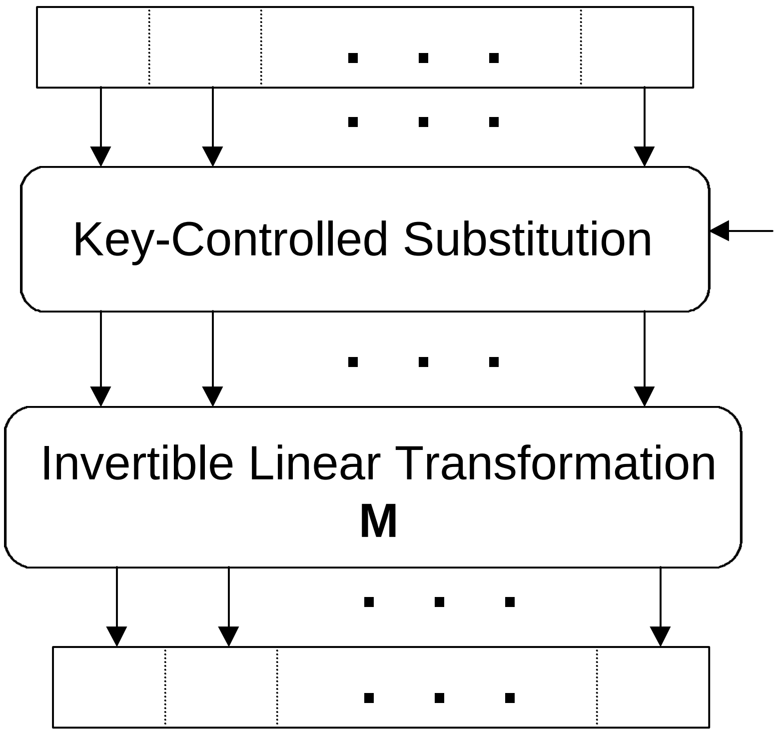
On the Optimality of SAFER+ Diffusion

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)

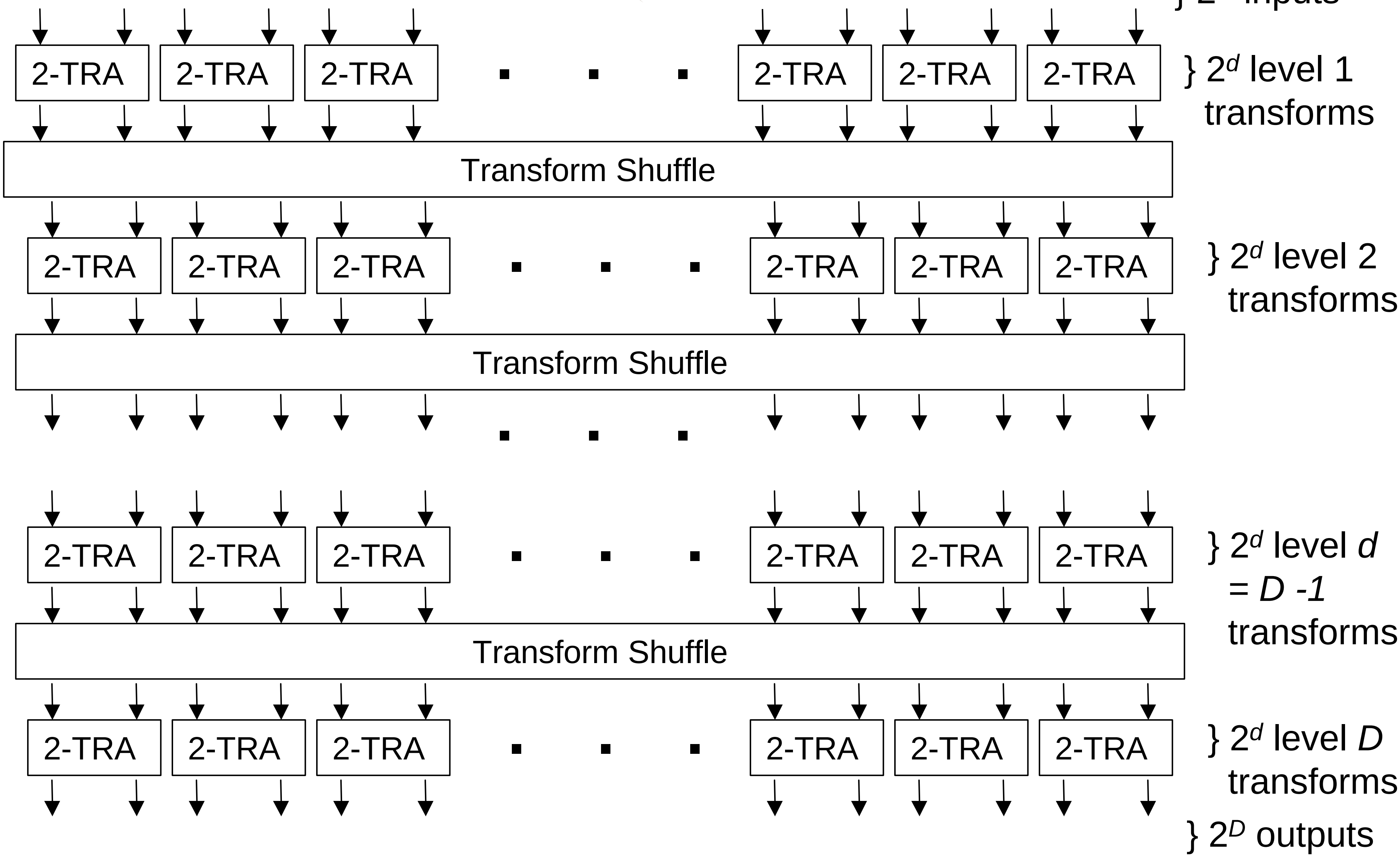
CYLINK



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

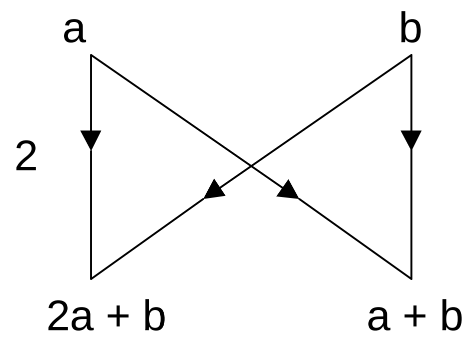
Substitution/Linear Transformation Cipher

Each component of the input vector ***x***, the output vector ***y***, and the matrix **M** is an *m*-bit symbol that is treated as an element of the ring of integers modulo 2^m, i.e. of $\mathbb{Z}_{2^m}$.



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

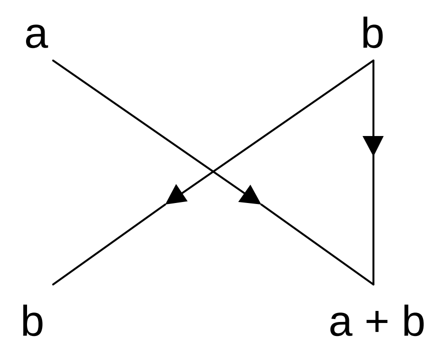
$$H_2 = \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix}$$



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

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

$$T_2 = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$$



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

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 1to 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 $D = 1 + d$.

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 <u>there is a directed path (necessarily unique) of length exactly *d* branches between every pair of vertices.</u>

CYLINK

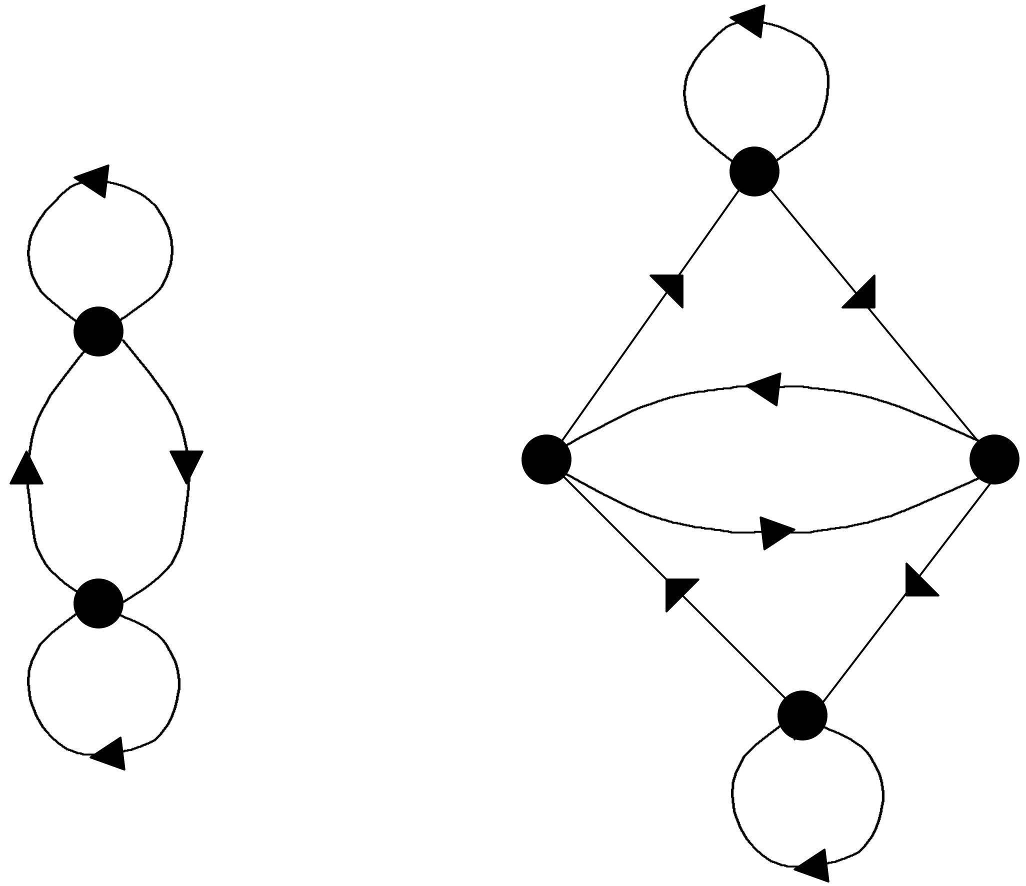
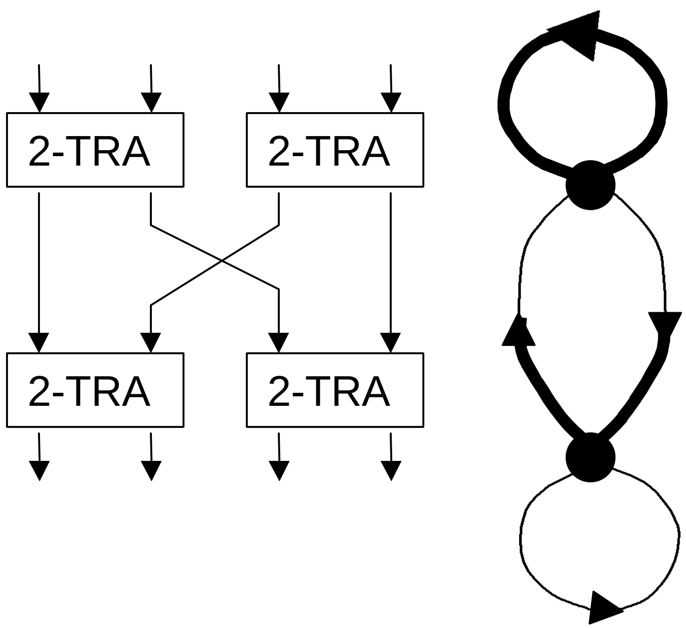


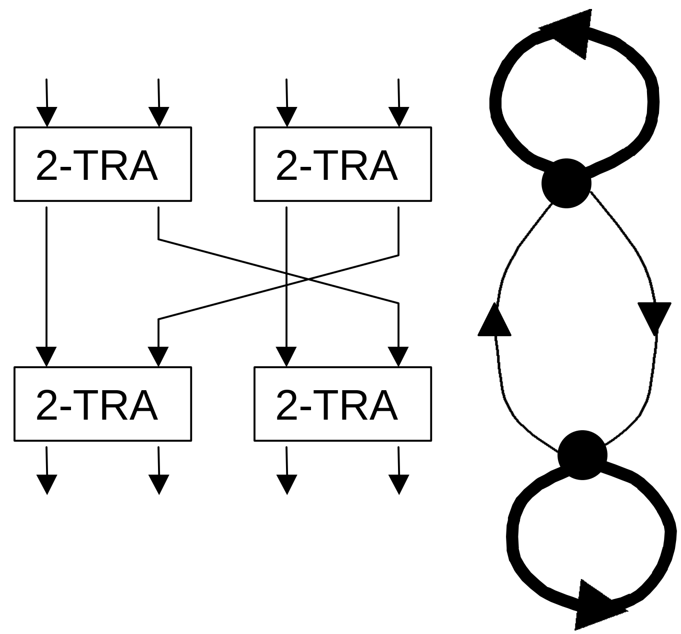
Fig. 5: The unique transform skeletons for $D = 2$ ($d = 1$) dimensional 2-point transforms and $D = 3$ ($d = 2$) dimensional 2-point transforms.

The **shuffle graph** is the transform skeleton "colored" so that 1) the first half of a branch leaving a vertex is a *thick line* if it leaves the first output of its 2-TRA box and is a *thin line* if it leaves the second output, and 2) the second half of a branch is a *thick line* if it enters the first input of the targeted 2-TRA box and is a *thin line* if it enters the second input of this 2-TRA box.

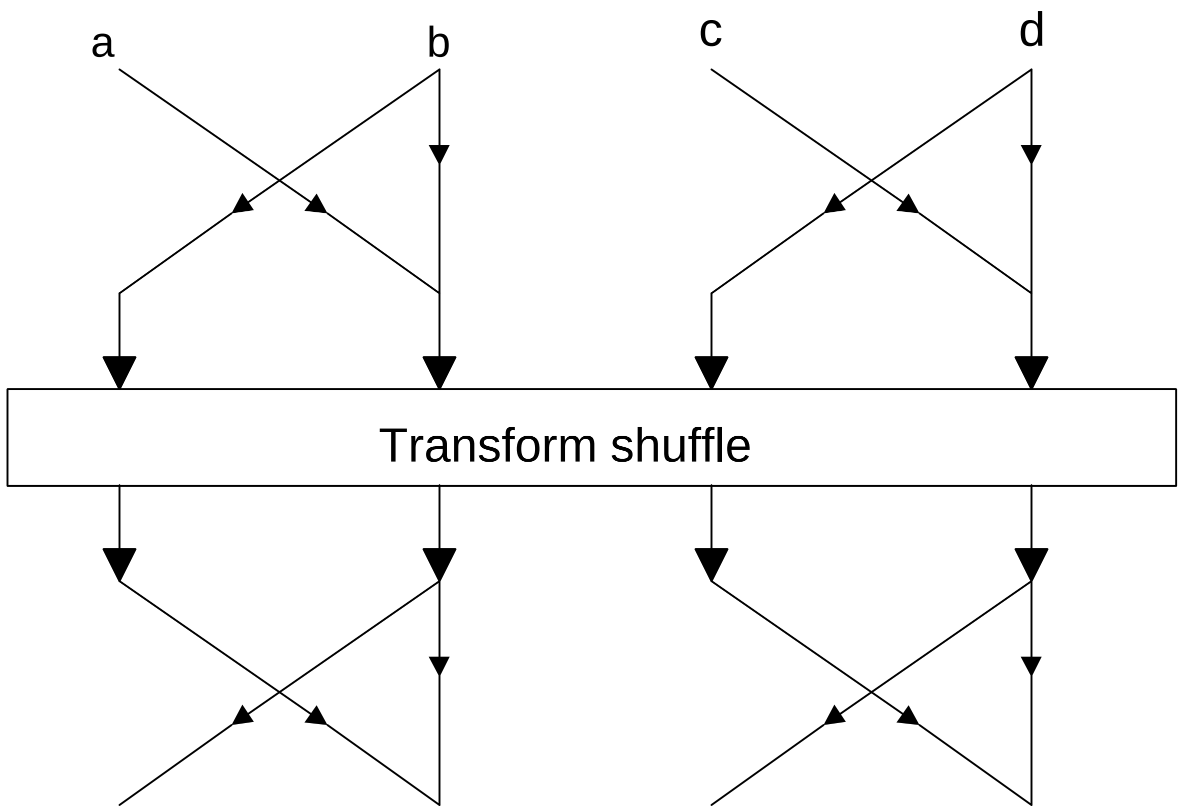


Shuffle [1 3 2 4]

"Hadamard Shuffle"



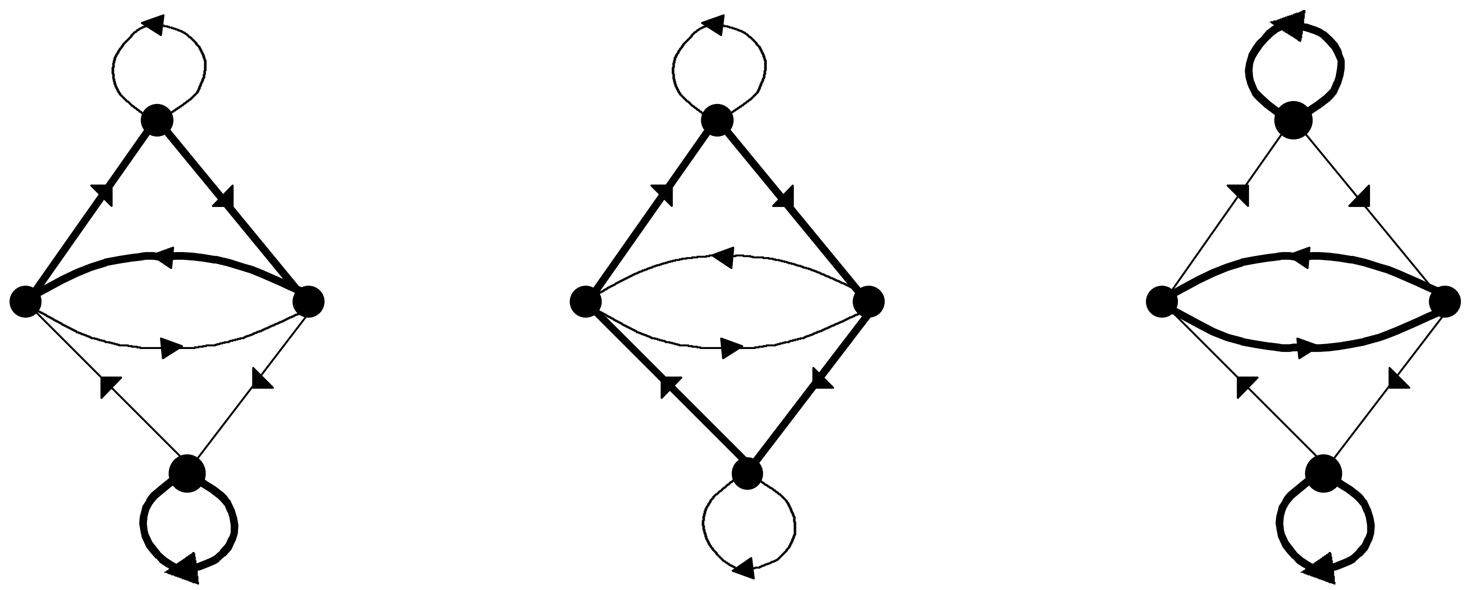
Shuffle [1 4 3 2]



The general situation for D = 2 (d = 1) transform diffusion.

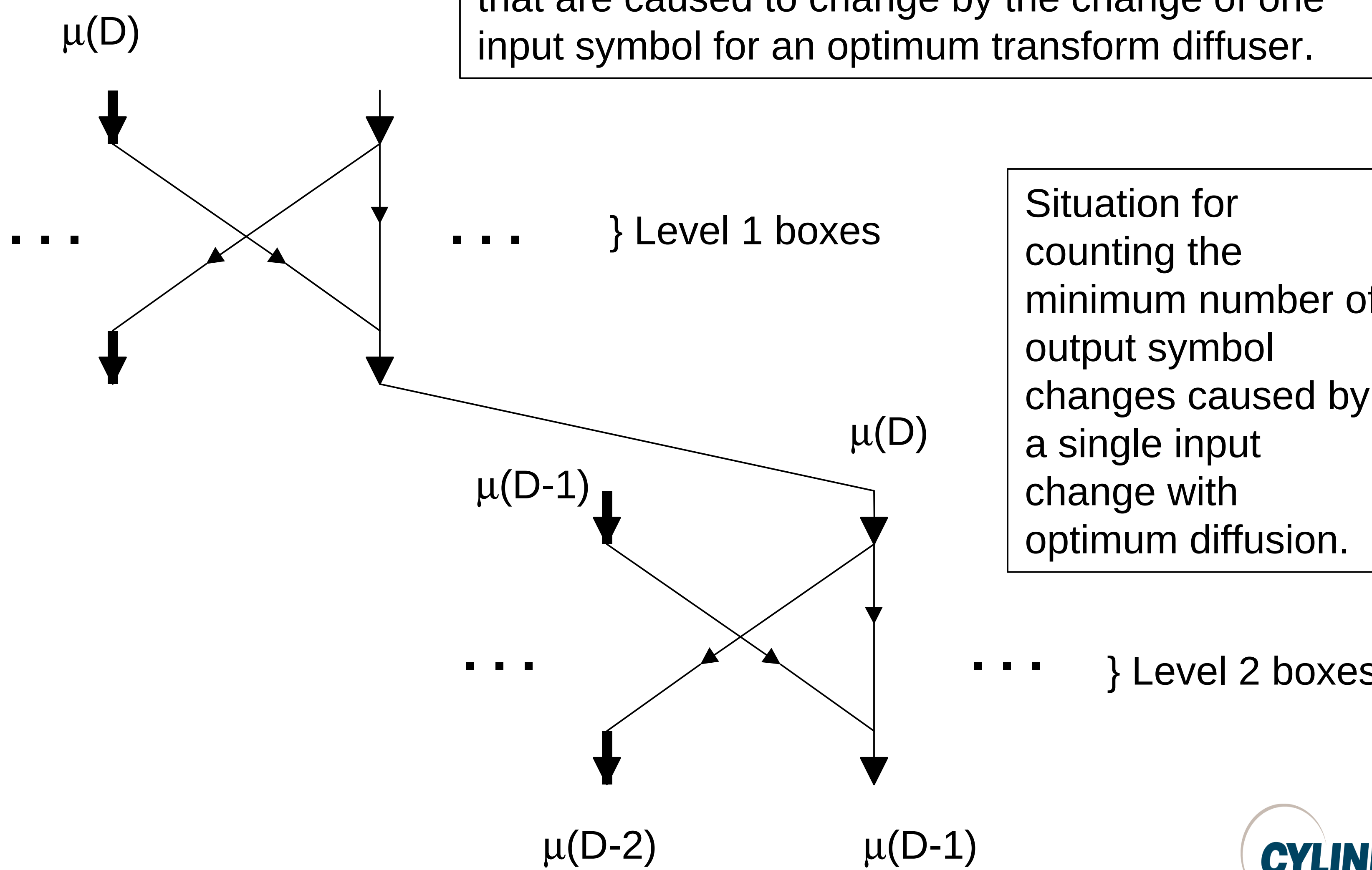
The coefficient of the transform from a given input to a given output is a **unit** of the ring Z_{2^m} (I.e., an odd integer) if and only if the transform shuffle creates a path from this input to this output in the above graph.

Proposition 1: A D = 1 + d dimensional 2-point transform based on any 2-TRA provides optimum diffusion if and only if the branch “coloring” of its shuffle graph is such that both halves of all branches have the same “color” (i.e., the entire branch is a thin line or that the entire branch is a thick line).



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

Let μ(***D***) be the minimum number of output symbols that are caused to change by the change of one input symbol for an optimum transform diffuser.



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

CYLINK

$\mu(1) = 1$ and $\mu(2) = 2$.

In general,

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

which is ***Fibonacci's recursion***, after Leonardo of Pisa, also called "Fibonacci," who in 1202 published his treatise, *Liber abaci*, which contained the famous "rabbit-counting" problem.

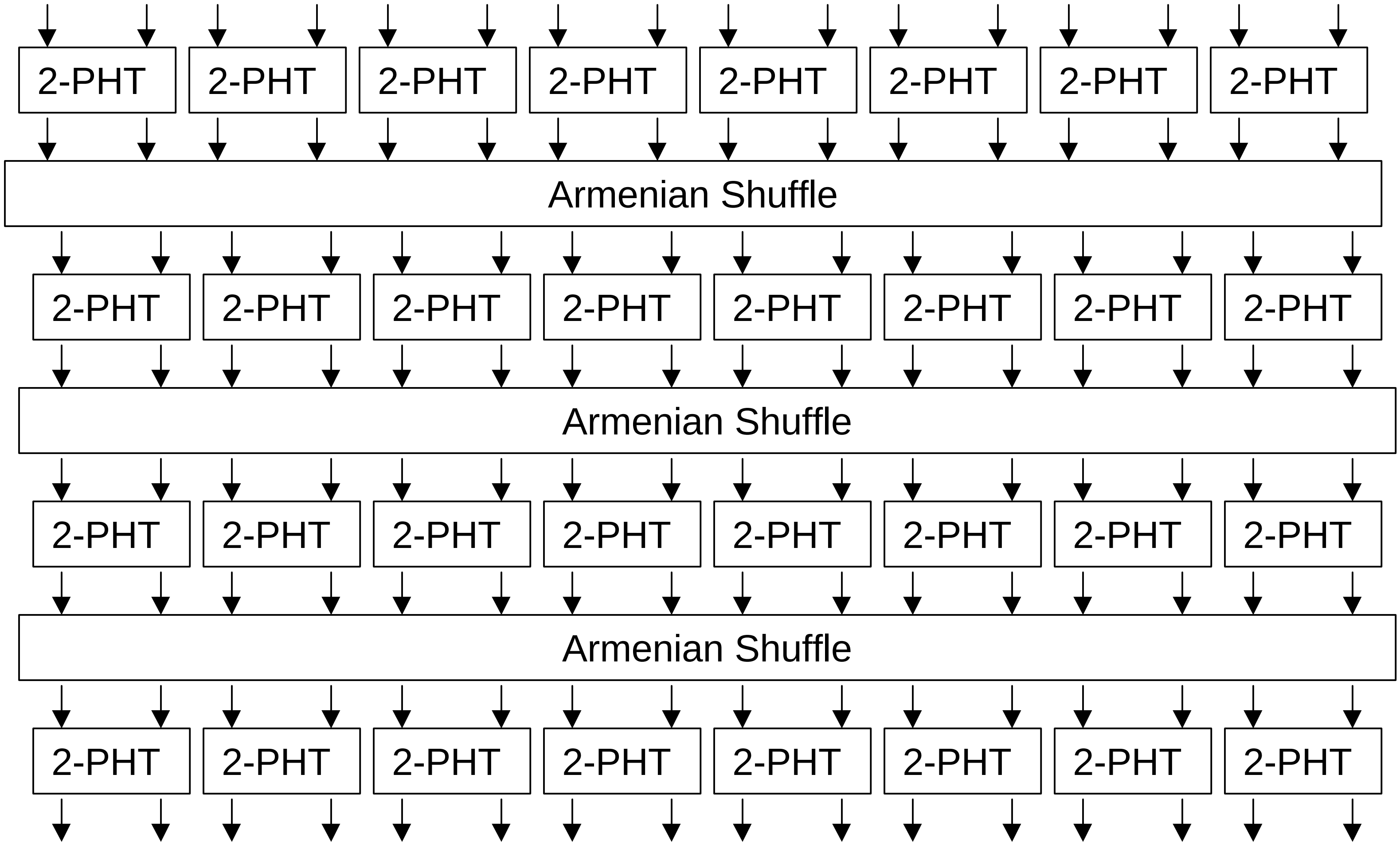
$\mu(1)$, $\mu(2)$, $\mu(3)$, $\mu(4)$, $\mu(5)$, … is the ***Fibonacci sequence***
1, 2, 3, 5, 8, … .

Thus, 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**.

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**.

CYLINK



The "Armenian Shuffle" is the coordinate permutation:

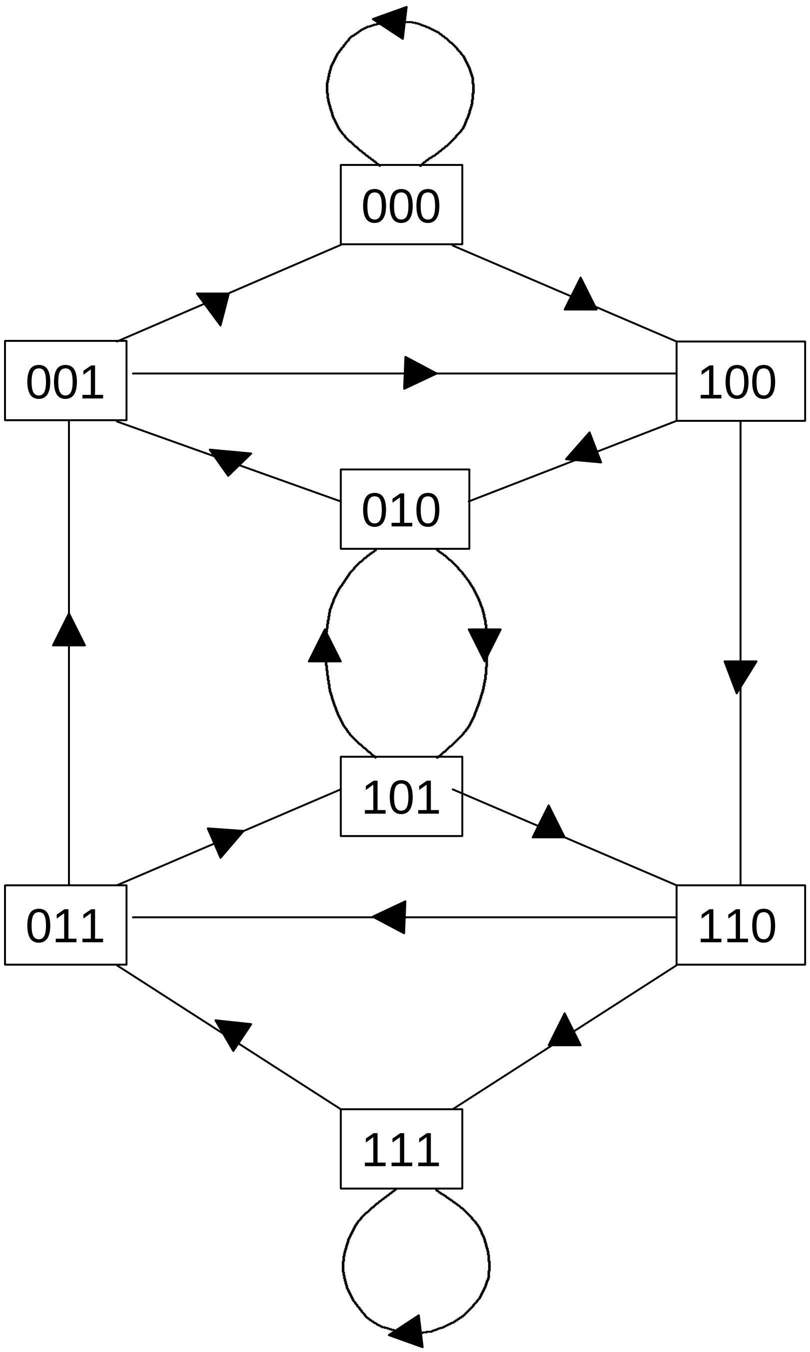
[**9 12 13 16 3 2 7 6 11 10 15 14 1 8 5 4**]

CYLINK

Realization of the SAFER+ linear transformation **M**.

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

The matrix **M** of SAFER+ .

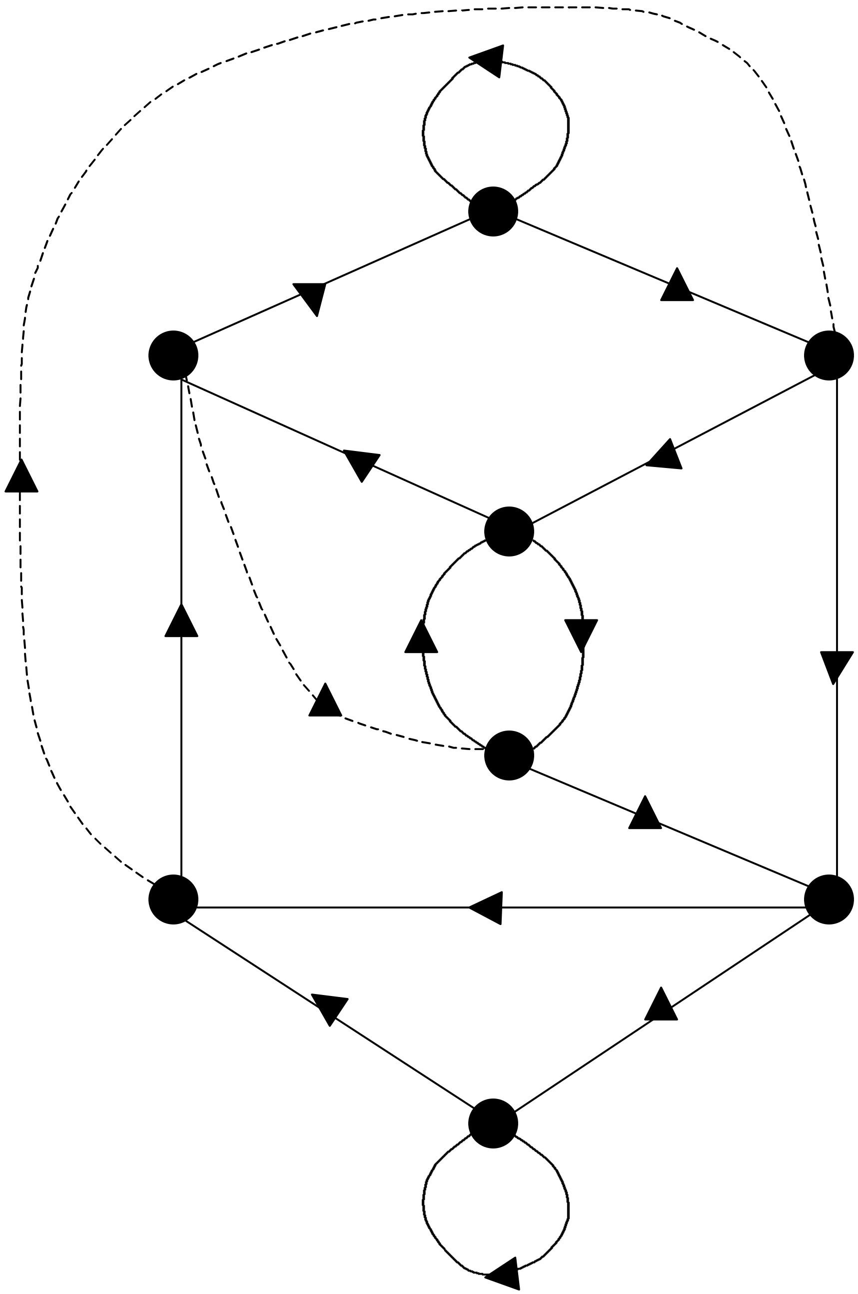


The *d* = 3 binary de Bruijn diagram.

The de Bruijn diagram of order d is a valid transform skeleton for a D = 1 + d dimensional 2-point transform, for every d.

Are there other valid transform skeletons?

CYLINK



The **“Armenian skeleton”**, which is the transform skeleton used in SAFER+.

The Armenian skeleton is **not** a de Bruijn graph!

N.B. There is a directed path of length exactly 3 branches from every vertex to every other vertex, which is the essential property required in a transform skeleton.

Everything, including the 2-PHT generalizes naturally to n-point transforms, cf. the paper.

Let me use this opportunity also to mention some major improvements in the implementation of SAFER+ .

For 0.25 micron CMOS cell based logic technology, the new hardware implementation with a system clock rate of 44 MHz requires only 181 nanoseconds to encrypt or decrypt a 128-bit block using a 128-bit key. This translates to an encryption / decryption rate of **704 Mbit/s in either ECB or CBC mode**. (The figure at submission was *58.9 Mbit/s*.)

For the ANSI C software implementation on a 200Mhz Pentium-pro processor, an encryption / decryption rate of **33 Mbit/s** has been achieved. (The figure at submission was *12.3 Mbit/s*.)

CYLINK