_e(x) = \begin{cases} x^e \bmod N & 0 \le x < N \\ x & N \le x < 2^n \end{cases}$$

Suppose also that T is a one-to-one function from $[0, 2^n - 1]$ onto itself which satisfies

$$T(x) < N \qquad \text{if } x \ge N \quad (1)$$

The blocking method then encrypts data in n-bit blocks. Suppose M is such a message block; then C, the corresponding ciphertext block, is obtained from M by

$$C = F_e\{T[F_e(M)]\}$$

The fact that T satisfies eqn. 1 ensures that M is always RSA-encrypted as least once. A typical choice for T (as suggested by Shimada and Tanaka[1]) would be

$$T(x) = (x + 2^{n-1}) \bmod 2^n$$

Limitations of technique: The main problem with the technique, as indicated by Shimada and Tanaka,[1] is that it does not completely conceal the message. If $C \ge N$ then it can immediately be deduced that M satisfies $M < N$ regardless of the choice for T; whereas if $C < N$ then M satisfies $M \ge N$ with probability $(2^n - N)/N$, again regardless of the choice of T as long as T is a one-to-one function. Shimada and Tanaka contend that this problem is minor since the amount of data thus leaked is always less than one bit in every n bits of message data (where a typical value for n might be 512).

However, in some circumstances this leakage is a major problem. Basically, if the leakage was distributed over all n bits of the message block (i.e. the cryptanalyst can only deduce very small amounts of information about each of the n message bits), then the problem would not be so severe. However, this is not the case for the system under consideration.

Consider the following scenario. Suppose N is quite close to 2^{n-1}. To be more specific suppose, say, that N satisfies

$$2^{n-1} < N < 2^{n-1} + 2^{n-6}$$

which, if N is chosen at random, would be expected to occur for every 1 in 32 such N.

Then, given any C, there are two cases to consider: $C < N$ and $C \ge N$; if M is random then these will occur roughly equally often. If $C < N$ then $M \ge N$ with probability greater than 31/33. If $C \ge N$ then we know with certainty that $M < N$. Hence, as far as the most significant bit of M is concerned, roughly half the time we know this bit is probably 0, and the other half of the time we know the bit is probably 1. In other words, the most significant bit of M is sent virtually unencrypted!

In the same scenario, even worse things might occur. Suppose we know with certainty (by some other means) that the most significant bit of M is 1. Then, if M is otherwise random, the probability that M satisfies

$$2^{n-1} \le M < N \quad (2)$$

could be as much as 1/33. The above analysis tells us that, if M does satisfy expr. 2, then it is very likely that $C \ge N$, and hence knowledge of C will reveal that M satisfies expr. 2. However, if M does satisfy expr. 2, then the five next most significant bits of M will all be zero. Hence, in this scenario, knowledge of C could reveal five bits of the plaintext message block!

One response to the above analysis would be to require that N is always chosen to be substantially larger than 2^{n-1}; however, unless N is always chosen to be quite close to 2^n, potentially serious leakage problems will remain. Such a tight restriction on the value of N is probably impractical and is potentially a security risk in itself.

Finally, note that although the penalties for using the proposed scheme are potentially very high, the rewards for its use are minimal. The data expansion of unmodified RSA is very small (typically 1 bit in 512), so the saving offered is relatively trivial. Moreover, use of this scheme also virtually doubles the number of RSA operations. Even with 'fast' RSA hardware the time for an RSA operation is still significant, and in software the overhead would be very great.

Conclusion: The proposed blocking scheme has been shown to have very serious data leakage problems. Moreover, the gains to be obtained by using it are minimal by comparison with the leakage problem and the considerable computational overhead it imposes. These limitations make the scheme completely unusable.

C. MITCHELL *27th July 1989*

Hewlett-Packard Laboratories
Filton Road, Stoke Gifford, Bristol BS12 6QZ, United Kingdom

REPLY

In general, if we choose N and integer $x > 0$ such that

$$N \le 2^{n-1} + 2^{n-x-1} \quad (3)$$

Mitchell's attack could reveal x bits of a plaintext M. However, if we chose N such that

$$N > 2^{n-1} + 2^{n-2} \quad (4)$$

the attack could not reveal any bits of M deterministically. Note that the right-hand side of the above inequality is not so close to 2^n. Thus, we can probably make any other statistical attacks ineffective, without imposing so tight a restriction on the value of N as to make the cryptosystem impractical.

Mitchell has said that the rewards for the use of the proposed scheme are minimal. This is true, as far as we can design the information processing system on which we implement the RSA cryptosystem. However, in many circumstances

the information processing system has already been designed, when we come to design the cryptosystem, and we would struggle with the expanded bits. Suppose we implement the cryptosystem on a disc drive system which has 1024 bytes per sector, and we encrypt a plaintext of 1024 bytes on it. In this case, one bit expansion doubles the time for reading/writing a plaintext. Furthermore, if the time for an RSA operation is shorter than the disc read/write time per sector ('fast' RSA hardware makes it possible), the proposed scheme could improve the performance of the disc drive system. This shows that the one bit saving is not always trivial.

We should emphasise that the proposed scheme of Reference 1 is usable in many circumstances.

M. SHIMADA

9th October 1989

Satellite Communications Systems Development Department
Microwave & Satellite Communications Division
NEC Corporation
4035 Ikebe-cho, Midoriku, Yokohama 213, Japan

K. TANAKA

Information Basic Research Laboratory
C&C Information Technology Research Laboratories
NEC Corporation
1-1 Miyazaki 4-chome, Miyamae-ku, Kawasaki, Kanagawa 213, Japan

References

1 SHIMADA, M., and TANAKA, K.: 'Blocking method for RSA cryptosystem without expanding cipher length', *Electron. Lett.*, 1989, **25**, pp. 773–774

2 RIVEST, R. L., SHAMIR, A., and ADLEMAN, L.: 'A method of obtaining digital signatures and public key cryptosystems', *Commun. ACM*, 1978, **21**, pp. 120–126

DISTANCE-INVARIANT ERROR CONTROL CODES FROM COMBINATORIAL DESIGNS

Indexing terms: Codes and coding, Information theory, Error-detection codes

Recently proposed techniques for constructing nonlinear distance-invariant codes from combinatorial designs are generalised. Such codes are of particular interest among nonlinear codes because their decoding error probabilities can be readily calculated.

Introduction: A recent letter[1] described methods of construction for distance-invariant (DI) codes from combinatorial designs. As defined by Delaney and Farrell[1] a code is distance-invariant if the number of codewords at distance i from a codeword (N_i) is independent of the choice of codeword. If a code is DI (and the values of N_i are known) then the probability of undetected errors can easily be computed. This makes DI codes of interest. Note that all linear codes are DI; in a linear code N_i is simply the number of codewords of weight i.

In this letter I give general constructions for DI codes from combinatorial designs which include all the examples of Delaney and Farrell[1] as special cases. For notation and results about designs see Beth *et al.*[2] or Hughes and Piper.[3]

Construction method: Suppose A is the $v \times b$ incidence matrix of a $2-(v, k, \lambda)$ design with b blocks and r blocks incident with every point, where

$$bk = vr \tag{1}$$

and

$$\lambda(v-1) = r(k-1) \tag{2}$$

Then, by definition of design, every row of the incidence matrix contains r ones (and $b-r$ zeros) and every pair of rows has exactly λ ones in the same positions (i.e. the logical AND of the two rows will contain exactly λ ones). Note that we assume that $v > k > 0$ and $\lambda > 0$, and hence $r \neq b/2$.

Following Reference 1, we derive three codes from A:

(1) *Type 1:* Take as codewords the rows of A.

(2) *Type 2:* The codewords of type 1 with their complements.

(3) *Type 3:* The codewords of type 2 with the all-zero and all-one codewords.

If we define an (N, M, d)-code to be one which has M codewords of length N and minimum distance d, then the next result follows immediately from the definition of a 2-design. Note that the main result of Reference 1 corresponds precisely to theorem 1 for the case $v = b$ (and hence $r = k$).

Theorem 1: Type 1 codes have parameters $[b, v, 2(r-\lambda)]$, with equal energy codewords, and are DI with $N_0 = 1$ and $N_{2(r-\lambda)} = v - 1$. Type 2 codes have parameters $\{b, 2v, \min[b-2(r-\lambda), 2(r-\lambda)]\}$, and are DI with $N_0 = 1$, $N_{2(r-\lambda)} = v-1$, $N_{b-2(r-\lambda)} = v-1$ and $N_b = 1$. If $(b-r) = 2(r-\lambda)$ then type 3 codes have parameters $[b, 2v+2, \min(r, b-r)]$, and are DI with $N_0 = 1$, $N_{2(r-\lambda)} = v$, $N_{b-2(r-\lambda)} = v$ and $N_b = 1$.

In fact, when the condition for type 3 codes (namely that $(b-r) = 2(r-\lambda)$) is combined with eqns. 1 and 2, it simplifies to either $k = v$ (a trivial case) or $k = (v-1)/2$. In the square ($v = k$) case this means that the set of nontrivial designs satisfying the type 3 condition is precisely the well known family of Hadamard designs. Delaney and Farrell[1] pointed out that the Hadamard designs satisfy the type 3 code conditions, but they do not note the converse. In fact, the type 3 codes obtained from the Hadamard designs correspond precisely to the Hadamard codes B_n described on p. 49 of Reference 4.

Further generalisations:

(*a*) A 't-class association scheme' is defined as a set V of v elements and a mapping f from the 2-subsets of V into $\{1, 2, \ldots, t\}$ with the following properties:

(i) There exist constants $v_1, v_2, \ldots, v_t$ such that, for any element P of V, there are precisely v_i other elements Q of V such that $f(\{P, Q\}) = i$ (and hence $v_1 + v_2 + \ldots + v_t = v - 1$).

(ii) There exist constants w_{ijk}, such that if P and Q are any elements of V satisfying $f(\{P, Q\}) = k$ then the number of other elements R in V satisfying $f(\{P, R\}) = i$ and $f(\{Q, R\}) = j$ is w_{ijk}.

Note that if $f(\{P, Q\}) = i$, then we say that P and Q are ith associates.

Observe that 2-class association schemes correspond precisely to strongly regular graphs.

(*b*) A 'partially balanced design with t associate classes' [PBD(t)] is then a $1-(v, k, r)$ design with a t-class association scheme defined on its v points, such that if any two points are ith associates they are commonly incident with $\lambda(i)$ blocks, for some constant $\lambda(i)$. In incidence matrix terms this means that, if A is the $v \times b$ incidence matrix of a PBD(t), then if two rows correspond to points which are ith associates, then these two rows have $\lambda(i)$ positions in which they both contain a one. Note that many examples of PBD(t) designs are known to exist.

If we derive type 1, type 2 and type 3 codes from A as we did previously (and we assume that each point has v_i ith associates) then we obtain the following.

Theorem 2: Type 1 codes have parameters $\langle b, v, \min_i\{2[r-\lambda(i)]\}\rangle$, with equal energy codewords, and are DI with $N_0 = 1$ and $N_{2[r-\lambda(i)]} = v_i$. Type 2 codes have parameters $\langle b, 2v, \min_i\{b-2[r-\lambda(i)], 2[r-\lambda(i)]\}\rangle$, and are DI with $N_0 = 1$, $N_{2[r-\lambda(i)]} = v_i$, $N_{b-2[r-\lambda(i)]} = v_i$ and $N_b = 1$. If $(b-r) = 2[r-\lambda(j)]$ for some j, then type 3 codes have parameters $\langle b, 2v+2, \min_i\{b-2[r-\lambda(i)], 2[r-\lambda(i)]\}\rangle$, and are DI with $N_0 = 1$, $N_{2[r-\lambda(i)]} = v_i$ $(i \neq j)$, $N_{2[r-\lambda(j)]} = v_j + 1$, $N_{b-2[r-\lambda(i)]} = v_i$ $(i \neq j)$, $N_{b-2[r-\lambda(j)]} = v_j + 1$ and $N_b = 1$.