1986

Encryption methods based on combinatorial designs

Dinesh G. Sarvate

Jennifer Seberry
University of Wollongong, jennie@uow.edu.au

Encryption methods based on combinatorial designs

Abstract

We explore the use of some combinatorial designs for possible use as secret codes. We are motivated to use designs as (1) combinatorial designs are often hard to find, (2) the algorithms for encryption ond decryption are of reasonable length, (3) combinatorial designs have very large numbers of designs in each equivalence class lending themselves readily to selection using a secret key.

Disciplines

Physical Sciences and Mathematics

Publication Details

Sarvate, DG and Seberry, J, Encryption methods based on combinatorial designs Ars Combinatoria, 21A, 1986, 237-246.

Encryption Methods Based on Combinatorial Designs

Dinesh G. Sarvate and Jennifer Seberry
Basser Department of Computer Science,
University of Sydney
NSW, 2006,
Australia.

Abstract.

We explore the use of some combinatorial designs for possible use as secret codes. We are motivated to use designs as

(1) combinatorial designs are often hard to find,

(2) the algorithms for encryption and decryption are of reasonable length,

(3) combinatorial designs have very large numbers of designs in each equivalence class lending themselves readily to selection using a secret key.

1. Introduction.

We explore some possible ways combinatorial designs might be used as secret codes. We hope our ideas will encourage much more research into applications of combinatorial cryptography. Cryptosecurity can be enhanced by using different methods for producing sequence of random permutations (see Sloane[1983]) and also by permuting the encoded message with a random permutation using a secret key (see Ayoub[1981]).

Where we have considered combinatorial designs which are well known we refer the reader to standard texts such as Hall [1967], Raghavarao[1971] or Wallis, Street and Wallis[1972] for definitions and constructions. For less frequently used or less well known designs a definition or reference is given.

All these methods lend themselves to further opacity if random number generators (an excellent survey can be found in Sloane[1983]) are used to apply permutations at any or all stages of encryption.

ARS COMBINATORIA 21-A (1986), pp. 237-246

2. Encryption method using mutually orthogonal Latin Squares.

Suppose we have a set of k mutually orthogonal latin squares of order n. A key is used which chooses a pair of the k-set at random. Encryption is now achived by transmitting for massage i,j the i,j th position of the selected pair of orthogonal squares.

Example. The following are three 4 X 4 mutually orthogonal matrices:

$$A = \begin{matrix} 1&2&3&4 \\ 2&1&4&3 \\ 3&4&1&2 \\ 4&3&2&1 \end{matrix} \quad B = \begin{matrix} 1&2&3&4 \\ 4&3&2&1 \\ 2&1&4&3 \\ 3&4&1&2 \end{matrix} \quad C = \begin{matrix} 1&2&3&4 \\ 3&4&1&2 \\ 4&3&2&1 \\ 2&1&4&3 \end{matrix}$$

Suppose the key chooses the third and first latin squares.Then to transmit the message 1,4 we send the (1,4) th element of the third and first latin squares i.e. 4,4.

Decryption is achieved by looking at which row and columns of the squares contain the pair 4,4 and that is the (1,4) th position.

Extra security is ensured by

(a) permutations of the rows and columns of the latin squares as a set,

(b) permutations of the elements within one or more of the latin squares,

(c) the key can change the pair of latin squares used after every two byte message if needed,

(d) the key can alter the size of the pairs of the latin squares being used after every two byte message if needed,

(e) the key can be used to choose another inequivalent and non-isomorphic pair at any stage.

Mutually orthogonal latin squares of size n can used to send any of the n^2 possible two byte messages.

Longer messages use *orthogonal F-squares and n-dimensional arrays.*

We illustrate via an example. Suppose A, B, C are, as before, pairwise mutually orthogonal latin squares then

$$A_1 = \begin{matrix} A & A \\ A & A \end{matrix} \qquad B_1 = \begin{matrix} B & B \\ B & B \end{matrix} \qquad C_1 = \begin{matrix} 1\,2\,3\,4\,2\,1\,4\,3 \\ 3\,4\,1\,2\,4\,3\,2\,1 \\ 4\,3\,2\,1\,3\,4\,1\,2 \\ 2\,1\,4\,3\,1\,2\,3\,4 \\ 3\,4\,1\,2\,4\,3\,2\,1 \\ 1\,2\,3\,4\,2\,1\,4\,3 \\ 2\,1\,4\,3\,1\,2\,3\,4 \\ 4\,3\,2\,1\,3\,4\,1\,2 \end{matrix}$$

are mutually orthogonal in the sense that each of the 4^3 messages from a 4-ary alphabet occur in the position i,j position of A_1, B_1, C_1. For example, the message 1,4,3 occurs in the 2,6 position.

This process of adding more mutually orthogonal faces to a higher dimentional array allows

(a) a key to be used to choose any subset of the faces of the array,

(b) the rows and columns of the faces to be permuted,

(c) the elements of the faces to be permuted,

(d) compression of the message,

(e) the key to be used to choose inequivalent higher dimensional arrays at any stage of the encryption process.

3. Encryption methods using Room squares.

Room squares can also be used to send messages in a fashion similar to that described for latin squares. As currently defined not all messages are available. For example consider the Room square

01	45	27	-	36	-	-
-	02	56	31	-	47	-
-	-	03	67	42	-	52
62	-	-	04	71	53	-
-	73	-	-	05	12	64
75	-	14	-	-	06	23
34	16	-	25	-	-	07

The situation becomes a little better for encryption if we note this example is of a skew Room square and so if the i,j entry is empty the j,i entry, i ≠ j is not.Thus we can send any message.

Example. Use the modified Room square

11	45	27	-	36	-	-
-	22	56	31	-	47	-
-	-	33	67	42	-	51
62	-	-	44	71	53	-
-	73	-	-	55	12	64
75	-	14	-	-	66	23
34	16	-	25	-	-	77

Then to encode the message 76 we observe 67 in the 3,4th position and send 43.

All the permutations that were previously used for the latin squares can still be used.

We note further that the Room square of the example is constructed using the starter-adder technique and each element can be found from the first row

11 45 27 - 36 - -

so that if the 1,j element is x,y the i,j+i-1 element (with j+i-1 reduced mod n , the size of the Room square) is x+i-1,y+i-1 where x+i-1 and y+i-1 are reduced mod n, but n = n(mod n).

The differences between the elements of the first row are all different so to encipher 76 we first note that 6-7=-1 and 45 has difference 1 hence 76 can also be encrypted by -1,2 meaning

(a) start with the pair distance 1 apart,

(b) add two to both,

(c) reverse the order.

Thus to decode -2,4 we note 7 and 2 are -2 appart and so decode as 64.

To encrypt longer messages the higher dimensional anlogues of skew Room squares are most useful.

4. Designs with two way elimination of heterogeneity.

These designs were first studied in connection with estimating tobacco mosaic virus by Youden[1937] and have subsequently been studied by a number of authors including Agrawal [1966i,ii], Agrawal and

Mishra[1971] Preece[1966i,ii], Seberry[1979i], Street[1981], Sterling and Wormald[1976]. A number of infinite families as well as one-off examples are known.

These designs comprise two designs with parameters (v_1,b,r_1,k,λ_1) and (r_1,b,v_1,k,λ_2), such that the incidence matrices N_1 and N_2 of the designs satisfy the additional property

$$N_1 N_2^T = kJ.$$

Example. Let the designs have the parameters

$$v_1=r_2=9,\ r_1=v_2=4,\ b=12, k=3$$

and treatments A,B,C,D,E,F,G,H,I and a,b,c,d respectively.

The two way design is

N_{12} =

A	b			a			d			c		
B	c				a			d			b	
C	d					a			b			c
D		c		d				a				b
E		d			c				a	b		
F		b				d	a				c	
G			b	c					d		a	
H			c		d		b					a
I			d			c		b		a		

Note that the blocks of N_2 are

b,	c,	b,	a,	a,	a,	d,	d,	b,	c,	b,	c
c	d	c	d	c	d	a	a	a	b	c	b
d	b	d	c	d	c	b	b	d	a	a	a

The design N_1 has blocks

A,	D,	G,	A,	B,	C,	A,	B,	C,	A,	B,	C
B	E	H	D	E	F	F	D	E	E	F	D
C	F	I	G	H	I	H	I	G	I	G	H

The two-way design is

Ab	Dc	Gb	Aa	Ba	Ca	Ad	Bd	Cb	Ac	Bb	Cc
Bc	Ed	Hc	Dd	Ec	Fd	Fa	Da	Ea	Eb	Fc	Db
Cd	Fb	Id	Gc	Hd	Ic	Hb	Ib	Gd	Ia	Ga	Ha

There are a number of encryption methods possible using these designs.

(1) the treatment of N_1 is sent to indicate the message given by the r_1 -tuple of treatments of N_2 associated with that treatment.

In the above example sending F would actually send the message (b,d,a,c).

(2) the block of N_1 is sent to indicate the message given by the k_2-tuple of treatments of N_2 associated with that block.

In the example sending 5 would actually send the message (a,c,d).

(3) A pair of treatments of N_1 are sent. Since N_1 is a block design any pair of treatments occur in λ_1 blocks and the message is those pairs (in the order given by the treatments of N_1).

In the example sending AG actually sends the message ac, where GA sends ca.

Now a secret key can be used to

(a) permute the rows of the two-way designs,
(b) permute the columns of the two-way design,
(c) permute the treatments of the second design,
(d) permute the blocks of the second design.

The advantages of using such designs are

(a) message compression,
(b) ease of decoding/encoding,
(c) if used in reverse it is asymmetric,
(d) the reverse procedure can combine encryption with error correction,
(e) these designs are hard to find even before permutations are used on them.

5. Crypto and coloured designs.

Some designs exist which may be more useful for encryption method 3 of the previous section. For example in the following design on five symbols every pair of elements (x,y), x, y $\in$ {a,b,c,d,e} occurs as an intersection of some pair of rows.

A	a	b	c				
B	a			d	e		
C	b					e	e
D		b		b		a	
E		c			a		e
F			c		d	c	
G			d	d			b

So to send say (a,c) we send DC but to send (e,a) we send CD. All the permutations that can be effected by the secret key are available.

Similar designs where pairs (or t-tuples) occur exactly once in a row or column have not been widely studied and offer a fruitful area of research.

Cryptodesigns with the less restrictive condition that every element occurs once in a row (so every row is an r-tuple) but each element in column is different are called *coloured designs* and have proved extremely useful in constructing new BIBDs and SBIBDs(see Seberry(1985ii), Sarvate and Seberry(1985) and de Launey and Seberry(1985).).

6. Encryption method using ordered designs.

The method described in this section is for encrypting an k-ary message by using combinatorial designs with blocks,whose elements are ordered. We encrypt a message of length t into a message of length 2, in other words we compress the message.

Example of such designs are modified directed balanced incomplete block designs i.e. DBIBD (see Seberry and Skillicorn [1980] , Street and Wilson[1980], Colbourn and Colbourn[1984]), cyclic BIBD (see Colbourn and Colbourn[1984]) and directed packings (see Skillicorn and R.G.Stanton[1982], Dawson, Seberry, and Skillicorn [1984]) over v treatments , $v \geq k$. The method can be easily extended to unordered designs.

Crucial observation of a DD(t,k,v) where k-ary alphabet is used in blocks of size v where each ordered t-tuple occurs at least once, is that if we number $n_1, n_2, \ldots, n_s$, the $s = \binom{v}{t}$ ways of selecting a t-tuple from the block. Then any t-digit message can be sent by transmitting two symbols the first giving the block number and the second the number n_a which corresponds to the required t-tuple.

The sender needs a large dictionary the receiver needs only a list of the blocks and the way of choosing the n_i^{th} t-tuple from each block.

This method has advantages of

(1) message compression of a high order

(2) small storage and time needed for decryption.

For example, in transmission to space-shuttles, undersea activities or other remote receivers.

Example: Let the message be aab dcc adc. Suppose we use the following design, DD(3,4,4) together with 14 extra blocks to cover all the possible triples.

DD(3,4,4) :	B_1= a b c d	B_2= b a d c	B_3= c a d b
	B_4= d a c b	B_5=d b c a	B_6=c b d a
Extra blocks :	B_7=a b a b	B_8=a c a c	B_9=a d a d
	B_{10}=b c b c	B_{11}=b d b d	B_{12}=c d c d
	B_{13}=a b a a	B_{14}=b c b b	B_{15}=c d c c
	B_{16}=d d a d	B_{17}=d b b a	B_{18}=c d a a
	B_{19}=c c a b	B_{20}=d d b c	

Suppose n_1 indicates we should choose positions 123 of the block, n_2,n_3,n_4 indicate choosing positions 124, 134, 234 respectively of the block. Then since aab is found in B_7, aab is encoded as $7,n_3$. dcc is encoded $15,n_4$ and adc is encoded $2,n_4$.

This design is not optimal in the sense that many pairs and triples occur 2 and 3 times. Optimal solutions where each possible t-tuple occurs and the fewest number of blocks used would be of great interest.

7. A practical Method.

An interesting application of the Rubic cube, in games or teaching, is when the message is of length less than or equal to 54 units. The sender and the receiver know how to read the message on the cube. The sender applies operations $P_1,P_2,...P_n$ and sends the cube via a messenger. The receiver applies $P_n^{-1},...,P_1^{-1}$ and recovers the message.

References:

Agrawal, H.L.(1966i), *Some Methods of construction of designs for two way elimination of heterogeneity*, I. J. Amer. Statist. Assoc.,61,1153-1171.

Agrawal, H.L.(1966ii), *Some systematic methods of construction of designs for two-way elimination of heterogeneity*, Calcutta Statist. Assoc. Bull., 15, 93-108.

Agrawal, H.L. and Mishra, R.I.(1971), *Some methods of construction of 4DIB designs*, Calcutta Statist. Assoc. Bull., 20, 89-92.

Ayoub, F.(1981), *Encryption with keyed random permutations*, Electronics Letters, 17, 583-585.

Bose, R.C.(1942), *A Note on the resolvability of balanced incomplete block designs*, Sankhya, 6,105-110.

Colbourn, C.J. and Colbourn, M. J.(1984), *Every two-fold triple system can be directed*, J. Combinatorial Theory, A, 34, 375-378.

Colbourn,M.J. and Colbourn,C.J.(1984), *Recursive constructions for cyclic designs*, J.Stat.Plan.and Inf.,10, 97-103.

Dawson, J.E. ,Seberry, J. and Skillicorn, D.B.(1984), *The directed packing numbers DD(t, v, v), t≥4*, Combinatorica, 4, (2-3) 121-130.

Hall, M. Jr.(1967), *Combinatorial Theory*, Ginn (Blaisdell), Boston.

Hess, P. and Wirl, K.(1983), *A voice scrambling system for testing and demonstration*, Cryptography, Lecture notes in Computer Science , Springer-Verlag(Berlin), Edited T.Beth,149, *147-156*..

Launey, W.de. and Seberry J. (1985), New group divisible designs obtained via matrices associated with generalized Hadamard matrices, (preprint).

Preece, D.A.(1966i), *Some row and column designs for two sets of treatments*, Biometrics,22,1-25.

Preece, D.A.(1966ii), *Some balanced incomplete block designs for two sets of treatments*, Biometrika, 53,497-506.

Raghavrao, D.(1971), *Construction and combinatorial Problems in Design of Experiments*, John Wiley, New York.

Sarvate D.G. and Seberry J.(1985) Colourable designs and new group divisible designs, (preprint).

Seberry, J.(1979i), *A note on orthogonal graeco-latin designs* ,Ars Combinatoria, 8, 85-94.

Seberry, J.(1985ii) Generalized Hadamard matrices in the construction of regular GDDs with two and three associate classes (preprint).

Seberry, J. and Skillicorn, D.B.(1980), *All directed BIBDs with k=3 exist*, J. Combinatorial Theory, A, 29, 244-248.

Skillicorn, D.B.and Stanton, R.G.(1982), *The directed packing numbers DD(t, v, v)*, Proceedings of the Eleventh Manitoba Conference on Numerical Mathematics and Computing, Winnipeg, Manitoba,1981, Congressus Numerantium, 34, 247- 252.

Sloane, N.J.A.(1983), *Encrypting by random rotations*, Cryptography, Lecture notes in Computer Science Springer-Verlag(Berlin), Edited by T.Beth,149, 71-127.

Sterling, L.S. and Wormald, N.(1976), *A remark on the construction of designs for two-way elimination of heterogeneity*, Bull. Austral. Math. Soc.,14, 383-388.

Street, D. and Seberry, J.(1980), *All DBIBDs with block size four exist*, Utilitas Mathematica, 18, 27-34.

Street, D.(1981), *Graeco latin and nested row and column designs*. Combinatorial Mathematics VIII, edited by K.L.McAvaney, Vol. 884, Lecture Notes in Mathematics, Springer-Verlag, Berlin- Heidelberg-New York, 304-313.

Street, D. and Wilson, W.(1980), *On directed balanced incomplete block designs with block size five*, Utilitas Mathematica,18, 161-174.

Wallis, W. D. , Street, A.P. and Wallis Seberry, J.(1972), *Combinatorics*, Lecture Notes in Mathematics, vol 292, Springer - Verlag, Berlin-Heidelberg-New York.

Youden, W.J.(1937), *Use of incomplete block replications in estimating tobacco mosaic virus*, Contributions from Boyce Thompson Institute, 9, 41-48.