On the Optimality of SAFER+ Diffusion

James L. Massey
Cylink Corporation, Sunnyvale, CA, USA
(Corresponding address:
Trondhjemsgade 3, 2t.h.
DK-2100 Copenhagen East
Denmark
e-mail: 101767.233@compuserve.com)

Abstract: A general theory is presented of optimum diffusion via multi-dimensional 2-point transforms over the ring of integers modulo a power of 2. This theory, which makes extensive use of graph-theoretic techniques, establishes the optimality of the transform diffuser used in the cipher SAFER+. A complete characterization is given of the matrix that describes an optimum transform diffuser. Finally, some open problems are identified and the theory is generalized to the case of multi-dimensional *n*-point transforms.

1. Introduction

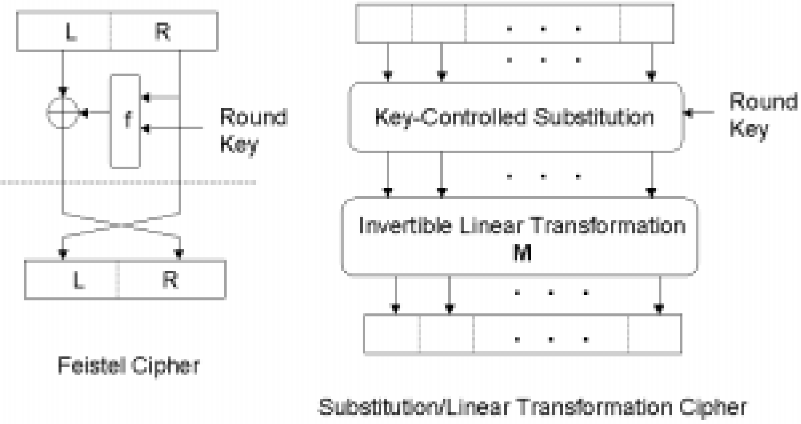
Fifty years after the publication of Shannon's seminal paper [1] on secrecy systems, Shannon's principles of "confusion" and "diffusion" remain the most widely accepted principles for the design of block ciphers. The Data Encryption Algorithm of the Data Encryption Standard (DES) [2] was explicitly designed in light of these principles, as were many of the algorithms that are in the competition for selection as the Advanced Encryption Standard (AES), including the cipher SAFER+ of our co-design [3]. In spite of the acknowledged importance of Shannon's principles, there is little agreement on their precise meaning and even less theory to suggest how much "confusion" and/or "diffusion" can be achieved. The present paper aims to remedy this lack of theory, at least to some small degree, for the principle of "diffusion".

We begin in the next two sections by describing the use of *D*-dimensional 2-point transform diffusers as the invertible linear transformation of a substitution/linear-transformation cipher. SAFER+ makes use of such a 4-dimensional transform diffuser. Two directed graphs, the transform skeleton and the shuffle graph are introduced to describe such transform diffusers. Section 4 presents the necessary and sufficient condition for a transform diffuser to provide optimum diffusion and gives a rather complete characterization of the resulting linear transformation. In particular, the transform diffuser of SAFER+ is shown to provide optimum diffusion. Section 5 connects transform skeletons to the well-known de Bruijn diagrams that are used in shift-register analysis, but leaves open the question of characterizing those transform skeletons that differ from de Bruijn graphs. In Section 6 we give the generalization of the theory to *n*-point transforms, and we close in Section 7 with a few remarks.

2. Substitution/Linear-Transformation Ciphers

Fig. 1 shows the well-known round structure of a Feistel cipher and of a general substitution/linear-transformation cipher, which includes the Feistel structure as a special case.

In the Feistel structure, which is used in the Data Encryption Algorithm of the Data Encryption Standard (DES) [2] and has been adopted in many later ciphers, the round input is separated into its left half, L, and right half, R, an arbitrary function f is applied to R and the round key as arguments, the output of f is added bit-by-bit modulo-two to L to produce a new left half, and finally the left and right halves are “swapped” to produce the round output. The section of the Feistel round structure above the dashed line in Fig. 1 constitutes the “key-controlled substitution” of the round structure of a general substitution/linear-transformation cipher. A key-controlled substitution is a function of the round input and round key that, for every fixed value of the round key, is a permutation (i.e., an invertible mapping) on the round input. That this section of the Feistel round structure indeed gives a key-controlled substitution is easily seen by the fact that, for any fixed value of the round key, this section realizes a mapping that is its own inverse, i.e., an “involution”. The section of the Feistel round structure below the dashed line in Fig. 1, i.e., the simple “swapping of halves” coordinate permutation, constitutes the “invertible linear transformation” **M** of the round structure of a general substitution/linear-transformation cipher.



Feistel Cipher

Substitution/Linear Transformation Cipher

Fig. 1: The round structure of a Feistel cipher and of a general substitution/linear-transformation.

Although the Feistel round structure has many positive features, including the fact that the same structure can be used for encryption and decryption rounds (when the “swapping of halves” is omitted from the final round), we chose the more general substitution/linear-transformation round structure for SAFER+ (as we did for the previous ciphers in the SAFER family). cf. [3]. The main reason for choosing this more general structure was to take advantage of the opportunity that it offers for choosing the the invertible linear transformation **M** of the round structure to obtain demonstrably good “diffusion”, i.e., to ensure that changing of a single symbol in the vector of symbols input to this transformation causes many output symbols to change. To state these considerations more precisely, we write the operation of the invertible linear transformation in the manner

$$y = x\ \mathbf{M}$$

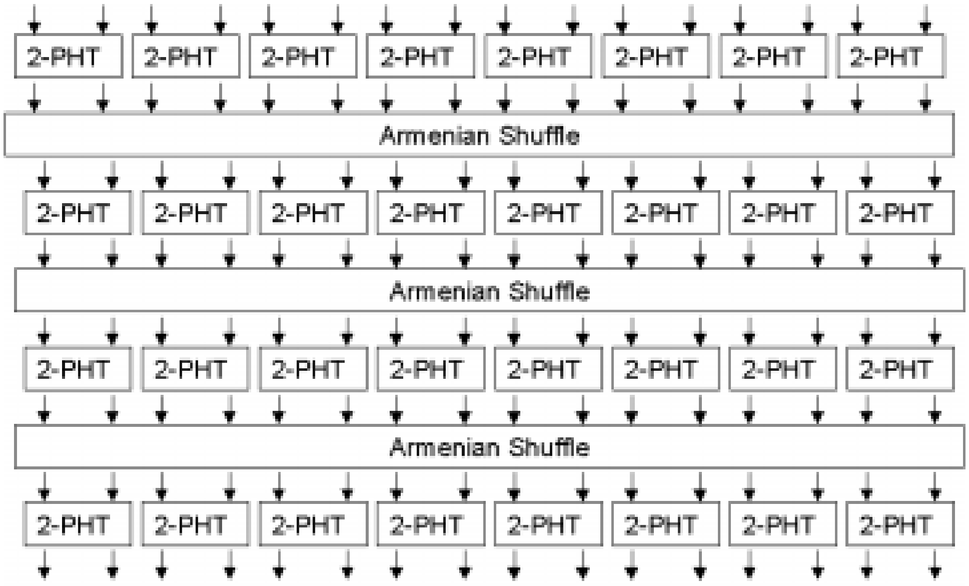
where the row vectors $\boldsymbol{x} = [x_1, x_2, \dots , x_L]$ and $\boldsymbol{y} = [y_1, y_2, \dots , y_L]$ are the input and output, respectively, of the linear transformation described by the $L \times L$ invertible matrix $\mathbf{M}$. Each of the components of $\boldsymbol{x}$, $\boldsymbol{y}$ and $\mathbf{M}$ is an m-bit symbol that is treated as an element of the ring of integers modulo 2^m, which ring we denote as $Z_2{}^m$. The length N in bits of the round input and round output, i.e., the block size of the cipher, is related to the length L in symbols of the vectors $\boldsymbol{x}$ and $\boldsymbol{y}$ in the manner $N = mL$.

We illustrate these ideas for SAFER+. The symbols of $\boldsymbol{x}$ and $\boldsymbol{y}$ are bytes, i.e., $m = 8$, and hence the arithmetic used is that of Z_{256}, arithmetic modulo 256. The block size is $N = 128$ and hence the length of $\boldsymbol{x}$ and $\boldsymbol{y}$ is $L = N/m = 16$ symbols. The matrix $\mathbf{M}$ of the SAFER+ linear transformation is the 16×16 matrix

$$\mathbf{M} = \begin{bmatrix}
2 & 2 & 1 & 1 & 16 & 8 & 2 & 1 & 4 & 2 & 4 & 2 & 1 & 1 & 4 & 4 \\
1 & 1 & 1 & 1 & 8 & 4 & 2 & 1 & 2 & 1 & 4 & 2 & 1 & 1 & 2 & 2 \\
1 & 1 & 4 & 4 & 2 & 1 & 4 & 2 & 4 & 2 & 16 & 8 & 2 & 2 & 1 & 1 \\
1 & 1 & 2 & 2 & 2 & 1 & 2 & 1 & 4 & 2 & 8 & 4 & 1 & 1 & 1 & 1 \\
4 & 4 & 2 & 1 & 4 & 2 & 4 & 2 & 16 & 8 & 1 & 1 & 1 & 1 & 2 & 2 \\
2 & 2 & 2 & 1 & 2 & 1 & 4 & 2 & 8 & 4 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & 1 & 4 & 2 & 4 & 2 & 16 & 8 & 2 & 1 & 2 & 2 & 4 & 4 & 1 & 1 \\
1 & 1 & 2 & 1 & 4 & 2 & 8 & 4 & 2 & 1 & 1 & 1 & 2 & 2 & 1 & 1 \\
2 & 1 & 16 & 8 & 1 & 1 & 2 & 2 & 1 & 1 & 4 & 4 & 4 & 2 & 4 & 2 \\
2 & 1 & 8 & 4 & 1 & 1 & 1 & 1 & 1 & 1 & 2 & 2 & 4 & 2 & 2 & 1 \\
4 & 2 & 4 & 2 & 4 & 4 & 1 & 1 & 2 & 2 & 1 & 1 & 16 & 8 & 2 & 1 \\
2 & 1 & 4 & 2 & 2 & 2 & 1 & 1 & 1 & 1 & 1 & 1 & 8 & 4 & 2 & 1 \\
4 & 2 & 2 & 2 & 1 & 1 & 4 & 4 & 1 & 1 & 4 & 2 & 2 & 1 & 16 & 8 \\
4 & 2 & 1 & 1 & 1 & 1 & 2 & 2 & 1 & 1 & 2 & 1 & 2 & 1 & 8 & 4 \\
16 & 8 & 1 & 1 & 2 & 2 & 1 & 1 & 4 & 4 & 2 & 1 & 4 & 2 & 4 & 2 \\
8 & 4 & 1 & 1 & 1 & 1 & 1 & 1 & 2 & 2 & 2 & 1 & 2 & 1 & 4 & 2
\end{bmatrix}$$

It should be noted that every row of $\mathbf{M}$ contains at least five 1 entries (and all odd-numbered rows contain exactly five 1 entries), which means that changing any single input symbol will change at least five output symbols. We will see later that this is optimum in a very strong sense. Moreover, there are changes of an input symbol that will cause only this minimum number of output symbols to change, namely a change by 128 in any odd-numbered symbol position. One notes further that every column of $\mathbf{M}$ contains at least five 1 entries (and all odd-numbered columns contain exactly five 1 entries), which means that for each output symbol there are at least five input symbols for which a change in any of those input symbols is guaranteed to change that output symbol.

The matrix $\mathbf{M}$ of the SAFER+ linear transformation can be realized in the manner shown in Fig. 2. In this figure, the boxes labelled “2-PHT”, where PHT stands for “pseduo-Hadamard transform”, implement the simple linear transformation whose matrix, corresponding “butterfly”, and inverse matrix are shown in Fig. 3.

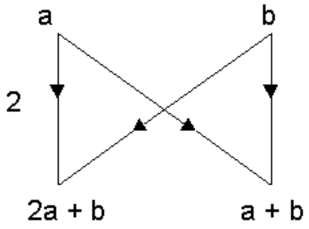


[The "Armenian Shuffle" is the coordinate permutation:
9 12 13 16 3 2 7 6 11 10 15 14 1 8 5 4]

Fig. 2: Realization of the SAFER+ linear transformation **M**.

One sees from Fig 3 that two byte additions suffice to implement the 2-PHT. The first byte addition of the inputs a and b give the second output a + b. A second byte addition of a to this result gives the first output 2a + b. Thus, the 32 2-PHT operations shown in Fig. 2 can be implemented with just 64 byte additions. The only other operation required to implement the matrix **M** of SAFER+ is the coordinate permutation that we have called the "Armenian Shuffle" in Fig. 2 in honor of its inventors, Gurgen Khachatrian and Melsik Kuregian, who are both with the Armenian Academy of Sciences and who are also co-designers of the SAFER+ algorithm. In the notation of DES [2], the Armenian Shuffle is the coordinate permutation [9 12 13 16 3 2 7 6 11 10 15 14 1 8 5 4] with the meaning that the first output of the permutation is the ninth input symbol, the second output is the twelfth input symbol, etc. The use of the Armenian Shuffle and its determination of the matrix **M** given above constitutes the major improvement of SAFER+ over the ciphers in the previous SAFER family of ciphers, cf. [3].

$$H_2 = \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix}$$



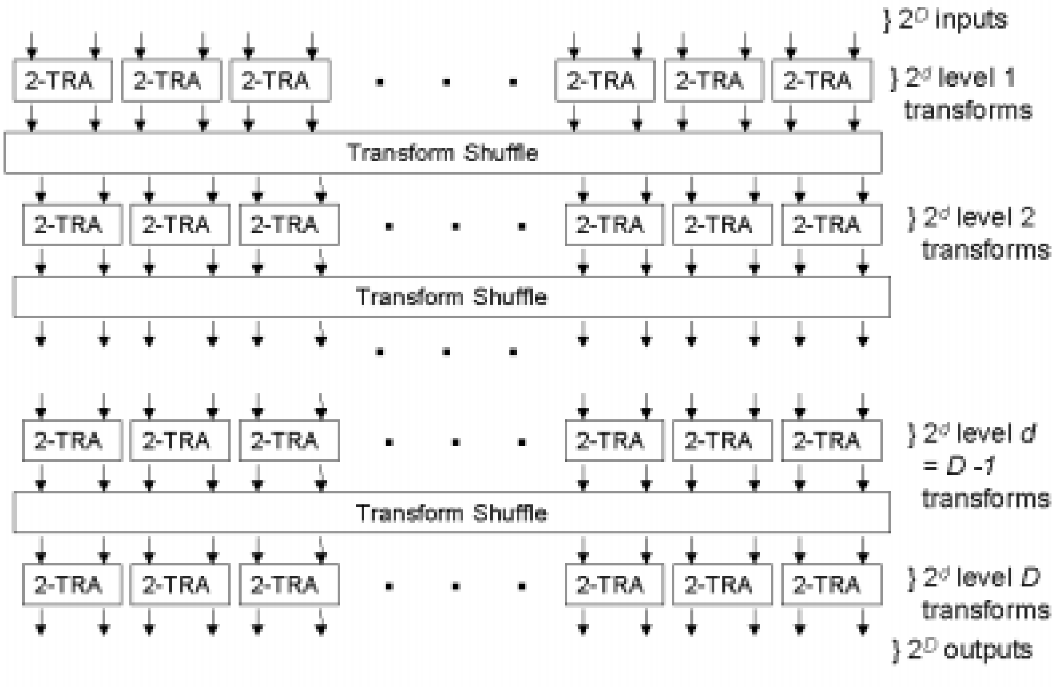
$$H_2^{-1} = \begin{bmatrix} 1 & -1 \\ -1 & 2 \end{bmatrix}$$

Fig. 3: The matrix, butterfly, and inverse matrix of the 2-PHT.

In the next section, we place the SAFER+ linear transformation into the general context of “transform diffusers” and introduce a graphical representation that we will use to study optimum diffusion with such transform diffusers.

3. Multi-Dimensional 2-Point Transform Diffusers

The SAFER+ linear transformation discussed in the previous section is a special case of what we call a *multi-dimensional 2-point transform diffuser*, the general form of which for the $D = 1 + d$ dimensional case is shown in Fig. 4. The parameter d, which will play a central role in the subsequent theory, is just the number of *additional dimensions* added to a basic 1-dimensional transform by “shuffling” among the coordinates.



} 2^D inputs
2-TRA
} 2^d level 1 transforms
Transform Shuffle
} 2^d level 2 transforms
} 2^d level d = D -1 transforms
} 2^d level D transforms
} 2^D outputs

Fig. 4: General $D = 1 + d$ dimensional 2-point transform diffuser.

In Fig. 4, the boxes labeled “2-TRA” represent an arbitrary linear transform for a “time axis” with only two points. Such a transform is equivalent to an operation with an invertible 2 × 2 matrix with entries in Z_{2^m}. Writing this matrix as

$$\mathsf{H} = \begin{bmatrix} a & b \\ c & d \end{bmatrix},$$

we see that the condition for invertibility is just that the determinant, $ad - bc$, of H be a unit of the ring Z_{2^m} (i.e., an element with a multiplicative inverse), which is just the requirement that $ad - bc$ be an odd integer. In particular, this precludes that all four entries of H themselves be units, i.e., odd integers. For this reason, the usual Walsh-

Hadamard 2-point transform for which $a = b = c = 1$ and $d = -1$ cannot be used in the ring $\mathbf{Z}_{2^m}$ as it is not invertible.

We now consider the general meaning of a transform shuffle for a D-dimensional 2-point transform as illustrated in Fig. 4. The *transform shuffle* is a coordinate permutation with the property that it creates a path from each of the 2^d "2-TRA" boxes at level 1 in Fig. 4 to each of the 2^d 2-TRA boxes at level $D = 1 + d$. Because the transform shuffle creates only two paths from a 2-TRA box connected to its input to 2-TRA boxes connected to its output, it follows that a transform shuffle creates a *unique* path from each of the 2^d 2-TRA boxes at level 1 to each of the 2^d 2-TRA boxes at level $D = 1 + d$. It is convenient to describe the box interconnections made by a transform shuffle with what we will call a "transform skeleton". A *transform skeleton* (for a $D = 1 + d$ dimensional 2-point transform) is a directed graph having 2^d vertices and having two branches that enter each vertex and two branches that leave each vertex such that there is a directed path (necessarily unique) of length exactly d branches between every pair of vertices. Upon associating the vertices with the 2^d 2-TRA boxes at any level of the transform, the branches from any vertex of the transform skeleton point to the vertices representing the two 2-TRA boxes at the next level that are connected to the 2-TRA box represented by this vertex.

Fig. 5 shows the unique $d = 1$ transform skeleton and the unique $d = 2$ transform skeleton. [The uniqueness of these transform skeletons will be obvious to the reader who spends a few moments trying to construct transform skeletons for $d = 1$ and for $d = 2$.] One sees immediately that these are instances of the well-known de Bruijn graphs that are widely used in the study of linear-feedback shift registers [4]. We will soon have more to say about de Bruijn graphs.

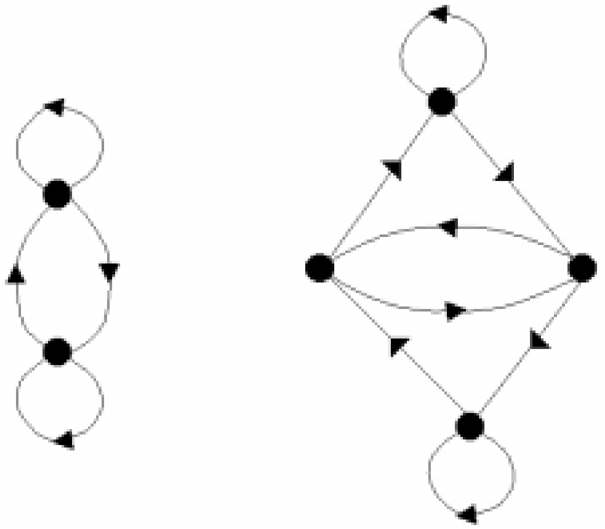
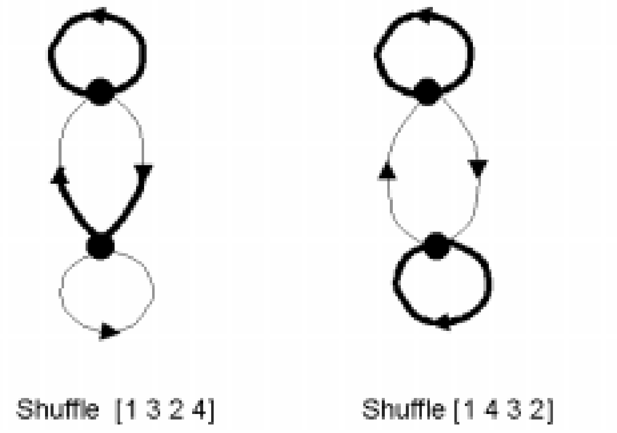


Fig. 5: The unique transform skeletons for $D = 2$ ($d = 1$) dimensional 2-point transforms and $D = 3$ ($d = 2$) dimensional 2-point transforms.

The transform skeleton does not completely describe a transform shuffle (assuming an association of the vertices with the 2^d 2-TRA boxes at any fixed level of the transform) because it does not indicate which of the two outgoing branches from a vertex is the first output and which is the second output of the 2-TRA box corresponding to this vertex, nor does it indicate which of the two incoming branches at a vertex is the first input and which is the second input of the 2-TRA box corresponding to this vertex. We remedy this deficiency of the transform skeleton by “coloring” its branches in such a way as to specify these connections and to warrant the description “shuffle graph” for the resulting colored graph. Our “coloring” rules are 1) to draw the first half of a branch leaving a vertex with a *thick line* if it leaves the first output of the corresponding 2-TRA box and with a *thin line* if it leaves the second output, and 2) to draw the second half of a branch with a *thick line* if it enters the first input of the 2-TRA box corresponding to the entered vertex and with a *thin line* if it enters the second input of the 2-TRA box corresponding to the entered vertex.

Fig. 6 shows the shuffle graphs for two different transform shuffles, both with the convention that the upper vertex corresponds to the first 2-TRA box and the lower vertex to the second 2-TRA box at any level of the transform. The first graph shows that the first output of the first 2-TRA box is directed to the first input of the same box at the next level, that the second output of this box is connected to the first input of the other box at the next level, etc.



Shuffle [1 3 2 4]

Shuffle [1 4 3 2]

Fig. 6: The shuffle graphs for two different shuffles for D = 2 (d = 1) dimensional 2-point transforms.

4. Optimum *D*-Dimensional 2-Point Transform Diffusers

We will say that a D-dimensional 2-point transform diffuser operating on symbols of the ring $Z_2{}^m$ is *optimum* if, among all such transform diffusers, it maximizes the minimum number of output symbols that are caused to change by the change of one input symbol and, in case of ties for this number, also maximizes the next smallest number of output symbols that are caused to change by the change of one input symbol. If **M** is the $L \times L$ matrix over $Z_2{}^m$ that describes the D-dimensional 2-point transform diffuser, then this optimality is equivalent to the condition that the minimum number of units (i.e., odd integers) that appear in any row of **M** is maximum and, in case of ties, the second smallest number of units in any row is also maximum. This follows from the fact that a change by 2^{m-1} in any input symbol causes changes in precisely those output symbols corresponding to the odd entries (i.e., the units) in the row of **M** that corresponds to this input symbol because $\alpha\cdot 2^{m-1} = 0$ modulo 2^m for any even integer α.

We write $\mu(D)$ to denote the minimum number of output symbols that are caused to change by the change of one input symbol for an optimum transform diffuser. We begin our development of the theory of optimum 2-point transform diffusers by considering the 1-dimensional case where we claim that the 2-PHT is optimum. Recall from Fig. 3 that this linear transformation has the matrix

$$H_2 = \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix}.$$

We have already seen that the matrix of a 2-point transform cannot have all odd entries. It follows that the 2-PHT is an optimum 1-dimensional diffuser and that $\mu(1) = 1$. Moreover, every other optimum 1-dimensional diffuser is essentially equivalent to the 2-PHT because it must also have exactly three odd entries. Because a product of ring elements is a unit if and only if each factor is a unit, it follows from the definition of a transform shuffle that the odd entries (i.e., the units) in the matrix **M** of a $D = 1 + d$ dimensional 2-point transform are determined entirely by the odd entries in the matrix of the underlying 2-point transform. We could with no loss of essential generality confine our attention to $D = 1 + d$ dimensional 2-point transforms based on the 2-PHT when developing the theory of optimum diffusing transforms. In fact, we may and will confine our attention even more narrowly to $D = 1 + d$ dimensional 2-point transforms based on the 2-TRA whose matrix $\mathbf{T}_2$ is the matrix $\mathbf{H}_2$ with its single non-unit entry 2 replaced by 0 when developing the theory of optimum diffusing transforms. Figure 7 shows the matrix $\mathbf{H}_2$ and its corresponding "butterfly".

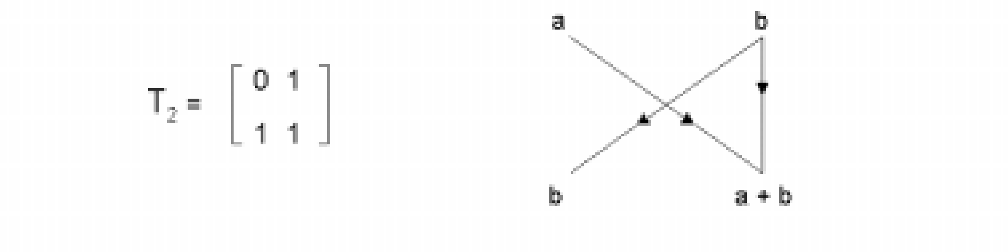


Fig. 7: The matrix and butterfly of the 2-TRA used to study optimum diffusion.

We are now ready to consider optimum diffusion with multi-dimensional 2-point transforms. Fig. 8 shows the general situation for a $D = 2$ dimensional ($d = 1$) 2-point transform based on $\mathbf{T}_2$. We first observe the simple fact that the number of 1's among the four output symbols produced by the input a = 1 will be strictly less than the number of 1's among the four output symbols produced by the input b = 1. Similarly, the number of 1's among the four output symbols produced by the input c = 1 will be strictly less than the number of 1's among the four output symbols produced by the input d = 1. It follows that the transform shuffle will give optimum diffusion if and only if it causes the second and fourth input symbols to become the second and fourth output symbols (in either order). This of course implies that the first and third input symbols must then become the first and third output symbols. (To be a valid transform shuffle, each of the two boxes at level one must be connected to both of the boxes at level two, which precludes that the transform shuffle be the simple identity map or the “swapping of halves” coordinate permutation.) But this is entirely equivalent to the condition that the branch “coloring” of the shuffle graph for this transform shuffle be such that both halves of all branches have the same “color”, i.e., that the entire branch is drawn as a thin line or that the entire branch is drawn as a thick line. We have proved the D = 2 case of the following result.

Proposition 1: *A $D = 1 + d$ dimensional 2-point transform based on the 2-PHT provides optimum diffusion if and only if its transform shuffle connects even-numbered inputs only to even-numbered outputs (and hence also odd-numbered inputs only to odd-numbered outputs) or, equivalently, if and only if the branch “coloring” of the shuffle graph is such that both halves of all branches have the same “color” (i.e., the entire branch is drawn as a thin line or that the entire branch is drawn as a thick line).*

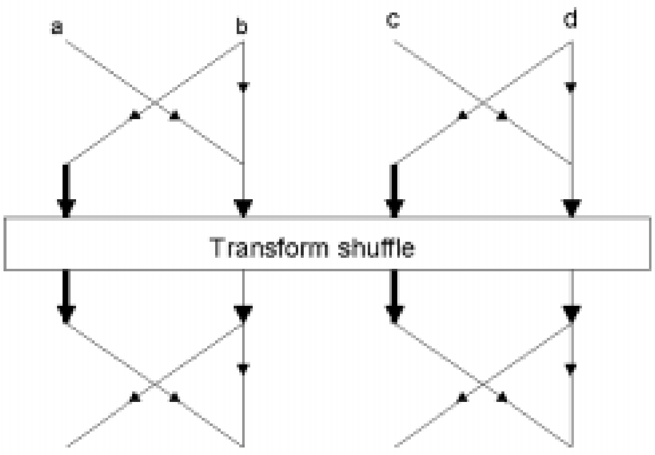


Fig. 8: The situation for $D = 2$ ($d = 1$) transform diffusion.

Example: It follows from the proposition that of the two shuffles in Fig. 6 only the second gives optimum diffusion. The matrices of these two D =2 dimensional transforms based on the 2-PHT are:

$$\mathbf{M}_{[1\,3\,2\,4]} = \begin{bmatrix} 4 & 2 & 2 & 1 \\ 2 & 1 & 2 & 1 \\ 2 & 2 & 1 & 1 \\ 1 & 1 & 1 & 1 \end{bmatrix} \qquad \mathbf{M}_{[1\,4\,3\,2]} = \begin{bmatrix} 4 & 2 & 1 & 1 \\ 2 & 1 & 1 & 1 \\ 1 & 1 & 4 & 2 \\ 1 & 1 & 2 & 1 \end{bmatrix}$$

from which the superior diffusion of $\mathbf{M}_{[1\,3\,2\,4]}$ is clear and its optimality establishes that $\mu(2) = 2$, i.e., that any change in one of the four input symbols will change at least two of the four output symbols. Incidentally, the transform shuffle [1 3 2 4] that gives non-optimum diffusion is the “Hadamard shuffle” (also called “decimation by two”) that is used in the standard 2-dimensional Walsh-Hadamard transform. Indeed, the transform shuffle used in the previous ciphers in the SAFER family made use of the Hadamard shuffle and hence the diffusion thereby provided was not optimum.

Proposition 1 follows by a simple induction from the proof for the $D = 2$ case that was presented above. One merely takes the situation of Fig. 8 (with a suitable increase in the number of boxes in each layer) to be that of any two successive layers in the general case. The same argument that was used for $D = 2$ above carries through again with the same conclusion: diffusion is optimum if and only if the transform shuffle connects even-numbered inputs only to even-numbered outputs.

Fig. 9 displays shuffle graphs for the three essentially different $D = 3$ ($d = 2$) dimensional 2-point transforms based on the 2-PHT that produce optimum diffusion. By essentially different, we mean that we ignore the particular assignment of 2-PHT boxes to the vertices of the graph; thus, each of these shuffle graphs with 4 vertices corresponds to 4! = 24 “different” such transforms.

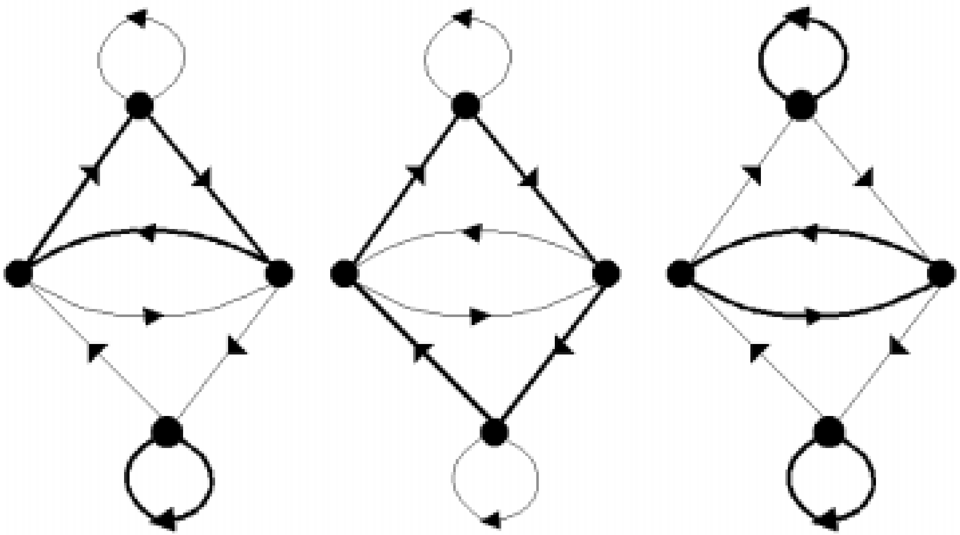


Fig. 9: The three shuffle graphs for $D = 3$ ($d = 2$) dimensional 2-point transforms based on the 2-PHT that produce optimum diffusion.

We now determine the function $\mu(D)$ defined above, i.e., the minimum number of output symbol changes caused by a single input symbol change in a D-dimensional 2-point transform with optimum diffusion. We consider the situation shown in Fig. 10 of two 2-TRA boxes at levels one and two of the transform. By the symmetry of the argument used to prove Proposition 1, we know that from every odd-numbered input to the transform there will be exactly $\mu(D)$ paths (with weight 1 on each branch) to output symbols (and the branches with weight 0 may be ignored). One such odd-numbered input symbol is isolated in Fig. 10 and marked with the number $\mu(D)$ of paths from it to output symbols. But, because there is only one path from this symbol through the 2-TRA box itself, this implies that there are also $\mu(D)$ paths from the even numbered input of the 2-TRA box to which the even-numbered output of the former 2-TRA box is connected. Moreover, the odd-numbered input of the latter 2-TRA box must have $\mu(D\text{-}1)$ paths to outputs, which implies that there must also be $\mu(D\text{-}1)$ paths to outputs from the even-numbered output of this latter 2-TRA box. Finally, the odd-numbered output of this latter 2-TRA box must be connected to the odd-numbered input of some 2-TRA box at level 3 and hence must have $\mu(D\text{-}2)$ paths to outputs. But the number of paths to output symbols from the even-numbered input of any 2-TRA box is the sum of the number of paths to output symbols from its two outputs and hence

$$\mu(D) \;=\; \mu(D\text{-}1) + \mu(D\text{-}2),$$

which is just *Fibonacci's recursion.* Recalling that $\mu(1) = 1$ and $\mu(2) = 2$, we see that $\mu(1), \mu(2), \mu(3), \mu(4), \mu(5), \ldots$ is just the *Fibonacci sequence* 1, 2, 3, 5, 8, … . This shows for instance that an optimum transform diffuser for $D = 4$ (the situation for SAFER+) will have a minimum of 5 units (which are all 1's for optimum-diffusing transforms based on the 2-PHT) in each row of its corresponding matrix **M**. Because the matrix **M** of SAFER+, given in Section 2 above, has a minimum of five 1's in each row, it follows that the linear transformation of SAFER+ is an optimum transform diffuser.

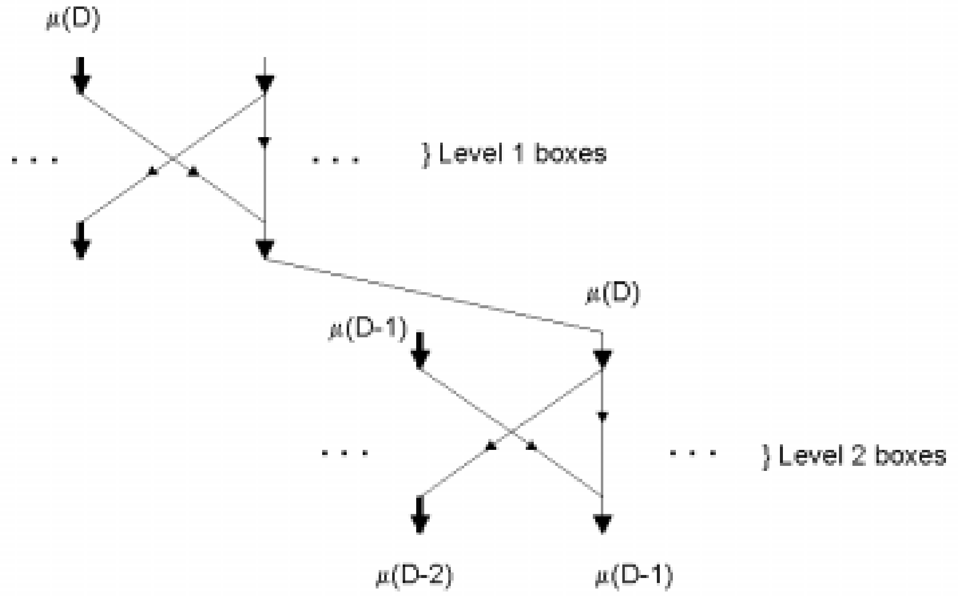


Fig. 10: Situation for counting the minimum number of output symbol changes caused by a single input change with optimum diffusion.

We now summarize the most important properties of optimum transform diffusers. We omit a detailed proof since the assertions are simple consequences of the arguments used above.

Proposition 2: *The matrix* ***M*** *of an optimum D-dimensional 2-point transform diffuser operating on symbols of the ring* $Z_2{}^m$ *is a* $2^D \times 2^D$ *matrix with entries in* $Z_2{}^m$ *such that*

- *each odd-numbered row of* ***M*** *contains* $\mu(D)$ *entries that are units of* $Z_2{}^m$ *(which units are all 1's if the 2-TRA used is the 2-PHT),*
- *each even-numbered row of* ***M*** *contains* $\mu(D) + \mu(D\text{-}1) = \mu(D\text{+}1)$ *entries that are units of* $Z_2{}^m$ *(which units are all 1's if the 2-TRA used is the 2-PHT),*
- *every pair of even-numbered rows of* ***M*** *differ only by a permutation of their entries,*

- *every pair of odd-numbered rows of* **M** *differ only by a permutation of their entries, and*
- *the transpose of* ***M*** *is also an optimum D-dimensional 2-point transform diffuser, viz. the one whose shuffle graph is obtained by reversing the direction of all branches in the shuffle graph of the transform diffuser corresponding to* ***M****.*

Note that the second point of this proposition explains why the matrix **M** of the SAFER+ transform diffuser, which is given in Section 2, has exactly $\mu(5) = 8$ 1's in each of its even-numbered rows. The last point explains why the odd-numbered columns of **M** all contain $\mu(4) = 5$ 1's and the even-numbered columns of **M** all contain $\mu(5) = 8$ 1's.

We emphasize here the generality of the ideas presented. For instance, if one used 1-bit symbols ($m = 1$) for the block size of $N = 128$ bits, then the length L of the transform would be $L = N/m = 128 = 2^7$ symbols. Thus, a $D = 7$ ($d = 6$) dimensional transform diffuser would be required. The matrix **M** of an optimum 7-dimensional 2-point transform diffuser would have $\mu(7) = 21$ 1's in each of its odd-numbered rows and in each of its odd-numbered columns, and would have $\mu(8) = 34$ 1's in each of its even-numbered rows and in each of its even-numbered columns. This means, for instance, that changing a single input bit to the linear transformation **M** would be guaranteed to change at least 21 of the 128 output bits.

5. Transform Skeletons and de Bruijn Diagrams

We now return briefly to the connection between de Bruijn diagrams and transform skeletons.

A binary de Bruijn diagram with parameter d is used to study the possible state behavior of binary feedback shift registers of length d. Fig. 11 gives the binary de Bruijn diagram for $d = 3$. The $2^3 = 8$ vertices of this graph are labeled with the possible states or contents of the shift register, for instance the state 100. The feedback function of the register operates on this state to produce a binary digit which is fed into the shift register on the left causing the previous contents to be displaced one position to the right, except for the rightmost digit which leaves the register. Thus, the two possible successors of state 100 are the states 010 (which results if the feedback function produces a 0) and 110 (which results if the feedback function produces a 1). This is shown in the de Bruijn diagram by a directed branch from the vertex labeled 100 to the vertex labeled 010 and a directed branch from the vertex labeled 100 to the vertex labeled 110.

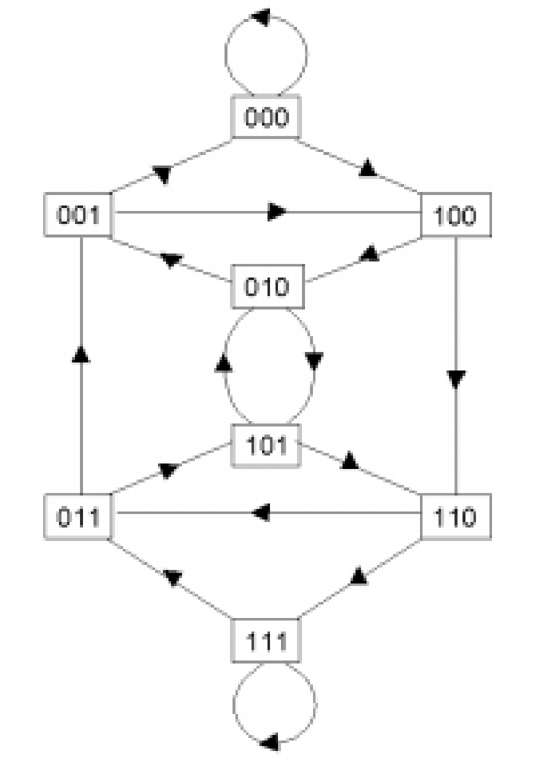


Fig. 11: The $d = 3$ binary de Bruijn diagram.

There is a unique directed path of length d between any pair of states in the binary de Bruijn diagram with parameter d. This is easily seen from Fig. 11. Starting from any state, the feedback sequence 1, 1, 0 will move the state to 011. The same argument goes through in general, the required feedback sequence being just the reverse of the digits in the "target" state. This property of the de Bruijn diagram means that, if the state labels are removed (i.e., replaced by unmarked vertices), then this diagram (which we will call a binary "de Bruijn graph") becomes a transform skeleton for a $D = 1 + d$ dimensional 2-point transform as defined in Section 3 above.

We have already mentioned in Section 3 that the *only* transform skeleton for a $D = 2$ dimensional 2-point transform and for a $D = 3$ dimensional 2-point transform is the $d = 1$ and $d = 2$ binary de Bruijn graph, respectively, which graphs are shown in Fig. 5. It thus was quite surprising to us to find that, for $D > 3$ ($d > 2$), there are transform skeletons that are *not* de Bruijn graphs. Fig. 12 shows such a transform skeleton for $d = 3$, which we have called the "Armenian skeleton" because it is the transform skeleton corresponding to the Armenian shuffle that is used in SAFER+ and was described in Section 2. The Armenian skeleton differs from the $d = 3$ de Bruijn graph in that the vertices on which the two branches drawn dashed in Fig. 12 terminate are interchanged. The reader is invited to check that the Armenian skeleton is indeed a transform skeleton for $d = 3$, i.e., that it has the property that there is a directed path of length $d = 3$ branches between every pair of vertices. The example of the Armenian skeleton suggests an interesting new graph-theoretic problem: find all the transform skeletons for $D = 1 + d$ dimensional 2-point transforms with $d > 2$.

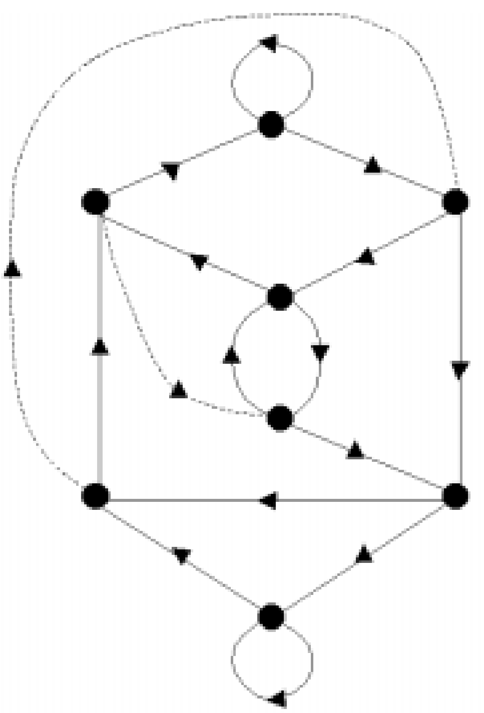


Fig. 12: The "Armenian skeleton".

6. Generalization to n-Point Transforms

We now show that the theory of the preceding sections, which treated 2-point transforms, has a natural generalization to *n*-point transforms over Z_2^m. First, the 2-PHT, whose matrix H_2 is given in Fig. 3, generalizes naturally to what we will call the *n*- PHT whose matrix is the $n \times n$ matrix

$$H_n = \begin{bmatrix} 2 & 1 & 1 \ldots 1 & 1 \\ 1 & 2 & 1 \ldots 1 & 1 \\ & & \vdots & \\ 1 & 1 & 1 \ddots 2 & 1 \\ 1 & 1 & 1 \ldots 1 & 1 \end{bmatrix}$$

The operation of this matrix can be implemented with 2(*n* –1) symbol additions (which are byte additions when *m* = 8), viz. *n* – 1 additions to form the sum represented by the last row of H_n and one further addition to form the sum represented by each of the *n* - 1 preceding rows. The determinant of H_n is 1 as is easily seen by subtracting the last row from each of the preceding rows, which operations do not change the determinant. Hence, the matrix H_n is indeed invertible. The inverse matrix is easily verified to be

$$H_n^{-1} = \begin{bmatrix} 1 & 0 & 0 \ldots 0 & -1 \\ 0 & 1 & 0 \ldots 0 & -1 \\ & & \vdots & \\ 0 & 0 & 0 \ddots 1 & -1 \\ -1 & -1 & -1 \ldots -1 & n \end{bmatrix}.$$

The theory developed above for 2-point transform diffusers goes through virtually unchanged for the *n*-point case. In particular, the following generalization of Proposition 1 holds.

Proposition 3: *A D = 1 + d dimensional n-point transform based on the n-PHT provides optimum diffusion if and only if its transform shuffle connects inputs with index 0 modulo n only to outputs with index 0 modulo n.*

Moreover, *n*-ary de Bruijn graphs with parameter *d* can be used as transform skeletons, but it is likely that other graphs can also be used just as was seen above for the binary case.

7. Concluding Remarks

We have given a fairly complete treatment of multi-dimensional *n*-point transform diffusers over the ring of integers $Z_2{}^m$. This theory establishes the optimality of the linear transformation **M** used for diffusion in the cipher SAFER+, but it also opens the door for the use of similar transformations in future ciphers. It seems to us not unreasonable that optimum transform diffusers as considered in this paper may find applications in cryptography and coding theory beyond simply serving as the linear transformation in substitution/linear-transformation ciphers.

Finally, we wish to mention that very significant improvements in the software and hardware implementations of SAFER+ have been made since the time of its submission as an AES candidate [3]. The interested reader is directed to the SAFER+ Forum at the N.I.S.T. web site: www.nist.gov/aes for details of these improvements.

References

[1] C. E. Shannon, “Communication Theory of Secrecy Systems,” *Bell System Tech. J.*, vol. 28, pp. 656-715, Oct., 1949.

[2] U. S. Department of Commerce/National Bureau of Standards, FIPS Pub 46, Data Encryption Standard, April 1977.

[3] Nomination of SAFER+ as Candidate Algorithm for the Advanced Encryption Standard (AES), Submission document from Cylink Corporation to N.I.S.T., June 1998.

[4] S. W. Golomb, *Shift Register Sequences*. San Francisco: Holden-Day, 1967.